convibra
www.convibra.org

CIBERSEGURANÇA E INOVAÇÃO EM SERVIÇOS: UM ESTUDO BIBLIOMÉTRICO

Andre Lozano Ferreira
Universidade Presbiteriana Mackenzie
andre.lozanox@gmail.com

Gilberto Perez
Universidade Presbiteriana Mackenzie
gilberto.perez@mackenzie.br

RESUMO

Com a transformação digital nas organizações e o uso crescente da internet, surgem diferentes forças de inovação digital, entre elas o uso de *machine learning*, *big data*, *Blockchain*, inteligência artificial, Internet das Coisas e o uso da nuvem, fortalecendo as forças inovadoras e, na mesma proporção, as vulnerabilidades relacionadas à cibersegurança. Assim, o objetivo principal deste estudo é investigar a cibersegurança e suas relações com a inovação digital em empresas de serviços, por meio de uma análise bibliométrica, utilizando as bases *Web of Science* e *Scopus*. A análise bibliométrica mostrou uma oportunidade que permeia os conceitos de cibersegurança e inovação em serviços e que merece um estudo profundo, com benefícios claros para a proteção de ambientes tecnológicos e infraestruturas relacionadas, gerando conhecimento e valor agregado para produtos e serviços inovadores.

Palavras-Chave: Cibersegurança, Digital, Tecnologias

CYBERSECURITY AND INNOVATION IN SERVICES: A BIBLIOMETRIC STUDY

ABSTRACT

With the digital transformation in organizations and the increasing use of the internet, different forces of digital innovation arise, including the use of machine learning, big data, Blockchain, artificial intelligence, Internet of Things, and the use of the Cloud, strengthening the innovative forces and in the same proportion the vulnerabilities related to cybersecurity. Thus, the main objective of this study is to investigate cybersecurity and its relationship with digital innovation in service companies, through a bibliometric analysis, using the Web of Science and Scopus databases. The bibliometric analysis showed an opportunity that permeates the concepts of cybersecurity and innovation in services and that deserves a deep study, with clear benefits for the protection of technological environments and related infrastructures, generating knowledge and added value for innovative products and services.

Keywords: Cybersecurity, Digital, Technologies

1 INTRODUÇÃO

A economia mundial está mudando dinamicamente com a expansão da Tecnologia da Informação (TI). A mudança não está acontecendo apenas no nível da indústria de tecnologia. Outras indústrias também estão sendo impactadas com o surgimento de fábricas inteligentes, carros autônomos, comércio eletrônico inteligente e similares (Cooke et al., 2019).

A economia torna-se cada vez mais digital com a ajuda de tecnologias digitais como nuvem, inteligência artificial, *big data*, segurança cibernética e comutação quântica, por exemplo. A forma de funcionamento dos negócios muda drasticamente. A digitalização nos ajuda a integrar as tecnologias digitais nas experiências cotidianas, com o uso de internet das coisas e a indústria 4.0. As novas tecnologias estão surgindo a cada dia e inovando as indústrias. Com as novas tecnologias, surgem novas ameaças à segurança cibernética, como acesso não autorizado, uso indevido de informações e a necessidade de proteger a infraestrutura digital (Gupta, 2019).

As economias digitais compreendem ativos digitais tangíveis e ativos digitais não tangíveis e sua infraestrutura relacionada. A transformação digital é uma tendência contínua em todas as economias e sistemas financeiros. De acordo com o relatório *Digital spillover*: Medindo o verdadeiro impacto da economia digital (Huawei Inc. e Oxford Economics, 2017), em 2017, 15,5% (US$ 12 trilhões) da economia global foi relatada como digital e, em 2025, estima-se que isso será de 25% (US$ 23 trilhões) (Unal et al., 2020).

Assim, segundo Almeida et al. (2020), à medida que a tecnologia digital avança na economia e na sociedade, suas vulnerabilidades também aumentam. Passa a ser importante proteger o ciberespaço contra incidentes, atividades maliciosas e uso indevido dos dados e ferramentas. No entanto, os incidentes de segurança cibernética, intencionais ou acidentais, estão aumentando a um ritmo alarmante e podem interromper as operações comerciais e os serviços essenciais (por exemplo, água, eletricidade, saúde). Além disso, a cibersegurança e a privacidade dos dados também serão vistas como elementos-chave na adoção de novas soluções tecnológicas e inovadoras. Não podemos, entretanto, esquecer que a digitalização traz soluções que ajudam empresas a adaptar-se e a superar desafios, por exemplo, os desafios criados pelo COVID-19 (Almeida et al., 2020).

Para Avdeeva et al. (2021), o funcionamento estável e sólido dos serviços digitais determina tendências positivas no desenvolvimento da sociedade, da informação e de seus

elementos estruturais, uma cobertura cada vez mais ampla da digitalização. Neste contexto, o problema da cibersegurança de seus recursos digitais e elementos estruturais dos sistemas da vida digital é agudo (Avdeeva et al., 2021).

A Internet das Coisas (*Internet of Things - IoT*) começa a evoluir para a internet de todas as coisas, o novo ecossistema que combina redes de sensores sem fio, computação em nuvem, dados analíticos, tecnologias interativas, bem como dispositivos inteligentes, para fornecer soluções nas quais os objetos são incorporados com conectividade de rede e um identificador para aprimorar as interações de objeto para objeto. A inovação da IoT está avançando e fornece diversas soluções ou aplicativos inteligentes. Da mesma forma, a tendência crescente de ataques cibernéticos à infraestrutura de sistemas aliada às vulnerabilidades inerentes ao sistema apresenta uma fonte de preocupação não apenas para os fornecedores, mas também para o consumidor (Tweneboah-Koduah et al., 2017).

