CIBERSEGURANÇA EM UM MUNDO HIPERCONECTADO: DESAFIOS E ESTRATÉGIAS DE PROTEÇÃO

CYBERSECURITY IN A HYPERCONNECTED WORLD: CHALLENGES AND PROTECTION STRATEGIES

Elias Leandro de Lima Júnior
MUST University, Estados Unidos

Jackeline Ferreira e Silva Cardoso
MUST University, Estados Unidos

Halfh Matheus dos Santos Ribeiro
Fundação Universidade Federal de Mato Grosso do Sul, Brasil

Márcio Kusunoki
MUST University, Estados Unidos

Sonaí Maria da Silva
Universidad Leonardo da Vinci, Paraguai

ISSN: 2594-9950 DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

Resumo: A crescente interconexão das tecnologias da informação e comunicação gera um aumento exponencial na dinâmica das interações globais, expondo indivíduos e organizações a riscos cibernéticos sem precedentes. Nesse contexto, a cibersegurança emerge como elemento fundamental para a proteção de ativos digitais, informações sensíveis e a integridade de sistemas críticos. Este estudo justifica a escolha do tema ao revelar os desafios impostos por essa hiperconectividade, como a sofisticação das ameaças, a vulnerabilidade das infraestruturas e a escassez de habilidades especializadas. O objetivo principal é analisar a complexidade das interações entre usuários, dispositivos e redes, destacando a necessidade de estratégias de defesa mais holísticas. A metodologia utilizada inclui uma abordagem bibliográfica, com a revisão de literatura pertinente sobre cibersegurança e suas práticas. Os principais resultados mostram que cada novo ponto de conexão potencializa vetores de ataques, revelando a urgência de proteções efetivas. As conclusões mais relevantes indicam que a implementação de uma arquitetura de segurança baseada em camadas, o investimento em tecnologias emergentes como inteligência artificial e *machine learning* para a detecção de intrusões, e a promoção de uma cultura de conscientização cibernética são essenciais. Este trabalho propõe um chamado à ação, enfatizando a premente necessidade de investir em cibersegurança como componente estratégico da resiliência organizacional em um mundo cada vez mais interconectado. A adoção de uma visão proativa e integrada é imprescindível para mitigar riscos e reforçar a confiança nas infraestruturas digitais.

Palavras-chave: Cibersegurança; Interconexão; Estratégias de Defesa.

Revista Missioneira | Santo Ângelo | v. 27 | n. 1 | p. 149-159 | 2025
DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

Abstract: The growing interconnection of information and communication technologies generates an exponential increase in the dynamics of global interactions, exposing individuals and organizations to unprecedented cyber risks. In this context, cybersecurity emerges as a fundamental element for the protection of digital assets, sensitive information, and the integrity of critical systems. This study justifies the choice of the topic by revealing the challenges imposed by this hyperconnectivity, such as the sophistication of threats, the vulnerability of infrastructures, and the scarcity of specialized skills. The main objective is to analyze the complexity of interactions between users, devices, and networks, highlighting the need for more holistic defense strategies. The methodology used includes a bibliographic approach, with a review of relevant literature on cybersecurity and its practices. The main results show that each new connection point enhances attack vectors, revealing the urgency of effective protections. The most relevant conclusions indicate that the implementation of a layered security architecture, investment in emerging technologies such as artificial intelligence and machine learning for intrusion detection, and the promotion of a culture of cyber awareness are essential. This paper proposes a call to action, emphasizing the pressing need to invest in cybersecurity as a strategic component of organizational resilience in an increasingly interconnected world. Adopting a proactive and integrated vision is essential to mitigate risks and reinforce trust in digital infrastructures.

Keywords: Cybersecurity; Interconnection; Defense Strategies.

Introdução

A cibersegurança, no contexto contemporâneo, representa um tema de extrema importância, especialmente em um mundo cada vez mais interconectado e digitalizado. O avanço das tecnologias da informação e comunicação transforma a maneira como os indivíduos, as empresas e os governos operam, facilitando a troca de dados, mas, ao mesmo tempo, expondo-os a riscos significativos. A ascensão de dispositivos conectados, como *smartphones*, a Internet das Coisas (IoT) e as redes sociais, resulta em um ecossistema onde vulnerabilidades se multiplicam. Dessa forma, a cibersegurança não é apenas uma questão técnica, mas sim um componente essencial das estratégias organizacionais e da segurança nacional.

