DISSERTAÇÃO DE MESTRADO PROFISSIONAL

METAVERSO E PERCEPÇÃO DE GESTORES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO: ESTUDO EM INSTITUIÇÃO FINANCEIRA PÚBLICA NO BRASIL

Bárbara Silva Cabral

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Metaverso e percepção de gestores da área de segurança da informação: estudo em instituição financeira pública no Brasil

Bárbara Silva Cabral

Orientador: Prof.Carlos André de Melo Alves, Ph.D., PPEE/UnB

PUBLICAÇÃO: PPEE.MP.082
BRASÍLIA-DF, MARÇO - 2025

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

METAVERSO E PERCEPÇÃO DE GESTORES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO: ESTUDO EM INSTITUIÇÃO FINANCEIRA PÚBLICA NO BRASIL

Bárbara Silva Cabral

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof.Carlos André de Melo Alves, Ph.D.,PPEE/UnB _____
Orientador

Prof.Rafael Rabelo Nunes, Ph.D.,PPEE/UnB _____
Examinador Interno

Prof. Rosalvo Ermes Streit, Ph.D., UCB _____
Examinador externo

Prof. Robson de Oliveira Albuquerque, Ph.D.,PPEE/UnB _____
Membro suplente

FICHA CATALOGRÁFICA

CABRAL,BÁRBARA SILVA
METAVERSO E PERCEPÇÃO DE GESTORES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO: ESTUDO EM INSTITUIÇÃO FINANCEIRA PÚBLICA NO BRASIL [Distrito Federal] 2025.
xvi, 55p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Metaverso
2. Segurança da Informação
3. Instituição finananceira pública
4. Análise de Conteúdo

I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

CABRAL, B. S. (2025). *METAVERSO E PERCEPÇÃO DE GESTORES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO: ESTUDO EM INSTITUIÇÃO FINANCEIRA PÚBLICA NO BRASIL*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 55p.

CESSÃO DE DIREITOS

Bárbara Silva Cabral
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por me permitir superar todas as barreiras e por me manter sempre motivada a concluir este trabalho.

À toda equipe da Secretaria do PPEE, nas pessoas da Adriana, Cristiana e Tayná, por todo suporte e orientação; e, especialmente, ao Coordenador Prof. Dr. Rafael Rabelo Nunes pelo incentivo para ingressar no Mestrado.

Aos meus amigos de jornada acadêmica, especialmente Jaqueline Damacena, Hyago Santana e Marcos Cason, pela força e troca de conhecimentos.

À minha querida família, pelo apoio incondicional e pela compreensão diante das minhas ausências.

Ao meu esposo, Herbet, por sua compreensão e apoio fundamentais durante todo esse período para a conclusão desta etapa.

Ao meu orientador, Prof. Carlos André de Melo Alves, pela confiança e suporte ao longo do curso e na elaboração deste trabalho, orientando-me com profissionalismo e compreensão em todos os momentos. Sou imensamente grata pela paciência, presença e apoio em toda essa trajetória.

Aos professores da UnB, que mesmo diante das mudanças de metodologia de ensino provocadas pela pandemia da COVID- 19, ministraram as disciplinas deste curso com dedicação. Seus ensinamentos foram fundamentais para o meu amadurecimento e para a construção deste trabalho.

Por fim, ao comitê executivo de gestores da Instituição Financeira Pública, pelo apoio essencial à realização desta pesquisa, permitindo a coleta de dados.

RESUMO

O objetivo geral deste estudo é investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre aspectos do metaverso. Foi realizada uma pesquisa descritiva com enfoque qualitativo abrangendo a coleta de documentos e de entrevistas com os referidos gestores. O tratamento dos dados abrangeu análise documental e análise de conteúdo, baseando-se em aspectos selecionados do metaverso citados por Park e Kim (2022) e na fundamentação teórica, em especial o conceito de metaverso, componentes e abordagens do metaverso, bem como benefícios e desafios sobre metaverso. Os principais resultados indicaram o conceito de metaverso vinculado a uma extensão da interação humana em um espaço digital, focado na experiência do usuário e nas aplicações. Ressaltaram-se os componentes do metaverso abrangendo hardware, software e conteúdo. As abordagens do metaverso evidenciaram a interação com os usuários, a implementação e as aplicações. Em complemento, foram identificados cinco benefícios e sete desafios relacionados ao metaverso. Este trabalho busca contribuir para enriquecer a literatura sobre o metaverso, em especial sobre a percepção de gestores de segurança da informação sobre o tema. O estudo pode contribuir, também, para a formulação de estratégias na adoção do metaverso por instituições financeiras públicas no país.

Palavras-chave: Metaverso; Segurança da informação; Instituições financeiras públicas; Análise de conteúdo.

ABSTRACT

The general objective of this study is to investigate the perception of information security managers of a Brazilian public financial institution regarding aspects of the metaverse. Descriptive research with a qualitative focus was carried out, including the collection of documents and interviews with the aforementioned managers. Data processing included documentary analysis and content analysis, based on selected aspects of the metaverse cited by Park and Kim (2022) and on the theoretical basis, in particular the concept of metaverse, components and approaches of the metaverse, as well as benefits and challenges regarding the metaverse. The main results indicated the concept of metaverse linked to an extension of the human interaction in a digital space, focused on user experience and applications. The components of the metaverse were highlighted, including hardware, software, and content. The approaches to the metaverse highlighted interaction with users, implementation, and applications. In addition, five benefits and seven challenges related to the metaverse were identified. This work seeks to contribute to enriching the literature on the metaverse, especially on the perception of information security managers on the topic. The study can also contribute to the formulation of strategies for the adoption of the metaverse by public financial institutions in the country.

Keywords: Metaverse; Information security; Public financial institutions; Content analysis.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

SIGLA	DESCRIÇÃO
ABNT	Associação Brasileira de Normas Técnicas
AR	Realidade Aumentada
APF	Administração Pública Federal
BCB	Banco Central do Brasil
BIS	Bank for International Settlements
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CBSB	Comitê da Basileia de Supervisão Bancária
CISA	Cybersecurity and Infrastructure Security Agency
CCPA	California Consumer Privacy Act
CMN	Conselho Monetário Nacional
DDoS	Distributed Denial of Service
ENISA	Agência Europeia para a Segurança das Redes e da Informação
FSB	Financial Stability Board
GDPR	Regulamento Geral sobre a Proteção de Dados
GPU	Unidade de Processamento Gráfico
HMD	Head-Mounted Displays
IA	Inteligência Artificial
IFP	Instituição Financeira Pública
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
MR	Realidade Mista
NIST	National Institute of Standards and Technology
RE	Realidade Estendida
RSL	Revisão Sistemática de Literatura
SGSI	Sistemas de Gestão da Segurança da Informação
TI	Tecnologia da Informação
UX	User Experience
VR	Realidade Virtual
XR	Realidade Estendida

1 INTRODUÇÃO

Nesta seção são apresentados a contextualização do tema investigado, a definição do problema de pesquisa, o objetivo geral, os objetivos específicos, a justificativa, as publicações resultantes desta pesquisa e a estrutura da dissertação.

1.1 CONTEXTUALIZAÇÃO

O termo "metaverso"é uma combinação semântica que carrega profundas implicações tecnológicas e sociais. Com o prefixo “meta,” que denota transcendência, e o sufixo “verso,” uma abreviação de universo, o metaverso representa a fusão de um mundo virtual com o mundo físico, criando uma dimensão de existência e interação (1).

Este conceito de metaverso é concebido como um espaço virtual coletivo, compartilhado por inúmeros usuários através da Internet, e moldado pela convergência de um espaço virtual fisicamente persistente e uma realidade física virtualmente aprimorada (2). O impacto dessa convergência está apenas começando a ser explorado, mas suas ramificações prometem ser profundas.

Com os avanços nas tecnologias, como 5G, realidade estendida, inteligência artificial e *blockchain*, a construção de aplicativos no metaverso deixa de ser apenas uma possibilidade teórica e se torna uma realidade tangível. Grandes corporações de tecnologia, incluindo o Facebook (renomeado como "Meta"), *Microsoft, Apple e Nvidia*, estão na vanguarda desse movimento.

Entretanto, o metaverso, ainda em seus estágios iniciais, suscita uma série de reflexões sobre os princípios que devem nortear a implementação de suas aplicações e a interação dos usuários nesse ambiente. As oportunidades oferecidas por este novo mundo digital vêm acompanhadas de desafios significativos, especialmente no que diz respeito à segurança da informação. O metaverso amplia a superfície de ataque para cibercriminosos, expondo os usuários e as empresas a uma variedade de ameaças, como o roubo de identidade, ataques cibernéticos através de malwares, ataques de negação de serviço distribuído (DDoS), exploração de vulnerabilidades e práticas de engenharia social. Assim, os desenvolvedores e as empresas que operam no metaverso devem estar extremamente vigilantes quanto aos aspectos de segurança e privacidade, implementando medidas robustas para proteger os usuários e seus dados (3).

Do ponto de vista acadêmico, os estudos que exploram a interseção entre o metaverso e a segurança da informação são necessários. Pesquisas sobre este tema podem revelar a evolução do conhecimento científico, destacando quais continentes estão na vanguarda dessa produção, as principais instituições acadêmicas envolvidas e as palavras-chave mais recorrentes.

Além disso, há estudos que investigam taxonomias do metaverso. O estudo de Park e Kim (4), por exemplo, aborda aspectos do metaverso, contemplando o conceito de metaverso, seus componentes e diferentes abordagens, buscando oferecer uma base teórica para a compreensão e o desenvolvimento seguro do metaverso. A produção científica sobre o metaverso pode não apenas iluminar os caminhos já trilhados,

mas também apontar para as lacunas que ainda precisam ser exploradas (5).

A segurança e privacidade dos usuários é um dos maiores problemas do mundo real. Com o advento do metaverso, inaugura-se um campo de possibilidades e transformações, especialmente no contexto da segurança da informação pois a quantidade de dados coletados será sem precedentes. (6). Nesse contexto, a integração dos mundos físico e virtual traz consigo complexidades que exigem novas abordagens para mitigar as ameaças emergentes. Ainda, segundo Ning et al(6), a segurança da informação, que já é uma preocupação central em ambientes digitais tradicionais, assume uma importância ainda maior no metaverso, onde as interações são mais imersivas e os riscos potencialmente mais elevados, exercendo uma atenção prioritária.

À medida que a tecnologia avança, conduzindo a sociedade a novos horizontes, o surgimento do metaverso se destaca como um marco significativo, conforme explorado por Park e Kim (4) em suas análises sobre a taxonomia do metaverso. Esses autores discutem o metaverso como um ambiente virtual expansivo, onde indivíduos podem interagir, criar e comercializar em tempo real, além de apresentar oportunidades revolucionárias, mas também desafios sem precedentes. Delinear estratégias eficazes para enfrentar esses desafios é crucial para garantir que o metaverso se desenvolva como um espaço seguro e confiável para todos os seus usuários (6).

Empresas de setores específicos, como o bancário, sinalizam iniciativas para explorar esse novo ambiente, vislumbrando oportunidades de inovação em serviços e interações com os clientes. No contexto das instituições financeiras, tanto públicas quanto privadas, o metaverso abre novas possibilidades para a inovação, mas também exige uma reflexão profunda por parte dos profissionais de segurança da informação. Este estudo busca enfatizar a percepção dos gestores na área de segurança da informação sobre os aspectos do metaverso em uma instituição financeira pública.

1.2 PROBLEMA DE PESQUISA

O conceito de metaverso, um ambiente virtual imersivo que integra o mundo físico e digital, tem ganhado atenção em diversas áreas, incluindo a segurança da informação. Entre os profissionais de segurança da informação, especialmente aqueles que atuam em instituições financeiras públicas, o metaverso apresenta tanto oportunidades quanto desafios. A inovação tecnológica traz consigo a necessidade de novas abordagens para garantir a integridade, confidencialidade e disponibilidade dos dados, o que gera uma série de questionamentos e preocupações. Assim, entender como esses profissionais percebem o metaverso é oportuno para desenvolver estratégias de segurança adequadas, conforme explorado por Di Pietro e Cresci (7).

Este estudo tem seu lócus em uma instituição financeira pública, cuja identidade não será revelada para os fins da pesquisa, sendo referida apenas pela sigla IFP. Essa instituição financeira é uma das mais importantes do Brasil, com uma história de inovação e segurança em suas operações, além de uma estrutura que inclui uma vasta rede de agências e serviços digitais.

A estrutura da IFP é suportada por uma política de segurança da informação, com foco em proteger os dados dos clientes e garantir a continuidade dos negócios. Em um cenário em que o metaverso pode

emergir como uma possível fronteira para as interações digitais, a referida IFP sinaliza enfrentamento dos eventuais desafios de segurança que esse ambiente pode trazer.

Se por um lado o metaverso pode oferecer novas formas de interação e negócios, por outro, também pode expor a IFP a riscos ainda não completamente compreendidos. Os gestores da área de segurança da IFP desempenham um papel necessário para a proteção dos ativos digitais da instituição. Com o advento do metaverso, esses gestores precisam estar atentos às novas ameaças e vulnerabilidades que podem surgir.

A forma como esses gestores percebem aspectos do metaverso, abrangendo seu conceito, seus componentes, abordagens, benefícios e desafios no uso do metaverso, pode influenciar as estratégias de segurança adotadas pela IFP. Diante do exposto na contextualização e nesta seção, surge o problema de pesquisa: qual a percepção dos gestores da área de segurança da informação da instituição financeira pública brasileira sobre os aspectos do metaverso?

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre aspectos do metaverso.

1.3.2 Objetivos Específicos

A partir do objetivo geral citado na Subseção 1.3.1, os seguintes objetivos foram propostos:

- Identificar as percepções dos gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre o conceito de metaverso;
- Verificar as percepções dos referidos gestores sobre os componentes do metaverso;
- Diferenciar as percepções dos gestores considerando as abordagens de metaverso;
- Descrever as percepções dos gestores sobre os principais benefícios e desafios na adoção do metaverso.