Entretanto, o risco e a incerteza em relação à perda de privacidade tornam-se mais difíceis de medir, especialmente quando as contas de dados dos indivíduos tornam-se cada vez mais complexas. Isso torna os problemas de segurança cibernética mais difíceis de prever. Embora o risco seja sistêmico, as consequências podem ser críticas para usuários individuais, pois eles podem se tornar mais vulneráveis a ameaças de segurança cibernética. Além disso, a vulnerabilidade no nível social pode minar as instituições digitais existentes, pois as pessoas perdem a confiança no todo (Ng & Wakenshaw, 2017).

Assim, o problema da pesquisa deste estudo é identificar a relação entre inovação e cibersegurança, principalmente para empresas de serviços. A principal pergunta de pesquisa para a qual as respostas são buscadas neste estudo é: **Qual é o perfil da produção científica sobre a inovação digital em serviços e cibersegurança?**

O principal objetivo deste estudo é investigar a produção científica envolvendo cibersegurança e suas relações com a inovação digital em empresas de serviços, por meio de uma análise bibliométrica. Os objetivos específicos decorrentes do objetivo principal foram definidos de acordo com a Lei de Lotka (Lotka, 1926)a Lei de Bradford (Bradford, 1934) e a Lei Zipf (Zipf, 1949). Assim, os objetivos específicos estão relacionados à identificação da base de conhecimento dos estudos levantados, as palavras-chave mais utilizadas pelos autores, os autores mais citados, as produções científicas realizadas e as principais revistas. No

entanto, este estudo apresentará uma análise nas próximas seções, servindo como base para estudos inovadores de pesquisadores e profissionais interessados.

Este estudo é composto pela introdução, o capítulo do referencial teórico, que aprofunda o conceito relevante para o trabalho, o detalhamento do processo metodológico, análise, discussão e considerações finais.

2 REFERENCIAL TEÓRICO

2.1 Inovação

A substituição de produtos já existentes por novos produtos ocorre por conta de um agente econômico inovador, que educa os consumidores, caso seja necessário, e os ensina a desejarem novos produtos, gerando novos hábitos de consumo. Não foram as inovações que criaram o capitalismo, mas o capitalismo que criou as inovações necessárias para sua existência (Schumpeter, 1934). Desta forma, a inovação transforma o mercado e é fundamental para o desenvolvimento econômico, a inovação é tratada como um processo de destruição criadora (Hawtrey & Schumpeter, 1944).

Greenhalgh et al. (2004) apresenta um conceito de inovação em organizações de serviços como um novo conjunto de comportamentos, rotinas e formas de trabalho que visam melhorar os resultados.

Para Carlborg et al. (2014), a literatura foca no desenvolvimento de processos como área chave na qual inovação em serviços toma lugar. Entretanto, em ambientes dinâmicos em que tecnologia e mercados precisam mudar rapidamente, a gestão da inovação em serviços não significa apenas habilidade no desenho do conceito do serviço, mas também no contínuo redesenho, nova adaptação e serviços existentes para direcionar mudanças e oportunidades.

Na visão de Sundbo (1997), inovações devem ser definidas em termos de atos radicais e uma inovação não precisa ser extremamente radical. Então, em seu estudo sobre a gestão da inovação em serviços, a inovações deve estar próxima ao fenômeno da aprendizagem organizacional, mas trata o tema como de grande complexidade. A inovação, em relação a aprendizagem organizacional, cria saltos na evolução organizacional (Sundbo, 1997).

Entretanto, Teece (2010) considera que os desenvolvimentos na economia global mudaram o equilíbrio tradicional entre cliente e fornecedor. Novas tecnologias de comunicação e computação e o estabelecimento de regimes de comércio global

razoavelmente abertos significam que os clientes têm mais opções, necessidades dos clientes podem se expressar e as alternativas de fornecimento são mais transparentes. As empresas, portanto, precisam ser mais centradas no cliente, especialmente porque a tecnologia evoluiu para permitir o fornecimento de informações e soluções de clientes com custos mais baixos. Esses desenvolvimentos, por sua vez, exigem que as empresas reavaliem continuamente as propostas de valor que apresentam aos clientes e, em muitos setores, a lógica orientada pelo lado da oferta da era industrial se tornou inviável. Esse novo ambiente também amplificou a necessidade de considerar não apenas como atender às necessidades dos clientes com mais astúcia, mas também como capturar valor do fornecimento de novos produtos e serviços. Sem um modelo de negócios bem desenvolvido, os inovadores não conseguirão entregar ou capturar o valor de suas inovações. Um bom projeto e implementação de modelo de negócios, juntamente com uma análise estratégica cuidadosa, são necessários para que a inovação tecnológica tenha sucesso comercial: caso contrário, até mesmo as empresas criativas fracassarão (Teece, 2010).

2.2 Cibersegurança - Conceitos

Na atual 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 e 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).

Os ataques cibernéticos segundo Agrafiotis et al. (2018), incluem roubo de segredos corporativos, sabotagem de sistemas a fim de comprometer serviços e integridade de sistemas, e a cópia de dados de clientes para vender suas identidades na *dark web* (a fim de facilitar outros crimes) são todos exemplos dos tipos de atos que são perpetrados e podem resultar em danos a uma empresa 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 através de infraestruturas digitais, e as informações, dispositivos e aplicativos de software que essas infraestruturas são compostas. Os principais tipos de dano 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).