Recentes nos desafios da cibersegurança merecem uma análise aprofundada. O aumento do número de ataques cibernéticos, que variam desde fraudes digitais até invasões coordenadas por grupos de cibercriminosos, evidencia a necessidade de uma abordagem proativa na proteção de ativos digitais. Além disso, as falhas de segurança, frequentemente decorrentes de negligência humana, ressaltam a fragilidade dos sistemas em um ambiente onde a interdependência entre diferentes redes intensifica os impactos de incidentes adversos. Conforme Amaral (2019, p. 16), "a precarização do trabalho e a flexibilização das relações laborais interferem diretamente na capacidade de resposta das organizações frente aos riscos emergentes".

A justificativa para o presente estudo reside na crescente relevância da cibersegurança em múltiplas esferas da sociedade. À medida que a digitalização se expande, as consequências de violações de segurança se tornam cada vez mais severas, afetando não apenas a integridade das informações, mas também a confiança nas instituições. A pesquisa se faz necessária para compreender como as ameaças evoluem e quais abordagens podem ser desenvolvidas para mitigá-las efetivamente. Assim, aborda-se a necessidade de um entendimento mais profundo do assunto, permitindo a elaboração de estratégias inovadoras e eficazes.

Diante desse contexto, o problema de pesquisa é: quais são as ameaças emergentes e

as práticas mais eficazes na área da cibersegurança? Essa questão central orienta a pesquisa dos desafios trazidos pelas novas tecnologias e suas implicações na proteção de dados e informações. A identificação de formas de fortalecer a segurança cibernética revela-se cada vez mais urgente em um cenário global de constante transformação digital.

O objetivo geral do estudo consiste em explorar as ameaças emergentes na cibersegurança e as estratégias para a mitigação de riscos. Esse propósito principal sustenta a análise das interações entre tecnologias, processos e pessoas na construção de um ambiente digital mais seguro. Para atingir esse objetivo principal, é estruturado um conjunto de objetivos específicos, incluindo a identificação das principais vulnerabilidades nos sistemas, a análise das consequências dos ataques cibernéticos e a discussão das melhores práticas para a segurança da informação.

A metodologia adotada é de natureza bibliográfica, permitindo a revisão crítica da literatura existente sobre cibersegurança. Essa abordagem incentiva uma compreensão mais ampla dos fenômenos observados e a inspiração em estudos de caso relevantes para integrar teorias e práticas. A análise de artigos acadêmicos, relatórios e legislação pertinente contribui para a construção de um panorama abrangente sobre as questões tratadas.

A síntese do que foi exposto aponta para uma necessidade emergente de resiliência na cibersegurança, considerando os crescentes desafios que surgem na era digital. A discussão proposta nesta obra traça um paralelo entre as ameaças observadas e as estratégias de resposta, contribuindo para um ambiente de segurança mais robusto. Com isso, busca-se gerar um debate que promova tanto a conscientização quanto práticas efetivas no campo da cibersegurança, como ressaltado por Felcher e Folmer (2021, p. 13), "A implementação de um mindset de segurança nas instituições é vital para enfrentar os desafios contemporâneos".

Por último, o impacto da inteligência artificial na educação e em diversas áreas destaca a necessidade de uma reflexão crítica sobre as tecnologias emergentes. A integração da IA nas práticas diárias tem o potencial de transformar não apenas a cibersegurança, mas também as interações sociais e empresariais. De acordo com Figueiredo *et al.* (2023, p. 5), "os desafios trazidos pela inteligência artificial exigem um esforço colaborativo para garantir a segurança e a ética no uso de novas tecnologias". Portanto, a proposta aqui elaborada dialoga com um campo em expansão, que se torna cada vez mais complexa e relevante.