1.4 JUSTIFICATIVAS

A revisão de literatura realizada por Cabral e Alves (5), apontou uma escassez de estudos sobre o metaverso em certos continentes, especialmente na América do Sul, em face de uma substancial concentração de estudos no continente Asiático. Verifica-se também uma escassez de pesquisas voltadas para a percepção dos gestores de segurança da informação sobre o metaverso em instituições financeiras públicas, sendo essa uma lacuna de conhecimento que o presente estudo busca preencher à luz de estudos científicos, como o proposto por Park e Kim (4), para guiar futuras investigações.

Nesse sentido, verifica-se a importância de desenvolver um estudo sobre os aspectos do metaverso com base na percepção desses gestores, especialmente em instituições financeiras públicas, dada a relevância dessas organizações para a sociedade, com vistas a contribuir significativamente para o campo acadêmico.

Este trabalho busca entender a percepção dos profissionais que atuam em segurança da informação em uma instituição financeira pública. Dada a rápida evolução tecnológica, compreender como esses gestores percebem os aspectos do metaverso pode ajudar a preencher lacuna de conhecimento sobre o tema. O foco em instituição financeira acrescenta um elemento de novidade e relevância à pesquisa, diferenciando de outros estudos que podem ter abordado o tema de forma mais geral, distinto do financeiro.

Ainda que as instituições financeiras estejam estudando a melhor forma de se utilizar o metaverso, a necessidade de adaptação, com a evolução tecnológica, demanda uma reflexão estratégica sobre segurança. Torna-se necessário entender como os gestores percebem os aspectos do metaverso, especialmente em termos de segurança da informação. O conhecimento alcançado neste estudo pode contribuir para que os decisores possam sentir-se mais confortáveis ao adotar essa tecnologia.

O estudo de aspectos do metaverso é relevante sob a perspectiva prática porque pode contribuir para reflexões de organizações públicas e privadas, acadêmicos e profissionais que atuam em segurança da informação, bem como outras partes interessadas. A construção de uma base de conhecimentos sobre o metaverso permitirá que os decisores estejam mais bem preparados para lidar com os desafios e oportunidades que surgem com a integração dessa tecnologia em suas operações.

Dada a ascensão do interesse no metaverso e seu impacto potencial nas atividades do setor financeiro, compreender as percepções dos gestores de segurança da informação pode ser útil para antecipar os desafios e oportunidades no uso dessa tecnologia. À medida que o metaverso se torna mais integrado nas operações financeiras, garantir que essas tecnologias sejam seguras e bem compreendidas pelos gestores de segurança da informação é essencial para a proteção dos interesses da sociedade.

Ademais, o estudo aborda um tema relevante que traz reflexões sobre segurança no metaverso, contribuindo para a gestão de organizações públicas e privadas, para o avanço acadêmico e para a sociedade. A segurança das operações no metaverso tem implicações diretas para a confiança pública nas instituições financeiras, tornando essa pesquisa vital não apenas para o setor financeiro, mas também para a estabilidade e segurança econômica mais ampla.

1.5 PUBLICAÇÕES RESULTANTES DESTA PESQUISA

As publicações descritas na sequência foram escritas e publicadas no decorrer da elaboração desta pesquisa, servindo de subsídio para o referencial teórico, como também para a discussão dos resultados obtidos neste estudo.

Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade

Cabral, B. S., & Alves, C. A. de M.(2023).Metaverso e segurança: Análise da produção de artigos publicados em bases de dados acadêmicas no período de 2018 a 2023. São Paulo, Brasil.

Revista Caderno Pedagógico

Cabral, B. S., & Alves, C. A. de M. (2024).Metaverso e segurança: Análise de artigos publicados em bases acadêmicas de 2018 a 2023. Caderno Pedagógico, 21(7), e6064. Disponível em: <https://doi.org/10.54033/cadpedv21n7-239>.

1.6 ESTRUTURA DA DISSERTAÇÃO

O presente estudo está dividido da seguinte maneira: no capítulo 1 a Introdução, abordando tópicos como: contextualização, formulação do problema, objetivo geral e objetivos específicos, justificativas e publicação de trabalhos relacionados.

No Capítulo 2, são abordados os tópicos que serviram como referencial teórico para o trabalho. Inicialmente, apresentando o metaverso, destacando sua caracterização e seus aspectos. Em seguida, é introduzida a segurança da informação, enfatizando aspectos gerais e segurança da informação em instituições financeiras públicas.

O Capítulo 3 apresenta a metodologia utilizada na elaboração do estudo, indicando a tipologia da pesquisa, a caracterização dos instrumentos de pesquisa, a caracterização da organização em estudo, o perfil dos participantes, os procedimentos de coleta de dados e os procedimentos para análise dos dados.

O Capítulo 4 traz os resultados obtidos através das entrevistas realizadas e respostas ao questionário. Os resultados do estudo sobre o metaverso foram organizados em quatro seções principais:

- Seção 4.1: discutiu-se a percepção sobre o conceito de metaverso, revelando como esse espaço virtual é entendido e interpretado pelos entrevistados;
- Seção 4.2: apresentou a verificação das percepções dos gestores sobre os componentes do metaverso, enfatizando a relevância de hardware, software e conteúdo;
- Seção 4.3: diferenciou as percepções segundo abordagens de interação, implementação e aplicação no metaverso;
- Seção 4.4: foram discutidos os principais benefícios e desafios associados à adoção do metaverso, destacando oportunidades, como a redução da distância entre usuários e o aumento do engajamento, assim como barreiras, incluindo desafios tecnológicos e a necessidade de regulamentação.

Em síntese, o capítulo explorou de forma ampla as dinâmicas do metaverso, suas implicações e o entendimento dos gestores sobre esse novo ambiente.

Finalizando com o Capítulo 5, este estudo apresenta as considerações finais, contendo a descrição do atingimento de cada objetivo específico, o atingimento de objetivo geral, as limitações e sugestões para possíveis trabalhos futuros baseados nesta pesquisa.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta o referencial teórico da dissertação. A Seção 2.1 trata do metaverso, começando com a caracterização (Subseção 2.1.1 e seguindo para outros aspectos selecionados do metaverso (Subseção 2.1.2. Em seguida, a Seção 2.2 aborda a segurança da informação, abrangendo conceitos empregados (Subseção 2.2.1, a segurança da informação no metaverso (Subseção 2.2.2 e a segurança da informação em instituições financeiras (Subseção 2.2.3).

Para a elaboração da fundamentação teórica, foi realizada uma revisão de literatura, utilizando artigos de bases de dados acadêmicas, bibliotecas digitais e documentos de entidades especializadas. No estudo do metaverso, foram investigados artigos de 2018 a 2023, com foco particular nas bases de dados ACM Digital Library e IEEE, totalizando a análise de 79 artigos (5). Complementando essa pesquisa, a seção sobre segurança da informação foi enriquecida com livros, artigos científicos e publicações de entidades de referência internacional, incluindo o Bank for International Settlements - BIS.

2.1 METAVERSO

Esta seção do referencial teórico enfatiza inicialmente a caracterização do metaverso (Subseção 2.1.1).Na sequência, discorre-se sobre aspectos selecionados do metaverso (Subseção 2.1.2).

2.1.1 Caracterização

Esta subseção apresenta uma caracterização detalhada do metaverso, enfatizando o seu conceito e de outros termos associados, destacando os principais benefícios e desafios desse ambiente virtual.

Considerando o conceito de metaverso citado na introdução, de acordo com Huang et al. (8), o termo combina "meta"(transcendência) e "verso"(universo), e descreve a fusão de mundos virtuais e físicos, criando uma dimensão de existência e interação. Gartner (2) acrescenta que o metaverso é um espaço virtual coletivo acessado por muitos usuários via Internet, onde o virtual e o físico se integram.

O metaverso apresenta três principais características: multitecnologia, sociabilidade e hiperespaço agregado de temporalidade (6). Trata-se de um ambiente que abrange plataformas e aplicativos que oferecem experiência virtual imersiva. Ning et al.(6) abordam que a multitecnologia integra uma variedade de novas tecnologias, oferecendo uma experiência imersiva baseada em tecnologia de realidade aumentada e blockchain. Quanto à sociabilidade, sendo o metaverso um novo tipo de forma social, ele inclui sistemas econômicos, sistemas culturais e sistemas legais, que estão intimamente relacionados à realidade, mas têm suas próprias características. Por fim, com relação à característica da hiperespaço-temporalidade, refere-se ao metaverso como um mundo virtual paralelo ao mundo real, quebrando os limites de tempo e espaço e oferecendo aos usuários uma experiência aberta, livre e imersiva (6).

Wang et al. (2023) (9)conduziram uma análise aprofundada do metaverso, revelando seu estado atual,

as tecnologias envolvidas, suas aplicações e os desafios enfrentados. A pesquisa destaca a evolução contínua do metaverso e identifica áreas essenciais que necessitam de mais investigação para avançar nesse campo. O metaverso é uma palavra composta de transcendência "meta"e universo "verso"e refere-se a um mundo virtual tridimensional onde avatares se envolvem em atividades políticas, econômicas, sociais e culturais (4).

Para uma compreensão completa do metaverso, é necessário familiarizar-se com os termos tecnológicos que fazem parte do contexto do metaverso, conforme descritos a seguir: *Web 3.0, blockchain*, Inteligência Artificial (IA), Avatares e Realidade Aumentada (RA). A RA é uma das tecnologias dentro do conceito mais amplo de Realidade Estendida (RE). Enquanto a RA se foca na sobreposição de dados digitais ao mundo físico, RE abrange um conjunto mais amplo de tecnologias que criam ou combinam experiências imersivas em diferentes níveis (4).

Além disso, a RA emerge como uma tecnologia que combina elementos digitais com o mundo físico, proporcionando uma integração fluida entre os ambientes real e virtual e enriquecendo a experiência do usuário (10).

A RA e o metaverso estão interligados, pois ambas as tecnologias trabalham em conjunto para criar experiências digitais mais ricas, imersivas e interativas.

À medida que essas tecnologias continuam a evoluir, sua sinergia proporcionará novas e excitantes formas de interação, tornando o metaverso uma extensão ainda mais envolvente e acessível da nossa realidade cotidiana, conforme explorado por Park e Kim (2022) (4)em suas análises sobre a taxonomia do metaverso.

A *Web 3.0* marca a terceira geração da *internet*, promovendo uma revolução em que a descentralização e a autonomia dos usuários se tornam pilares centrais. Essa evolução abre caminho para experiências virtuais ainda mais personalizadas e seguras, redefinindo a interação online (Cabral & Alves, 2024)(5). A Web 3.0 e o metaverso estão interligados, pois ambos contribuem para a próxima evolução da internet, na qual a descentralização, a interatividade imersiva e a propriedade digital são elementos centrais.

Ainda, a Web 3.0 fornece as bases tecnológicas que permitem ao metaverso existir e prosperar, oferecendo aos usuários controle total sobre seus dados, ativos e experiências. À medida que a Web 3.0 continua a evoluir, ela impulsionará o desenvolvimento do metaverso, transformando a maneira como interagimos, trabalhamos e vivemos em mundos virtuais.

Outro termo vinculado ao metaverso é blockchain. Essa tecnologia vincula-se ao uso de registro descentralizado que garante a integridade e autenticidade das transações digitais no metaverso, contribuindo para a segurança e a propriedade dos ativos virtuais (11). Ademais, blockchain está associado à garantia de segurança, confiança e descentralização em um ambiente virtual altamente interconectado. O metaverso requer uma infraestrutura robusta para suportar suas complexas operações digitais. A tecnologia blockchain, por permitir registrar transações de forma imutável e transparente, contribui para a implementação do metaverso.

A IA surge como uma tecnologia que se vincula, também, ao metaverso. Ela pode impulsionar interações mais naturais ao criar avatares e assistentes virtuais que contribuem para aprimorar a experiência dos usuários (12). A IA é um componente do metaverso que oferece bases para uma experiência imersiva, personalizada e segura. Desde a criação e gestão de conteúdo até a personalização da interação do usuário

e a segurança do ambiente virtual, a IA enriquece o metaverso e permite que ele evolua de forma dinâmica e adaptativa. À medida que o metaverso continua a crescer e se desenvolver, a integração da IA será vital e cada vez mais essencial para criar experiências virtuais inovadoras para conectar o mundo virtual e o mundo real através de seus três elementos principais: dados, algoritmo e poder de computação (Ning et al.,(6))

Os avatares são a principal interface através da qual os usuários se conectam, interagem e experimentam o ambiente virtual no metaverso. À medida que o metaverso venha a evoluir, os papéis que os avatares irão desempenhar poderão ser cada vez mais sofisticado.

O termo 'avatar' já foi usado como uma forma exagerada predefinida de representar o usuário no mundo virtual, em vez de refletir o mundo real. No entanto, gradualmente muda para uma forma ideal que projeta a aparência externa do usuário e reflete o seu ego. Um avatar pode desempenhar um papel social adequado para um trabalho e uma personalidade no metaverso (4)

Ainda, segundo Park e Kim (4), o metaverso oferece benefícios significativos, incluindo a criação de oportunidades inovadoras para colaboração, aprendizado e entretenimento, permitindo que pessoas de diversas origens se conectem e interajam de maneiras criativas. Wang et al.(9) destacam que o metaverso pode transformar a educação e promover novos modelos de inovação. Li et al. (13)sugerem que o metaverso pode ser usado para desenvolver cenários educacionais avançados, facilitando um aprendizado mais imersivo e interativo.

Quanto aos desafios, o metaverso apresenta a necessidade de proteger dados sensíveis e a privacidade dos usuários em um ambiente altamente interconectado (12);(8). Esse desafio ressalta a relevância desta pesquisa, a qual aborda o estudo com gestores de segurança da informação. A segurança da informação é detalhada na Seção 2.1.2 deste estudo.

