

ESTUDO DE SEGURANÇA DA INFORMAÇÃO NO UNIVERSO DO METAVERSO

Carolina Florentino Santos, Graciele Ribeiro dos Santos, Wdson de Oliveira

RESUMO

O metaverso traz consigo, além de grandes expectativas, uma série de dúvidas. Entre essas dúvidas, para muitos, pode-se destacar aquelas acerca dos eventuais efeitos negativos em relação à segurança da informação e proteção de dados. Saber como os dados de usuários serão coletados, armazenados e utilizados pelas empresas deve ser um ponto de atenção. É provável que, assim como acontece hoje em dia, hackers tentarão explorar as vulnerabilidades existentes, a fim de promover atividades maliciosas. Por isso, o principal desafio será mostrar como o metaverso é um lugar seguro e protegido para os usuários. Cada dia mais se concretiza a ideia de que as pessoas em breve interagirão como se estivessem dentro desse universo online, sendo necessário para acessá-la, atualmente, apenas alguns equipamentos. Contudo, com o surgimento de novos hardwares, a preços mais acessíveis, este acesso poderá ser ainda mais facilitado, o que levará a uma maior democratização do metaverso. Mas como a Internet, a tecnologia metaverso também traz seus perigos ao usuário e, portanto, o estudo em questão justifica-se pelo fato de que é de extrema importância que se tenha ciência dos riscos e, desta maneira, prevenir-se contra as ameaças contidas nesse ambiente em que poderá ocorrer violações de privacidade, golpes, violência e principalmente a desinformação. Portanto, para que se possa abraçar essa nova era e gozar dos privilégios que ela oferece é preciso que haja investimento em segurança da informação, definindo ferramentas, políticas de segurança e processos específicos para esta seguridade.

Palavras-chave: metaverso, segurança, informação.

ABSTRACT

The metaverse brings with it, in addition to high expectations, a series of uncertainties. Among these uncertainties, one of the most prominent concerns, for many, revolves around the potential negative effects on information security and data protection. Understanding how user data will be collected, stored, and utilized by companies should be a focal point of attention. It is likely that, just as we see today, hackers will attempt to exploit existing vulnerabilities to carry out malicious activities. Therefore, the primary challenge will be to demonstrate how the metaverse can be a safe and secure environment for users. The concept that people will soon interact as though they are within this online universe is becoming increasingly tangible, with access currently requiring only a few devices. However, with the advent of new, more

affordable hardware, access to the metaverse could be further facilitated, leading to a greater democratization of this virtual space. Like the Internet, the metaverse also presents dangers to its users. This study is therefore justified by the fact that it is crucial to understand the risks involved and, consequently, to take preventive measures against the threats inherent in this environment, where privacy violations, fraud, violence, and, most importantly, misinformation could occur. Thus, to embrace this new era and reap its benefits, it is essential to invest in information security, defining appropriate tools, security policies, and processes to ensure its protection.

Keywords: Metaverse; Security; Information.

1 INTRODUÇÃO

Segundo Haynes (2022) desde meados do século XX, o mundo tem sido testemunha de uma incessante e cada vez mais veloz transformação digital. Se nos primórdios desta transformação os computadores estavam disponíveis a poucos estudiosos e restritos aos domínios dos laboratórios mais abastados, hoje é difícil pensar no cotidiano do cidadão comum sem o uso dos computadores.

Cada vez mais leves e portáteis, por vezes na forma de um smartphone, eles estão por toda a parte. As pessoas, por sua vez, dependem mais e mais do uso de computadores. Tarefas rotineiras como pagar uma conta, fazer compras de supermercado ou conversar com amigos, que outrora eram feitas presencialmente, tornaram-se digitais. De uma forma geral, é possível afirmar que o uso de computadores se tornou indispensável para a vida moderna. (HAYNES, 2022)

Neste contexto, em que a dependência digital só aumenta, a segurança da informação emerge como um dos temas mais relevantes e necessários. É fato que a humanidade necessita do poder dos sistemas computacionais todos os dias. Porém, sem políticas de segurança adequadas, coloca-se em risco dados e informações de valor inestimável. A importância da implantação de procedimentos de segurança da informação, com medidas voltadas para a proteção dos dados, vem ganhando destaque na mesma velocidade em que a transformação digital se desenrola. (FERNANDES, 2022)

De acordo com Edison Fontes (2021, p. 10), “Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação. Na qual baseia-se em três pilares

principais, sendo eles: A confidencialidade, que diz respeito à restrição de acesso dos dados; a integridade, que garante que os dados estejam livres de alterações; e a disponibilidade, que defende que os dados estejam sempre acessíveis e disponíveis para uso”.

