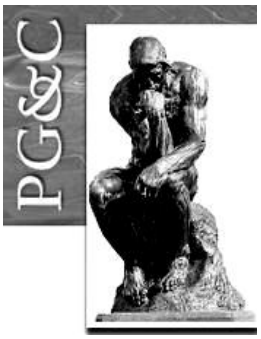
MEMÓRIA DE EVENTO CIENTÍFICO-PROFISSIONAL



ANÁLISE BIBLIOMÉTRICA SOBRE A GESTÃO DO CONHECIMENTO NO CONTEXTO DA SEGURANÇA CIBERNÉTICA

André Lozano Ferreira
Doutorando em Administração pela Universidade Presbiteriana Mackenzie, Brasil.
E-mail: andre.lozanox@gmail.com

Gilberto Perez
Doutor em Administração pela Universidade de São Paulo, Brasil.
Professor da Universidade Presbiteriana Mackenzie, Brasil.
E-mail: gilberto.perez@mackenzie.br

Resumo
O estudo investiga a produção científica relacionada com a gestão do conhecimento nas organizações no contexto da segurança cibernética. Em um trabalho inédito, são fornecidas implicações para as organizações à medida que desenvolvem capacidades relacionadas à segurança cibernética e à gestão do conhecimento para competir de forma eficaz na economia digital. Utilizou-se a metodologia da análise bibliométrica que aborda a pesquisa em um modelo predominante quantitativo, demonstrando a importância da análise do tema abordado. Como resultados são apresentadas as principais características da literatura, possibilitando identificar temas que podem ser aprofundados em estudos futuros, como a colaboração e o compartilhamento de conhecimento. São apresentadas ainda lacunas relacionadas ao tema de gestão de identidade digital, com seus impactos e consequências relacionadas ao indivíduo e à gestão do conhecimento, tratando também de barreiras como os preconceitos organizacionais quanto ao compartilhamento de conhecimento entre os *stakeholders*.

Palavras-chave: segurança cibernética; gestão do conhecimento; estratégia; colaboração.

BIBLIOMETRIC ANALYSIS ON KNOWLEDGE MANAGEMENT IN THE CONTEXT OF CYBERSECURITY

Abstract
This study aims to investigate the scientific production involving knowledge management in organizations in the context of cybersecurity. In first-of-its-kind work, implications are provided for organizations as they develop capabilities related to cybersecurity and knowledge management to compete effectively in the digital economy. We used the methodology of bibliometric analysis that approaches the research in a predominant quantitative model, demonstrating the importance of the study of the theme addressed. As a result, the main characteristics of the literature are presented, making it possible to identify themes that can be deepened in future studies, such as collaboration and knowledge sharing. Gaps related to the theme of digital identity management, with its impacts and consequences related to individual and knowledge management, are also presented, addressing barriers such as organizational biases regarding sharing knowledge among stakeholders.

Keywords: cybersecurity; knowledge management; strategy; collaboration.

1 INTRODUÇÃO

Com este estudo busca-se investigar a evolução da produção científica relacionada com a gestão do conhecimento nas organizações, no contexto da segurança cibernética. A

economia digital fundamenta-se nas novas tecnologias ofertadas pelo mercado. Em geral, segundo Lettieri (2021), a economia digital experimenta um crescimento exponencial e molda as novas relações de oferta e demanda em todo o ecossistema econômico. Embora a tecnologia tenha levado a avanços significativos para a economia digital, particularmente pelo uso da Internet, Agrafiotis *et al.* (2018) argumentam que a Internet também expôs organizações e indivíduos a uma série de novos riscos resultantes de ataques através de interfaces digitais. É essencial que as organizações adotem e implementem uma forte abordagem de segurança cibernética para mitigar perdas financeiras. Proteger de forma inteligente os sistemas relevantes é uma questão-chave a ser analisada com urgência (Sarker *et al.*, 2020).

Em um cenário em que a única certeza é a incerteza, assim atua a segurança cibernética, a forma de se criar vantagem competitiva para as organizações é o conhecimento. A transformação dos mercados com novas tecnologias, competidores multiplicando-se e os produtos tornando-se obsoletos a cada dia, fazem das organizações verdadeiras máquina de processamento de conhecimento (Takeuchi; Nonaka, 2009), tanto para a inovação, quanto para a defesa da organização.

Surge assim, a necessidade de estreita colaboração entre as organizações, com o compartilhamento de informações sensíveis. Isto permite a agilidade na gestão das operações de segurança cibernética, com o apoio da gestão das informações, base da estratégia e da ciberdefesa. Construir uma base de conhecimento comum de segurança cibernética é uma maneira eficiente de colaboração e compartilhamento de aprendizagens (Takahashi; Kadobayashi, 2015).

Entretanto, para Heinrich *et al.* (2018), a segurança cibernética é mais comportamental do que puramente técnica. Assim, gera a necessidade de colocar o foco no fator humano para criar uma visão de gestão do conhecimento, promover a mudança comportamental e fornecer entidades de conhecimento relevantes. Identificar, avaliar e treinar as habilidades e conhecimentos necessários é o caminho para aumentar a segurança cibernética, quando trata a educação e o treinamento de conscientização como abordagens importantes para o tema. No entanto, surpreendentemente pouco se sabe sobre a questão do que ensinar exatamente e por qual motivo específico. Não deveria existir uma crise em larga escala na segurança cibernética. Economicamente, ataques e violações bem-sucedidos são um desastre, tanto financeiramente quanto em termos de reputação. Embora o tema seja fortemente discutido no meio científico e público, as empresas invistam grandes quantias em segurança cibernética e as regulamentações governamentais busquem impor políticas e procedimentos rigorosos, a realidade é vista como um cenário de guerra, com ameaças e ataques diários. Como os indivíduos são a maior ameaça à segurança cibernética, o tópico também é relevante no nível organizacional (Heinrich *et al.*, 2018).

A segurança cibernética também é uma questão de pessoas, e a pesquisa comportamental sobre segurança da informação é crítica. O aprendizado individual sobre segurança cibernética não é formal e linear, mas complexo e baseado em rede. A forma como o conhecimento é criado e compartilhado está em constante mudança na era digital. As pessoas nas organizações realizam ações que influenciam a postura de segurança cibernética de uma organização e essas ações recebem influências políticas, de procedimentos e ferramentas, como a gestão do conhecimento (Patnayakuni *et al.*, 2017).

A Gestão do Conhecimento nos ambientes corporativos é de suma importância para a sustentação da cadeia de valor das empresas. Ela emprega metodologias para que haja a criação e o compartilhamento de conhecimento entre os indivíduos em um ambiente propício para essa construção. Em contrapartida, há o conceito de Segurança da Informação, que visa proteger a informação e orientar os processos para que haja a menor exposição possível. O estudo de Buogo *et al.* (2020) evidencia a importância que a segurança cibernética possui

diante da criação do conhecimento nas Organizações, com a necessidade de uma Gestão do Conhecimento Segura.

No Brasil, por exemplo, o Ministério da Ciência, Tecnologia e Inovação (MCTI, 2023) lançou o programa Hackers do Bem para o fortalecimento do conhecimento e da segurança cibernética, com a capacitação de profissionais em larga escala. Ao todo serão investidos R$ 32,6 milhões em recursos para formar mais de 30 mil pessoas até 2025. Além do processo de formação, o objetivo também é construir um hub nacional de cibersegurança, integrar *stakeholders* e buscar principalmente a inovação para a sociedade (MCTI, 2023).

A Agência Espacial Europeia (ESA), como um exemplo prático, realizou um desafio para os especialistas em segurança cibernética do setor espacial para interferir na operação de um nano satélite de demonstração da agência. Os participantes deveriam utilizar técnicas éticas de ataques hackers para assumir o controle do sistema. Demonstrou-se assim, que o acesso não autorizado a este ambiente pode causar danos graves ao satélite ou levar a perda do controle da missão, com a necessidade de um alto nível de resiliência cibernética no ambiente operacional específico do espaço (Padilha, 2023).