Falchuk, Loeb e Neff (14) exploram a privacidade em ambientes digitais interativos ao oferecer soluções para proteger dados pessoais em contextos nos quais os usuários interagem frequentemente e compartilham informações de forma dinâmica. Os autores destacam a importância de criar mecanismos de controle que permitam aos usuários gerenciar como suas informações são coletadas, compartilhadas e utilizadas em plataformas sociais.

Por outro lado, Kang, Koo e Kim (15) concentram-se em estratégias para enfrentar os desafios específicos da privacidade em contextos sociais, como redes sociais e ambientes colaborativos. Eles propõem métodos para garantir que as informações pessoais dos usuários sejam protegidas de maneira eficaz, mesmo em situações de alta interação e compartilhamento de dados. Suas abordagens incluem a implementação de políticas de privacidade robustas e o uso de tecnologias avançadas para proteger dados contra acessos não autorizados. Nesse contexto, Ryu et al.(11) propuseram um sistema de autenticação mútua segura baseado em blockchain para enfrentar desafios de segurança e autenticação no metaverso.

Ambos os estudos contribuem para a compreensão de como a privacidade pode ser gerida em ambientes sociais e interativos, oferecendo diretrizes e estratégias que ajudam a equilibrar a necessidade de interação social com a proteção de dados pessoais.

Outro grande desafio do metaverso é a necessidade de marcos regulatórios específicos para o metaverso, abordando os aspectos jurídicos emergentes que devem ser tratados para garantir uma regulamentação

adequada. Serec (16) argumenta que a integração de soluções inovadoras, como criptografia avançada, controles de acesso mais rigorosos e mecanismos de anonimização, contribuem para manter a privacidade em ambientes interativos e dinâmicos. As necessidades de uma governança eficaz e a conscientização dos usuários também são apontadas como fatores-chave para garantir uma proteção adequada em contextos em que a coleta e o compartilhamento de dados são intensificados.

2.1.2 Aspectos Selecionados

Esta subseção aborda aspectos selecionados do metaverso, baseados na taxonomia proposta por Park e Kim (2022)(4). Essa taxonomia é útil neste estudo para entender a complexidade e a diversidade do metaverso, proporcionando uma base para o estudo do tema e seu desenvolvimento futuro. A referida taxonomia é descrita na Figura 2.1. Para os fins deste estudo, os seguintes conceitos dessa taxonomia são aproveitados neste trabalho: conceito de metaverso, componentes do metaverso e abordagens do metaverso.

Primeiramente, sobre os conceitos vinculados ao metaverso citados na Figura 2.1, cabe destacar que, além do conceito, os conceitos semelhantes: 'Avatar' e 'Realidade Estendida' foram previamente caracterizados na Subseção 2.1.1 deste referencial teórico.

A Figura 2.1 apresenta, também, os componentes do metaverso. Eles são divididos em componentes de hardware, componentes de software e conteúdo. A descrição desses componentes é feita, na sequência.

Componentes de *Hardware* – O *hardware* no Metaverso não apenas desempenha um papel importante na experiência imersiva, mas também é uma barreira tecnicamente limitante. No metaverso, o *hardware* é aprimorado pelos efeitos do avanço tecnológico, mas ainda precisa de melhorias em comparação com a experiência do mundo real. Inclui dispositivos como *head-mounted displays* (HMDs), que oferecem experiências visuais imersivas, e outros dispositivos auxiliares físicos. A melhoria contínua em tecnologias de hardware, como memória GPU e redes 5G, contribui para suportar a complexidade e a interatividade do metaverso (4)

Componentes de *Software* (Reconhecimento e Renderização) – Uma ilusão cognitiva desempenha um papel essencial na imersão na realidade objetiva do espaço físico e na realidade subjetiva que os usuários percebem.

Existem dois tipos de cognição: cognição estática e cognição dinâmica. A cognição estática são os sentidos proprioceptivos (por exemplo, visão, audição e tato), enquanto a cognição dinâmica é o equilíbrio sensorial e o movimento corporal. O *software* desempenha um papel na renderização e no processamento de grandes volumes de dados visuais para garantir uma experiência imersiva. A baixa latência é essencial para evitar problemas como tontura e enjoo causados por confusão sensorial.

A respeito dos componentes de conteúdo, são componentes que mantêm o metaverso e são usados para fornecer uma experiência imersiva por meio de histórias bem-organizadas e eventos criados por usuários. Embora seja possível capturar o movimento 3D em tempo real de cenas com uma câmera monocromática e isolar estruturas do corpo humano (por exemplo, apertos de mão), o uso dos componentes de conteúdo ainda é limitado na captura de interações próximas (por exemplo, abraços).

Ainda a respeito dos componentes de conteúdo, a realidade da história, a experiência imersiva e a

Figura 2.1 – Taxonomia do Metaverso

Fonte: Park e Kim (2022).

integridade conceitual são importantes. Existem duas maneiras de criar conteúdo: um método de mudança de paradigma e um método para reutilizar o conteúdo existente.

As áreas que exigem design de ambiente são cenas, cor e iluminação, áudio, amostragem e navegação ambiental e conteúdo do mundo real. O conteúdo é a chave para a sustentabilidade do metaverso. Deve haver um enredo ou narrativa que permita diversas interações dos usuários em ambientes virtuais. Isso inclui a geração de conteúdo imersivo e a criação de histórias multimodais que envolvam os usuários de forma significativa.

Quanto à abordagem, tem-se a seguinte classificação com base na Figura 1: interações com usuário, implementações e aplicações do metaverso (4), detalhados conforme descrito na sequência.

A respeito das interações do usuário, a interação é uma condição essencial para aumentar a imersão no metaverso. Ela pode reproduzir rostos de amigos e celebridades para permitir interações realistas e incutir nos usuários a ilusão de lugares familiares e famosos. Dissociação temporária, concentração e prazer aumentado são fatores importantes na interação, e são utilizadas emoções de controle, curiosidade e motivação intrínseca.

O alvo da interação é principalmente humano e as mãos são uma característica importante. Os dispositivos de entrada são amplamente divididos em dispositivos portáteis e dispositivos de entrada não manuais. Foca em criar uma experiência que permita aos usuários interagir de forma imersiva e natural dentro do metaverso, utilizando técnicas como reconhecimento de visão e linguagem, e interação humano-robô (4).

A respeito da implementação, citada na Figura 2.1, no caso do metaverso, é dividida em uma fase de design, uma fase de treinamento de modelo, outra fase de operação e outra de avaliação. Ainda, abrange inferência multimodal, abordagens baseadas em RL e aprendizagem ao longo da vida para modelos de treinamento do Metaverso. Além disso, é necessário considerar a otimização multiagente, a otimização de integração e as considerações operacionais da perspectiva da operação do serviço Metaverso (4).

Por fim, segundo Park e Kim (4), no que diz respeito às aplicações, conforme citado na Figura 2.1, a maior parte das pesquisas sobre o metaverso visa fins de marketing e investimento, enfatizando a utilidade social. Os domínios onde o metaverso é mais popularmente utilizado são os jogos e alguns aplicativos de escritório.

Huggett (17) argumentou que existe uma separação entre a realidade presente e a realidade virtual da herança virtual e conduziu um estudo da existência e do realismo na realidade virtual. Skarbez (18) introduziu realidade mista, modelagem do mundo real e modelagem do mundo virtual. Para melhores aplicações do metaverso, é necessária uma abordagem para modelar e distinguir as diferenças e os mesmos pontos entre realidade virtual e realidade. Complementando, o uso do metaverso em diferentes contextos, como simulações, marketing, educação, entre outros, desempenham um papel crucial na definição das funcionalidades e do alcance do metaverso.

2.2 SEGURANÇA DA INFORMAÇÃO

2.2.1 Conceitos Empregados

A segurança da informação envolve um conjunto de práticas, políticas e procedimentos destinados a proteger as informações contra acessos não autorizados, uso indevido, divulgação inadequada, alterações ou destruição. Conforme definido por Whitman e Mattord (19), este conceito é sustentado por três pilares fundamentais: a confidencialidade, que assegura que as informações sejam acessíveis apenas a indivíduos devidamente autorizados; a integridade, que garante a precisão e a completude das informações; e a disponibilidade, que assegura que os dados estejam acessíveis sempre que necessário.

A segurança da informação é um campo fundamentado em princípios estabelecidos e normas reconhecidas internacionalmente, como a ISO/IEC 27001 (20), que fornece um modelo para a implementação, monitoramento e melhoria contínua de sistemas de gestão da segurança da informação (SGSI). Conceitos essenciais como confidencialidade, integridade, disponibilidade e autenticidade formam a base de qualquer estratégia de segurança, conforme explorado em Whitman e Mattord (19), e Stallings e Brown (21).

Várias soluções e abordagens de segurança têm sido propostas, conforme descrito de forma exemplificativa na Tabela 2.1.

A Tabela 2.1 aborda práticas essenciais com base no framework do National Institute of Standards and Technology NIST (22) e ISO/IEC 27001 (20) para garantir a segurança da informação no Metaverso, destacando cinco áreas principais.

A Criptografia e Autenticação Forte são essenciais para proteger a confidencialidade e autenticidade das comunicações e transações, prevenindo acessos não autorizados. Blockchain e Contratos Inteligentes garantem a integridade dos dados e automatizam acordos de forma segura. A Gestão de Identidade Descentralizada (DID) permite que os usuários controlem suas identidades digitais de forma segura. A Auditoria e Conformidade assegura que as práticas de segurança estejam alinhadas com normas e regulamentações. Por fim, a Educação e Conscientização dos usuários é crucial para mitigar riscos como phishing e engenharia social.

2.2.2 Segurança da Informação no Metaverso

Os desafios de segurança da informação podem ser ampliados e tornando-se ainda mais complexos no metaverso. A gestão da identidade digital, por exemplo, exige mecanismos robustos para garantir que os usuários sejam autenticados e autorizados de forma segura, prevenindo acesso não autorizado e fraudes. Além disso, em nível internacional e conforme a jurisdição, a proteção de dados pessoais no metaverso deve atender a regulamentações, como o Regulamento Geral sobre a Proteção de Dados (GDPR)(23) na Europa e leis referentes a privacidade aplicáveis ao consumidor, como California Consumer Privacy Act (CCPA), válido no estado norte-americano da Califórnia.(24)

A segurança das transações e dos ativos virtuais dentro do metaverso, também, requer atenção especial. Com o crescimento da economia virtual, a proteção contra fraudes e roubos torna-se uma prioridade para garantir a confiança dos usuários. Além disso, o metaverso enfrenta diversas ameaças cibernéticas,

Tabela 2.1: Descrição de soluções e abordagens de segurança

Característica	Descrição
Criptografia e Autenticação Forte	O uso de criptografia robusta e autenticação multifatorial pode ajudar a proteger a confidencialidade e autenticidade das comunicações e transações no Metaverso
Blockchain & Contratos Inteligentes	A tecnologia blockchain oferece um meio descentralizado e imutável para registrar transações e garantir a integridade dos dados, enquanto os contratos inteligentes podem automatizar a execução segura de acordos dentro do Metaverso
Gestão de Identidade Descentralizada (DID)	Abordagens de DID baseadas em blockchain permitem aos usuários manter o controle de sua identidade digital de forma descentralizada, reduzindo o risco de comprometimento de identidade
Auditoria e Conformidade	Implementar processos de auditoria e conformidade regulatória ajuda a garantir que as práticas de segurança da informação no Metaverso estejam alinhadas com os padrões e regulamentações de segurança relevantes
Educação e Conscientização	Promover a educação e a conscientização dos usuários sobre as melhores práticas de segurança da informação é fundamental para mitigar o risco de ataques como phishing e engenharia social

Fonte: A autora, com base em NIST(2023) e ISO/IEC 27001(2022).

incluindo malware, phishing e ataques de negação de serviço (DDoS- Distributed Denial of Service), que exigem a implementação de medidas de segurança cibernética cada vez mais robustas.

Portanto, a aplicação de princípios tradicionais de segurança da informação, aliada à gestão eficaz de vulnerabilidades de softwares, são essenciais para enfrentar os desafios únicos e emergentes do metaverso. Esses princípios são aplicáveis a diversos contextos digitais, incluindo a gestão de vulnerabilidades de softwares, que é crucial para mitigar riscos em qualquer ambiente dependente de tecnologia. Dada a complexidade dos ambientes virtuais e a crescente interconectividade, a identificação e correção de vulnerabilidades no software se tornam fundamentais para prevenir exploração por parte de atacantes.

A percepção dos usuários sobre segurança e confiança no metaverso tem sido objeto de estudos, como o realizado por Al-Kfar et al. (25), que conduziu uma revisão abrangente dos fatores influentes nesse contexto. As descobertas descritas no estudo citado neste parágrafo revelam que a confiança dos usuários é moldada por uma série de aspectos, incluindo a proteção de dados pessoais e a integridade das interações virtuais. O autor aponta para a importância dessas questões no fortalecimento da confiança no ambiente do metaverso.

O impacto da segurança da informação na satisfação do usuário dentro do metaverso também foi explorado por Jo e Park (26). Este estudo identificou que a implementação de medidas de segurança eficazes é fundamental para promover experiências positivas. Eles argumentam que a satisfação do usuário está diretamente ligada à percepção de segurança, o que reforça a necessidade de práticas robustas de proteção de dados e privacidade para garantir a longevidade e o sucesso das plataformas do metaverso.

No campo das interações sociais e da identidade virtual, Zhang et al (27) investigaram como as diferenças de gênero e idade dos usuários representados pelos avatares influenciam as interações e a busca por ajuda dentro do metaverso. Seus achados sugerem que a identidade virtual não apenas molda as interações sociais, mas também influencia as necessidades de segurança, indicando que abordagens personalizadas podem ser necessárias para atender a diferentes grupos de usuários.