Não é de hoje que a tecnologia alimenta e move o mundo. Nos últimos anos, a humanidade testemunhou o advento e o avanço de várias soluções tecnológicas, dentre as quais destacam-se a modelagem 3D, a realidade virtual, o *cloud computing*, a Internet Web 3.0 e o 5g. Recentemente, contudo, uma nova tecnologia emergiu e vem ganhando destaque: o metaverso. Popularizada em 2021, sobretudo com a mudança do Facebook Inc para Meta, trata-se de uma realidade paralela, que pode ser definida como um ambiente digital estimulado que faz uso da realidade aumentada (AR), da realidade virtual (VR), e do *blockchain*, que consiste em uma estrutura na qual os dados são armazenados em blocos imutáveis e interligados por meio de chaves que são geradas com base no conteúdo de cada bloco. Desta forma, alterar o conteúdo de um bloco levaria a uma chave diferente que, por sua vez, quebraria a cadeia de blocos. (REDDY, 2022)

É notável que o metaverso hoje é um objeto de grande interesse de empresas, marcas e pessoas, que desejam embarcar e promover negócios neste novo mundo. Estima-se que o mercado do metaverso pode chegar a cerca de 800 bilhões de dólares em 2024. Possibilidades como jogos imersivos, provedores virtuais para vestuário e calçados, transmissões de shows, eventos e reuniões por meio de avatares 3D demonstram a todos o imenso potencial do metaverso. (ANDRADE; CENDÃO, 2022)

Contudo, em meio a tantas experiências de troca nesses mundos virtuais, o tema da segurança não deve ser ignorado. Para que todo o potencial do metaverso seja devidamente explorado, é preciso que se garanta a segurança e a privacidade de dados dos ativos. Para isso, os pilares de segurança da informação como integridade de dados dos usuários, disponibilidade de acesso, confiabilidade das informações e autenticidade, devem ser considerados como uma prioridade, de modo que se valide a autorização dos usuários para acessar, transmitir e receber suas informações.

É fato que somente conhecendo esses princípios pode-se construir uma base sólida para analisar, planejar e implementar as soluções de segurança que ajudarão a

reduzir riscos e a proteger a informação das diversas ameaças que certamente estarão presentes nesse novo universo do metaverso. (ANDRADE; CENDÃO, 2022)

A segurança da informação é fundamental em qualquer ambiente digital, incluindo o metaverso, desempenha um papel fundamental, uma vez que se trata de um ambiente virtual onde usuários interagem, compartilham informações e realizam transações. O metaverso é um espaço digital tridimensional, criado pela combinação de realidade virtual, realidade aumentada e outras tecnologias imersivas, onde as pessoas podem experimentar interações sociais, explorar ambientes virtuais e participar de atividades diversas, tomando tudo isso como base, o objetivo proposto desse trabalho em questão é expor as particularidades desse mundo vasto do metaverso apontando a grande importância da segurança da informação nesse ambiente interacional

2 REFERENCIAL TEÓRICO

Serão apresentadas, a seguir, os principais conceitos para fundamentar o tema do artigo em questão.

O avanço das tecnologias digitais tem levado ao desenvolvimento de conceitos inovadores, como o Metaverso, uma realidade virtual compartilhada e imersiva. O Metaverso promete transformar a forma como interagimos e consumimos informações, oferecendo uma experiência virtual altamente envolvente. No entanto, com essa nova fronteira tecnológica, surgem também desafios e preocupações em relação à segurança da informação. Este referencial teórico explora a importância da segurança da informação no Metaverso, analisando os riscos e as medidas necessárias para proteger os usuários e as suas informações.

A segurança da informação no Metaverso é um desafio em constante evolução, à medida que a tecnologia avança. Para aproveitar plenamente os benefícios do Metaverso, é essencial abordar os riscos de segurança de forma proativa. Isso envolve a implementação de medidas técnicas, políticas adequadas, colaboração entre diferentes partes interessadas e educação dos usuários.

2.1 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada (FONTES, 2006, n.p.).

Desde seus primórdios a espécie humana acumula informações, seja através da fala ou forma física, demonstrando o grande valor para sua evolução e crescimento. Portanto, a segurança torna-se um ativo de grande importância e que deve ser protegido.