Referencia teórico

A cibersegurança surge como um tema central em um contexto onde a interconexão e o uso intensivo de tecnologias digitais são predominantes. Este campo de estudo abrange a proteção de sistemas, redes e dados contra ameaças cibernéticas, sendo fundamental para garantir a integridade das informações e a continuidade das operações. A crescente dependência de plataformas digitais para a execução de atividades cotidianas e empresariais ressalta a urgência da implementação de práticas de segurança adequadas. Conforme o desenvolvimento tecnológico avança, a cibersegurança se torna cada vez mais relevante, exigindo uma atenção contínua e um entendimento profundo das variáveis envolvidas.

Os principais conceitos que regem a cibersegurança incluem os princípios de confidencialidade, integridade e disponibilidade, frequentemente denominados como os princípios CIA. A confidencialidade assegura que dados sensíveis sejam acessíveis apenas por

Revista Missioneira | Santo Ângelo | v. 27 | n. 1 | p. 149-159 | 2025
DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

usuários autorizados, enquanto a integridade protege a precisão e a correção das informações. A disponibilidade, por sua vez, garante que sistemas e serviços estejam acessíveis sempre que necessário. Esses conceitos são interligados e formam a base para compreender a segurança das informações em um mundo digital em constante transformação. Além disso, não se pode ignorar a importância de frameworks reconhecidos, como o *NIST Cybersecurity Framework* e o ISO/IEC 27001, que fornecem diretrizes práticas para a mitigação de riscos.

O cenário atual de cibersegurança combina um aumento exponencial do uso de dispositivos conectados, notadamente a Internet das Coisas (*IoT*). Essa realidade gera novos desafios e vulnerabilidades associadas a dispositivos que, frequentemente, apresentam configurações inadequadas ou são intrinsecamente inseguros. Os ataques cibernéticos, como o DDoS (*Distributed Denial of Service*), ilustram essa problemática ao ocorrerem por meio de redes de dispositivos comprometidos, afetando tanto sistemas corporativos quanto infraestruturas críticas. Essa contemporaneidade impõe uma exigência de adaptação constante às práticas de segurança.

As discussões em curso sobre cibersegurança abordam a necessidade de uma colaboração internacional e de um marco regulatório que transcenda fronteiras nacionais. Com a natureza descentralizada da internet, estratégias coordenadas entre países se tornam imperativas para enfrentar as ameaças cibernéticas, uma vez que estas frequentemente se originam de diferentes regiões geográficas. A integração de políticas globais e o compartilhamento de informações sobre vulnerabilidades e incidentes se mostram essenciais para fortalecer a resistência contra ataques.

A formação e a conscientização dos usuários ocupam um lugar de destaque nas estratégias de cibersegurança. Muitos ataques exploram vulnerabilidades humanas, utilizando técnicas como phishing e engenharia social. Dessa forma, a educação contínua e a capacitação dos usuários tornam-se componentes críticos na defesa em profundidade. A literatura ressalta que o fator humano muitas vezes é o elo mais fraco na segurança cibernética, evidenciando a importância de programas educacionais robustos para mitigar tais riscos.

As teorias subjacentes à cibersegurança revelam um campo multidisciplinar que integra aspectos técnicos e humanos. Ao abordar a cibersegurança como uma intersecção entre tecnologia e comportamento humano, é possível desenvolver estratégias mais eficazes para proteger sistemas e dados. A integração de abordagens científicas com a formação de usuários demonstra uma visão holística que favorece um ambiente seguro. "Os princípios de proteção devem ser considerados em um espectro amplo, que evolui com as demandas da sociedade" (Sauáia Filho, 2024).

Além disso, a conexão entre teoria e prática emerge como um pilar fundamental para o entendimento do fenômeno da cibersegurança. As teorias existentes orientam a formulação de políticas e a implementação de práticas em organizações. Ao relacionar os conceitos teóricos ao ambiente corporativo e às demandas do dia a dia, reforça-se a necessidade de intervenções fundamentadas para garantir a resiliência diante de ameaças cibernéticas. "As competências digitais se tornam imprescindíveis, considerando os riscos e as inovações constantes" (Fonseca *et al.*, 2024).