Vadlamudi (2022) propôs uma taxonomia que classifica sistematicamente as diversas ameaças de segurança no metaverso e suas contramedidas correspondentes. Esta estrutura categoriza ameaças como roubo de identidade, ataques cibernéticos e invasões de privacidade, organizando-as de acordo com suas características e impactos. Além de identificar as ameaças, essa taxonomia de Vadlamudi também sugere soluções específicas, como técnicas de autenticação forte, criptografia e monitoramento contínuo, para mitigar os riscos e proteger usuários e ativos no metaverso.

Enquanto Vadlamudi(3) oferece uma abordagem prática e voltada para aplicação direta, Park e Kim (4) tendem a fornecer uma estrutura mais teórica, adequada para análises aprofundadas e desenvolvimento de novas estratégias de segurança. Ambos os trabalhos podem servir a propósitos distintos, mas complementares, dentro do campo da segurança da informação no metaverso.

As ameaças e vulnerabilidades cibernéticas específicas do metaverso foram analisadas por Sharma e Zamfiroiu (28), que destacaram a necessidade de medidas proativas para mitigar os riscos. Eles argumentam que, devido à natureza altamente interativa e imersiva do metaverso, as ameaças cibernéticas podem ter consequências mais profundas e de longo alcance, tornando a segurança um aspecto prioritário.

A arquitetura de confiança zero, investigada por Al Shehhi e Otoum (29), apresenta uma abordagem

inovadora para lidar com as preocupações de segurança no metaverso. A adoção dessa arquitetura visa eliminar a confiança implícita dentro da rede, oferecendo uma camada adicional de proteção ao garantir que todas as entidades sejam autenticadas e verificadas continuamente, o que pode ser crucial no ambiente dinâmico do metaverso.

Kang et al.(15) concentraram-se nos requisitos de segurança e privacidade das aplicações no metaverso, destacando a necessidade de abordagens específicas para garantir a proteção dos dados e a confiança dos usuários. Eles argumentam que cada aplicação dentro do metaverso pode apresentar riscos únicos que exigem soluções sob medida para mitigar possíveis vulnerabilidades.

2.2.3 Segurança da Informação em Instituições Financeiras

As organizações públicas enfrentam desafios de segurança da informação que são únicos e críticos, principalmente devido à natureza sensível dos dados que gerenciam. Wu et al.(30) destaca que essas entidades são alvos frequentes de ameaças cibernéticas sofisticadas, incluindo ataques de phishing, ransomware e hacking, resultantes da vasta quantidade de informações confidenciais sob sua custódia. A natureza crítica dessas informações não só aumenta o risco de ataques, mas também amplifica as consequências de uma eventual violação, afetando diretamente a confiança pública e a estabilidade institucional.

A complexidade tecnológica presente nas organizações públicas, caracterizada por infraestruturas de TI complexas e heterogêneas, torna a implementação de medidas de segurança um verdadeiro desafio. A diversidade de sistemas e redes dificulta a aplicação de uma estratégia de segurança consistente, exacerbando as vulnerabilidades e criando brechas que podem ser exploradas por atacantes, como também apontado no estudo de Kang et al.(15).

Além disso, a crescente pressão para garantir compliance com regulamentações rigorosas, como a Lei Geral de Pro teção de Dados (LGPD) no Brasil e o GDPR na Europa (23), adicionam uma camada de complexidade. A conformidade com essas regulamentações, conforme a jurisdição do país, são essenciais não apenas para evitar penalidades, mas também para assegurar que a privacidade e a integridade dos dados sejam mantidas. (31)

Para mitigar esses riscos, as organizações públicas devem adotar estratégias de segurança da informação. A criação e implementação de políticas abrangentes de segurança da informação que abordem desde o controle de acesso até a gestão de incidentes, podem contribuir para estabelecer uma base consistente de proteção. Investir em tecnologias avançadas, como firewalls, sistemas de detecção de intrusos e criptografia, é igualmente crucial para prevenir e responder a ameaças cibernéticas. Essas tecnologias devem ser complementadas por programas contínuos de treinamento e conscientização dos funcionários, que são frequentemente o elo mais fraco na cadeia de segurança, como observado por Vadlamudi (3).

Além das estratégias internas, o monitoramento contínuo e a avaliação das práticas de segurança são necessários para identificar e mitigar vulnerabilidades em potencial antes que elas sejam exploradas. Este enfoque proativo permite às organizações, inclusive as organizações públicas, a manter um estado de alerta constante, ajustando suas defesas à medida que novas ameaças surgem, uma prática alinhada às recomendações de Al Shehhi e Otoum (29).

Diante da crescente complexidade das ameaças cibernéticas, parcerias estratégicas e colaborações com outras entidades, como agências de segurança cibernética, o setor privado e instituições acadêmicas, são cada vez mais necessárias. Essas parcerias não apenas facilitam o compartilhamento de informações e recursos, mas também promovem a adoção de melhores práticas que fortalecem a resiliência cibernética em um ambiente cada vez mais interconectado e ameaçador.

No cenário internacional, diversos organismos desempenham um papel fundamental na regulamentação e supervisão da segurança cibernética em instituições financeiras. O Financial Stability Board (FSB)(32) lidera os esforços para coordenar e recomendar implementação de políticas financeiras globais, incluindo aquelas relacionadas à cibersegurança, promovendo a estabilidade financeira mundial ao endereçar vulnerabilidades nos sistemas financeiros internacionais (32)

O Banco de Compensações Internacionais (BIS) e o Comitê da Basileia de Supervisão Bancária (CBSB) (33), também, são atores-chave na promoção de normas de cibersegurança robustas para o setor financeiro. O CBSB, em particular, estabelece diretrizes e melhores práticas para garantir que os bancos sejam resilientes diante das ameaças cibernéticas Sharma & Zamfiroiu, (28).

Na União Europeia, a Agência Europeia para a Segurança das Redes e da Informação (ENISA)(34) desempenha um papel central na orientação sobre proteção das infraestruturas críticas e na promoção da segurança cibernética na Europa. Segundo Al-Kfairy et al.(25), a ENISA atua como um facilitador essencial, promovendo o intercâmbio de informações, boas práticas e experiências entre os diversos atores do ecossistema de segurança cibernética.

No Brasil, o Conselho Monetário Nacional (CMN)(35) e o Banco Central do Brasil (BCB) (36)são as principais entidades que influenciam a regulamentação e supervisão da segurança cibernética em instituições financeiras. O CMN estabelece as diretrizes para a política monetária e financeira do país, incluindo aspectos ligados à estabilidade financeira e à gestão de riscos nessas entidades. Enquanto o BCB é responsável por supervisionar a implementação dessas diretrizes pelas instituições financeiras.(36)

As ações coordenadas dessas entidades garantem que o sistema financeiro brasileiro esteja alinhado com as melhores práticas internacionais em cibersegurança, contribuindo para a estabilidade e confiança no mercado financeiro.

Além disso, o Sistema de Informações de Segurança Bancária serve como um mecanismo para que as instituições financeiras compartilhem informações sobre ameaças e incidentes de segurança cibernética. O BIS (Bank for International Settlements)(37), ou Banco de Compensações Internacionais, é uma entidade financeira internacional que serve como um banco para bancos centrais. Fundado em 1930, ele tem sede em Basileia, Suíça, e atua como um fórum para a cooperação entre bancos centrais, promovendo a estabilidade monetária e financeira global além de fortalecer a resiliência do setor bancário contra ataques cibernéticos, facilitando a troca de inteligência e a colaboração entre bancos, reguladores e autoridades governamentais.

Por meio desse sistema, as instituições financeiras conseguem identificar padrões de ataques, antecipar ameaças emergentes e implementar medidas proativas para proteger seus sistemas e dados. A eficácia do BIS, conforme Al Shehhi e Otoum (29), depende da confiança mútua entre os participantes, da qualidade das informações compartilhadas e da rapidez na resposta a incidentes cibernéticos.

3 METODOLOGIA

Este capítulo apresenta a metodologia deste estudo estruturada em seis seções, a saber: 3.1) Tipologia da pesquisa; 3.2) Caracterização dos instrumentos de pesquisa; 3.3) Caracterização da organização em estudo; 3.4) Perfil dos participantes e da organização; 3.5) Procedimentos de coleta dos dados; e 3.6) Procedimentos de análise dos dados.

3.1 TIPOLOGIA DE PESQUISA

Neste estudo, realizou-se uma pesquisa descritiva (Sampieri; Collado & Lucio (38). A pesquisa descritiva busca descrever características de uma população ou fenômeno. A abordagem é qualitativa, e por meio dela, procura-se analisar a percepção dos servidores da área de segurança da informação sobre os aspectos do metaverso, aprofundando em suas experiências e pontos de vista, na maneira como enxergam sua realidade. O nível de análise do estudo é organizacional.

3.2 CARACTERIZAÇÃO DOS INSTRUMENTOS DE PESQUISA

Neste estudo, o instrumento de pesquisa utilizado foi um roteiro de entrevista semiestruturado (Gil (39) para coleta de dados primários. De acordo com Sampieri, Collado e Lucio (38), as entrevistas possibilitam obter dados particulares detalhados, empregados quando o problema de estudo é muito difícil de ser observado, seja por ética ou por complexidade.

O detalhamento do roteiro de entrevistas consta do Apêndice B deste trabalho. O roteiro abrange oito perguntas, sendo as cinco primeiras perguntas referentes ao conteúdo e outras três questões são demográficas. O teor das perguntas referentes ao conteúdo versa sobre aspectos selecionados do metaverso, abrangendo conceito, componentes, abordagens do metaverso, complementado pelo questionamento dos benefícios e desafios do metaverso. Para a elaboração e organização das questões de conteúdo, foi consultado o referencial teórico, especialmente, a taxonomia de metaverso de Park e Kim (4).

Antes do uso do roteiro de entrevistas, realizou-se um teste piloto por meio da consulta a três servidores da área de segurança da informação, que atuaram como avaliadores das perguntas do roteiro. Os servidores selecionados possuíam características semelhantes aos entrevistados (Alexandre; Coluci (40). O referido teste piloto foi realizado após a autorização do pedido de coleta de dados, citada no Apêndice A, ter sido previamente deferida pela instituição, entre 27/09/2024 e 30/09/2024.

3.3 CARACTERIZAÇÃO DA ORGANIZAÇÃO EM ESTUDO E PERFIL DOS PARTICIPANTES DO ESTUDO

A organização em questão se trata de uma instituição financeira pública, sendo o lócus de estudo a sua área de segurança da informação. Esta IFP foi intencionalmente selecionada por conta de sua representatividade para o Sistema Financeiro Nacional (SFN) e pela fácil acessibilidade aos dados.

A IFP possui um presidente e oito vice-presidências. A estrutura organizacional da Direção-Geral do órgão, na época de realização desta pesquisa, foi composta por diretorias e unidades, entre estas, a Unidade de Segurança Digital e da Informação. Para atingir os objetivos deste estudo, não foi necessário indicar o nome da IFP nas análises e a própria IFP não autorizou a divulgação de seu nome, sendo então suficiente indicar a instituição somente por meio da sigla.

Os gestores consultados foram selecionados entre aqueles que ocupam cargos de gerência, situados na Unidade de Segurança Digital e da Informação citada no parágrafo anterior. Na data base de agosto de 2024, os ocupantes do cargo de gerência dessa unidade totalizaram 33 potenciais candidatos a entrevista, sendo efetivamente entrevistados dez desses servidores.

O critério para selecionar os gestores para as entrevistas que participaram do estudo contemplou uma estratificação mesclada entre nível hierárquico e localização do gestor na Unidade de Segurança Digital e da Informação.Tal seleção buscou reduzir a chance de viés que poderia ser causado na seleção de entrevistados de uma parte específica da referida unidade.

A listagem com o perfil dos entrevistados desta pesquisa consta na Tabela 3.1, a seguir descrita. Ainda, a referida tabela apresenta o perfil dos entrevistados desta pesquisa, destacando suas qualificações acadêmicas e experiência profissional. Como destaque, temos 4 profissionais com nível de doutorado e mestrado e 6 entrevistados possuem especialização completa e mais de 12 anos de atuação na IFP, refletindo um alto nível de expertise na área. Além disso, todos possuem vasta experiência em segurança da informação, com tempos de atuação variando de 3 a mais de 12 anos. Esse perfil diversificado e experiente dos entrevistados contribui significativamente para a credibilidade e profundidade das análises realizadas na pesquisa. A combinação de formação acadêmica avançada e extensa experiência prática proporciona uma visão abrangente e detalhada sobre o tema estudado.

Tabela 3.1: Descrição do perfil dos entrevistados

Entrevistado	Escolaridade	Tempo de atuação na IFP	Tempo de atuação na área de segurança da informação
E1	Doutorado	Mais de 12 anos	Mais de 12 anos
E2	Especialização completa	Mais de 12 anos	Mais de 12 anos
E3	Mestrado	Mais de 12 anos	6 a 9 anos
E4	Especialização completa	Mais de 12 anos	6 a 9 anos
E5	Especialização completa	Mais de 12 anos	3 a 6 anos
E6	Especialização completa	Mais de 12 anos	3 a 6 anos
E7	Especialização completa	Mais de 12 anos	9 a 12 anos
E8	Especialização completa	Mais de 12 anos	Mais de 12 anos
E9	Mestrado	Mais de 12 anos	Mais de 12 anos
E10	Mestrado	Mais de 12 anos	Mais de 12 anos

Fonte: elaborado pela autora, a partir de dados da pesquisa.

Por fim, segundo descrito no referido quadro, um servidor possui doutorado, três possuem mestrado e seis possuem especialização completa. Quanto ao tempo de atuação na instituição, todos os dez servidores atuam na IFP há mais de doze anos. Quanto ao tempo de atuação na área de segurança da informação, cinco servidores possuem mais de doze anos na área, enquanto um servidor atua entre nove e doze anos, dois servidores entre seis e nove anos e dois servidores entre três e seis anos atuam na segurança da informação.