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 (Solms & Niekerk, 2013).

2.3 Cibersegurança e Inovação

Para Gupta (2019) as novas tecnologias inovadoras trazem novas ameaças à segurança cibernética. O acesso não autorizado, o uso indevido de informações e a necessidade de proteger a infraestrutura digital passam a necessitar de evoluções inovadoras na mesma proporção. Ter uma rede descentralizada que é fortemente criptografada permite que muitos dos medos de exploração sejam resolvidos. Os objetivos com a Indústria 4.0 precisarão se concentrar em garantir que as informações pessoais e financeiras relacionadas às empresas e seus funcionários sejam bem guardadas.

Para enfrentar esses desafios, o *Blockchain* surge como uma solução tecnológica inovadora e ampla, permitindo cadeias de valor mais ágeis, inovações de produtos mais rápidas, relacionamentos mais próximos com os clientes e integração mais rápida com a tecnologia de *IoT* e nuvem (Ahram et al., 2017).

O conceito de transformação digital global da sociedade moderna implica a introdução generalizada de tecnologias de TI em todas as áreas de sua vida, nos sistemas e infraestrutura de serviços digitais. O funcionamento estável e sólido desses serviços determina tendências

positivas no desenvolvimento da sociedade da informação e seus elementos estruturais, uma cobertura cada vez mais ampla da digitalização da infraestrutura humana. Os cyber-ataques compõem uma parte significativa das ameaças cibernéticas, enquanto as tendências para sua melhoria são tais que, no contexto do desenvolvimento de tecnologias inovadoras, as comunidades de hackers usam amplamente dispositivos digitais como fonte de ataques de computadores a elementos da infraestrutura digital da sociedade (Avdeeva et al., 2021).

Na definição de inovação apresentada por Sundbo (1997), há um relacionamento entre a inovação e a aprendizagem organizacional, suportando ao conceito de dinamismo na inovação, nos modelos de negócio e na geração de valor (Teece, 2010). Entretanto, os conceitos de cibersegurança apresentados por Solms e Niekerk (2013) e por Agrafiotis et al. (2018) apresentam modelos conceituais relacionados à proteção das organizações e das pessoas, sem considerar a aprendizagem organizacional, a agilidade e o dinamismo que a competitividade e a inovação exigem.

Em complemento, Huang e Madnick (2020) apresentam um estudo que completa este elo de relacionamentos. Gerenciar as preocupações de segurança cibernética para serviços no ambiente de negociação digital não é apenas uma questão de conformidade com a regulamentação, requer colaboração global, incluindo setores da indústria e formuladores de políticas, para trabalhar em conjunto e estabelecer regras para gerenciar sistematicamente os riscos de segurança cibernética (Huang & Madnick, 2020).

3 PROCEDIMENTOS METODOLÓGICOS

Este capítulo apresenta os procedimentos metodológicos que apoiaram o estudo bibliométrico, auxiliando na compreensão e alcance dos objetivos propostos. 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 predominantemente qualitativo, com abordagem interpretativa e construtivista. O processo 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 inovação e o papel atual desempenhado pela cibersegurança (Lezzi et al., 2018).

O processo de coleta de dados, segundo Aria e Cuccurullo (2017), 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 bilbiometrix com o uso da ferramenta R. Este pacote implementa vários testes bibliométricos. A interpretação dos resultados é meramente descritiva, mas *insights*, críticas ou previsões foram inseridas quando aplicável. Os dados fornecidos pelo software VOSviewer (https://www.vosviewer.com) também foram utilizados, de forma complementar, mas apresentando resultados relevantes para o estudo.

Na coleta de dados, os estudiosos selecionam o banco de dados que contém os dados bibliométricos, filtram o conjunto de documentos principais e exportam os dados do banco de dados selecionado. A pesquisa foi realizada nos bancos de dados da Web of Science (WoS) - Clarivate (https://www.webofscience.com/wos/woscc/basic-search) e Scopus (https://www-scopus.ez347.periodicos.capes.gov.br/) para artigos.

Como a abordagem de pesquisa relacionada à segurança cibernética e a inovação é relativamente nova, foram incluídos artigos de fontes secundárias que não são Web of Science e/ou Scopus. Por razões de relevância dos estudos, utilizou-se a ordem dos artigos por quantidade de citações. As pesquisas ocorreram entre junho e agosto de 2022.

A definição dos critérios de pesquisa utiliza as palavras-chave "*cybersecurity*", "*innovation* e "*service**", realizando a busca por tópicos para o primeiro e segundo termos e o terceiro termo realizando a busca por todos os campos, na base Web of Science. Realizando a busca por título, abstract, palavras-chave, limitado a "cp", *conference-paper*, e artigos para a base Scopus, uma vez que o volume de estudos em busca concentrada em títulos apresentou uma quantidade insuficiente de dados para as análises. O termo de pesquisa foi elaborado com as fórmulas TS=(CYBERSECURITY) AND TS=(Innovation) AND ALL=(SERVICE*) para a base de dados Web of Science e (TITLE-ABS-KEY (cybersecurity) AND TITLE-ABS-KEY (innovation) AND TITLE-ABS-KEY (service*) AND (LIMIT-TO (DOCTYPE, "cp") or limit-to (DOCTYPE, "ar")) 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 150 documentos, com a eliminação das duplicidades, restam 116 documentos, utilizando os recursos do Software R, para a análise do trabalho.