Em meio a um cenário de rápido desenvolvimento e compartilhamento de informações, o universo dos conteúdos digitais está sujeito a várias ameaças que podem comprometer a segurança da informação dos seus usuários (SOTO, 2022).

Sendo assim, a segurança da informação protege de maneira geral o uso das informações, o acesso não autorizado, o seu uso indevido, a sua divulgação, a modificação, gravação, sua correta forma de destruição e a interrupção de informações. Para a proteção dos usuários e a informação, compreende-se colocar em prática os pilares da segurança da informação: Confidencialidade, Integridade, Disponibilidade. O pilar da integridade é responsável por manter as características originais dos dados, assim a informação não pode ser alterada sem autorização. Necessitando de implementação de controles para impedir a alteração das informações. A confidencialidade visa estabelecer a proteção dos acessos não autorizados, mantendo a privacidade dos dados. Pode se fazer o controle dos acessos através de senhas, criptografia, autenticação ou biometria. A disponibilidade garante que os dados estejam disponíveis para o que for necessário, garantindo o acesso dos usuários. Importante manter a estabilidade do sistema para garantir o acesso aos usuários. (FONTES, 2006)

2.2 METAVERSO

De acordo com Zompero (2022), a etimologia do termo metaverso deriva da junção das palavras meta, que em grego significa além, com o sentido de transmitir ideias de mudança e transformação, com a palavra verso, que remete à ideia de universo. A palavra metaverso, portanto, sugere um universo que transforma.

Apesar do termo ter ganhado popularidade recentemente, o metaverso é um conceito relativamente antigo, cuja origem remonta à década de 1980, vindo da literatura *cyberpunk*¹, com o livro *Snow Crash*, escrito por Neal Stephenson, que o publicou três anos após a invenção da Internet, o livro descreve dimensões que eram transmitidas aos usuários através de fones de ouvido e óculos. O famoso jogo *Second Life* é outro exemplo que aproxima da concepção de metaverso. (GLEN, 2022)

O conceito do metaverso define-se por uma realidade paralela, na qual, por meio de recursos como a realidade virtual aumentada e a inteligência artificial, o mundo é construído e vivenciado, sendo seu principal objetivo a mimetização do mundo físico. Tal objetivo pode ser alcançado com a criação de um avatar que, ao mover-se livremente, interagindo e acessando informações em um ambiente 3d, assim como no mundo real, pode agir de modo que suas ações produzam efeitos no ambiente, assim como em outros avatares que eventualmente nele estejam. (THERRIEN, 2023)

Tipicamente explorado pelas indústrias de jogos eletrônicos, filmes e livros, com o avanço da internet, a era da Web 3.0, o metaverso começa a imprimir seu impacto em outros setores da sociedade. Atividades que outrora eram realizadas exclusivamente no mundo físico passaram a ser possíveis dentro do mundo virtual. Simulações como prova de peças de roupas e calçados em provadores virtuais, simulação de intervenções cirúrgicas com modelos realistas e a transmissão de shows e espetáculos por meio de figuras de avatares são exemplos destas atividades.

O metaverso parte do princípio da descentralização baseada em *blockchains*. De modo resumido, isso significa que os dados são salvos em um banco de dados público e distribuído, em que a adulteração dos dados é bastante difícil. Essa característica possibilita que os usuários não apenas interajam e troquem dados, mas também que participem da governança e operação dos próprios projetos relacionados à tecnologia. (REVOREDO, 2019)

O metaverso é um universo em crescimento, com uma experiência única de troca de informações entre usuários, portanto permite ser alvo de perigos e crimes

¹ Cyberpunk: é um subgênero da ficção científica que se caracteriza por apresentar um ambiente distópico e futurista, onde a tecnologia avançada coexiste com uma sociedade desigual, corrupta e dominada por grandes corporações. O termo "cyberpunk" é uma combinação das palavras "cybernetics" (cibernética) e "punk", refletindo a fusão entre o avanço tecnológico e uma atitude contracultural.

virtuais por pessoas más intencionadas. Os atacantes poderão cometer crimes virtuais como roubo de identidades, usando logins de usuários, com credenciais usadas para acesso em outras plataformas para cometer diversas fraudes. Os golpes de engenharia social também poderão ocorrer devido ao aumento da interação entre os usuários e os relacionamentos, podendo os atacantes se passarem por pessoas para cometer golpes e perseguições. Possivelmente apresentar problemas relacionados com *blockchain*², o qual garante a integridade do usuário ao seu ativo virtual (SEREC, 2022).