3.4 PROCEDIMENTOS DE COLETA DE DADOS

A coleta de dados foi realizada por meio de entrevistas, complementada pela coleta de documentos não sigilosos. Para viabilizar o acesso a dados, inicialmente foi efetuado o pedido de acesso a dados à IFP, tendo como referência para o pedido o disposto no Apêndice A deste projeto, cujo deferimento ocorreu em 13/09/2024.

Sobre as entrevistas, primeiramente, foi realizada uma abordagem inicial aos entrevistados, solicitando a participação voluntária. Em seguida, os potenciais entrevistados que aceitaram o convite para entrevista foram chamados para entrevistas individuais com base no roteiro de entrevistas, previamente citado na Seção 3.2 e descrito no Apêndice B. Foram realizadas dez entrevistas gravadas pelo Google Meet e posteriormente transcritas para análise. A coleta dessas entrevistas foi finalizada quando foi atingida a saturação teórica (41).

Além da coleta realizada por meio das entrevistas, nesta pesquisa efetuou-se a coleta de documentos não sigilosos da IFP, para subsidiar as análises das entrevistas. Foram consultados tanto documentos de natureza pública, quanto documentos internos não sigilosos além de documentos audiovisuais não sigilosos.

Por fim, a coleta dos documentos citados no parágrafo anterior e a realização das entrevistas previamente citadas nesta seção, foram efetuadas nos períodos 11/10/2024 a 21/11/2024.

3.5 PROCEDIMENTOS DE ANÁLISE DOS DADOS

Os procedimentos utilizados para analisar os dados coletados abrange a análise de conteúdo e análise documental (Bardin, (42). De acordo com Bardin (1977), a análise documental é uma etapa inicial da documentação, visando representar de forma concisa as informações contidas. Essa análise documental foi particularmente importante para consultar os documentos não sigilosos contendo informações sobre o metaverso e ações adotadas pela IFP. Desses documentos, foram selecionadas as informações mais importantes, e deve ser reforçada sua extrema importância para construção do conteúdo.

A referida análise categorizou os dados coletados de entrevistas e de documentos citados na Seção 3.5, considerando os seguintes aspectos selecionados do metaverso: 1. 'Conceitos', 2. 'Componentes' e 3. 'Abordagens do metaverso' (Park & Kim (4), complementado por benefícios e desafios do metaverso, citados no referencial teórico deste estudo, especialmente na Seção 2.1.1.

A Tabela 3.2 apresenta de forma resumida o vínculo entre objetivos e procedimentos de coleta e de análise de dados neste estudo.

Miles e Huberman (1994) e Creswell (2014) enfatizam a importância de adotar uma abordagem sistemática e transparente na análise dos dados para garantir a validade e confiabilidade dos resultados. Dessa forma, foi realizado teste piloto e efetuada a triangulação dos dados obtidos em entrevistas e documentos não sigilosos. Por fim, a partir das análises realizadas, foram elaborados gráficos, quadros e nuvem de palavras, para indicar as principais evidências obtidas a partir das análises dos dados. A elaboração do gráfico e dos quadros empregou o software Micrsosoft Excel. Para elaboração da nuvem de palavras empregou-se o software wordcloud. Os resultados e a discussão dos achados encontram-se no Capítulo 4 deste estudo.

Tabela 3.2: Relação entre objetivos, coleta e análise dos dados

Objetivo Geral	Objetivo Específico	Coleta de Dados	Análise de Dados
Investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre aspectos do metaverso	Identificar as percepções dos gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre o conceito de metaverso	Entrevistas e documentos	Análise documental e de conteúdo
	Verificar as percepções dos referidos gestores sobre os componentes do metaverso	Entrevistas e Documentos	Análise de conteúdo
	Diferenciar as percepções dos gestores considerando as abordagens de metaverso	Entrevistas e Documentos	Análise de conteúdo
	Descrever as percepções dos gestores sobre os principais benefícios e desafios na adoção do metaverso	Entrevistas e Documentos	Análise de conteúdo

Fonte: elaborado pela autora, a partir de dados da pesquisa.

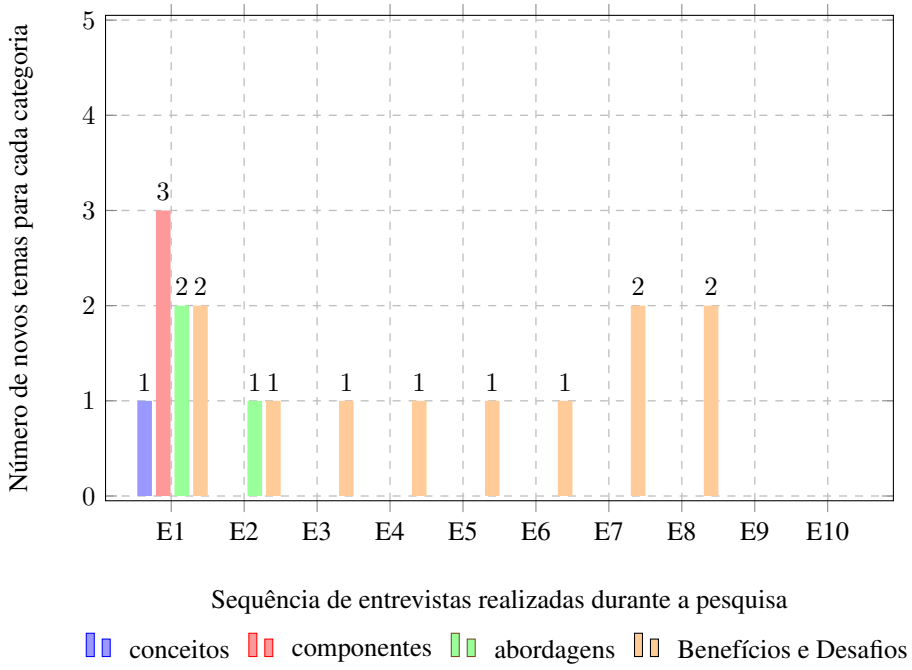
4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Este capítulo discorre sobre os resultados encontrados neste estudo e sobre a discussão deles, considerando o alinhamento com os objetivos propostos neste estudo. Primeiramente, na Seção 4.1 é apresentada a percepção dos gestores de segurança da informação sobre o conceito de metaverso. Na Seção 4.2 ocorre a verificação das percepções dos gestores sobre os componentes do metaverso. Na Seção 4.3 apresenta-se a diferenciação das percepções segundo abordagens de metaverso, e por fim, na Seção 4.4, discorre-se sobre percepções dos principais benefícios e desafios do metaverso.

Dando início aos resultados do estudo, analisa-se o gráfico descrito na Figura 4.1. O gráfico fornecido exibe a dinâmica de saturação das entrevistas (E1 a E10), cujos resultados foram categorizados em "conceito", "componentes", "abordagens"e "benefícios e desafios". Essa segmentação tem a sua sustentação na taxonomia de metaverso apresentada por Park e Kim (4), previamente citada no referencial teórico e na metodologia deste estudo.

Em resumo, a Figura 1 mostra uma profusão inicial de ideias novas nas primeiras entrevistas, que então diminuem em várias entrevistas até que um ressurgimento aconteça antes de um platô final onde a saturação de dados é alcançada, levando-se ao total de dez entrevistas. Enquanto para as categorias ‘Conceito’ e ‘Componentes’ há novidades trazidas na 1ª entrevista, a categoria ‘Abordagem’ apresenta novas informações até a 2ª entrevista. A categoria mais recorrente com novas informações foi "benefícios e desafios", sugerindo que esse aspecto permaneceu em discussão até a 8ª entrevista.

Figura 4.1: Dinâmica de saturação, conforme sequência das entrevistas



Na sequência, serão detalhados os elementos novos e recorrentes que foram identificados para cada categoria na Figura 1, que vão fomentar a argumentação qualitativa e, consequentemente o alcance gradual dos resultados que possibilitarão atingir os objetivos deste estudo.

4.1 PERCEPÇÃO SOBRE O CONCEITO DE METAVERSO

Neste tópico, serão exploradas as percepções dos entrevistados sobre o conceito de metaverso, refletindo de que maneira o metaverso está sendo entendido e interpretado em diferentes contextos. A este respeito, a Tabela 4.1 apresenta a distribuição de declarações sobre o metaverso oriundas das dez entrevistas realizadas com os gestores.

Tabela 4.1: Distribuição dos enunciados referentes a 'Conceito de Metaverso'

Tipos de enunciado	**Entrevistas**										**Total de recorrências**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Conceito de metaverso	**X**	x	x	x	x	x	x	x	x	x	9
Total de novos enunciados para cada entrevista	1	0	0	0	0	0	0	0	0	0	–

Fonte: elaborado pela autora, a partir dos dados da pesquisa. Legenda: 'X' é novo tipo de enunciado; 'x' são recorrências.

A coluna de Total de recorrências, ao final da Tabela 4.1, fornece uma visão global das ocorrências de cada tipo de declaração, permitindo uma análise sobre como o conceito do metaverso se desenvolve e se refina, capturando a evolução de ideias e percepções.

A seguir, são apresentados trechos extraídos das entrevistas que materializam as percepções extraídas e apresentadas na Tabela 4.1 sobre o conceito de metaverso:

> **E01:** Vínculo entre o mundo físico que vivemos com o digital, um mundo virtual onde você consegue ter propriedades, negócios, ligação do ambiente físico com o digital.
> **E05:** Plataforma onde você pode se colocar a partir de avatares e se comunicar com as pessoas, realizar construções e deixar sua marca, com outra cara e nome, mas com uma identidade rastreada.
> **E10:** É a realidade trasposta para o ambiente digital.

Os trechos das entrevistas acima revelam percepções que se alinham com o conceito de metaverso encontrado na revisão da literatura, especialmente conforme descrito por Park e Kim (4). No depoimento do entrevistado E01, observa-se a ênfase no vínculo entre o mundo físico e o digital, apresentando um entendimento do metaverso como um espaço virtual que possibilita a propriedade e a realização de negócios, refletindo o conceito da literatura.

O entrevistado E05 complementa essa visão ao descrever o metaverso como uma plataforma baseada em avatares, na qual a comunicação e a construção de identidade são possíveis. Essa percepção sugere

um reconhecimento da complexidade das interações sociais no ambiente virtual, evidenciando elementos que são consistentes com as definições acadêmicas do conceito, que vincula o conceito ao termo ‘Avatar’, conforme citado no referencial teórico deste estudo.

Por fim, o comentário de E10 destaca a ideia de uma “realidade transposta” para o ambiente digital, um conceito que ressoa com a fundamentação teórica do metaverso, conforme abordado por Park e Kim (2022), citado no referencial teórico deste estudo. Juntos, os relatos dos entrevistados selecionados corroboram para com as definições estabelecidas na literatura por Park e Kim (2022) (4)e enriquecem a compreensão do metaverso como uma extensão da interação humana em um espaço digital. Dando sequência ainda ao entendimento do conceito de metaverso, foi possível elaborar uma nuvem de palavras baseada nas entrevistas, ilustrada na Figura 4.2. Essa figura apresenta os termos mais recorrentes e significativos:

Juntos, os relatos dos entrevistados selecionados corroboram para com as definições estabelecidas na literatura por Park e Kim (4) e enriquecem a compreensão do metaverso como uma extensão da interação humana em um espaço digital.

Dando sequência ainda ao entendimento do conceito de metaverso, foi possível elaborar uma nuvem de palavras baseada nas entrevistas, ilustrada na Figura 4.2. Essa figura apresenta os termos mais recorrentes e significativos:

Figura 4.2: Nuvem de Palavras baseada nas Entrevistas – Conceito de Metaverso

Constata-se a partir da Figura 4.2 a presença de palavras que se relacionam com termos da taxonomia de metaverso proposta por Park e Kim (2022)(4), explicado na revisão de literatura. A seguir estão relacionadas as palavras mais recorrentes.

Inicialmente, a palavra ‘Virtual’, citada na Figura 4.2, é a palavra que aparece com mais frequência (nove vezes), enfatizando a natureza digital do ambiente de metaverso. Em adição, a palavra ‘Ambiente’ tem destaque, aparecendo também nove vezes, refletindo a natureza imersiva e espacial do metaverso

indicando que o foco está na experiência geral dentro do espaço virtual.

É possível ainda identificar na Figura 4.2 a palavra ‘Mundo’ que aparece no total de seis vezes e ‘Digital’, que também aparece 6 vezes. O termo reforça o aspecto digital do ambiente, sugerindo o escopo e a escala desse ambiente virtual, implicando uma experiência completa e imersiva, num ‘mundo digital’.

Para além das palavras previamente destacadas na Figura 4.2 estão palavras que descrevem recursos e funcionalidades, incluindo: 1. ‘Avatar’, previamente citado nesta seção e no referencial teórico, que representa a presença do usuário no mundo virtual, aparecendo quatro vezes na nuvem de palavras; 2. ‘Real’, termo que pode ser vinculado ao realismo nas experiências imersivas, o qual apareceu também 4 vezes.

A nuvem de palavras descreve termos que podem ser vinculados a um ambiente virtual que é imersivo, interativo e potencialmente realista, permitindo que os usuários criem, conectem e experimentem um mundo digital. As escolhas de palavras sugerem um foco na experiência do usuário, interação social, criação e manipulação de um espaço digital.

Em complemento, com base em evidências documentais, verificou-se que conceito de metaverso proposto pela IFP é o conceito descrito por Gartner (2) “Um espaço virtual coletivo, compartilhado, criado através da convergência de melhorias das realidades físicas e digitais”. Por sua vez, as respostas das entrevistas refletem o conceito de metaverso mais focado na experiência do usuário e em suas aplicações. Dessa forma, a percepção dos entrevistados apresenta-se um pouco diferente do conceito apresentado pela IFP, segundo as evidências disponibilizadas.