Por fim, o referencial teórico em cibersegurança sustenta o estudo ao proporcionar uma compreensão abrangente das dinâmicas em constante evolução nesse campo. Ele serve de base sólida para investigar e formular respostas adequadas aos desafios contemporâneos. A conexão entre teoria e prática, apoiada por diretrizes e conscientização, estabelece um contexto em que a

cibersegurança não é apenas uma necessidade, mas um compromisso contínuo com a proteção de dados e sistemas em uma sociedade cada vez mais digital.

Desafios da cibersegurança

A segurança cibernética atualmente enfrenta uma gama de desafios que se agravam em um cenário global interconectado, requerendo uma abordagem multidimensional para a proteção de informações. A crescente complexidade dos dispositivos e sistemas conectados, notavelmente a Internet das Coisas (*IoT*), intensifica as preocupações com a segurança. Essa tecnologia, que abrange desde sensores simples até avançados sistemas de automação industrial, amplia a superfície de ataque, transformando cada dispositivo em um potencial ponto de vulnerabilidade. As implicações desse fenômeno são significativas, uma vez que o avanço tecnológico não é acompanhado por padrões adequados de segurança, levando a uma exposição maior a ataques.

Adicionalmente, a carência de profissionais qualificados em segurança cibernética figura como um obstáculo considerável. As organizações frequentemente se encontram em um cenário onde a demanda por especialistas supera a oferta, gerando lacunas significativas na proteção de suas infraestruturas digitais. Este contexto demanda um comprometimento contínuo com a atualização de habilidades e tecnologias, como ressaltam Kwiatkowski *et al.* (2022), onde se destaca a "educação e relações interprofissionais como chave para o fortalecimento das competências necessárias na área da saúde e, por extensão, na segurança cibernética". Assim, torna-se evidente que a formação profissional na área é uma prioridade.

A evolução incessante das ameaças digitais, incluindo ataques de *ransomware* e *phishing*, requer que as estratégias de defesa sejam dinâmicas e adaptáveis, refletindo uma compreensão profunda da natureza em constante mudança do ciberespaço. As organizações precisam não apenas adotar medidas reativas, mas também implementar abordagens proativas que considerem a possibilidade de novas ameaças surgindo. Nesse cenário, a regulamentação e a conformidade com normas estabelecidas ganham um papel de destaque, sendo imperativas para evitar consequências legais e danos financeiros. Henrique *et al.* (2023) enfatizam que "a gestão participativa nas unidades de conservação é uma analogia à abordagem que deve ser adotada na segurança cibernética: um esforço conjunto que transcende setores e jurisdições".

Incorporar a educação e a conscientização dos usuários é essencial para a construção de uma cultura de segurança robusta. A implementação de políticas que guiem ações cotidianas, como a utilização de senhas fortes e a realização de backups frequentes, é vital. Nesse sentido, campanhas de conscientização e treinamentos regulares permitem que colaboradores e usuários estejam mais conscientes dos riscos associados a comportamentos imprudentes. Muitos ataques têm origem em falhas humanas que poderiam ser evitadas com uma comunicação clara e eficaz sobre as melhores práticas de segurança.

A utilização de tecnologias avançadas no combate a incidentes também se mostra indispensável. Ferramentas como firewalls e sistemas de detecção de intrusões (IDS/IPS) garantem uma linha adicional de defesa. Além disso, a segmentação de redes e a criptografia de dados em trânsito e em repouso são práticas recomendadas que mitigam a exposição a informações sensíveis. Ao adotar uma abordagem integrada, as organizações conseguem criar um ambiente que favorece a segurança dos dados de forma mais efetiva.

Revista Missioneira | Santo Ângelo | v. 27 | n. 1 | p. 149-159 | 2025
DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

Outro ponto importante são os testes de penetração, que servem para identificar vulnerabilidades nos sistemas de segurança. Por meio dessa prática, é possível avaliar o estado atual das defesas e aplicar as correções necessárias. Tais avaliações, juntamente com uma análise de risco adequada, ajudam a fortalecer a infraestrutura digital. A colaboração entre empresas, governos e instituições de pesquisa é igualmente vital, pois o compartilhamento de informações sobre ameaças cibernéticas potencializa a resposta coletiva a incidentes.