Tabela 1 – Resultados Gerais das Buscas dos Termos "cybersecurity", "innovation" e "service" nas Bases de Pesquisa *Web of Science* e *Scopus*.

Bases científicas	**Termos de pesquisa**	**Quantidade**	**Totais**
WoS	TS=(CYBERSECURITY) AND TS=(Innovation) AND ALL=(SERVICE*)	64	64
Scopus	(TITLE-ABS-KEY (cybersecurity) AND TITLE-ABS-KEY (innovation) AND TITLE-ABS-KEY (service*) AND (LIMIT-TO (DOCTYPE, "cp") or limit-to (DOCTYPE, "ar"))	86	150
Duplicidades Eliminadas		34	116

Fonte: Elaborado pelos autores.

As principais informações identificadas sobre o acervo total analisado, utilizando o Bilbiometrix, foram resumidas na Tabela 2. O período em que foram achadas publicações é de 2011 a 2022. Não foram utilizados filtros relacionados a períodos nas buscas nas bases de dados. Foram identificadas 105 revistas, 116 documentos, com um crescimento médio anual de 34,93 % das publicações. Foram identificados também 401 autores, 426 palavras-chave destes autores, 1363 referencias utilizadas e 9,776 citações médias por documento.

Tabela 2 – Principais Informações do Acervo Identificado na Pesquisa.

Item	**Informação**
Período pesquisado	2011:2022
Revistas	105
Documentos	116
Crescimento médio anual de publicações	34,93 %
Autores	401
Palavras-chave dos autores	426
Referências	1363
Média de citações por documento	9,776

Fonte: Elaborado pelos autores.

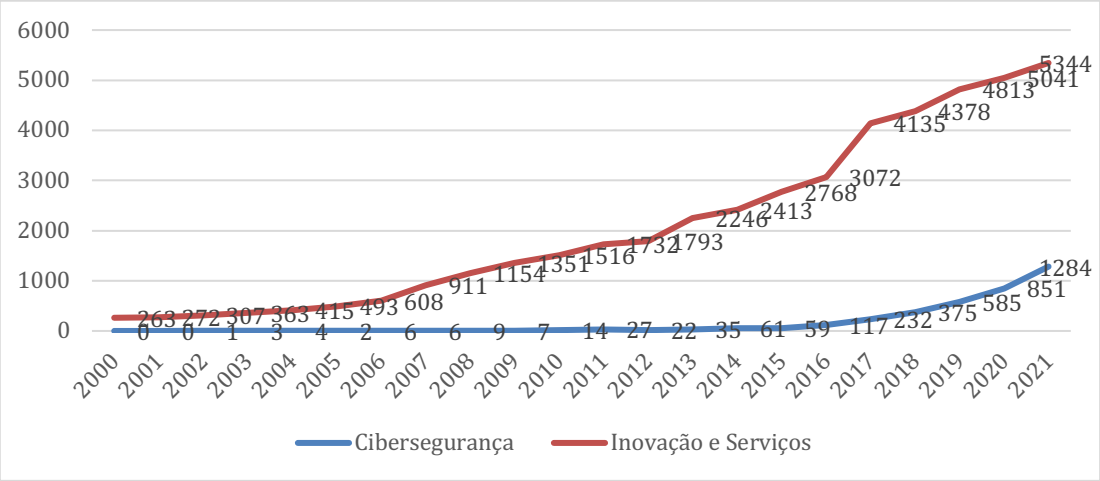
A taxa de crescimento anual média identificada na tabela 2 demonstra que existem oportunidades crescentes de análises e publicações que possam apresentar maior profundidade ao tema.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Analisando-se a produção científica entre os anos de 2000 e 2021, pode-se identificar que os termos inovação e serviços evoluíram de forma constante, com maior produção científica a partir de 2017, conforme a Figura 1. Entretanto, o termo cibersegurança apresenta um crescimento maior após o ano de 2019, demonstrando que o tema é relativamente novo e

que apresenta grandes oportunidades de crescimento. O ano de 2022 foi excluído da análise pois apresenta dados imparciais no período de coleta.

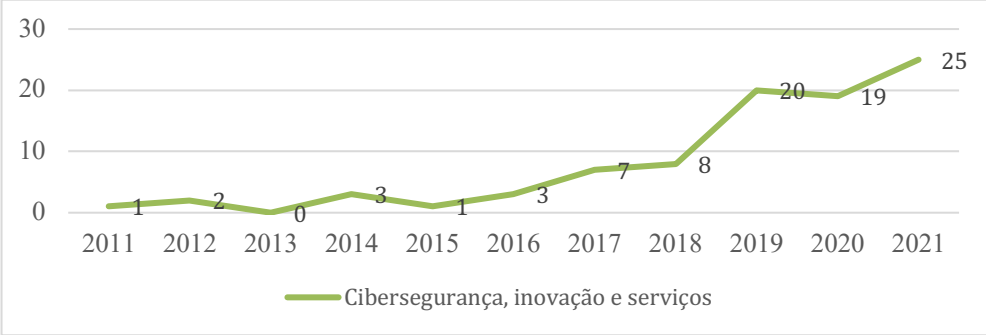
Figura 1 – Evolução da Produção Científica (2000 à 2021).



Fonte: Elaborado pelos autores.

Entretanto, na Figura 2, o termo de pesquisa que envolve este estudo, cibersegurança, inovação e serviços, teve sua primeira publicação em 2011, com aumento em 2019. O ano de 2022 foi excluído da análise pois apresenta dados imparciais no período de coleta.