4.2 VERIFICAÇÃO DAS PERCEPÇÕES DOS GESTORES SOBRE OS COMPONENTES DO METAVERSO

A Tabela 4.2 apresenta a distribuição dos enunciados relacionados aos ’Componentes do metaverso’ com base nas entrevistas realizadas. Os dados são organizados em colunas que representam diferentes entrevistas, com um total de 10 entrevistas consideradas. Para cada tipo de componente - hardware, software e conteúdo - são indicados os novos tipos de enunciados (marcados com ’X’) e as recorrências (marcadas com ’x’).

Tabela 4.2: Distribuição de enunciados referentes a ‘Componentes do metaverso’

Tipos de enunciado	**Entrevistas**										**Total de recorrências**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Componentes de hardware	**X**	x	x	x	x	x	x	x	x	x	9
Componentes de software	**X**	x	x	x	x		x	x	x	x	8
Componentes de conteúdo	**X**	x	x	x	x	x	x	x	x	x	9
Total de novos enunciados para cada entrevista	3	0	0	0	0	0	0	0	0	0	–

Fonte: Elaborado pela autora, a partir dos dados da pesquisa.
Legenda: X – novo enunciado; x – recorrência.
Observação: 1. Park e Kim (2022) (4).

A Tabela 4.2 proporciona uma visão da ênfase dada a cada componente dentro do contexto das entrevistas, refletindo a relevância e a frequência de menções durante as discussões. A análise dos enunciados permite compreender melhor as percepções e as prioridades dos entrevistados em relação ao metaverso. A seguir, serão descritos separadamente os componentes do metaverso que foram identificados nas entrevistas.

Inicialmente, a respeito dos componentes de *hardware*, a Tabela 4.2 mostra que foram identificadas nove ocorrências. Entre os entrevistados, surgiram referências a dispositivos imersivos, como óculos de realidade virtual, que são essenciais para a experiência do metaverso.

Uma evidência do componente de *hardware* foi a menção de um entrevistado que enfatizou: *"(...) soluções de hardware buscam trazer sensibilidade do que acontece no mundo físico no mundo virtual a exemplo de luvas, que dão sensação de toque e óculos virtual que dão sensação de presença"*. Essa afirmação está alinhada com a documentação da instituição financeira, que destaca a necessidade de investimentos em tecnologia avançada para suportar ambientes virtuais ricos e interativos.

Segundo um relatório elaborado em 2022 por uma instituição financeira internacional, e apresentado internamente pela IFP, o metaverso deve atingir o valor de USS 2,5 trilhões em volume transacionado em 2030, corroborando as percepções dos entrevistados.

A respeito dos componentes de software, a Tabela 4.2 indica que foram abordados com oito ocorrências registradas. Os entrevistados frequentemente mencionaram a importância de plataformas que facilitam interações sociais dentro do metaverso. Por exemplo, um dos entrevistados citou: "(...) para que as coisas aconteçam de forma fluida e com alta resolução, você tem que ter um bom “software". Essa declaração encontra respaldo em documentos da instituição financeira que enfatizam a necessidade de soluções de software que integrem funcionalidades colaborativas para atender à dinâmica de trabalho remoto e interação social.

A IFP ressalta em documentos internos que o desenvolvimento de interfaces amigáveis é necessário para o engajamento dos usuários, visto que no Brasil existem aproximadamente 67 milhões de gamers, que juntos com os demais usuários internacionais, somam 40 de toda a população mundial. Isso significa os chamados “metaversers” (potenciais usuários do metaverso), são justamente oriundos da indústria Gamer.

No que diz respeito aos componentes de conteúdo, a Tabela 4.2 mostra oito ocorrências, com um foco na diversidade e na qualidade do conteúdo disponibilizado no metaverso. Um dos entrevistados destacou:

> *"(...) O conteúdo no metaverso tem a ver com o que eu posso criar, se eu tiver num mundo de fantasia que gere comportamentos, posso gerar um conteúdo que faça com que alguém ganhe dinheiro, gerar uma percepção do meu comportamento ou de outras pessoas e vender itens ali. A partir desse novo valor ou de experiencias com outras pessoas ou de uma vitória em um jogo, pode ser criado conteúdos diferentes"*.

A opinião do entrevistado descrita no parágrafo imediatamente anterior está em consonância com a documentação da instituição financeira, a qual cita que o investimento em conteúdos imersivos e ferramentas colaborativas é necessário para atrair usuários e garantir a sustentabilidade de espaços virtuais, inclusive

na própria organização.

4.3 DIFERENCIAÇÃO DAS PERCEPÇÕES SEGUNDO ABORDAGENS DE METAVERSO

A Tabela 4.3 apresenta a distribuição de enunciados relacionados às abordagens do metaverso, categorizados em três tipos: interações com usuários, implementação e aplicação. A tabela mostra a ocorrência de cada tipo de enunciado em dez entrevistas diferentes. A coluna "Total de recorrências"indica o número total de vezes que cada tipo de enunciado apareceu em todas as entrevistas. A legenda esclarece que "X"representa um novo tipo de enunciado e "x"indica recorrências de tipos já mencionados.

Tabela 4.3: Distribuição de enunciados referentes a 'Abordagens do metaverso'

Tipos de enunciado	**Entrevistas**										**Total de recorrências**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Interações com usuários	**X**	x	x	x	x	x	x	x	x	x	9
Implementação		**X**	x	x	x				x	x	5
Aplicação	**X**	x	x	x	x		x	x	x	x	8
Total de novos enunciados para cada entrevista	2	1	0	0	0	0	0	0	0	0	-

Fonte: Elaborado pela autora, a partir dos dados da pesquisa.
Legenda: 'X' é novo tipo de enunciado; 'x' são recorrências

De acordo com a Tabela 4.3, a abordagem 'Interações com usuários' apresenta um total de nove recorrências, indicando discussões sobre como os usuários interagem no metaverso. Durante as entrevistas, um dos participantes destacou: "A interação com os usuários eu achei muito legal, algo como a gamificação, você interage com o avatar juntamente com outros usuários e desafios que tem no game". Outro entrevistado destacou: "O metaverso não é um mundo computacional apenas, é uma interação entre pessoas. Metaverso permite que eu reduza distâncias".

Estes testemunhos são corroborados pela documentação da instituição financeira, que menciona a importância do design centrado no usuário em suas estratégias digitais, reforçando que iniciativas devem ser adaptadas com base nas necessidades e nas interações da clientela. Teoricamente, isso se relaciona ao conceito de "user experience (UX)", que enfatiza a importância da experiência do usuário como um fator determinante na aceitação e no sucesso de plataformas digitais.

Com relação a abordagem 'implementação', refere-se ao processo de traduzir as abordagens e conceitos do metaverso em realidade prática, onde a tabela revela um total de cinco enunciados para essa abordagem. Um participante da entrevista afirmou: "Há uma limitação na implementação do metaverso, que passa por questões de infraestrutura e capacidade tecnológica e cultural". Esse comentário reforça a documentação coletada da IFP, que menciona a necessidade de infraestrutura técnico-administrativa robusta para suportar iniciativas inovadoras no metaverso .

Por fim, a respeito à abordagem "aplicação", destaca-se a utilidade prática das interações e implementações discutidas, com uma totalização de oito enunciados. Durante o processo de entrevistas, um

respondente comentou: “A aplicação será do conteúdo específico para o usuário que está no metaverso”. Outro entrevistado comentou: “Baseado no blockchain, base da segurança, as empresas vão criar aplicações de transações financeiras, negociais, compra e venda”. Essas visões estão alinhadas com evidências presentes na documentação coletada da IFP, que destaca dentre as aplicações no metaverso, a venda de imóveis digitais e os registros cartorários utilizando a tecnologia do blockchain. Essa interconexão sugere que a aplicação efetiva das tecnologias do metaverso pode redefinir as interações no setor financeiro, promovendo uma transformação digital significativa.

4.4 DESCRIÇÃO DAS PERCEPÇÕES DOS GESTORES SOBRE OS PRINCIPAIS BENEFÍCIOS E DESAFIOS DA ADOÇÃO DO METAVERSO

Esta seção apresenta as percepções dos gestores sobre os principais benefícios e desafios do metaverso. Inicialmente, a Tabela 4.4 mostra a distribuição da frequência de enunciados relacionados aos benefícios do metaverso. A tabela registra a ocorrência de cada tipo de enunciado de benefício em cada entrevista, utilizando "X"para indicar um novo tipo de enunciado e "x"para indicar recorrências. A última linha apresenta o total de novos tipos de enunciados por entrevista. A fonte indica que a tabela foi elaborada a partir dos dados da pesquisa, com base no trabalho de Park e Kim (4).

Tabela 4.4: Distribuição de frequência de enunciados referentes a ‘Benefícios do Metaverso’

Tipos de enunciado	**Entrevistas**										**Total de recorrências**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Redução de distância entre usuários	**X**	x	x			x					3
Aumento das oportunidades de negócios				**X**							0
Aumento do engajamento de usuários						**X**					0
Melhoria das simulações de cenários							**X**		x	x	2
Aprimoramento da identificação do usuário								**X**			0
Total de novos enunciados para cada entrevista	1	0	0	1	0	1	1	1	0	0	-

Fonte: Elaborado pela autora, a partir dos dados da pesquisa.
Legenda: ‘X’ é novo tipo de enunciado; ‘x’ são recorrências

Foram identificados cinco benefícios categorizados na Tabela 4.4: 1. “Redução de distância entre usuários”; 2. “Aumento das oportunidades de negócios”; 3. “Aumento do engajamento dos usuários”; 4. “Melhoria das simulações de cenários” e 5. “Aprimoramento da identificação do usuário”.

Com relação ao primeiro benefício citado na Tabela 4.4, intitulado “Redução de distância entre usuários” de forma geral e o metaverso, destacou-se como um benefício recorrente em três entrevistas . Um entrevistado compartilhou o seguinte:

“A proximidade com os clientes é intensificada por meio de avatares inteligentes que representam os gerentes, proporcionando calor humano e interação próxima que nenhuma máquina isolada consegue oferecer, complementando os demais canais de distribuição da empresa".

Em adição, o benefício citado no parágrafo anterior é apoiado por um relatório da instituição financeira que relata que a adoção no metaverso por grandes instituições financeiras traz dentre vários benefícios a valorização da experiência dos usuários de produtos e serviços por meio digital, sobretudo os mais jovens.

A respeito do segundo benefício do metaverso citado na Tabela 4.4, intitulado “”aumento das oportunidades de negócio”, um entrevistado informou o seguinte: "(...) Como é algo novo, tem oportunidades de negócio ou algo mais específico”. Este benefício é apoiado por um relatório da instituição financeira que menciona até 2030 o potencial de negócio que a adoção no metaverso poderá proporcionar chegará ao montante de 13 trilhões de dólares, principalmente com a criação de ativos digitais. Este benefício está alinhado com a crescente importância do comércio eletrônico e da economia digital, que dependem de plataformas que facilitam as transações e conexões a distância.

Com relação ao terceiro benefício “Aumento do engajamento de usuários” consta da Tabela 4.4 como citado em uma entrevista. A este respeito, um entrevistado mencionou “(...) Para mim, um benefício é atingir o público jovem. Aqui na organização, que quer atingir esse público, creio que seja atingido”. A experiência imersiva do metaverso pode criar um maior nível de envolvimento dos usuários, resultando em interações mais significativas e duradouras.

As evidências citadas no parágrafo anterior são corroboradas por um estudo realizado pela IFP, que mencionou que a confiança dos consumidores na tecnologia está crescendo globalmente. Mais 75 dos participantes da pesquisa afirmaram que sua vida depende da tecnologia, percentual que aumenta para 79 quando consideramos apenas o público da Geração Z (até 24 anos) e para 80 entre os Millenials (25 a 41 anos).

Quanto ao quarto benefício, intitulado ‘melhoria da simulação de cenários’, observou-se duas menções na Tabela 4.4, destacando-se a capacidade do metaverso de criar e simular cenários diversos, para fins de treinamento, planejamento ou teste de produtos/serviços. Instituições financeiras poderiam utilizar o metaverso para simular situações de mercado e testar estratégias de investimento, antes de sua implementação no mundo real.

Ainda a respeito do quarto benefício, durante a entrevista um entrevistado mencionou: “O metaverso pode ser usado para fazer simulações do mundo real sem efetivamente correr riscos”. Tal afirmação condiz com o que foi mencionado em documentos coletados contendo estudos realizados pela IFP, citando grandes instituições adotando o metaverso como experimentos em ambientes virtuais.

Quanto ao quinto benefício, intitulado “Aprimoramento da identificação do usuário”, observou-se uma menção a este benefício na Tabela 4.4. Durante a entrevista, um entrevistado mencionou: “Em relação ao aprimoramento da cadeia de identidade, o metaverso vai fomentar como o cartório eletrônico e vai beneficiar as empresas”. Essa afirmativa é corroborada com estudos realizados pela instituição que cita como benefício da adoção do metaverso sua utilização em imóveis virtuais, inclusive pela integração com a tecnologia do blockchain.

Dando sequência às análises, a Tabela 4.5 apresenta a distribuição de frequência de diferentes tipos de

enunciados relacionados aos desafios do metaverso. Cada linha representa um desafio e indica em quais entrevistas (colunas numeradas de 1 a 10) esse desafio foi mencionado (marcado com "X"). A última coluna mostra o total de vezes que cada desafio foi citado nas entrevistas.