Estes exemplos apresentam ações importantes que envolvem a gestão do conhecimento no contexto da segurança cibernética, mas o que a literatura apresenta sobre o tema, apesar dos melhores esforços é um déficit significativo. Além disso, esforços significativos são necessários para definir funções específicas de segurança cibernética com mais cuidado para a próxima geração de ameaças cibernéticas por meio do conhecimento, de forma contínua e evolutiva (Samtani *et al.*, 2023).

Diante da relevância do tema, um estudo bibliométrico sobre a gestão do conhecimento e da segurança cibernética pode apresentar contribuições importantes para estudiosos, interessados pelo tema e especialistas, com a possibilidade de identificar lacunas importantes e até mesmo a necessidade de aprofundar estudos já realizados.

2 GESTÃO DO CONHECIMENTO

A história da filosofia desde o período grego pode ser vista como o processo de busca de uma resposta à pergunta “O que é o conhecimento?”. Apesar das diferenças fundamentais entre o racionalismo e o empirismo, os filósofos ocidentais em geral concordam que conhecimento é a “crença verdadeira justificada”, um conceito introduzido inicialmente por Platão em Ménon, Pédon e Teeteto. Assim, as duas principais abordagens à epistemologia, o racionalismo e o empirismo, diferem radicalmente quanto ao que constitui a verdadeira fonte de conhecimento. Outra diferença fundamental é o método através do qual se obtém o conhecimento. O racionalismo alega que se pode obter o conhecimento por dedução, recorrendo-se a construtos mentais como conceitos, leis ou teorias. O empirismo, por outro lado, argumenta que o conhecimento é obtido por indução, a partir de experiências sensoriais específicas (Takeuchi; Nonaka, 2009).

Para Davenport et. al (1998) conhecimento é informação combinada com experiência em determinado contexto, com interpretação e consequente reflexão. Conhecimento é informação, que agrega alto valor e que está pronta para ser utilizada em decisões e ações. Embora o conhecimento e a informação possam ser difíceis de distinguir, ambos são mais valiosos e envolvem mais participação humana do que os dados brutos nos quais esbanjamos a informatização durante os últimos quarenta anos. Dada a importância de tal ativo, não é surpreendente que as organizações em todos os lugares estejam prestando atenção ao conhecimento – explorando o que é e como criá-lo, transferi-lo e usá-lo de forma mais eficaz.

A análise conceitual, entretanto, é de pouca utilidade para os profissionais que se deparam com questões sobre o que especificamente devem fazer como gestores do conhecimento. Uma maneira de uma organização fazer isso é tratar o conhecimento como

qualquer outro ativo em seu balanço. No entanto, quando uma empresa enfrenta concorrentes com bom desempenho, a diferença entre sucesso e fracasso pode depender da eficiência com que ela gerencia o seu conhecimento (Davenport *et al.*, 1998).

Para Sanchez e Mahoney (1996), em estudo sobre a modularidade tanto em projetos de produtos quanto em projetos de organizações, à medida que mais empresas começam a usar a modularidade não apenas para criar maior variedade de produtos, mas também como uma nova estrutura para aprendizado estratégico agressivo e gestão do conhecimento mais eficaz, novas dinâmicas de inovação estão sendo criadas cujas implicações para a competição impulsionada pela tecnologia convidam a uma investigação mais aprofundada (Sanchez; Mahoney, 1996).

Da mesma forma, no estudo de Alavi e Leidner (2001), o conhecimento pode ser tratado como um recurso organizacional e significativo. Para eles, as empresas grandes e globais, as tecnologias da informação serão entrelaçadas com estratégias e processos de gestão do conhecimento organizacional. O maior interesse no conhecimento organizacional e na gestão do conhecimento decorre da transição para a economia do conhecimento, onde o conhecimento é visto como a principal fonte de criação de valor e vantagem competitiva sustentável. A visão do conhecimento como um objeto sugere uma perspectiva de gestão do conhecimento que se concentra em construção e gestão de estoques de conhecimento. Ver o conhecimento como um processo implica em uma capacidade cognitiva ou intelectual ou ambas. A gestão do conhecimento permite que as empresas melhorem a qualidade das soluções para os clientes, aos problemas do cliente, reduzir as chamadas de serviço de campo e tornar-se mais orientado para o cliente estabelecer soluções consistentes para os mesmos tipos de problemas, aumentar a resolução na primeira chamada (Alavi; Leidner, 2001).

Esses conhecimentos tratados como ativos se originaram nas mentes criativas dos funcionários e gerentes dentro da organização. A gestão do conhecimento é o que uma organização faz para criar valor, tratando da conceituação, revisão, consolidação, e fases de ação de criar, proteger, combinar, coordenar e recuperar conhecimento. O processo é difícil para uma organização dominar, a menos que primeiro crie um ambiente de compartilhamento de conhecimento no qual todos promovam e utilizem ativamente o sistema de gestão do conhecimento. A cultura corporativa tem um papel importante na gestão do conhecimento e construir uma cultura de compartilhamento é o elemento chave para o desenvolvimento de uma cultura organizacional que nutre aprendizagem organizacional e inteligência organizacional (Mcgriff, 2000).

Os processos de criação do conhecimento desencadeiam a criatividade organizacional (Lee; Choi, 2003). Embora uma empresa tenha acesso ao conhecimento, habilidades e experiência dos funcionários, ela pode precisar possuir boas capacidades de gerenciamento de ferramentas de gestão do conhecimento para garantir a utilização eficaz do capital humano no desenvolvimento da experiência organizacional para inovação. A gestão do conhecimento pode influenciar a relação entre as práticas estratégicas de RH e o desempenho da inovação. Um melhor nível de capacidade de gestão do conhecimento pode estimular pensamentos criativos e inovadores que podem levar a um melhor desempenho da inovação (Chen; Huang, 2009).

A gestão do conhecimento combina processos e a possibilidade de compartilhar com a aplicação de ferramentas tecnológicas para digitalizar, armazenar e tornar universalmente disponível, via redes eletrônicas, enfatizando o compartilhamento do conhecimento, a conversão entre o conhecimento implícito e o conhecimento explícito, a comunidade de prática e a inovação do conhecimento, portanto, fornece um suporte essencial para a construção do conhecimento, avanço da sabedoria individual e coletiva (Gan; Zhu, 2007).

Assim, a gestão do conhecimento desempenha um papel potencialmente mediador na conexão do contexto organizacional e da estratégia com a eficácia organizacional. Acredita-se

que a gestão do conhecimento bem-sucedida tenha o potencial de aumentar a vantagem competitiva de uma organização, o foco no cliente, as relações e o desenvolvimento dos funcionários, a inovação, devido ao relacionamento do tema com os aspectos da cultura organizacional, estrutura e tecnologia que estão diretamente relacionados à gestão do conhecimento. A gestão do conhecimento não é apenas uma prática gerencial independente, mas também um mecanismo central que alavanca a influência cultural, estrutural e estratégica organizacional na eficácia organizacional.

Projetar projetos de gestão do conhecimento geralmente envolve mudanças organizacionais. É crucial ter uma visão holística, considerando todos os três fatores ao projetar e realizar as mudanças pretendidas (Zheng *et al.*, 2010). O relacionamento da gestão do conhecimento ao indivíduo e à estratégia organizacional apresentam uma forte possibilidade de fortalecer as ações de segurança cibernética, considerando os conceitos apresentados na seção seguinte.

3 SEGURANÇA CIBERNÉTICA

A segurança cibernética é uma disciplina complexa e multidisciplinar baseada em computação que tem suas raízes na década de 1960, no primeiro artigo sobre segurança e privacidade em sistemas de computador publicado por Ware (1967). Assim, Ware (1970) apresenta os controles de segurança para sistemas de computador e enfatiza o design de um sistema seguro para fornecer proteção contra os vários tipos de vulnerabilidades, como divulgação acidental, penetração deliberada, infiltração ativa e ataque físico (Lechner, 2017).