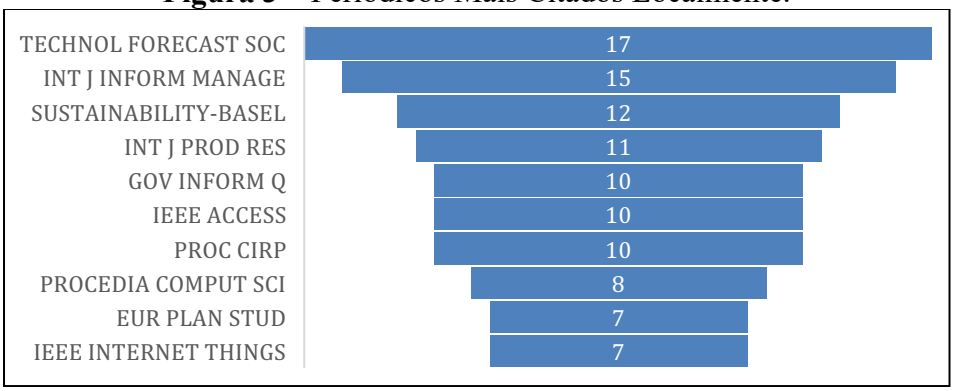
Figura 2 – Evolução da Produção Científica (2011 à 2021).



Fonte: Elaborado pelos autores.

Os periódicos são os meios onde os artigos são publicados. Foram avaliados os principais periódicos relacionados aos temas de pesquisa em segurança cibernética, inovação e serviços. O periódico de destaque citado localmente é a *Technology forecasting social change* com 17 publicações e a *International journal information management* com 15 publicações no período, demonstrados na Figura 3.

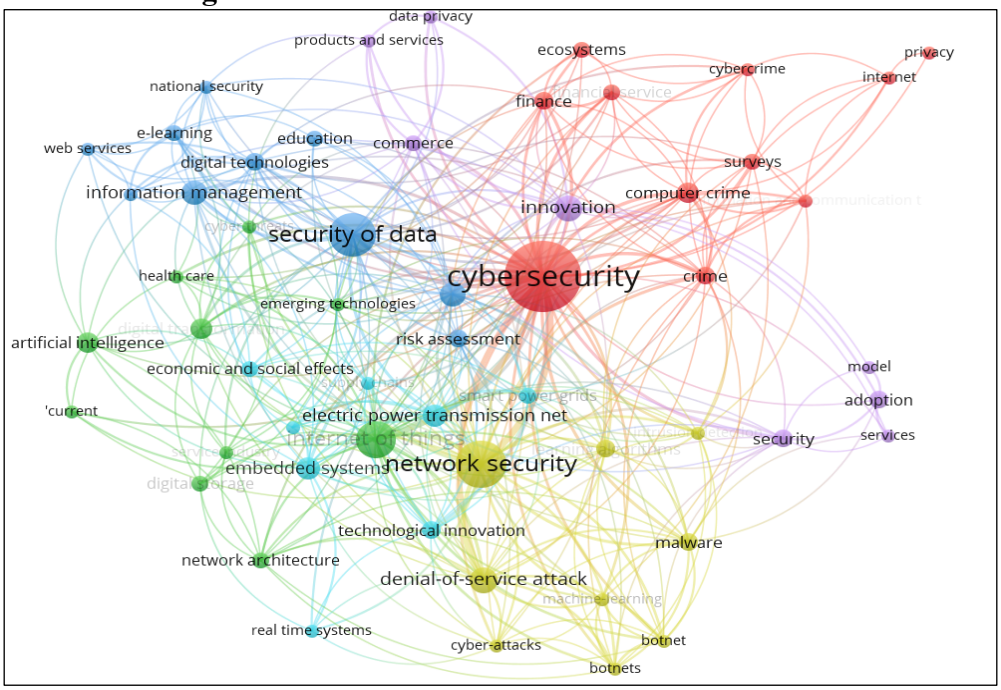
Figura 3 – Periódicos Mais Citados Localmente.



Fonte: Web of Science (2022) and Scopus (2022).

Em relação à frequência de palavras, a Figura 4 exibe a rede de palavra-chave *plus* usando o mapa de co-ocorrência. As palavras-chave *plus* consistem em palavras e frases colhidas dos títulos dos artigos citados (Joshi, 2016). Dentro da palavra-chave *plus*, o termo *cybersecurity* foi mencionado 45 vezes, *network security* - 23 vezes, *security of data* - 20 vezes e *internet oh things* -16 vezes.

Figura 4 – Co-ocorrência de Palavras-Chave *Plus*.



Fonte: Web of Science (2022) e Scopus (2022), VOSviewer.

Mapas temáticos são muito intuitivos e permitem aos pesquisadores analisar a evolução dos tópicos nos quatro quadrantes diferentes, identificados com base em sua centralidade (traçando no eixo X) e densidade (traçando no eixo Y). Mais 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.