Tabela 4.5: Distribuição de frequência de enunciados referentes a 'Desafios do Metaverso'

Tipos de enunciado	**Entrevistas**										**Total de recorrências**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Melhoria da evolução do hardware	**X**										0
Limitação tecnológica		**X**									0
Integração do fator humano na prestação de serviços			**X**								0
Redução do engajamento de usuários				**X**					x	x	2
Ausência de regulamentação					**X**	x					1
Dificuldade para capacitação							**X**				0
Resistência cultural								**X**			0
Total de novos enunciados para cada entrevista	1	1	1	1	1	0	1	1	0	0	-

Fonte: Elaborado pela autora, a partir dos dados da pesquisa.
Legenda: 'X' é novo tipo de enunciado; 'x' são recorrências

Foram identificados sete desafios categorizados na Tabela 4.4: 1. "Melhoria da evolução do hardware"; 2. "Limitação tecnológica"; 3. "Integração do fator humano na prestação de serviços"; 4. "Redução do engajamento de usuários"; 5. "Ausência de regulamentação"; 6. "Dificuldade para capacitação de pessoas" e 7. "Resistência cultural".

Sobre o primeiro desafio do metaverso citado na Tabela 4.5, intitulado "Melhoria da evolução do hardware", um entrevistado mencionou o seguinte: "(...) é preciso haver evolução dos hardwares, senão fica parecendo como jogos simples, precisam ter vestimentas que permitem sensações, óculos de realidade virtual (...)". Em adição, exame de evidências documentais coletadas na IFP parecem reforçar o argumento do entrevistado, com relatórios de pesquisa sobre tendências tecnológicas, indicando a importância da inovação em hardware como um fator para o sucesso do metaverso. Em complemento, a literatura deste estudo, em especial a taxonomia do metaverso baseada em Park e Kim (4), ressalta os componentes de hardware entre os componentes do metaverso.

O segundo desafio do metaverso citado na Tabela 4.5 foi "Limitação tecnológica". A este respeito, um participante afirmou que "(...) há uma limitação tecnológica, talvez a ideia do metaverso ainda não esteja madura."Baseado no relato desse entrevistado, o metaverso apresenta complexidade para sua operacionalização e implementação. Adicionalmente, a coleta de documentos da IFP indicou a importância do poder computacional, ou seja, a habilitação e fornecimento de poder de processamento computacional para suporte a diversas funções do metaverso como processamento de gráficos, dados e inteligência artificial. Assim, as evidências citadas neste parágrafo reforçam a limitação tecnológica como um desafio para a implementação do metaverso.

O terceiro desafio do metaverso identificado na Tabela 4.5 foi "A integração do fator humano na prestação de serviços'. A este respeito, um entrevistado mencionou que "(...) é um desafio fazer a inteligência

ser capaz de suprir um ser humano". Esta percepção destaca a importância do fator humano, mesmo em ambientes virtuais. Documentos da instituição financeira que tratam sobre a importância da experiência do cliente reforçam a necessidade de manter elementos humanizados nas interações digitais.

O quarto desafio citado na Tabela 4.5 foi “Redução do engajamento dos usuários”. A este respeito, um entrevistado destacou que “(...) é um desafio o engajamento pois nem sempre todo mundo tem tempo para coisas novas. Tem que ser algo que tenha proposito muito forte para ter engajamento (...)". Em adição, foi possível consultar relatórios da IFP quantificando taxas de engajamento em plataformas digitais após lançamento de estratégias digitais para público jovem que contribuíram para corroborar a afirmação do entrevistado, e de certa maneira evidenciando a importância de estratégias para manter o envolvimento do engajamento de usuários.

O quinto desafio presente na Tabela 4.5 é “Ausência de regulamentação”, o qual foi mencionado por um entrevistado, conforme segue: "(...) por ser totalmente novo, não sabe como vai funcionar a segurança, a parte de regulamentação. O regulamento é o principal desafio (...)". A IFP oferece dados sobre o estado atual das políticas de regulamentação, que não evidenciam normas específicas sobre metaverso e indicam a oportunidade de poder avançar em uma estrutura regulatória a respeito do tema, em especial para contribuir para o fomento seguro dessa tecnologia. De acordo com o BIS, o metaverso será a força disruptiva no setor financeiro, mas precisa ser regulado.

O sexto desafio do metaverso citado na Tabela 4.5 foi a “Dificuldade de capacitação’. A este respeito, um entrevistado enfatizou que "(...) é um desafio capacitar pessoas para atuar no metaverso, ter pessoas capacitadas e interessadas nas pesquisas sobre o tema (...)”. Essa preocupação é apoiada por pesquisas da instituição financeira que discutem a formação profissional e as lacunas existentes no mercado de trabalho.

O sétimo e último desafio identificado do metaverso na Tabela 4.5 foi “Resistência cultural’. Sobre esse assunto, um participante afirmou o seguinte: "(...) outro desafio será o cultural, das pessoas lidar com esse universo paralelo ao seu mundo real (...)". Documentos da instituição financeira fornecem o contexto sobre a aceitação cultural da tecnologia em diferentes demografias. Segundo Park e Kim (4), o fator cultural pode influenciar a aceitação e integração do metaverso e outras tecnologias na sociedade.

Em síntese, o metaverso oferece uma gama de benefícios, sendo cinco deles identificados neste estudo. Contudo, os sete desafios destacados revelam pontos de atenção a serem superados para implementação do metaverso. As entrevistas indicam uma necessidade de inovação em hardware e um maior foco em fator humano nas interações. A superação desses desafios poderá abranger um esforço técnico da IFP, mas também identificado que aprimoramentos regulatórios poderão contribuir para materializar plenamente os potenciais do metaverso.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo geral investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública brasileira sobre aspectos do metaverso.

A pesquisa, de natureza descritiva, seguiu uma abordagem qualitativa fundamentada na coleta de entrevistas e documentos e análise dos dados por meio de documental e análise de conteúdo, considerando a taxonomia do metaverso proposta por Park e Kim (4) e pontuada por elementos adicionais da revisão de literatura que realçaram benefícios e desafios do metaverso.

O alcance do objetivo geral deu-se por meio de quatro objetivos específicos a ele vinculados. O primeiro objetivo específico foi identificar as percepções dos gestores da área de segurança da informação de uma instituição financeira pública sobre o conceito de metaverso. Efetuou-se análise das entrevistas realizadas sobre este tópico, conforme citado na Seção 4.1 deste estudo. Na análise dos enunciados sobre o "Conceito de metaverso", os dados coletados revelam a compreensão do metaverso como uma extensão da interação humana em um espaço digital, focada na experiência do usuário e nas aplicações. A partir da Figura 3 contendo nuvem de palavras, constatou-se, também, a presença de termos da taxonomia de metaverso citada na literatura, baseada em Park e Kim (4). Em complemento, a percepção sobre o conceito de metaverso foi diferente do conceito apresentado pela IFP, segundo as evidências disponibilizadas nesta pesquisa.

O segundo objetivo enfatizou a verificação das percepções dos referidos gestores sobre os componentes do metaverso. Os resultados do objetivo específico estão detalhados na Seção 4.2 deste trabalho. A análise das percepções dos gestores sobre os componentes do metaverso, conforme apresentado na Tabela 2, revela a predominância dos componentes de hardware, software e conteúdo, com nove, oito e oito recorrências, respectivamente.

Em seguida, o terceiro objetivo buscou diferenciar as percepções dos gestores considerando as abordagens de metaverso. A análise das percepções sobre as abordagens do metaverso, apresentada no item na Tabela 3 do item 4.3 revela que a categoria interação com os usuários apresentou nove ocorrências. Por sua vez, a categoria implementação apresentou cinco ocorrências e aplicação, oito.

O quarto e último objetivo buscou descrever as percepções dos gestores sobre os principais benefícios e desafios na adoção do metaverso. A análise das percepções dos gestores sobre os benefícios e desafios da adoção do metaverso, conforme apresentado nas Tabelas 4 e 5, evidencia tanto as oportunidades quanto as barreiras enfrentadas pelas organizações. Entre os benefícios, a redução da distância entre usuários foi frequentemente mencionada, revelando como avatares inteligentes podem melhorar a interação e atender às expectativas dos consumidores modernos.

Em síntese, o metaverso oferece uma gama de benefícios, sendo cinco deles identificados neste estudo. Contudo, os sete desafios destacados revelam pontos de atenção a serem superados para implementação do metaverso. As entrevistas indicam uma necessidade de inovação em hardware e um maior foco no fator humano nas interações. A superação desses desafios poderá abranger um esforço técnico da IFP, mas também identificou-se que aprimoramentos regulatórios poderão contribuir para materializar plenamente

os potenciais do metaverso.

O alcance dos quatro objetivos específicos possibilitou atingir o objetivo geral e responder o problema de pesquisa. Os aspectos do metaverso percebidos por gestores de segurança da informação da IFP brasileira abrangeram o conceito de metaverso vinculado a uma extensão da interação humana em um espaço digital, focado na experiência do usuário e nas aplicações. Ressaltaram-se os componentes do metaverso abrangendo hardware, software e conteúdo. As abordagens do metaverso evidenciaram a interação com os usuários, a implementação e as aplicações. Em complemento, foram identificados cinco benefícios e sete desafios relacionados ao metaverso.

Os achados sublinham a importância de uma estratégia bem estruturada para a adoção do metaverso, que considere tanto os benefícios quanto os desafios identificados. À medida que a IFP busca se adaptar e inovar em um ambiente digital em constante evolução, a compreensão aprofundada dessas percepções permitirá a formulação de iniciativas que promovam a integração bem-sucedida do metaverso em suas operações, assegurando assim sua relevância e competitividade no mercado.

Este estudo não apenas atingiu seus objetivos propostos, mas também abriu caminhos para aprofundar o entendimento e a percepção do metaverso perante os gestores de segurança da informação da IFP, contribuindo para reflexões sobre o metaverso, seus benefícios e especialmente seus desafios. Como contribuições para enfrentar tais desafios, o estudo permite propor recomendações para a IFP, conforme segue:

1. Investimento em Tecnologia Imersiva: priorizar investimentos em hardware para a criação de ambientes virtuais mais interativos, buscando engajamento do usuário;
2. Desenvolvimento de Software Centrado no Usuário: criar ou aprimorar plataformas que sigam os princípios de design centrado no usuário, focando na usabilidade e acessibilidade;
3. Programas de Capacitação e Treinamento: implementar programas de capacitação contínua para funcionários, focando no uso e na gestão de tecnologias do metaverso;
4. Criação de Ambientes Virtuais de Networking: projetar e lançar ambientes virtuais onde clientes e potenciais investidores possam interagir, participar de eventos e realizar networking;
5. Estratégias Voltadas para o Metaverso: desenvolver campanhas inovadoras que utilizem o metaverso para engajar usuários. Isso pode incluir eventos virtuais, promoções e jogos que incentivem a participação dos clientes;
6. Pesquisa e Desenvolvimento Contínuos: estabelecer uma equipe dedicada à pesquisa e desenvolvimento de novas aplicações e serviços no metaverso;
7. Discussão sobre Regulamentação: participar ativamente de fóruns e grupos de trabalho que discutam a regulamentação do metaverso e das tecnologias associadas;
8. Promoção da Inclusão Digital: criar iniciativas que ajudem a superar as barreiras tecnológicas e culturais, promovendo a inclusão digital;
9. Monitoramento e Avaliação: implementar métricas para monitorar e avaliar o impacto das soluções implementadas no metaverso, garantindo um ciclo contínuo de feedback e melhoria;

10. Colaboração com Startups e Inovadores: estabelecer parcerias com startups e empresas inovadoras do setor de tecnologia, permitindo a troca de conhecimento e o desenvolvimento conjunto de novas soluções no metaverso.

Este trabalho busca contribuir para enriquecer a literatura sobre o metaverso, em especial com pesquisas sobre a percepção de gestores de segurança da informação sobre essa tecnologia. O estudo pode contribuir, também, para a formulação de estratégias na adoção do metaverso por instituições financeiras públicas no Brasil. É adequado citar, entre as delimitações desta pesquisa, que existiram aspectos fora do controle da autora, como o tempo decorrido para realização da coleta de dados que dependeu, também, da disponibilidade dos entrevistados.

Adicionalmente, levando em conta as formalidades requeridas para pedir autorização para a coleta de dados na IFP, optou-se por não citar o nome da referida instituição financeira nas análises, fazendo a remissão a ela, quando necessária, por meio da referida sigla de três letras. Em complemento, é adequado lembrar que as conclusões deste estudo consideram os dados que foram coletados, e por se tratar de uma pesquisa cujo lócus abrangeu uma IFP específica, deve-se ter cautela no tocante a generalizações. Todos os argumentos citados neste e no parágrafo anterior, contudo, não limitaram o atingimento do objetivo geral proposto neste estudo.

Por fim, é adequado informar que os achados deste estudo, também, podem fornecer subsídios para auxiliar a formulação de outras pesquisas. Podem ser consideradas como sugestões para estudos futuros, inclusive abrangendo a percepção de gestores de outras instituições financeiras, sejam elas públicas ou privadas, os seguintes pontos:

1. Impacto do Metaverso na Experiência do Cliente: realizar um estudo aprofundado sobre como a experiência do cliente nas plataformas do metaverso se compara às interações tradicionais. A pesquisa pode incluir a análise de satisfação, engajamento e chances de retenção de clientes;
2. Abordagens de Segurança da Informação no Metaverso: investigar as práticas de segurança e privacidade necessárias para proteger dados sensíveis em ambientes de metaverso, bem como seus riscos envolvidos, especialmente devido à natureza transacional do setor financeiro;
3. Avaliação da Acessibilidade e Inclusão Digital: examinar a acessibilidade das plataformas de metaverso para diferentes demografias, incluindo populações com deficiências e idosos, e propor soluções para tornar esses ambientes mais inclusivos;
4. Efeitos das Tecnologias de Blockchain no Metaverso: analisar como a tecnologia blockchain pode ser integrada ao metaverso para transações financeiras, segurança e rastreamento de ativos digitais, e quais implicações isso pode ter para a regulamentação e a confiabilidade;
5. Percepção Cultural do Metaverso: realizar estudos que explorem como diferentes culturas percebem e interagem com o metaverso, e como essas percepções moldam a adoção e a implementação dessa tecnologia em setores financeiros em diversas regiões geográficas;
6. Gamificação e Engajamento: investigar como elementos de gamificação podem ser utilizados em plataformas do metaverso para aumentar o engajamento dos usuários e melhorar a educação financeira;

7. Tendências de Inovação no Setor Financeiro: estudar as inovações emergentes relacionadas ao metaverso e seu impacto no setor financeiro, como novas formas de ativos, serviços financeiros e plataformas de investimento;

8. Estratégias de Marketing no Metaverso: analisar a eficácia de diferentes estratégias de marketing no metaverso e como essas abordagens podem influenciar as decisões dos consumidores em relação a produtos e serviços financeiros;

9. Ética e Sustentabilidade no Metaverso: explorar as questões éticas relacionadas ao uso do metaverso em finanças, incluindo impactos ambientais, práticas de negócios sustentáveis e responsabilidade social corporativa;

10. Modelos de Negócio Emergentes: investigar como os modelos de negócio nas instituições financeiras estão evoluindo com a adoção do metaverso e quais novas oportunidades de receita estão surgindo.