Na literatura, a segurança cibernética é usada como um termo amplo. A União Internacional de Telecomunicações (ITU) define a segurança cibernética como a coleta de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamento, melhores práticas, garantias e tecnologias que possam ser usadas para proteger o ambiente cibernético, a organização e os ativos do usuário. A segurança cibernética se esforça para garantir a realização e manutenção das propriedades de segurança da organização e dos ativos do usuário contra riscos relevantes de segurança no ambiente cibernético (Solms; Niekerk, 2013).

Para Xin *et al.* (2018), a segurança cibernética é um conjunto de tecnologias e processos projetados para proteger computadores, redes, programas e dados contra-ataques e acesso, alteração ou destruição não autorizados, consistindo em um sistema de segurança incluindo firewalls, software antivírus e sistemas de detecção de intrusões (IDS). Os IDSs ajudam a descobrir, determinar e identificar comportamentos não autorizados do sistema, como uso, cópia, modificação e destruição.

Os ataques cibernéticos, segundo Agrafiotis *et al.* (2018), incluem furtos de segredos corporativos, sabotagem de sistemas e a cópia de dados de clientes para vender suas identidades na *dark web*, para facilitar outros crimes. São exemplos dos tipos de atos que são perpetrados e podem resultar em danos a uma organização que depende de tecnologias digitais para conduzir seus negócios, e que muitas vezes são guardiões dos dados e metadados das pessoas.

Outra definição relacionada à segurança cibernética é o “dano cibernético”, definido por Agrafiotis *et al.* (2018) como o dano que surge como resultado direto de um ataque realizado total ou parcialmente, por meio de infraestruturas digitais, e as informações, dispositivos e aplicativos de software que essas infraestruturas são compostas.

Os principais tipos de danos cibernéticos relatados por Agrafiotis *et al.* (2018) são os danos físicos ou digitais (ou seja, danos que descrevem um efeito negativo físico ou digital em alguém ou algo), os danos econômicos (ou seja, danos relacionados a consequências financeiras ou econômicas negativas), os danos psicológicos (ou seja, dano que se concentra

em um indivíduo e seu bem-estar mental e psique), os danos reputacionais (ou seja, danos relativos à opinião geral sobre uma entidade) e os danos sociais e societais (ou seja, captura de danos que podem resultar em um contexto social ou sociedade de forma mais ampla) (Agrafiotis *et al.*, 2018).

Embora as soluções tecnológicas para a proteção da segurança cibernética tenham sido aprimoradas, para Andrade e Yoo (2019), é necessário considerar a utilização de estratégias proativas de defesa, ainda mais com o grande número de variantes de ameaças e ataques em expansão contínua com o uso de tecnologias emergentes. Alguns dos ataques que as organizações enfrentam diariamente são os ataques a sistemas industriais de *Internet of things* (IoT), a propagação de malware, a *botnet* IoT e os ataques *distributed denial-of-service* (DDoS) e ataques remotos. A segurança cibernética, por outro lado, não é necessariamente a proteção do ciberespaço em si, mas também a proteção de tudo que funciona no ciberespaço e qualquer um de seus ativos que podem ser alcançados via ciberespaço (Solms; Niekerk, 2013).

A estratégia de segurança cibernética da empresa envolve quatro camadas de proteção, que são preparação, prevenção, resposta e recuperação. A preparação refere-se a esforços que incluem políticas de segurança, padrões técnicos, programas de conscientização de funcionários, coordenação multifuncional, planejamento de segurança cibernética e participação em grupos de trabalho externos. Para tal, nas organizações existem diferentes agentes atuando nas questões de segurança cibernética, entre elas a área de tecnologia operacional e a tecnologia da informação. A importância de se definir prioridades de forma convergente está diretamente relacionada aos riscos cibernéticos e ao aumento de vulnerabilidades (Auffret *et al.*, 2017).

Agrafiotis *et al.* (2018) e Madnick *et al.* (2017) esclarecem que há estudos que abordaram a segurança cibernética focando especificamente nas questões técnicas, por exemplo, hardware e software, e elementos detalhados dos próprios sistemas de segurança ou eventos específicos, como o tempo médio-para-falha. Embora esses esforços sejam necessários, muitas vezes eles não olham para a segurança cibernética de forma holística e geralmente negligenciam considerar seus aspectos organizacionais (Madnick *et al.*, 2017).

Segundo Lettieri (2021), a Consultoria Deloitte fez uma pesquisa com 122 executivos de empresas brasileiras, das quais 41% confirmaram terem sido atacadas, ataque cibernético. As principais medidas adotadas por essas empresas foram a revisão da governança e procedimentos de segurança; a atualização da infraestrutura; a criação de programa de conscientização em toda a empresa; maiores investimentos em segurança cibernética; maior monitoramento dos incidentes; revisão de configurações de ambientes em cloud; criptografia de banco de dados e comunicação e maior rigidez com fornecedores e terceiros.

No Quadro 1 apresentam-se os autores e conceitos de segurança cibernética identificados durante a elaboração do estudo. Vale destacar que os dados identificados servem como contribuição ao entendimento dos conceitos de segurança cibernética e que não esgotam o tema.

Quadro 1 – Autores x Conceitos de Segurança Cibernética Identificados

Autores	**Conceitos**
Ware (1970)	Um sistema seguro deve fornecer proteção contra os vários tipos de vulnerabilidades, como divulgação acidental, penetração deliberada, infiltração ativa e ataque físico.
Solms e Niekerk (2013)	A segurança cibernética, por outro lado, não é necessariamente apenas a proteção do ciberespaço em si, mas também a proteção daqueles que funcionam no ciberespaço e qualquer um de seus ativos que podem ser alcançados via ciberespaço.

Autores	Conceitos
Solms e Niekerk (2013)	A União Internacional de Telecomunicações (ITU) define a segurança cibernética como a coleta de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamento, melhores práticas, garantias e tecnologias que possam ser usadas para proteger o ambiente cibernético, a organização e os ativos do usuário.
Fischer (2015)	O ato de proteger os sistemas de tecnologia da informação e comunicação e seus conteúdos.
Babiceanu e Seker (2016)	A cibersegurança é um campo em rápido crescimento na ciência da computação que se dedica a salvaguardar a privacidade, confidencialidade e integridade dos dados digitais armazenados e/ou transmitidos em qualquer formato através de redes internas e/ou pela Internet.
Radovan e Golub (2017)	A segurança cibernética para Tecnologia da Informação (TI) concentra-se na proteção necessária para garantir a confidencialidade, integridade e disponibilidade dos sistemas eletrônicos de comunicação de informações.
Xin *et al.* (2018)	A segurança cibernética é um conjunto de tecnologias e processos projetados para proteger computadores, redes, programas e dados contra-ataques e acesso, alteração ou destruição não autorizados, consistindo em um sistema de segurança incluindo firewalls, software antivírus e sistemas de detecção de intrusões (IDS)
Lykou *et al.* (2019)	A segurança cibernética pode ser definida como o conjunto de ferramentas, políticas, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de risco, treinamento, melhores práticas, garantias e tecnologias usadas para proteger o ambiente cibernético e os ativos das organizações.
Sarker *et al.* (2020)	A segurança cibernética é um conjunto de tecnologias e processos projetados para proteger computadores, redes, programas e dados contra possíveis ataques, danos ou acesso não autorizado.

Fonte: Elaborado pelos autores com base na literatura estudada

Identifica-se na parte conceitual da segurança cibernética a necessidade de proteção em todos as direções, envolvendo a proteção do ciberespaço, da privacidade de dados, das pessoas, dos sistemas, contra ameaças e ataques cibernéticos.

4 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo apresentam-se os procedimentos metodológicos que apoiaram o estudo bibliométrico, auxiliando na compreensão e investigação da literatura. Bibliometria é a aplicação de métodos estatísticos ao estudo de dados bibliográficos. Pode ser usado para determinar a estrutura intelectual de qualquer campo científico (Baker *et al.*, 2021).