Portanto, o metaverso ultrapassa o conceito de ser apenas um jogo simulando a vida real, ele transpõe dimensões, ligando uma gigantesca infraestrutura de mundos virtuais interligados, através de uma interface comum entre eles. Sendo muito mais uma ideia de um ambiente que fará cada vez mais uma enorme diferença na sociedade, incluindo a forma de aprendizado, no trabalho e na interação pessoal, influenciando a conscientização das pessoas a proteção dos seus dados pessoais.

2.3 A NOVA ERA DA TECNOLOGIA

Depois que o Facebook anunciou que estava mudando seu nome para Meta e pretendendo focar seus negócios inteiramente no design metaverso, o mundo estava acordando para essa nova era da tecnologia. Essa tecnologia vem sendo discutida há vários anos, reunindo jogadores em uma mesma instância de jogo para interagir e compartilhar experiências em ambientes como *Fortnite* e *Minecraft*, considerados exemplos de metaverso, e interações de realidade aumentada (AR) e realidade virtual. (ZOMPERO, 2022)

O metaverso ainda é considerado um espaço mais relevante para jogos como *Minecraft* e *Roblox*. Mas para os produtores seniores do *Decentraland*, que é um universo 3D governado por uma Organização Autônoma Descentralizada (DAO) criada em 2020, que combina jogos com uma plataforma de realidade virtual e é considerado um dos jogos de maior sucesso do metaverso. *Decentraland* é um

² Blockchain: é uma tecnologia de registro distribuído e descentralizado que permite o armazenamento e a verificação de transações de forma transparente, segura e imutável. É uma estrutura de dados que consiste em blocos encadeados, onde cada bloco contém uma série de transações e um hash criptográfico que conecta o bloco anterior, formando uma cadeia contínua.

universo 3D com um valor de mercado atual de cerca de US\$ 1,2 bilhão, o que equivale a quase 6,37 bilhões de reais.

Desenvolvido na blockchain Ethereum, combina jogos com uma plataforma de realidade virtual que permite criar avatares. Interagir com os outros e executar várias ações. As transações *Decentraland* são feitas com a criptomoeda MANA da plataforma, pode ser conquistado através de missões concluídas no jogo, mas também pode ser obtido em real (NEWS, 2018).

Existem vários terrenos virtuais no universo que são vendidos na forma de *tokens* não fungíveis (*NFTs*). Todos esses lotes são representados pelo *token* LAND e podem ser adquiridos com a criptomoeda local MANA. (STINSON, 2022)

A Heineken é uma das 70 empresas que se propuseram a atuar no metaverso descentralizado, incluindo Nike, Samsung, Itaú, Vans e Renner. A Heineken abriu uma cervejaria virtual de dois andares na maior plataforma do metaverso e lançando a Heineken Silver, uma nova cerveja de baixo teor alcoólico e baixa caloria.

Contudo, esta nova jornada tem pontos positivos e negativos. O Facebook recebeu um grande choque, após a revelação de que a americana Cambridge Analytica usou os dados de mais de 50 milhões de pessoas para propaganda política sem o seu consentimento, em 2018. A empresa Cambridge Analytica trabalhou com a equipe responsável pela campanha do republicano Donald Trump nas eleições norte-americanas de 2016. Na Europa, a empresa foi contratada por um grupo promotor do Brexit (a saída da Grã-Bretanha da União Europeia).

De acordo com uma investigação do The Guardian e do The New York Times, a Cambridge Analytica comprou acesso a dados pessoais de usuários do Facebook e usou esses dados para criar um sistema que poderia ter previsto e influenciado as escolhas dos eleitores. O material continha detalhes sobre a identidade das pessoas - como nome, ocupação, local de residência, gostos, hábitos e rede de contatos. O aplicativo explorou uma falha nas regras do Facebook, pois na época, a política da plataforma permitia que aplicativos externos coletassem dados de amigos das pessoas, mas dizia que deveria ser usado apenas para melhorar a experiência do próprio usuário no Facebook. Vender os dados ou usá-los para publicidade era proibido, mas o Facebook não tinha controle sobre seu uso (NEWS, 2018).

Portanto, uma coisa é muito importante analisar e cuidar: a segurança. Quando pensamos em indivíduos, temos dificuldade em afirmar uma identidade.