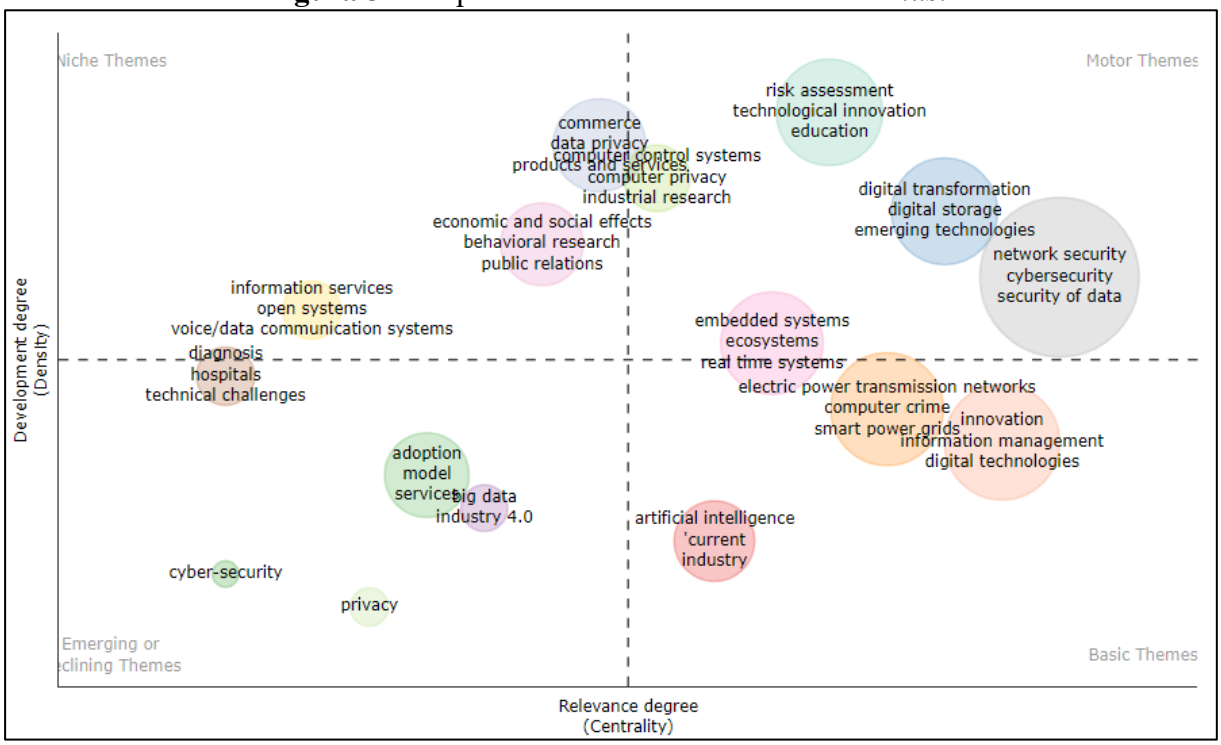
O quadrante inferior direito mostra temas transversais para uma disciplina, podendo influenciar outros tópicos (ou seja, eles têm alta centralidade), mas sendo fracamente estabelecidos internamente (ou seja, eles têm baixa densidade). O quadrante inferior esquerdo destaca tópicos que estão surgindo ou 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).

Observou-se, portanto, que como palavras-chave *network security, cybersecurity* e *security of data* possuem forte relacionamento, considerados temas motores durante o período analisado, na Figura 5. 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.

No entanto, a cybersecurity tem atraído cada vez mais atenção, tornando-se um tema motor, mas deixando *information services* e *data privacy* como temas bem desenvolvidos internamente, mas que não são capazes de influenciar muitos outros temas. Observou-se que o quadrante superior direito contém temas motores, sugerindo que temas capazes de influenciar o campo da pesquisa e bem desenvolvidos ao mesmo tempo.

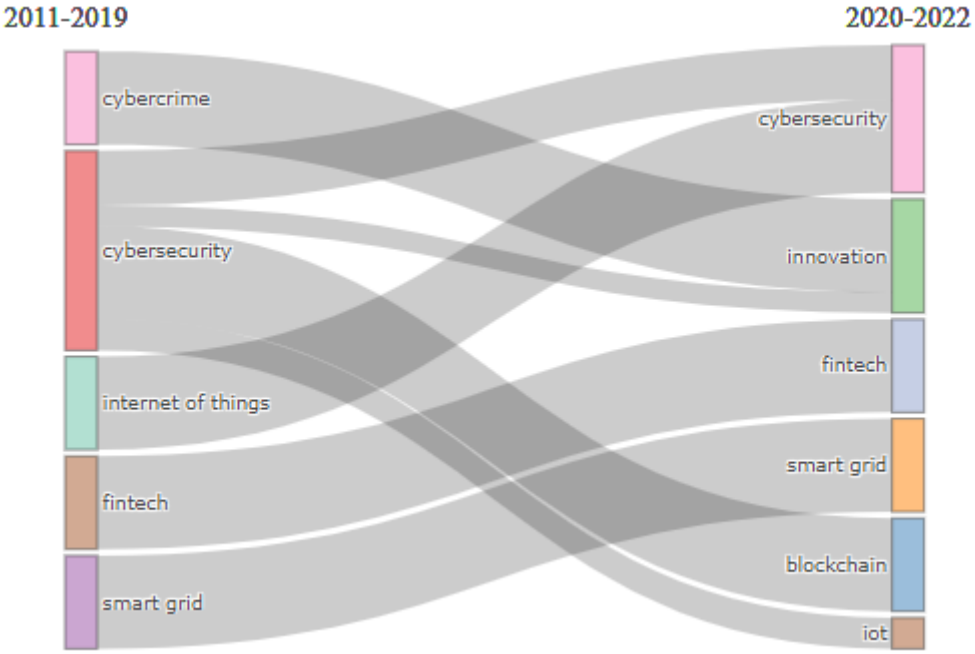
A Figura 6 apresenta a evolução temática das palavras-chave dos autores, demonstrando tendências e a evolução no período de 2011 a 2022. Os termos *cybercrime* migra para inovação e *cybersecurity* para *blockchain*. Esta análise confirma a importância de aprofundar estudos envolvendo temas de cibersegurança e inovação em organizações de serviços, com oportunidades e necessidades de aprofundamento.