Utilizou-se a metodologia bibliométrica para análise, que aborda a pesquisa em um modelo predominante quantitativo. O processo da bibliometria é baseado em palavras-chave e termos de pesquisa com uma estratégia de pesquisa replicável e definida. Embora este estudo não possa ser considerado exaustivo, isso fornece uma visão geral significativa da relação entre a gestão do conhecimento e o papel desempenhado pela cibersegurança (Lezzi *et al.*, 2018).

Segundo Aria e Cuccurullo (2017), o processo de coleta de dados considera cinco etapas principais, começando pelo desenho do estudo, a coleta de dados, a análise, visualização e interpretação. Em seguida, definem-se os critérios de pesquisa, seleção de artigos e, por fim, avaliação de estudos. Toda a análise principal foi construída com o apoio de um pacote bibliométrico chamado Bibliometrix® com o uso da ferramenta R e a utilização de

vários testes bibliométricos. A interpretação dos resultados é meramente descritiva, mas insights, críticas ou previsões foram inseridas quando aplicável.

Na coleta de dados, selecionaram-se os bancos de dados que contêm os dados bibliométricos, filtrou-se o conjunto de documentos principais e exportaram-se os dados do banco de dados selecionado. A pesquisa foi realizada nos bancos de dados da *Web of Science* (WoS) - Clarivate e Scopus. Por razões de relevância dos estudos, utilizou-se a ordem dos artigos por quantidade de citações. As pesquisas ocorreram em julho de 2023. A definição dos critérios de pesquisa utiliza as palavras-chave *knowledge management* e *cybersecurity*, como apresentado na Tabela 1, com a busca por tópicos para o primeiro termo e todos os campos para o segundo termos na base Web of Science. Foi realizada também a busca por título, abstract e palavras-chave, para a base Scopus. O termo de pesquisa foi elaborado com as fórmulas TS=("Knowledge management") AND ALL=(cybersecurity) para a base de dados Web of Science e (TITLE-ABS-KEY ("knowledge management") AND TITLE-ABS-KEY (cybersecurity)) no processo de pesquisa avançada do banco de dados Scopus.

A Tabela 1 apresenta os totais da busca em cada etapa do processo, sendo a unificação das bases WoS e Scopus totaliza 157 documentos, com a eliminação das duplicidades, restam 141 documentos, utilizando os recursos do Software R. A eliminação das duplicidades da base de dados Scopus ou Web of Science não apresentou diferenças nos relatórios gerados no Bibliometrix. Os filtros 1 e 2 foram aplicados à base de dados unificada. O filtro 1 tratou da eliminação de títulos sem relação com o tema da pesquisa ou qualquer relação com o objetivo do estudo, por meio da leitura individual. O filtro 2 tratou da análise dos resumos de cada um dos artigos restantes, totalizando 33 documentos ao final do processo.

Tabela 1 – Quantidades de estudos

Bases científicas	**Termos de pesquisa**	**Quantidade**
WoS	TS=("Knowledge management") AND ALL=(*cybersecurity*)	22
Scopus	(TITLE-ABS-KEY ("knowledge management") AND TITLE-ABS-KEY (*cybersecurity*))	135
Duplicidades Eliminadas	(-)	16
Subtotal (base unificada)	(=)	141
Filtro (1) – Análise de títulos	(-)	50
Filtro (2) – Análise de resumos	(-)	58
Total Final	(=)	**33**

Fonte: Elaborado pelos autores (2023)

As principais informações identificadas sobre o acervo total analisado, utilizando o Bibliometrix®, foram resumidas na Tabela 2. O período em que foram achadas publicações é de 2014 a 2023. Não foram utilizados filtros relacionados a períodos nas buscas nas bases de dados. Foram identificadas 31 revistas, 33 documentos, com um crescimento médio anual de 10,72 % das publicações. Foram identificados também 99 autores, 142 palavras-chave destes autores, 147 referências utilizadas e 6,03 citações médias por documento.

Tabela 2 – Principais informações do acervo

Item	Informação
Período pesquisado	2014:2023
Revistas	31
Documentos	33
Crescimento médio anual de publicações	10,72 %
Idade média dos documentos	2,88
Autores	99
Palavras-chave dos autores	142
Referências	147
Média de citações por documento	6,03

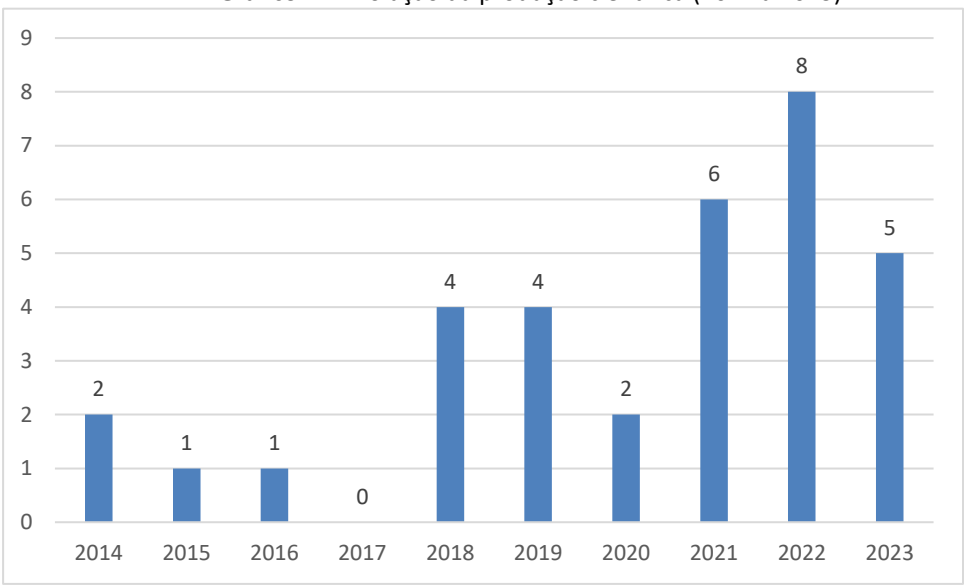
Fonte: Elaborado pelos autores (2023)

A taxa de crescimento anual média identificada na tabela 2 de 10,72% e a idade média dos documentos de 2,88 anos demonstram que existem oportunidades crescentes de análises e publicações que possam apresentar maior profundidade ao tema. Da mesma forma, o número de referências de 147 relacionado à média de 6,03 citações por documento apresentam a informação de concentração de autores utilizados nas referências dos estudos identificados.

5 RESULTADOS E ANÁLISE

A produção científica analisada no período entre 2014 e 2023 apresenta nos termos gestão do conhecimento e segurança cibernética uma evolução constante, com maior produção científica a partir de 2021, com pico em 2022 com 8 publicações, conforme o Gráfico 1. O termo de pesquisa que envolve este estudo, gestão do conhecimento e segurança cibernética, teve sua primeira publicação em 2014, considerando ser o tema segurança cibernética relativamente novo. O ano de 2023 apresenta dados parciais no período de coleta, mas foi mantido no Gráfico 1, considerando a importância de comparação ao ano anterior.

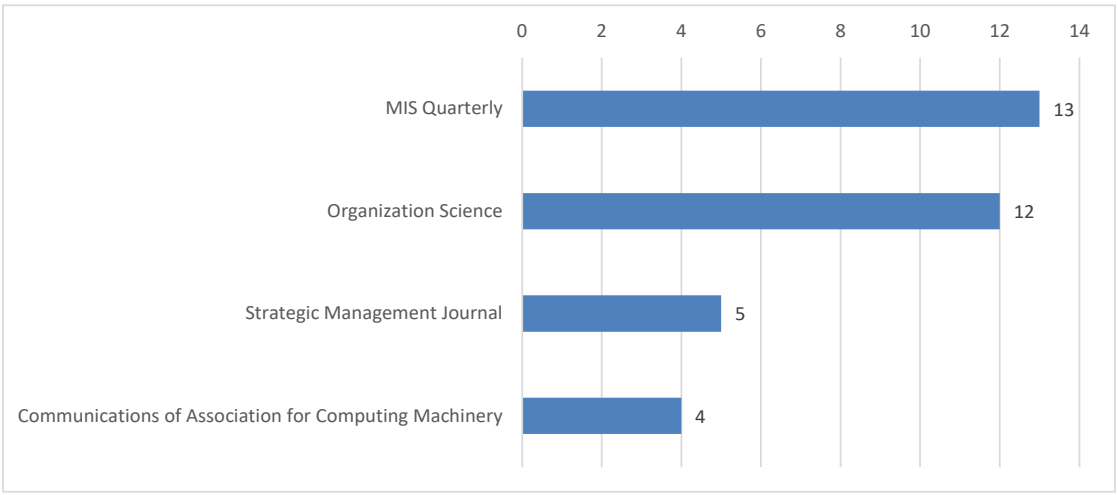
Gráfico 1 – Evolução da produção científica (2014 a 2023)



Fonte: Dados da pesquisa (2023)

Os periódicos são os meios em que os artigos são publicados. Foram avaliados os principais periódicos relacionados aos temas de pesquisa em IoT e serviços financeiros. Os periódicos de destaque citado localmente, considerando critérios de relevância, foram MIS Quarterly com 13 artigos publicados e Organization Science com 12 artigos publicados, demonstrados no Gráfico 2.