Como você sabe se a pessoa que está tentando se comunicar é ela mesma? Seus dados estão corretos? A forma como você se comunica atende aos padrões do espaço virtual? Comunicando-se fora do metaverso, por e-mail ou de outra forma, podemos nos proteger de possíveis golpes?

No nível corporativo, há muitas outras questões a serem consideradas para evitar fraudes, compras fraudulentas, interações fictícias e muito mais. Quanto mais interações houver, maior será a necessidade de usar a tecnologia também na parte de segurança, para garantir o sucesso dos esforços no metaverso. As empresas também devem estar atentas à legislação específica de cada setor em que atuam em relação à proteção dos dados pessoais de seus clientes e parceiros de negócios. Soma-se a este fator o cumprimento de todos os requisitos do Regulamento Geral de Proteção de Dados (LGPD).

2.4 LEI DE PROTEÇÃO DE DADOS NO METAVERSO

O metaverso refere-se a tecnologias capazes de reproduzir a realidade ou criar um universo paralelo por meio do uso de dispositivos e ambientes digitais, como jogos ou salas de aglomerações interativas. (ZOMPERO, 2022)

Portanto, o vocábulo não designa uma única tecnologia ou uma única empresa, mas ambientes virtuais com tal grau de imersão que conseguem reproduzir parcial ou totalmente as interações possíveis no mundo real.

O aumento da produção de conhecimento é uma tendência registrada nos últimos dois anos, com mais dados sendo produzidos em toda a história da natureza humana. Se hoje já é possível na internet mapear as tendências e hábitos de consumo dos usuários com base apenas em cliques, curtidas e tempo consumido em postagens, pode-se esperar recursos ilimitados para coleta e processamento de dados no mundo virtual. Pode haver mais dados para analisar em novas plataformas, como frequência cardíaca, expressões e reações a produtos e anúncios, além das interações existentes nas mídias sociais atuais. (HAYNES, 2022)

Efeitos comportamentais, espionagem, privacidade, roubo de identidade, golpe sofisticado de engenharia social e acessibilidade para crianças e/ou adolescentes. Esses são apenas alguns dos temas que precisam ser discutidos com urgência para acelerar a regulamentação. Qualquer uso indevido da infraestrutura do

metaverso e dos recursos de coleta de dados fornecidos pela plataforma pode resultar em violações graves. Apesar das vantagens que a plataforma pode trazer dessa forma, o metaverso permite que a inteligência artificial ceda conta do comportamento de todos os usuários em uma escala maior do que as redes sociais podem fazer atualmente. (HAYNES, 2022)

A lei 13.709, de 14 de agosto de 2018, popularmente conhecida como lei Geral de Proteção de Dados (LGPD), foi criada com o objetivo de proteger os direitos fundamentais à liberdade e privacidade e ao livre desenvolvimento da personalidade da pessoa natural, quanto aos dados pessoais que serão tratados, incluindo o tratamento de dados em ambiente digital. (LICKS; GUIMARÃES, 2022)

A melhor forma de o metaverso se enquadrar na LGPD é ter medidas rígidas sobre como os dados são tratados e armazenados, para evitar o compartilhamento indevido e quaisquer outros problemas que possam surgir a partir dele, além de ter passos muito claros sobre quais dados serão tornou-se público. Use e por quais motivos, ainda formule termos de licença de uso de dados.

O primeiro passo é que os auditores comecem a entender como vai funcionar a infraestrutura e a interoperabilidade da nova plataforma - atualmente existem vários mundos no metaverso, atualmente descentralizados e sem comunicação entre si, assim, o metaverso revolucionará a tecnologia e mudará a realidade, com efeitos colaterais positivos e negativos, que poderão ser monitorados e fiscalizados por ações conjuntas das autoridades competentes para regular a privacidade e proteção de dados conforme estipulado em nossa LGPD. (SEREC, 2022)

2.5 PROBLEMÁTICA ACERCA DA SEGURANÇA DA INFORMAÇÃO NO METAVERSO

O metaverso tem o potencial de definir como interagimos na web nos próximos anos. No entanto, além de novos negócios, esses mundos virtuais também têm o potencial de abrir toda uma nova gama de oportunidades para o cibercrime. O metaverso é aprimorado com base na experiência e na interatividade. As pessoas são o ativo mais importante neste mundo digital. Como tal, o roubo de identidade é uma ameaça constante no metaverso e um grande desafio.