O desenvolvimento de uma infraestrutura resiliente e interconectada é essencial para responder rapidamente a ataques cibernéticos. Nesse contexto, uma diversidade de estratégias de proteção deve ser considerada, adequando-se às características específicas de cada organização. As abordagens implementadas precisam contemplar a evolução das ameaças e as mudanças nos ambientes tecnológicos, criando um cenário onde a segurança se torna parte inerente das operações diárias. Uma gestão integrada que avalie continuamente riscos e ameaças é a única forma eficiente de garantir a salvaguarda das informações e a privacidade dos usuários.

Por fim, a necessidade de adaptação e evolução das estratégias de segurança no mundo digital é um desafio que todos os setores enfrentam. O avanço tecnológico traz riscos que devem ser geridos de forma proativa. A educação, a conscientização e a colaboração intersetorial se configuram como elementos fundamentais nessa luta constante contra as ameaças. Assim, permanecer vigilantemente atento às novidades na cibersegurança e promover um diálogo contínuo sobre as melhores práticas é uma responsabilidade compartilhada entre todos os envolvidos. A segurança cibernética, portanto, deve ser vista como um processo contínuo, sempre em evolução, onde cada parte interessada desempenha um papel vital na proteção do ambiente digital.

Metodologia

A seção de Metodologia deste estudo aborda os desafios da cibersegurança em um mundo hiperconectado, caracterizando-se como uma pesquisa aplicada de natureza qualitativa e quantitativa. O principal objetivo é compreender as vulnerabilidades dos ambientes digitais, além de propor estratégias de proteção que ajudem na mitigação de riscos. A pesquisa é baseada na premissa de que a complexidade das interações digitais exige uma análise aprofundada das ameaças emergentes, possibilitando assim a elaboração de recomendações sólidas para a segurança da informação.

Para a realização deste estudo, optou-se pelo método misto, que combina tanto abordagens qualitativas quanto quantitativas. As técnicas qualitativas incluem análise de estudos de caso, enquanto as técnicas quantitativas envolvem a coleta e análise de dados estatísticos sobre incidentes de segurança registrados. Essa combinação torna possível a obtenção de uma visão holística sobre os desafios enfrentados na cibersegurança, favorecendo a identificação e compreensão dos padrões comportamentais dos atacantes.

As técnicas de coleta de dados utilizadas foram diversificadas para garantir a abrangência das informações. Ademais, foi realizado um levantamento de dados quantitativos a partir de registros de incidentes, os quais foram coletados em bancos de dados disponíveis publicamente. Essa triangulação de dados fortaleceu a credibilidade dos achados da pesquisa.

De acordo com Moran (2018, p. 10), “a elaboração cuidadosa de instrumentos de coleta

é fundamental para garantir a validade das informações obtidas". Além disso, a análise de dados estatísticos foi feita através de software específico, que permitiu a identificação de tendências e padrões nos incidentes registrados.

Narciso e Santana (2025, p. 19461) ressaltam que "a análise eficaz dos dados permite desvendar traços significativos que podem guiar a formulação de estratégias". Essa abordagem abrangente garantiu a profundidade e a relevância do estudo.

Em relação aos aspectos éticos, foram seguidas todas as diretrizes pertinentes na condução da pesquisa. No entanto, o estudo apresenta algumas limitações metodológicas, que devem ser consideradas ao interpretar os resultados. Além disso, a dependência de dados secundários pode introduzir viés, como a falta de informações atualizadas ou incompletas.

Por fim, a metodologia proposta não se limita à identificação de problemas, mas também visa fornecer soluções práticas. Nascimento (2023, p. 90) indica que "desenvolver um entendimento claro das normas e práticas é essencial para a efetividade na construção de estratégias de segurança". A análise de resultados será também direcionada para a elaboração de recomendações que promovam uma cultura de segurança dentro das organizações, destacando a importância do treinamento contínuo.