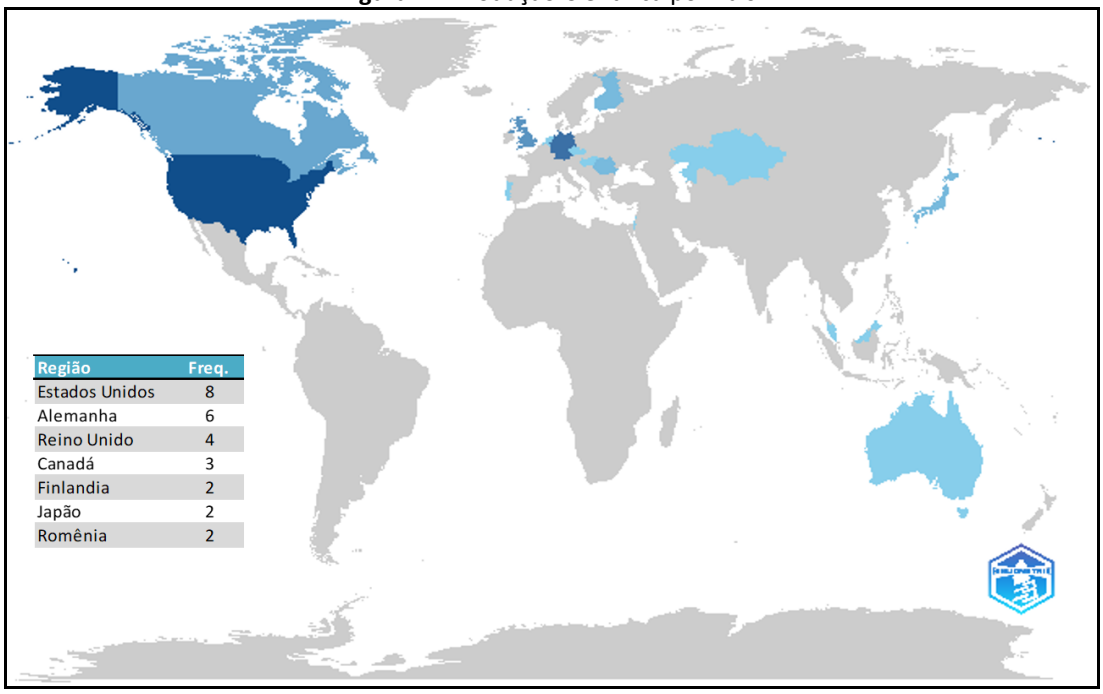
Gráfico 2 – Periódicos Mais Citados Localmente



Fonte: Web of Science (2023) e Scopus (2023)

A Figura 1 apresenta a produção científica dos sete países com maior produção, destacando os Estados Unidos com oito produções, a Alemanha com seis produções e o Reino Unido, com quatro produções. Com três produções, identificamos o Canadá e com duas produções identificamos a Finlândia, Japão e Romênia. No período analisado, foram identificados também que os países mais citados, considerando os Estados Unidos com 48 citações, o Japão com 27 citações, o Cazaquistão com 20 citações e a Alemanha com 17 citações, como os mais relevantes.

Figura 1 – Produção Científica por País.



Fonte: Web of Science (2023) e Scopus (2023)

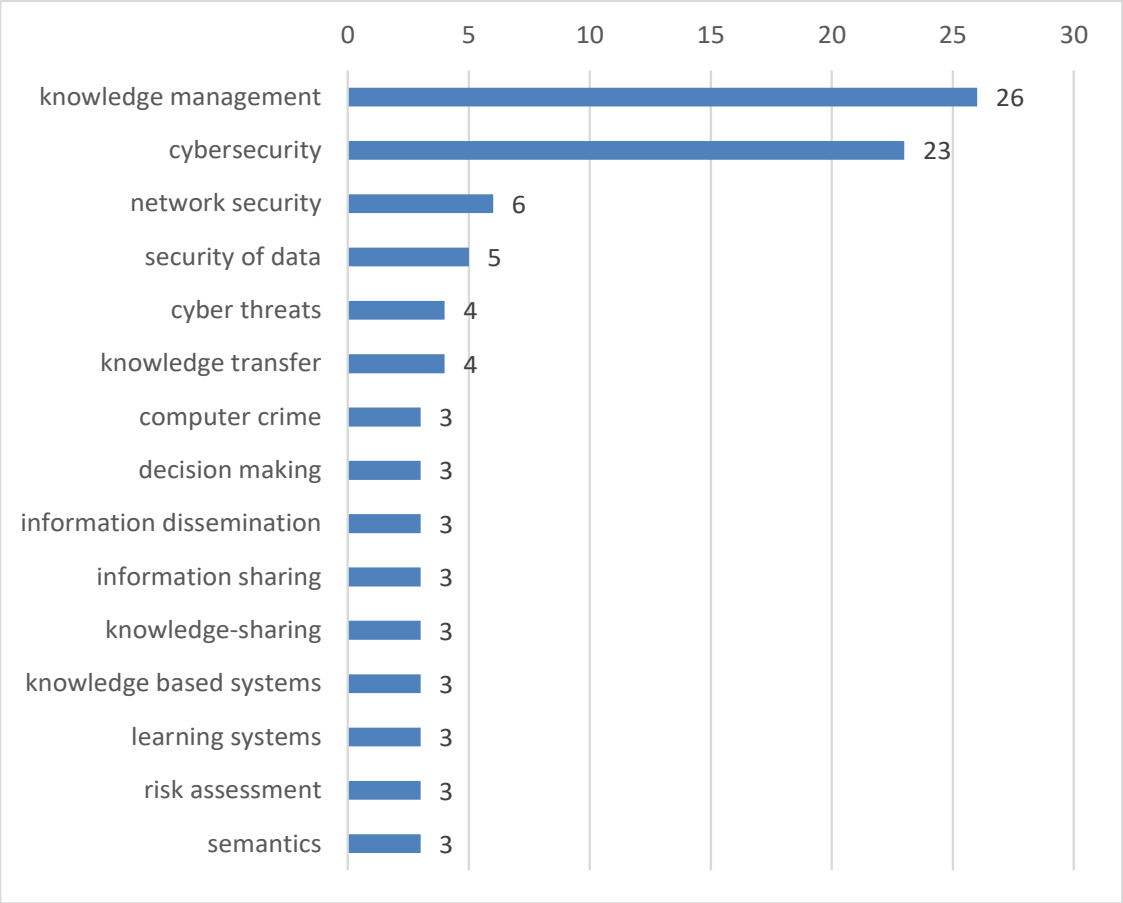
Em relação à frequência de palavras, o Gráfico 3 exibe a relevância das palavras-chave plus. As palavras-chave plus consistem em palavras e frases identificadas nos títulos dos artigos citados (Joshi, 2016). Na análise de relevância, o termo Knowledge management foi mencionado 26 vezes, cybersecurity - 23 vezes, network security - 6 vezes e security of data - cinco vezes, como os termos mais relevantes.