Questões éticas e moderação de conteúdo são outros grandes desafios no metaverso, pois experiências interativas em espaços digitais trazem à tona o lado sombrio do mundo real. Esse desafio aborda questões de privacidade e aponta para o mesmo problema: a falta de mecanismos regulatórios adequados para lidar com esses riscos. Ameaças do metaverso mostram um problema antigo no mercado de TI: novas tecnologias, reflexão e consideração de segurança são uma reflexão tardia. (LICKS; GUIMARÃES, 2022)

Enquanto os temas abordam novas tecnologias e ideias transformadoras, a segurança é sempre vista como um fator secundário. Não espere o futuro chegar para ver a necessidade de mudar essa mentalidade. A segurança é parte integrante da tecnologia e, quanto mais cedo entendermos isso, melhor. Uma experiência interativa em um espaço digital traz consigo o lado obscuro do mundo real, então questões éticas e moderação de conteúdo são outros grandes desafios do metaverso. Ao mesmo tempo, tornará todos esses ativos voláteis e, se forem roubados, a dificuldade de recuperá-los também é um problema. (ANDRADE; CENDÃO, 2022)

No geral, as mesmas recomendações são válidas em relação a segurança da carteira de criptomoeda, pelo menos no cenário atual do metaverso, ressaltando a importância do não compartilhamento de informações com terceiros, a utilização de computadores ou aparelhos seguros e essencialmente confiáveis para a conectividade. Outro ponto preocupante é que as crianças podem estar em perigo no metaverso. À medida que as tecnologias se tornam parte de nossas vidas diárias, é mais comum que as crianças também utilizem, com interação entre usuários, isso pode ser extremamente perturbador e pode criar experiências potenciais de reuniões quase “físicas” com abusadores de crianças. Portanto, é importante sempre tomar medidas de controle dos pais quando disponíveis, bem como evitar que as crianças entrem no metaverso sem supervisão. (FERNANDES, 2022)

3 METODOLOGIA

Com o objetivo de trazer melhor compreensão ao leitor sobre como o metaverso estabelecerá princípios fundamentais de segurança da informação, traçou-se a seguinte pesquisa de acordo com um desenvolvimento exploratório bibliográfico,

a partir de referências teóricas publicadas em artigos, livros, sites, dissertações e teses.

Quanto à natureza exploratória dessa pesquisa, justifica-se pela necessidade de buscar o estudo acerca de como o metaverso fundamentará a segurança da informação para seus usuários, pela observação de incidentes no ambiente virtual do metaverso ou que possam vir a ser

4 RESULTADOS E DISCUSSÃO

Pôde-se constatar que neste cenário analisado, o metaverso é um ambiente virtual em constante evolução, por isso a segurança da informação nesse ambiente requer um enfoque diferente e adaptado às suas mudanças. Conforme o desenvolvimento e crescimento dessa tecnologia, a segurança da informação se torna cada vez mais importante para interações seguras entre usuários em tempo real. Com isso, há um grande volume de dados e informações sensíveis sendo trocados e armazenados. (FONTES, 2006)

Os riscos de segurança no metaverso incluem roubo de dados pessoais, fraude, cibercrime, violações de privacidade e muito mais. Para mitigar esses riscos, é necessário adotar práticas de segurança específicas que levem em conta as características únicas do ambiente. (HAYNES, 2022)

Constatamos que algumas das medidas que podem ser tomadas incluem o uso de tecnologias de autenticação segura, como autenticação multifatorial e criptografia, a implementação de *firewalls* e softwares antivírus, além de monitoramento constante das atividades e do tráfego de dados no ambiente virtual. (FAR, 2022)

Portanto, a segurança da informação no metaverso é um desafio em constante evolução, e é importante que as empresas e os usuários estejam sempre atualizados sobre as ameaças e vulnerabilidades do ambiente para garantir a proteção de seus dados e informações sensíveis.

Diante dessas informações de acordo com Serec (2022) a Segurança no metaverso é uma preocupação crescente à medida que mais pessoas e empresas começam a explorar esse ambiente. Alguns pontos devem ser considerados como a autenticação e controle de acesso para garantir que apenas usuários autorizados

tenham acesso a áreas restritas no metaverso. Isso pode ser feito por meio de senhas, autenticação multifatorial ou mesmo por meio de biometria, como reconhecimento facial. O Monitoramento de segurança se faz essencial para identificar possíveis vulnerabilidades e ameaças no metaverso, podendo incluir o uso de ferramentas de monitoramento de rede, como IDS (sistema de detecção de intrusão) e IPS (sistema de prevenção de intrusão), bem como o uso de software de antivírus e firewalls. O uso da criptografia: A criptografia que garante a confidencialidade e a integridade das informações transmitidas no metaverso. Isso pode incluir o uso de criptografia de chave pública e privada para proteger a comunicação e o armazenamento de dados sensíveis. Uma política de segurança para definir o comportamento esperado dos usuários no metaverso. Isso pode incluir a proibição de compartilhamento de senhas, a implementação de verificações de antecedentes para funcionários e a criação de *backups* regulares de dados sensíveis.