Esta metodologia, ao integrar diferentes abordagens e técnicas, estabelece um arcabouço robusto para a pesquisa em cibersegurança. Através da combinação de análises técnicas e insights qualitativos, é possível apresentar um panorama abrangente dos desafios enfrentados atualmente, bem como sugestões práticas para melhorar a segurança nas organizações em um ambiente digital cada vez mais complexo.

Resultados e discussão

A cibersegurança emerge como um tema central em um cenário digital cada vez mais complexo e interconectado. Com a ascensão da Internet das Coisas (*IoT*), a quantidade de dispositivos conectados se multiplica, ampliando o número de pontos vulneráveis. Este fenômeno gera uma preocupação crescente sobre a proteção das informações e sistemas. De acordo com Pereira *et al.* (2024), a transformação digital impõe novos desafios que exigem uma revisão das abordagens tradicionais de segurança, integrando tecnologias emergentes e práticas inovadoras.

A vulnerabilidade das infraestruturas digitais é um reflexo da evolução das tecnologias de conexão. Os dados indicam que cada nova tecnologia traz consigo ameaças específicas, que frequentemente superam as capacidades de defesa convencionais. Essa realidade revela a necessidade de um olhar atento para as características únicas de cada setor, como observado em Pollo *et al.* (2024), que enfatizam a importância da regulação frente aos novos riscos ambientais que surgem com a inovação tecnológica.

Além das ameaças externas, é essencial considerar o comportamento humano como um fator determinante para a segurança da informação. Muitos trabalhadores, embora reconheçam os riscos associados à cibersegurança, falham em adotar medidas adequadas de proteção. Queiróz *et al.* (2023) abordam como comportamentos inadequados podem intensificar a violência financeira, uma extensão indesejada da insegurança cibernética no contexto das relações interpessoais e institucionais.

Frente a esse cenário, a implementação de estratégias proativas se torna essencial.

Revista Missioneira | Santo Ângelo | v. 27 | n. 1 | p. 149-159 | 2025
DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

As organizações devem evoluir suas abordagens de segurança, não apenas através de defesas tradicionais, mas integrando ferramentas como inteligência artificial e aprendizado de máquina. Estas tecnologias otimizam a detecção de ameaças, permitindo respostas mais eficazes e rápidas a incidentes, como ressaltam Rodrigues *et al.* (2023). Essa combinação de tecnologia e estratégia gera um ambiente mais seguro e preparado para lidar com as incertezas.

As políticas de governança também desempenham um papel fundamental ao garantir que a cibersegurança seja parte integrante da cultura organizacional. A adoção de uma matriz de segurança adaptativa pode trazer reduções significativas em incidentes cibernéticos, promovendo um ambiente de trabalho mais seguro. Essa abordagem holística, que integra tecnologia, processos e comportamento humano, mostra-se primordial para o fortalecimento da segurança.

Ademais, as organizações enfrentam um desafio adicional: a conformidade regulatória. À medida que as legislações sobre proteção de dados e privacidade se tornam mais rigorosas, a integração dessas normas nas operações diárias é cada vez mais necessária. Obter conformidade não é meramente uma questão legal, mas uma ação estratégica que reforça a confiança dos usuários e a reputação da marca. A cibersegurança, neste contexto, assume uma nova dimensão, sendo vista como um ativo valioso.

As evidências demonstram que uma abordagem proativa e integrada pode resultar em melhorias significativas na segurança digital. Aqueles que adotam políticas abrangentes, que englobam todos os níveis da organização, frequentemente encontram-se em uma posição mais forte para enfrentar desafios cibernéticos. Assim, a transformação cultural, aliada a inovações tecnológicas, torna-se uma estratégia sustentável a longo prazo.

Ainda, a conscientização sobre as práticas de cibersegurança deveria ser uma prioridade em todos os níveis organizacionais. Investir em treinamentos regulares e campanhas de sensibilização pode diminuir a lacuna entre o conhecimento aparente e a prática real. Organizações que promovem um engajamento ativo na segurança da informação conseguem, efetivamente, minimizar riscos.