Mapas temáticos são muito intuitivos e permitem aos pesquisadores analisarem a evolução dos tópicos nos quatro quadrantes diferentes, identificados com base em sua centralidade (traçada no eixo X) e densidade (traçada no eixo Y). Contudo, a centralidade muda o nível de interações entre clusters, ou seja, até que ponto um tópico está conectado a outros tópicos e, por sua vez, significativo em um domínio específico (Cobo *et al.*, 2011).

Por outro lado, a densidade mede o nível de coesão *intra-cluster*, especificando na medida em que as palavras-chave em cada cluster estão conectadas e, portanto, um tema é desenvolvido. Nesse sentido, o quadrante superior direito contém temas com alta centralidade e densidade: temas que podem influenciar o campo da pesquisa e são bem desenvolvidos.

O quadrante inferior direito mostra temas transversais para uma disciplina, podendo influenciar outros tópicos (ou seja, eles têm alta centralidade), mas sendo fracamente estabelecidos internamente (ou seja, eles têm baixa densidade). O quadrante inferior esquerdo destaca tópicos que estão surgindo ou desaparecendo, pois eles têm baixa centralidade e densidade. Por fim, o quadrante superior esquerdo inclui temas de nicho entre os estudiosos, que são internamente bem desenvolvidos (alta densidade), mas não são capazes de influenciar outros temas (baixa centralidade).

Gráfico 3 – Palavras mais relevantes – palavras-chave *plus*

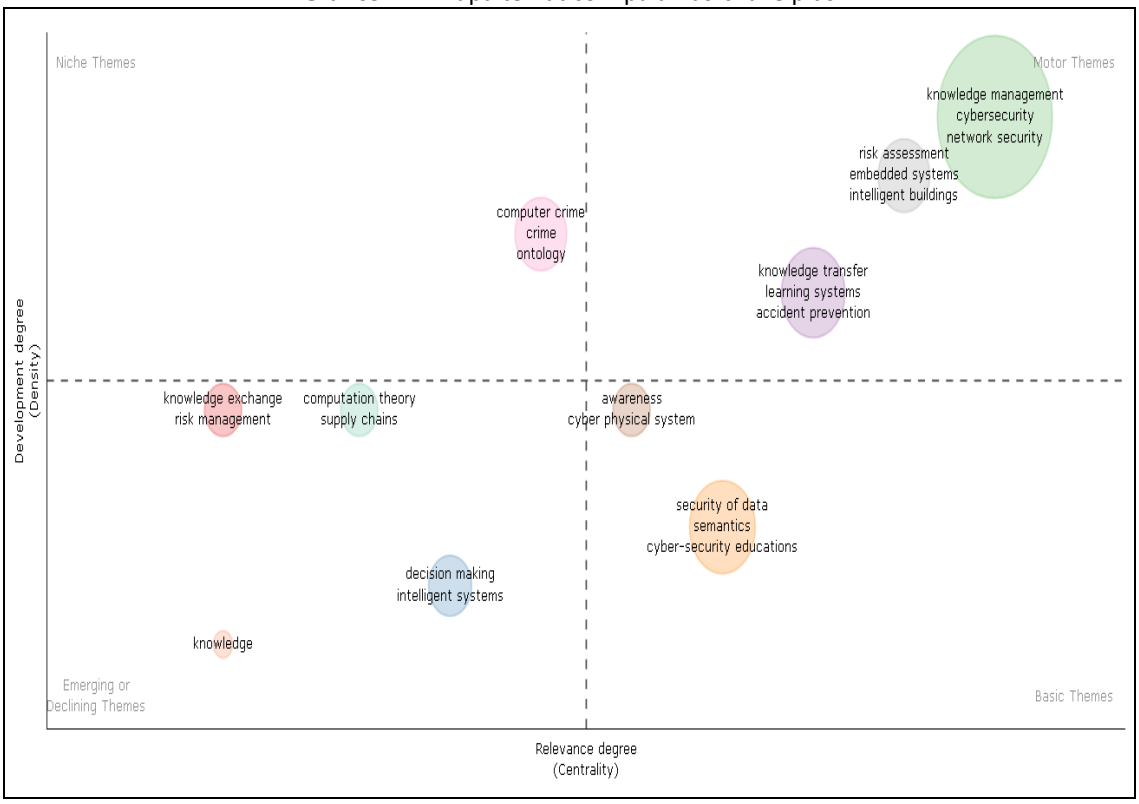


Fonte: Web of Science (2023) e Scopus (2023), Bibliometrix®

Observou-se, portanto, que como palavras-chave knowledge management, cybersecurity e network security possuem forte relacionamento, considerados temas motores durante o período analisado, no Gráfico 4. Na verdade, caracterizam-se por alta relevância e alta densidade, o que significa que podem influenciar outros temas, mas são desenvolvidos e apresentam oportunidades importantes para futuras pesquisas.

Da mesma forma, os termos *risk assessment, embedded systems e intelligent buildings*, são considerados temas motores com menor relevância, mas que são capazes de influenciar muitos outros temas. Observou-se que o quadrante superior direito contém temas motores, sugerindo que são temas capazes de influenciar o campo da pesquisa e bem desenvolvidos ao mesmo tempo. A análise do Gráfico 4 confirma a importância de aprofundar estudos envolvendo temas de gestão do conhecimento e segurança cibernética, com oportunidades e necessidades de aprofundamento.

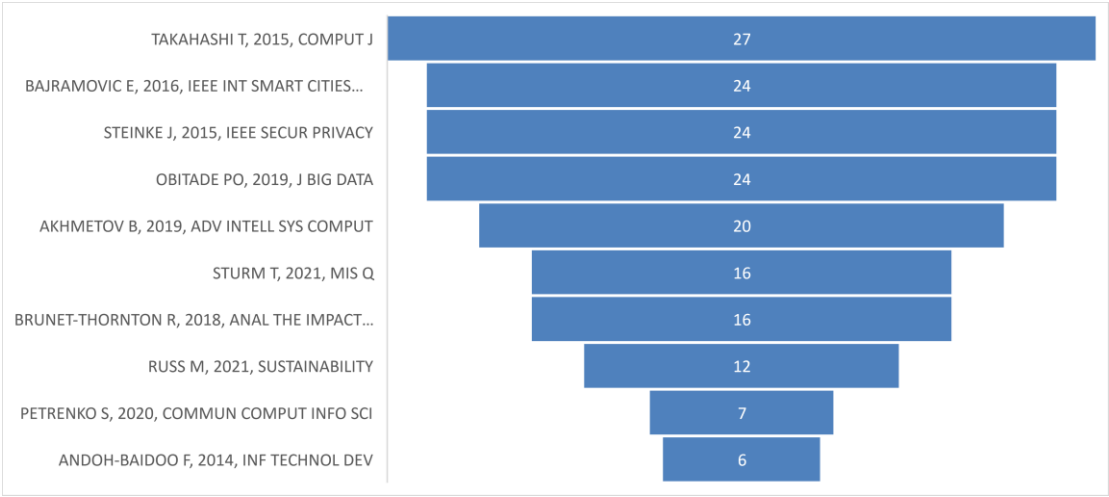
Gráfico 4 – Mapa temático – palavras-chave plus



Fonte: Web of Science (2023) e Scopus (2023), Bibliometrix®

No Gráfico 5, identificam-se os documentos mais citados globalmente, sendo que o artigo de Takahashi e Kadobayashi (2015), com 27 citações vem a ser o documento que mais contribuiu para os estudos identificados.

Gráfico 5 – Documentos mais Citados Globalmente



Fonte: Web of Science (2023) e Scopus (2023), Bibliometrix®

No processo de análise bibliométrica identifica-se um potencial considerável para aprofundar a literatura relacionada ao tema e ao objetivo do estudo, considerando o tema gestão do conhecimento e segurança cibernética, quando analisado em conjunto aos termos colaboração, compartilhamento e identidade digital.