Figura 5 – Mapa Temático das Palavras-Chave *Plus*.



Fonte: Web of Science (2022) e Scopus (2022), Bibliometrix.

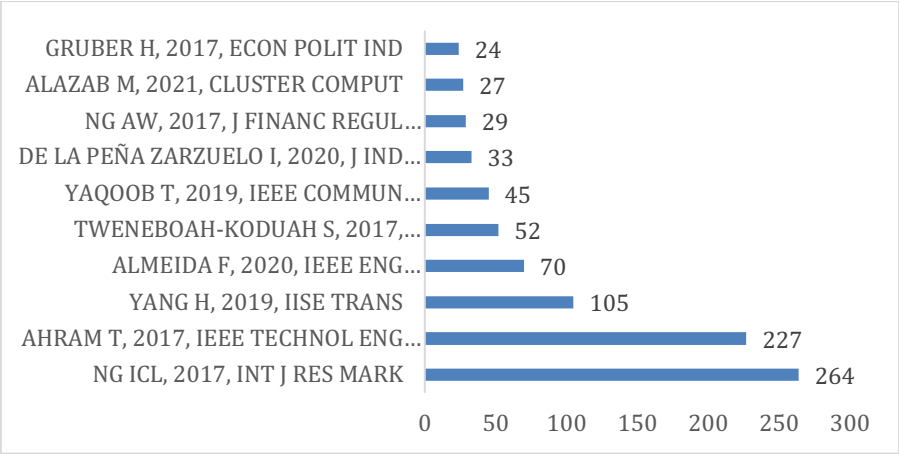
Figura 6 – Evolução temática das Palavras-chave dos Autores identificados na Pesquisa.



Fonte: Web of Science (2022) e Scopus (2022), Bibliometrix.

Na Figura 7 identificaram-se os documentos mais citados globalmente, sendo que Ng e Wakenshaw (2017) com 264 citações vem a ser o documento que mais contribuiu para os estudos identificados, Ahram et al. (2017) com 227 citações e Yang et al. (2019) com 105 citações são os mais relevantes.

Figura 7 – Documentos Mais Citados Globalmente.



Fonte: Web of Science (2022) e Scopus (2022), Bibliometrix.

Por fim, os principais autores analisados identificados foram Amro A., Anagnostopoupou A., Cooke P., Dooly Z., Gritzalis D., Lykou G., Pitner T., Power J. e Soloviev V. com 2 publicações cada.

No processo de utilização da linguagem R, foi possível criar uma base de dados única, excluir duplicidades e realizar revisões, bem como, a geração de um arquivo compatível com Bibliometrix e VOSviewer, garantindo sua integridade.

5 CONSIDERAÇÕES FINAIS

A análise bibliométrica mostrou uma oportunidade que permeia os conceitos de cibersegurança e inovação em serviços e que merece um estudo profundo, com benefícios claros para a proteção de ambientes tecnológicos e infraestruturas relacionadas, gerando conhecimento e valor agregado para produtos e serviços inovadores.

Com a transformação digital nas organizações, produtos e serviços, com o crescente uso de dispositivos de comunicação, com a chegada do 5G surgem diferentes forças de inovação digital, entre elas o uso de *machine learning*, o uso de *big data*, o desenvolvimento do *Blockchain*, o fortalecimento da indústria 4.0, a inteligência artificial, a *internet of things* e

o uso da nuvem, cada um com suas forças inovadoras e vulnerabilidades aos ataques cibernéticos (Araujo Cruz et al., 2021).

À medida que as organizações caminham para a era de *Internet* das Coisas, surge uma ruptura em um nível schumpeteriano que está em andamento. Como um exemplo simples, o copo em sua mesa contém informações sobre seu conteúdo, volume, cor e localização. Em um mundo analógico, essa informação só é conhecida por você, pois somente você é capaz de vê-la. Em um mundo digital, todas as informações sobre esse copo podem ser "vistas" por qualquer outra pessoa. O impulsionador das ações em uma era de *IoT* pode não ser a privacidade, mas a vulnerabilidade do ponto de vista da organização ou do indivíduo. O risco e a incerteza em relação à perda de privacidade tornam-se mais difíceis de medir, especialmente quando as contas de dados dos indivíduos se tornam cada vez mais complexas. Isso torna os problemas de segurança cibernética mais difíceis de prever (Ng & Wakenshaw, 2017).

Com o rápido avanço da *IoT*, por exemplo, prevê-se que a indústria de manufatura terá um número crescente de dispositivos, aplicativos e serviços baseados em *IoT* nos próximos anos. Como os equipamentos de fabricação fazem parte da infraestrutura crítica para o crescimento econômico, eles podem facilmente se tornar alvo de invasores mal-intencionados. A interconexão de dispositivos *IoT*, bancos de dados em nuvem e redes de informação torna o sistema *IoT* vulnerável a ataques cibernéticos. Portanto, a segurança cibernética da *IoT* é a principal preocupação na fabricação inteligente (Yang et al., 2019).