11. Regulação e Metaverso: estudar as iniciativas sobre regulação do metaverso passíveis de serem exploradas no setor financeiro, em diferentes jurisdições.

REFERÊNCIAS BIBLIOGRÁFICAS

1 HUANG, Y.; LI, Y. J.; CAI, Z. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, TUP, v. 6, n. 2, p. 234–247, 2023.

2 GLOBAL, G. G. C. *O que é um Metaverso?* 2023. <https://www.gartner.com.br/pt-br/artigos/o-que-e-um-metaverso>. Acesso em: 5 abr. 2023.

3 VADLAMUDI, S. A taxonomy for classifying threats and countermeasures in the metaverse. *Journal of Cybersecurity Research*, v. 15, n. 4, p. 345–362, 2022. Acesso em: 21 fev. 2024.

4 PARK, S. M.; KIM, Y. G. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, v. 10, p. 4209–4251, 2022.

5 CABRAL, B. S.; ALVES, C. A. d. M. Metaverso e segurança: análise de artigos publicados em bases acadêmicas de 2018 a 2023. *Caderno Pedagógico*, v. 21, n. 7, p. e6064, 2024. Acesso em: 21 fev. 2024.

6 NING, e. a. A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal*, v. 10, n. 16, p. 14671–14688, 2023.

7 PIETRO, R. D.; CRESCI, S. Desafios de segurança e privacidade no metaverso: uma análise abrangente. *Revista de Estudos de Segurança Digital*, v. 15, n. 2, p. 98–115, 2021. Acesso em: 21 fev. 2024.

8 HUANG, Y.; LI, Y. J.; CAI, Z. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, v. 6, n. 2, p. 234–247, 2023.

9 WANG, Y. e. a. A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 2023.

10 RITTERBUSCH, G. D.; TEICHMANN, M. R. Defining the metaverse: A systematic literature review. *IEEE Access*, v. 11, p. 12368–12377, 2023.

11 RYU, J.; KIM, H.; LEE, S.; PARK, J. An analysis of privacy and security challenges in the metaverse. *International Journal of Cybersecurity and Digital Forensics*, v. 12, n. 2, p. 45–62, 2022. Acesso em: 21 fev. 2024.

12 CHEN, B.; ZHU, X. Integrating generative ai in knowledge building. *Computers and Education: Artificial Intelligence*, v. 5, p. 100184, 11 2023.

13 LI, K. e. a. When internet of things meets metaverse: Convergence of physical and cyber worlds. *IEEE Internet of Things Journal*, v. 10, p. 4148–4173, Aug 2022.

14 FALCHUK, B.; LOEB, S.; NEFF, R. The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, v. 37, n. 2, p. 52–61, 2018.

15 KANG, J.; KOO, Y.; KIM, H. Security and privacy challenges in the metaverse: A review of current trends and future directions. *Journal of Cybersecurity Research*, v. 19, n. 4, p. 215–232, 2022. Acesso em: 21 fev. 2024.

16 SEREC, F. E. *Metaverso: Aspectos Jurídicos*. [S.l.: s.n.], 2023.

17 HUGGETT, M. Separação entre a realidade presente e a realidade virtual da herança virtual: estudo da existência e do realismo na realidade virtual. 2020.

18 SKARBEZ, R.; SMITH, M.; WHITTON, M. C. Revisiting milgram and kishino's reality-virtuality continuum. *Frontiers in Virtual Reality*, Frontiers Media SA, v. 2, p. 647997, 2021.

19 WHITMAN, M. E.; MATTORD, H. J. *Principles of information security*. [S.l.]: Cengage Learning, 2018.

20 TÉCNICAS, A. B. D. N. *ABNT NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos*. 2022. Rio de Janeiro.

21 STALLINGS, W.; BROWN, L. *Computer security: Principles and practice*. 3rd. ed. [S.l.]: Pearson, 2014.

22 STANDARDS, N. I. O.; TECHNOLOGY. *Security and Privacy Controls for Federal Information Systems and Organizations*. 2023. NIST Special Publication 800-53, Revision 5.1.1. Gaithersburg, MD.

23 European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

24 California Consumer Privacy Act. *California Consumer Privacy Act (CCPA)*. 2018. Aprovado em 28 de junho de 2018 e em vigor a partir de 1º de janeiro de 2020. Disponível em: <https://oag.ca.gov/privacy/ccpa>.

25 AL-KFAR, A.; SMITH, J.; JOHNSON, R. Innovations in data privacy protection. *Journal of Cybersecurity*, v. 15, n. 3, p. 45–67, 2023. Acesso em: 21 fev. 2024.

26 JO, H.; PARK, S. Analysis of data protection measures in cloud computing. *Journal of Information Security*, v. 18, n. 4, p. 567–580, 2022. Acesso em: 21 fev. 2024.

27 ZHANG, L.; LIU, Y.; WANG, X. Advances in machine learning techniques for cybersecurity. *Journal of Computer Security*, v. 28, n. 5, p. 123–145, 2020. Acesso em: 21 fev. 2024.

28 SHARMA, A.; ZAMFIROIU, C. Cybersecurity threats and vulnerabilities in the metaverse: Proactive measures for risk mitigation. *Journal of Digital Security*, v. 20, n. 2, p. 123–137, 2023. Acesso em: 21 fev. 2024.

29 SHEHHI, A. A.; OTOUM, S. Zero trust architecture: Enhancing security in the metaverse. *Journal of Network Security*, v. 35, n. 1, p. 45–60, 2023. Acesso em: 21 fev. 2024.

30 WU, Z. e. a. Cybersecurity in the financial sector: A systematic review of threats and solutions. *Journal of Information Security and Applications*, v. 65, p. 103017, 2022.

31 RAJAWAT, A. S.; GOYAL, S.; BEDI, P.; JAN, T.; WHAIDUZZAMAN, M.; PRASAD, M. Quantum machine learning for security assessment in the internet of medical things (iomt). *Future Internet*, MDPI, v. 15, n. 8, p. 271, 2023.

32 BOARD, F. S. *Global financial stability report: Addressing vulnerabilities in international financial systems*. 2023. Disponível em: <https://www.fsb.org/2023-report>. Acesso em: 21 fev. 2024.

33 Comitê da Basileia de Supervisão Bancária. *Comitê da Basileia de Supervisão Bancária*. n.d. Informações e publicações relacionadas a padrões de supervisão bancária. Disponível em: <https://www.bis.org/bcbs/>.

34 CYBERSECURITY, E. U. A. for. *ENISA - European Union Agency for Cybersecurity*. <https://www.enisa.europa.eu>. Acesso em: 20 jan. 2025.

35 NACIONAL, C. M. *Resolução nº X de 2022: Dispõe sobre...* 2022. <https://www.bcb.gov.br>. Acesso em: 20 abr. 2025.

36 BRASIL, B. C. do. *Banco Central do Brasil*. <https://www.bcb.gov.br>. Acesso em: 20 jan. 2025.

37 SETTLEMENTS, B. for I. *Bank for International Settlements*. <https://www.bis.org>. Acesso em: 20 jan. 2025.

38 SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. *Metodologia de pesquisa*. 5ª. ed. [S.l.]: Penso, 2013.

39 GIL, A. C. Como elaborar projetos de pesquisa. 12. reimpr. *São Paulo: Atlas*, v. 6, n. 1-1, 2009.

40 ALEXANDRE, N. M. C.; COLUCI, M. Z. O. Validade de conteúdo nos processos de construção e adaptação de instrumentos de medidas. *Ciência & Saúde Coletiva*, v. 16, n. 7, p. 3061–3068, 2011. Acesso em: 21 fev. 2024.

41 FONTANELLA, B. J. B.; LUCHESI, B. M.; SAIDEL, M. G. B.; RICAS, J.; TURATO, E. R.; MELO, D. G. Amostragem em pesquisas qualitativas: proposta de procedimentos para constatar saturação teórica. *Cadernos de Saúde Pública*, v. 27, n. 2, p. 388–394, 2011.

42 BARDIN, L. *Análise de conteúdo*. [S.l.]: Edições 70, 1977.

APÊNDICES

I. APÊNDICE A: E-MAIL DE AUTORIZAÇÃO PARA COLETA DE DADOS

Enviado em:
Assunto: Pedido de Autorização para Realização de Coleta de Dados

Trata-se de demanda que visa a autorização da chefia máxima da Unidade de Segurança Digital e da Informação do [redacted] para que haja acesso a dados com a finalidade de subsidiar a realização de pesquisa acadêmica de pós-graduação.

A pleiteante é aluna do Mestrado Profissional em Engenharia Elétrica da Universidade de Brasília – UnB. A dissertação que está em desenvolvimento na referida universidade, conta com a orientação do Prof. Dr. Carlos André de Melo Alves.

Objetiva-se, com a pesquisa, investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública sobre aspectos do metaverso. Para se atingir o objetivo proposto, estão previstas, inicialmente, consultas a documentação interna (de natureza não sigilosa) e a realização de entrevistas. Os dados coletados serão analisados para subsidiar a Dissertação de Mestrado desta signatária.

Nestes termos, na condição de pesquisadora da UnB e considerando a necessidade de obter o contato com gestores que atuam na Unidade de Segurança Digital e da Informação, pede- se deferimento, inclusive, para o contato com esses servidores para formalizar convites para as entrevistas.

Ressalte-se, por fim, que a coleta de dados atenderá aos critérios estabelecidos no Ofício Circular no 2/2021/CONEP/SECNS/MS, de 24 de fevereiro de 2021, que dá orientações para a realização de procedimentos de pesquisas em qualquer etapa no ambiente virtual. Em complemento, a pleiteante atenderá aos preceitos éticos, assumindo total responsabilidade pelas informações coletadas.

Destaca-se, também, que esses dados serão utilizados para fins acadêmicos, resguardando-se o sigilo das informações e o anonimato dos servidores que aceitarem ser entrevistados.

Respeitosamente,

Barbara Silva Cabral
Mestrando em Engenharia Elétrica pela Universidade de Brasília
(PPEE/UnB)

Barbara Silva Cabral
Mestranda em Engenharia Elétrica – PPEE/UnB
E-mail:
Telefone:

II. APÊNDICE B: ROTEIRO/FORMULÁRIO DE ENTREVISTAS APLICADO

1 - De acordo com sua percepção, o que significa metaverso?

2 - Em sua opinião, comente sobre os principais componentes do metaverso (ex: hardware, software e conteúdo).

3 - Em sua opinião, comente sobre as principais abordagens do metaverso (ex: interações com usuários, implementações e aplicações).

4 - Em sua opinião, quais são os principais benefícios e desafios da adoção do metaverso?

5 - Você teria alguma consideração/comentário adicional a fazer?

6 - Grau de escolaridade:

- ○ Nível Médio Completo
- ○ Nível Superior Incompleto
- ○ Nível Superior Completo
- ○ Pós-Graduação (Especialização, Mestrado, Doutorado, Pós-doutorado) Incompleta
- ○ Pós-Graduação (Especialização, Mestrado, Doutorado, Pós-doutorado) Completa

7 - Há quanto tempo atua na instituição?

- ○ Até 3 anos
- ○ Mais de 3 até 6 anos
- ○ Mais de 6 até 9 anos
- ○ Mais de 9 até 12 anos
- ○ Mais de 12 anos

8 - Você tem quanto tempo de serviço na área de Segurança da Informação?

- Até 3 anos
- Mais de 3 até 6 anos
- Mais de 6 até 9 anos
- Mais de 9 até 12 anos
- Mais de 12 anos

III. APÊNDICE C: SOLICITAÇÃO DE PARTICIPAÇÃO EM ENTREVISTA INDIVIDUAL

Prezado(a),

Meu nome é Bárbara Silva Cabral, sou Analista de segurança e estou desenvolvendo uma dissertação no âmbito do Mestrado Profissional Segurança Cibernética do Programa de Pós-Graduação em Engenharia Elétrica da Universidade de Brasília (PPEE/UnB), sob a orientação do Prof. Dr. Carlos André de Melo Alves.

Desse modo, na condição de pesquisadora da UnB, venho por meio do presente solicitar seu auxílio e participação em pesquisa, por meio de uma entrevista, conforme horário de sua disponibilidade. O objetivo do estudo é investigar a percepção de gestores da área de segurança da informação de uma instituição financeira pública sobre aspectos do metaverso.

A coleta de dados atenderá aos critérios estabelecidos no OFÍCIO CIRCULAR Nº 2/2021/CONEP/ SECNS /MS, de 24 de fevereiro de 2021, que dá orientações para a realização de procedimentos éticos em pesquisas que envolvam contato através do ambiente virtual. Ressalto que o anonimato do (a) entrevistado (a) será preservado. O estudo é de cunho exclusivamente acadêmico.

Caso haja dúvida ou necessite de algum esclarecimento, entre em contato no e-mail: [redacted]

Agradeço se puder responder esse convite em até 5 dias corridos.

Atenciosamente,

Bárbara Silva Cabral