Uma conscientização e treinamento são essenciais para garantir que os usuários do metaverso estejam cientes das ameaças de segurança e saibam como evitar possíveis ataques. Isso pode incluir o treinamento de *phishing*³ e engenharia social⁴, bem como a criação de um sistema de relatórios de incidentes de segurança.

Construir parcerias com fornecedores de plataforma são importantes para garantir que as medidas de segurança estejam em conformidade com os padrões do setor e evitem vulnerabilidades conhecidas. Isso pode incluir a realização de auditorias de segurança regularmente e o desenvolvimento de planos de contingência para incidentes de segurança.

5 CONSIDERAÇÕES FINAIS

Diante do exposto, podemos concluir que o metaverso, é um ambiente virtual compartilhado, que permite a simulação de interações humanas do mundo real em

³ Phishing: é um tipo de ataque cibernético em que os criminosos se passam por entidades confiáveis, como empresas, instituições financeiras ou governamentais, para obter informações pessoais e confidenciais das vítimas, como senhas, números de cartão de crédito, dados bancários ou informações de login.

⁴ Engenharia Social: refere-se a técnicas utilizadas para manipular e enganar pessoas, a fim de obter informações confidenciais, acesso a sistemas ou influenciar comportamentos. Ao contrário dos ataques cibernéticos que visam explorar vulnerabilidades técnicas, a Engenharia Social explora a natureza humana, buscando enganar as pessoas e explorar sua confiança, ingenuidade ou falta de conhecimento.

mundos virtuais paralelos, revolucionando as interações sociais e de trabalho, mas os perigos que o metaverso pode representar requerem a atenção imediata dos meta-empregadores e das empresas que eles estão tentando endereçar com virtual em vez de realidade física.

Marcas poderosas abraçaram essa nova realidade, cientistas e pesquisadores já estão navegando nessa nova realidade, esse é o futuro dos negócios, mas precisamos estar atentos aos riscos, desenvolver novas campanhas de prevenção e identificar formas de melhorar a conformidade, para que possamos beneficiar da tecnologia à medida que viajamos por essa nova realidade paralela.

Cabe ressaltar que os riscos são diversos, como riscos psicossociais, de doenças ocupacionais, de privacidade e proteção de dados e manifestações de irregularidades, além de riscos éticos e de assédio sexual que precisamos evitar e eliminar. Todos devem se preparar para essa nova realidade paralela e aumentada, mas buscar ética e transparência na nova relação com a realidade alvo.

Como é possível perceber o metaverso é um ambiente virtual em constante evolução, por isso a segurança da informação nesse ambiente requer um enfoque diferente e adaptado às suas características. Sendo necessário tomar algumas medidas para garantir uma segurança efetiva no metaverso, como autenticação e controle de acesso, monitoramento de segurança para identificar as possíveis vulnerabilidades e ameaças, criptografia, a implementação de uma política de segurança, conscientização e treinamento dos usuários e parcerias com fornecedores de plataforma para trabalhar em conjunto e garantir que as medidas de segurança sejam empregadas.

Em resumo, uma segurança efetiva no metaverso requer um enfoque abrangente que abranja autenticação, controle de acesso, monitoramento de segurança, criptografia, políticas de segurança claras, treinamento de usuários e parcerias com fornecedores de plataforma.

REFERÊNCIAS

ABNT. **Associação brasileira de normas técnicas**. [S.l]: ABNT, 2022. Disponível em: <https://www.abnt.org.br/>. Acesso em: 20 mar. 2023.

ANDRADE, Lia; CENDÃO, Fabio. **Direito, Metaverso e NFTs: Introdução aos desafios na Web3.** -: Saraiva Educação S.A, 2022. Disponível em: https://books.google.com.br/books?id=xeyKEAAAQBAJ&dq=metaverso+e+mercado+&lr=&hl=pt-BR&source=gbs_navlinks_s. Acesso em: 17 mar. 2023.