6 DISCUSSÃO

O fator humano está no centro da discussão da gestão do conhecimento (Chen; Huang, 2009) e, da mesma forma, da segurança cibernética (Heinrich *et al.*, 2018; Vasileva, 2022). Sem as pessoas, não haveria conhecimento e sem conhecimento não haveria defesa, proteção, inteligência ou estratégia. O fator humano, na literatura, apresenta relações importantes com a vantagem competitiva (Alavi; Leidner, 2001; Heinrich *et al.*, 2018), à cultura organizacional (Mcgriff, 2000), à necessidade de maior colaboração (Takahashi; Kadobayashi, 2015), do entendimento dos comportamentos das pessoas em ações proativas de proteção, como em ações colaborativas de defesa (Patnayakuni *et al.*, 2017).

O processo de decisão apoiado pela gestão do conhecimento e das caraterísticas da segurança cibernética deixam claro que as organizações estão mudando de uma abordagem reativa para uma abordagem proativa para proteger os ativos de informações, em que identificam e respondem às ameaças antes que um invasor possa causar danos (Obitade, 2019).

A gestão do conhecimento torna-se uma ferramenta para lidar com questões de segurança cibernética, desde que enfatize os fatores sociais, organizacionais e tecnológicos inter-relacionados envolvidos na segurança cibernética. Um sistema de gestão do conhecimento é um sistema sociotécnico de desenvolvimento e compartilhamento de conhecimento que é influenciado por diversos fatores humanos e culturais da organização, bem como pelos fatores de risco e prevalência da segurança cibernética (Wang; Wang, 2021).

Aprendizagem com incidentes em questões de segurança cibernética podem ser evitados com o compartilhamento de conhecimento e experiências. Os sistemas ciberfísicos, por exemplo, fazem parte de muitas infraestruturas críticas, como automação industrial e sistemas de transporte. Assim, os incidentes de segurança direcionados aos sistemas ciberfísicos podem ter consequências prejudiciais para ativos e pessoas. Como os incidentes tendem a ocorrer novamente, compartilhar conhecimento sobre esses incidentes pode ajudar as organizações a estarem mais preparadas para prevenir, mitigar ou investigar futuros incidentes. Em síntese, os incidentes de segurança representam uma enorme ameaça para a sociedade (Alrimawi *et al.*, 2022; Patterson *et al.*, 2023).

Para Ursache (2022), uma combinação de tecnologia, sistemas de gestão do conhecimento e assimilação de novos conhecimentos é o melhor caminho para a organização se manter competitiva com inovação. No contexto de crescente digitalização das economias, a preocupação em proteger informações vem com a mesma intensidade de assegurar o conhecimento organizacional. Para ele, uma forma de assegurar o conhecimento no mundo digital, ou pelo menos experimentá-lo, é via cibersegurança, um conceito através do qual podem ser encontradas soluções inovadoras (Ursache, 2022).

Há uma percepção crescente por parte dos legisladores, especialistas em políticas e profissionais de que os riscos cibernéticos e os vetores de ameaças constituem um desafio crítico e estratégico para todas as operações espaciais. A atenção profissional e os recursos dos *stakeholders* estão começando a se concentrar em medidas baseadas no conhecimento para mitigar esses riscos e ameaças. As atividades baseadas no espaço dependem da funcionalidade confiável dos sistemas de computador e das comunicações sem fio que os conectam por meio do uso do recurso do espectro eletromagnético, todos os quais constituem partes da infraestrutura do ciberespaço na Terra e no espaço (Housen-Couriel, 2023).

Samtani *et al.* (2023) apontam em seus estudos para algumas áreas promissoras de desenvolvimento de inteligência artificial que podem trazer benefícios significativos para a gestão do conhecimento e para a segurança cibernética. Estas áreas são: (a) Inteligência de ameaças cibernéticas que se concentra na identificação de ameaças emergentes e dos principais agentes de ameaças para ajudar a permitir processos eficazes de tomada de

decisões de segurança cibernética, (b) desinformação e propaganda computacional que busca identificar conteúdos falsos ou enganosos no ciberespaço e (c) centros de operações de segurança que visam produzir recursos operacionais de segurança cibernética para muitas organizações e abrangem tarefas como gerenciamento de vulnerabilidades e gerenciamento de senhas com técnicas de análise habilitadas, como aprendizado profundo, aprendizado de máquina, ciência de rede, modelos generativos, aprendizado por reforço, análise de texto e outras técnicas, podem funcionar para o Gerenciamento Seguro de Conhecimento e, de maneira mais ampla, para a segurança cibernética (Samtani *et al.*, 2023).

São identificadas diferentes tópicos e abordagens relacionadas à importância do fator humano, cultura, comportamentos, necessidades, experiências além das questões técnicas e sociotécnicas envolvidas em todos os processos organizacionais, apontando que a vantagem competitiva, a inovação e a estratégias ganham agilidade e eficácia no uso da gestão do conhecimento para o contexto da segurança cibernética.

7 CONSIDERAÇÕES FINAIS

Este estudo fornece implicações práticas para as organizações à medida em que estas desenvolvem capacidades para competir de forma eficaz na economia digital. Primeiro, os resultados demonstram a importância da análise da gestão do conhecimento para o contexto da segurança cibernética. Os resultados demonstram que as empresas que adotam e utilizam recursos de colaboração, compartilhamento e gestão têm maior possibilidade de obter resultados em ações de segurança cibernética.

A literatura analisada sugere que, embora a gestão do conhecimento possa contribuir para um desempenho empresarial superior e melhorar a proteção cibernética, os recursos adequados precisam estar presentes em uma organização para alcançar os resultados pretendidos.

A Gestão do Conhecimento nos ambientes corporativos é de suma importância para que a organização trate das ameaças e incidentes de segurança. A organização deve empregar metodologias para que haja a criação e o compartilhamento de conhecimento entre os indivíduos e *stakeholders* em um ambiente propício para essa construção (Buogo *et al.*, 2020).

Para que os indivíduos e organizações tomem decisões coerentes no contexto da segurança cibernética é necessária a construção de modelo de gerenciamento e aprendizado, sem preconceitos organizações, encapsulado em um quadro de dilema ético (Russ, 2021).

Como contribuição são apresentadas as principais características da literatura que permeia o os temas de gestão do conhecimento, possibilitando identificar temas que podem ser aprofundados em estudos futuros, como a colaboração e o compartilhamento de conhecimento. São apresentadas ainda lacunas relacionadas ao tema de gestão de identidade com seus impactos e consequências relacionadas ao indivíduo e à gestão do conhecimento.

Com a transformação digital nas organizações, produtos e serviços, com o crescente uso de dispositivos de comunicação e de inteligência artificial, surgem diferentes forças de inovação digital, criando diferentes níveis de desafios, obtendo benefícios claros para indivíduos, clientes, serviços e organizações.

Novos estudos poderão aprofundar a investigação realizada, abordando com maior detalhe a gestão do conhecimento no contexto da segurança cibernética, focando em suas possibilidades de utilização, como transpor preconceitos organizacionais relacionados a informações confidenciais e em questões organizacionais ou individuais, como proposta de valor para a sociedade.

REFERÊNCIAS

AGRAFIOTIS, Ioannis; NURSE, Jason R. C., GOLDSMITH, Michael; CREESE, Sadie; UPTON, David. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. **Journal of Cybersecurity**, v. 4, n. 1, p. 1–15, 2018.

ALAVI, M.; LEIDNER, D. E. Knowledge management and knowledge management systems: Conceptual foundations and research issues. **MIS Quarterly**, v. 25, n. 1, p. 107, mar. 2001.

ALRIMAWI, F. *et al*. Incidents are meant for learning, not repeating: Sharing knowledge about security incidents in cyber-physical systems. **IEEE Transactions on Software Engineering**, v. 48, n. 1, p. 120–134, 2020.

ANDRADE, R. O.; YOO, S. G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. **Journal of Information Security and Applications**, v. 48, p. 102352, 2019.