A pesquisa realizada por Ahram et al. (2017) indica que o *Blockchain* pode desempenhar um papel fundamental na transformação da digitalização de indústrias e aplicativos, permitindo estruturas de confiança seguras, criando uma produção ágil da cadeia de valor e uma integração mais estreita com tecnologias como computação em nuvem e *IoT*.

Gerenciar a segurança cibernética no ambiente digital não é apenas uma questão de conformidade com a regulamentação, requer colaboração global, incluindo setores da indústria e formuladores de políticas, para trabalhar em conjunto e estabelecer regras para gerenciar sistematicamente os riscos de segurança cibernética (Huang & Madnick, 2020).

O estudo apresentou os principais fatores relacionados à cibersegurança e inovação em serviços, fortalecendo as necessidades de ações colaborativas e conjuntas, envolvendo stakeholders e todo o ecossitema organizacional.

Novos estudos poderão aprofundar as relações entre a cibersegurança e a inovação em serviços, focando nas questões organizacionais e individuais, como proposta de valor para a sociedade.

REFERÊNCIAS

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017*, 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

Almeida, F., Duarte Santos, J., & Augusto Monteiro, J. (2020). The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World. *IEEE Engineering Management Review*, *48*(3), 97–103. https://doi.org/10.1109/EMR.2020.3013206

Araujo Cruz, A. R. S., Gomes, R. L., & Fernandez, M. P. (2021). An Intelligent Mechanism to Detect Cyberattacks of Mirai Botnet in IoT Networks. *Proceedings - 17th Annual International Conference on Distributed Computing in Sensor Systems, DCOS 2021*, 236–243. https://doi.org/10.1109/DCOSS52077.2021.00047

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. https://doi.org/https://doi.org/10.1016/j.joi.2017.08.007

Avdeeva, I., Golovina, T., Guzhina, G., Sulima, E., Suhanov, D., & Tihanov, E. (2021). The concept of preventive cybersecurity management of the IoT device market in the digital economy. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3487757.3490859

Baker, H. K., Kumar, S., & Pandey, N. (2021). Thirty years of the Global Finance Journal: A bibliometric analysis. *Global Finance Journal*, *47*(September 2019), 100492. https://doi.org/10.1016/j.gfj.2019.100492

Bradford, S. C. (1934). Sources of information on specifc subjects. *Engineering*, *137*, 85–86.

Carlborg, P., Kindstrom, D., & Kowalkowski, C. (2014). The evolution of service innovation research: A critical review and synthesis Per Carlborg Department of Management and Engineering. *The Service Industries Journal*, *34*(5), 373–398.

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). 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*, *5*(1), 146/166. https://doi.org/https://doi.org/10.1016/j.joi.2010.10.002

Cooke, P., Zhao, X., Yun, J. J., & Kim, Y. (2019). The digital, quaternary or 4.0 web economy: aspects, effects and implications. *International Journal of Knowledge-Based Development*, *10*(3), 193. https://doi.org/10.1504/ijkbd.2019.10024722

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of innovations in service organizations: Systematic review and recommendations. *Milbank Quarterly*, *82*(4), 581–629. https://doi.org/10.1111/j.0887-378X.2004.00325.x

Gupta, G. (2019). Education and digital economy: Trends, opportunities and challenges. *ACM International Conference Proceeding Series*, 88–92. https://doi.org/10.1145/3340997.3341013

Hawtrey, R. G., & Schumpeter, J. (1944). Capitalism, Socialism and Democracy. *Economica*, *11*(41), 40. https://doi.org/10.2307/2549943

Huang, K., & Madnick, S. (2020). Cyber securing cross-border financial services: The need for a financial cybersecurity action task force. *Journal of Information Systems Security*, *16*(2), 79–97. https://doi.org/10.2139/ssrn.3544325

Huawei Inc. and Oxford Economics. (2017). *Digital spillover: Measuring the impact of the digital economoy*. https://www.huawei.com/minisite/gci/en/digital-spillover/index.html

Joshi, A. (2016). Comparison Between Scopus & ISI Web of Science. *Journal Global Values ISSN*, *VII* (1), 976–9447.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Computers in industry cybersecurity for industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, *16*(12), 317–323.

Ng, I. C. L., & Wakenshaw, S. Y. L. (2017). The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing*, *34*(1), 3–21. https://doi.org/10.1016/j.ijresmar.2016.11.003

Schumpeter, J. (1934). The theory of economic development. In *Harvard University Press*. https://doi.org/10.4324/9781003146766

Solms, R. von, & Niekerk, J. van. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sundbo, J. (1997). Management of innovation in services. *Service Industries Journal*, *17*(3), 432–455. https://doi.org/10.1080/02642069700000028

Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning*, *43*(2–3), 172–194. https://doi.org/10.1016/j.lrp.2009.07.003

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber Security Threats to IoT Applications and Service Domains. *Wireless Personal Communications*, *95*(1), 169–185. https://doi.org/10.1007/s11277-017-4434-6

Unal, D., Hammoudeh, M., & Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. *ICT EXPRESS*, *6*(1), 43–47. https://doi.org/10.1016/j.icte.2019.07.002

Yang, H., Kumara, S., Bukkapatnam, S. T. S., & Tsung, F. (2019). The internet of things for smart manufacturing: A review. *IISE TRANSACTIONS*, *51*(11), 1190–1216. https://doi.org/10.1080/24725854.2018.1555383

Zipf, G. K. (1949). Human behavior and the principle of least effort. In *Addison-Wesley*.