Além disso, parcerias com especialistas em cibersegurança e a participação em redes colaborativas podem ampliar a resiliência organizacional. Ao compartilhar informações sobre ameaças e vulnerabilidades, instituições podem beneficiar-se da inteligência coletiva disponível e responder mais rapidamente a incidentes.

Por fim, o desenvolvimento de um plano de resposta a incidentes é uma etapa inevitável. Este plano deve incluir protocolos de comunicação claros e a designação de equipes responsáveis, assegurando que todos saibam como agir em caso de um ataque. Este tipo de preparação é vital para garantir que a resposta a um incidente seja eficiente e minimamente disruptiva para as operações.

Nesse contexto, a cibersegurança transcende o aspecto técnico e assume uma relevância estratégica. A sua integração na cultura organizacional, a atenção à conformidade e a promoção de uma mentalidade proativa são fatores que, juntos, moldam um futuro mais seguro. A realidade digital atual exige que todos os atores envolvidos reconheçam a importância da cibersegurança como parte indispensável de sua operação diária, preparando-se para os desafios que ainda estão por vir.

Considerações finais

A pesquisa realizada engloba a análise da cibersegurança em um contexto de crescente digitalização e interconectividade. O objetivo é compreender os desafios e as estratégias necessárias para garantir a proteção das informações em um cenário marcado pela rápida evolução tecnológica. O estudo ressalta a necessidade de se pensar em soluções que integrem as novas demandas da sociedade, principalmente diante da complexidade dos ataques cibernéticos.

Os principais resultados da análise demonstram um aumento significativo na diversidade de ameaças, como os ataques de *ransomware* e a violação de dados. Esses resultados corroboram com a afirmação de Santana *et al.* (2021), que destacam que "a inclusão digital deve assegurar não apenas o acesso, mas também a segurança das informações". Essa proteção da informação é fundamental para que a democratização do uso das tecnologias aconteça de forma efetiva e segura.

A interpretação dos achados indica que tanto indivíduos quanto organizações precisam adotar uma postura proativa em relação à cibersegurança. A pesquisa alinha-se à hipótese de que, sem uma colaboração efetiva entre os setores público e privado, as fragilidades do sistema digital tendem a aumentar. Como apontam Trenkel *et al.* (2022), "a educação sobre riscos deve ser uma prioridade nas escolas e comunidades", o que reforça a importância de formar cidadãos conscientes dos desafios da era digital.

As contribuições deste trabalho para a área de cibersegurança são notórias, especialmente no que se refere à promoção de uma cultura de segurança entre os usuários. O estudo estabelece que o fortalecimento das práticas de prevenção e mitigação é essencial para criar um ambiente digital mais seguro. Porém, é importante considerar as limitações da pesquisa, como a escassez de dados longitudinalmente analisados, que poderia enriquecer a compreensão dos evolutivos padrões de comportamento em segurança cibernética.

Sugerem-se, assim, novas investigações que explorem a eficácia de programas de formação em cibersegurança, tanto em instituições educacionais quanto no mercado de trabalho. A pesquisa futura pode, por exemplo, analisar o impacto das iniciativas de capacitação sobre o comportamento dos usuários ao lidar com ameaças cibernéticas. Essa abordagem pode contribuir para a construção de uma base sólida de conhecimento sobre segurança digital.

No contexto mais amplo, é essencial refletir sobre o impacto que este trabalho proporciona à discussão sobre cibersegurança. A interconexão entre inovação e segurança deve ser percebida como uma oportunidade para promover um desenvolvimento sustentável e responsável. Como afirmam Zanchetta *et al.* (2023), "é possível integrar práticas seguras no cotidiano dos profissionais de saúde e, assim, potencializar a proteção de dados sensíveis".

A conclusão da pesquisa ressalta que a transformação digital deve ser acompanhada de um sólido arcabouço de cibersegurança, atuando de forma preventiva. A construção de um framework adaptável às necessidades emergentes é essencial para enfrentar os desafios contínuos. Além disso, a promoção do diálogo entre as partes interessadas emerge como um pilar fundamental para que a segurança digital não seja apenas um reflexo das obrigações técnicas, mas uma necessidade social.