ARIA, Massimo; CUCCURULLO, Corrado. bibliometrix: An R-tool for comprehensive science mapping analysis. **Journal of informetrics**, v. 11, n. 4, p. 959-975, 2017. DOI: https://doi.org/10.1016/j.joi.2017.08.007.

AUFFRET, Jean-Pierre *et al*. Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. **Journal of Interconnection Networks**, v. 17, n. 01, p. 1740001, 5 mar. 2017.

BABICEANU, R. F.; SEKER, R. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. **Computers in Industry**, v. 81, p. 128–137, 1 set. 2016.

BAKER, H. K.; KUMAR, S.; PANDEY, N. Thirty years of the Global Finance Journal: A bibliometric analysis. **Global Finance Journal**, v. 47, n. September 2019, p. 100492, 2021.

BUOGO, Mateus; FACHINELLI, Ana Cristina; GIACOMELLO, Cíntia Paese. Gestão do conhecimento e segurança da informação. **AtoZ: novas práticas em informação e conhecimento**, v. 8, n. 2, p. 49-59, 2020. DOI: http://dx.doi.org/10.5380/atoz.v8i2.69867.

CHEN, C.-J.; HUANG, J.-W. Strategic human resource practices and innovation performance — The mediating role of knowledge management capacity. **Journal of Business Research**, v. 62, n. 1, p. 104–114, jan. 2009.

COBO, M. J., LÓPEZ-HERRERA, A. G., HERRERA-VIEDMA, E., HERRERA, F. An approach for detecting, quantifying, and visualizing the evolution of a research feld: A practical application to the fuzzy sets theory feld. **Journal of Informetrics**, v. 5, n. 1, p. 146-166, 2011.

DAVENPORT, T. H.; DE LONG, D. W.; BEERS, M. C. Successful knowledge management projects. **Sloan Management Review**, v. 39, n. 2, 1998.

FISCHER, E. A. Cybersecurity issues and challenges: In Brief. **Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities**, p. 45–54, 2015.

GAN, Y.; ZHU, Z. A learning framework for knowledge building and collective wisdom advancement in virtual learning communities. **Journal of Educational Technology & Society**, v. 10, n. 1, p. 206–226, 2007.

HEINRICH, P.; UHL, A.; JOSI, M. Designing for knowledge based cyber-security-episode 1: What should we teach? **AIS electronic library (AISeL),** p. 11–28, 2018.

HOUSEN-COURIEL, D. Information sharing for the mitigation of outer space–related cybersecurity threats. **Acta Astronautica**, v. 203, p. 546–550, 1 fev. 2023.

JOSHI, A. Comparison Between Scopus & ISI Web of Science. **Journal Global Values ISSN**, v. VII, n. 1, p. 976–9447, 2016.

LECHNER, N. H. An Overview of Cybersecurity Regulations and Standards for Medical Device Software. **Central European Conference on Information and Intelligent Systems**, p. 237–249, 2017.

LEE, H.; CHOI, B. Knowledge management enablers, processes, and organizational performance: An integrative view and empirical examination. **Journal of Management Information Systems**, v. 20, n. 1, p. 179–228, 2003.

LETTIERI, S. **Segurança cibernética e inovação aliadas para uma transformação digital**. 2021. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/seguranca-cibernetica-e-inovacao-aliadas-para-uma-transformacao-digital/. Acesso em: 2 jul. 2023.

LEZZI, M.; LAZOI, M.; CORALLO, A. Computers in industry cybersecurity for industry 4.0 in the current literature: A reference framework. **Computers in Industry**, 103, 97–110, 2018.

LYKOU, G.; ANAGNOSTOPOULOU, A.; GRITZALIS, D. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. **Sensors (Switzerland)**, v. 19, n. 1, 2019.

MADNICK, S. *et al*. Measuring stakeholders' perceptions of cybersecurity for renewable energy systems. **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**, v. 10097 LNAI, p. 67–77, 2017.

MCGRIFF, S. J. Um modelo de gestão do conhecimento corporativo. **Sistemas Instrucionais Corporativos**, 2000.

MCTI. **Programa Hackers do Bem vai fortalecer a cibersegurança no país**. 2023. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/05/programa-hackers-do-bem-vai-fortalecer-a-ciberseguranca-no-pais. Acesso em: 14 jul. 2023.

OBITADE, P. O. Big data analytics: A link between knowledge management capabilities and superior cyber protection. **Journal of Big Data**, v. 6, n. 1, p. 71, 2019.

PADILHA, L. **Thales assume o controle do satélite de demonstração da ESA no primeiro exercício de segurança cibernética do seu tipo**. 2023. Disponível em: https://www.defesaaereanaval.com.br/espaco/thales-assume-o-controle-do-satelite-de-demonstracao-da-esa-no-primeiro-exercicio-de-seguranca-cibernetica-do-seu-tipo. Acesso em: 14 jul. 2023.

PATNAYAKUNI, n.; PATNAYAKUNI, r.; GUPTA, J. N. D. Towards a model of social media impacts on cybersecurity knowledge transfer. Em: **Harnessing social media as a Knowledge Management tool**. [s.l.] IGI Global, 2017. p. 249–271.

PATTERSON, C. M.; NURSE, J. R. C.; FRANQUEIRA, V. N. L. Learning from cyber security incidents: A systematic review and future research agenda. **Computers & Security**, v. 132, p. 103309, 1 set. 2023.

RADOVAN, M.; GOLUB, B. **Trends in IoT security**. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings. **Anais** [...] Institute of Electrical and Electronics Engineers Inc., 10 jul. 2017.

RUSS, M. Knowledge management for sustainable development in the era of continuously accelerating technological revolutions: A framework and models. **Sustainability**, v. 13, n. 6, p. 3353, 18 mar. 2021.

SAMTANI, S.; ZHAO, Z.; KRISHNAN, R. Secure knowledge management and cybersecurity in the era of artificial intelligence. **Information Systems Frontiers**, v. 25, n. 2, p. 425–429, 18 fev. 2023.

SANCHEZ, R.; MAHONEY, J. T. Modularity, flexibility, and knowledge management in product and organization design. **Strategic Management Journal**, v. 17, n. S2, p. 63–76, dez. 1996.

SARKER, I. H. *et al*. Cybersecurity data science: an overview from machine learning perspective. **Journal of Big Data**, v. 7, n. 1, 1 dez. 2020.

SOLMS, R. Von; NIEKERK, J. Van. From information security to cyber security. **Computers and Security**, v. 38, p. 97–102, 2013.

TAKAHASHI, T.; KADOBAYASHI, Y. Reference ontology for cybersecurity operational information. **The Computer Journal**, v. 58, n. 10, p. 2297–2312, 1 out. 2015.

TAKEUCHI, H.; NONAKA, I. Gestão do conhecimento. **Bookman Editora**, 2009.

URSACHE, V.-M. Cybersecurity challenges in the knowledge economy. **Proceedings of the International Conference on Business Excellence**, v. 16, n. 1, p. 121–129, 1 ago. 2022.

VASILEVA, V. Application of a Human-Centric Approach in Security by Design for IoT Architecture Development. Em: **Communications in Computer and Information Science**. [s.l.] Springer Science and Business Media Deutschland GmbH, v. 1596 Cusp. 13–22. 2022.

WANG, S.; WANG, H. A sociotechnical systems analysis of knowledge management for cybersecurity. **International Journal of Sociotechnology and Knowledge Development**, v. 13, n. 3, p. 77–94, 1 jul. 2021.

WARE, W. H. Security and Privacy in Computer Systems. **The Rand Corporation**, 1967.

WARE, W. H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. **The Rand Corporation**, 1970.

XIN, Y. *et al*. Machine Learning and Deep Learning Methods for Cybersecurity. **IEEE Access**, v. 6, p. 35365–35381, 2018.

ZHENG, W.; YANG, B.; MCLEAN, G. N. Linking organizational culture, structure, strategy, and organizational effectiveness: Mediating role of knowledge management. **Journal of Business Research**, v. 63, n. 7, p. 763–771, jul. 2010.

Recebido em/Received: 09/02/2024 | Aprovado em/Approved: 21/04/2024