CNN. **Entenda o que é o metaverso e porque ele pode não estar tão distante de você.** São Paulo: Cnn, 2021. Disponível em: <https://www.cnnbrasil.com.br/business/entenda-o-que-e-o-metaverso-e-por-que-ele-pode-nao-estar-tao-distante-de-voce/>. Acesso em: 22 mar.2023.

FAR, Saeed Banaeian. **Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges.** S.l: Journal Of Metaverse, 2022. Disponível em: <https://dergipark.org.tr/en/pub/jmv/issue/67967/1072189>. Acesso em: 21 abr. 2023.

FERNANDES, Marquésia Pereira. **Crimes digitais na era do metaverso no Brasil.** Goiás: Pontifícia Universidade Católica de Goiás, 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4923>. Acesso em: 16 mar. 2023.

FERNANDES, Afonso Fonseca. **NOVIDADES DO MUNDO VIRTUAL: METAVERSO O QUE HÁ DE NOVO?** Ceará: Bius, 2022. Disponível em: <https://periodicos.ufam.edu.br/index.php/BIUS/article/view/10675>. Acesso em: 17 mar. 2023.

FONTES, Edison Luiz Goncalves. **Segurança da Informação.** Rio de Janeiro: Saraiva, 2006. 446 p.

GARANTIDO, Backup. **Quais são os pilares da segurança da informação e como colocá-los em prática?** São Paulo: Backup Garantido, 2018. Disponível em: <https://backupgarantido.com.br/blog/pilares-da-seguranca-da-informacao/>. Acesso em: 20 mar. 2023.

GLEN, Stephanie. **History of the Metaverse in One Picture**. [S.l]: -, 2022. Disponível em: <https://www.datasciencecentral.com/history-of-the-metaverse-in-one-picture/>. Acesso em: 17 mar. 2023.

HAYNES, David. **Segurança e o Metaverso**. São Paulo: Unesp And Ufsc Universities, 2022. Disponível em: <http://researchrepository.napier.ac.uk/Output/2958725>. Acesso em: 16 mar. 2023.

HENRIQUE, Gabriela. **Proteção de Dados no Metaverso**. 2022. 1 v. TCC (Doutorado) - Curso de Direito, Runa - Repositório Universitário da Ânima, S.I, 2022. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/27167>. Acesso em: 21 abr. 2023.

LICKS, Luiza dos Anjos Lopes; GUIMARÃES, Beatriz Ferreira. **APLICABILIDADE DA LGPD NA DISCRIMINAÇÃO ALGORÍTMICA POR MEIO DA INTELIGÊNCIA ARTIFICIAL**. Coimbra: VII Congresso Internacional de Direitos Humanos de Coimbra, 2022. Disponível em: <http://www.trabalhoscidhcoimbra.com/ojs/index.php/anaiscidhcoimbra/article/view/1713>. Acesso em: 17 mar. 2023.

NEWS, Bbc. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. São Paulo: Bbc News, 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 25 mar. 2023.

REDDY, Gadekallu Thippa. **Blockchain for the Metaverse: A Review**. -: Smieeee, 2022. Disponível em: <https://doi.org/10.48550/arXiv.2203.09738>. Acesso em: 16 mar. 2023.

REVOREDO, Tatiana. **Blockchain- Tudo que você precisa saber**. -: The Global Strategy, 2019.

STINSON, Liz. **Como o metaverso será projetado?** [S.l]: Metropolis, 2022. Disponível em: <https://www.archdaily.com.br/br/976621/como-o-metaverso-sera-projetado>. Acesso em: 17 mar. 2023.

SEREC, Fernando Eduardo. **Metaverso Aspectos Jurídicos**. São Paulo: Almedina, 2022.

SOTO, Fabio. **Os desafios de segurança que o metaverso nos traz**. São Paulo: Jornal Tribuna, 2022. Disponível em: <https://jornaltribuna.com.br/2022/10/os-desafios-de-seguranca-que-o-metaverso-nos-traz/>. Acesso em: 19 mar. 2023.

THERRIEN, Cristiano. **O metaverso e seus novos horizontes democráticos**. Rio de Janeiro: Its Rio, 2023. Disponível em: https://itsrio.org/wp-content/uploads/2023/03/relatorio-diVerso_NovosHorizontesDemocraticos_SL_2.pdf. Acesso em: 18 mar. 2023.

ZOMPERO, Eric. **Explicando o metaverso, simples e direto**. São Paulo: Eric Zompero, 2022.