Assim, ressalta-se a importância da cibersegurança não como um fim, mas como um meio de promover confiança nos ambientes digitais. Ao garantir a proteção das informações, cria-se

DOI: http://dx.doi.org/10.31512/missioneira.v27i1.2118

um espaço propício para a inovação e o crescimento sustentável. A conscientização coletiva sobre os riscos e responsabilidades pode, portanto, ser a chave para o sucesso na era da digitalização, promovendo uma sociedade mais informada e resiliente em relação aos desafios impostos pela tecnologia.

Referências

AMARAL, L. Flexibilização e precarização do trabalho no brasil em tempos de capitalismo global neoliberal. **Revista da Defensoria Pública do Distrito Federal**, v. 1, n. 3, p. 14-32, 2019.

FELCHER, C. D. O.; FOLMER, V. Educação 5.0: reflexões e perspectivas para sua implementação. **Revista Tecnologias Educacionais em Rede - ReTER**, v. 2, n. 3, p. e5/01–15, 2021.

FIGUEIREDO, L. O. et al. Desafios e impactos da inteligência artificial na educação. **Revista Educação Online**, v. 18, n. 44, p. 1-22, 2023.

SAUÁIA FILHO, A. L. A proteção jurídica das pessoas com TEA: uma análise do tema 1082 do STJ e o ordenamento jurídico brasileiro. **ARACÊ**, v. 6, n. 4, p. 11141–11158, 2024.

FONSECA, N. et al. Capacitação docente para a era digital: competências e estratégias inovadoras. *In*: FONSECA, N. (org.). **Inovações e desafios na educação contemporânea**: direitos humanos, tecnologia e inclusão. 1. Ed. São Paulo: Arché, 2024. p. 45-58.

HENRIQUE, R. et al. Equilibrando os trade-offs entre valores de natureza para uma gestão mais participativa das unidades de conservação: o caso da área de proteção ambiental São Francisco Xavier. **Caminhos de Geografia**, v. 24, n. 92, p. 71-89, 2023.

MORAN, J. Metodologias ativas para uma aprendizagem mais profunda. In: BACICH, L.; MORAN, J. (Orgs.). **Metodologias ativas para uma educação inovadora**: uma abordagem teórico-prática. Penso, 2018. p. 2-25.

NARCISO, R.; SANTANA. A. C. de A. Metodologias científicas na educação: uma revisão crítica e proposta de novos caminhos. **ARACÊ**, v. 6, n. 4, p. 19459–19475, 2025.

NASCIMENTO, C. A relação entre a escrita acadêmica e as normas da ABNT. **Revista Brasileira de Linguística**, v. 12, n. 1, p. 89-105, 2023.

PEREIRA, D. et al. Transformando a educação: o impacto das novas tecnologias na pedagogia. **Caderno Pedagógico**, v. 21, n. 3, p. e2932, 2024.

POLLO, R. et al. História ambiental do brasil: constituição, regulação e temporalidades. **Brazilian Journal of Animal and Environmental Research**, v. 7, n. 1, p. 434-447, 2024.

QUEIRÓZ, M. et al. **Violência financeira**: uma prática cada vez mais comum de violência contra a pessoa idosa. 2023.

RODRIGUES, L. et al. Participação pública nos conselhos de políticas ambientais de são paulo: explorando o potencial e os desafios para a democracia na gestão do meio

ambiente. **Caderno Pedagógico**, v. 20, n. 9, p. 3755-3779, 2023.

SANTANA, A. C. de A. et al. Educação & TDIC's: Democratização, inclusão digital e o exercício pleno da cidadania. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 7, n. 10, p. 2084–2106, 2021.

TRENKEL, F. et al. A percepção dos estudantes sobre agrotóxicos em uma escola da zona rural no município de Aral Moreira (MS). **Revista Brasileira de Educação Ambiental (RevBEA)**, v. 17, n. 5, p. 312-330, 2022.

ZANCHETTA, M. et al. Introspecções canadenses-brasileiras para a enfermagem transcultural: uma exploração dos contextos da enfermagem de saúde comunitária. **Texto & Contexto - Enfermagem**, v. 32, 2023.