RMP
Revista dos Mestrados Profissionais
UFPE / CCSA – MGP
https://periodicos.ufpe.br/revistas/rmp
ISSN – 2317 - 0115
V. 11 - n. 2 (2022)
Recife – PE

Cibersegurança em serviços: um estudo *bibliométrico*

André Lozano Ferreira, Universidade Presbiteriana Mackenzie
https://www.orcid.org/0000-0002-9260-499X - andre.lozanox@gmail.com
Fabio Marton, Universidade Presbiteriana Mackenzie
https://www.orcid.org/0000-0001-9298-8535 - fabiomarton@hotmail.com
Gilberto Perez, Universidade Presbiteriana Mackenzie
https://www.orcid.org/0000-0002-6624-0643 - gilberto.perez@mackenzie.br

Resumo: A economia digital se fundamenta nas tecnologias modernas. A disponibilidade de serviços da *web* está mudando a forma como os humanos dependem de dados e recursos de computação em geral. Um esforço adicional para a garantia da segurança e da privacidade em serviços está surgindo. Assim, o problema da pesquisa é identificar a literatura que envolve a *cibersegurança* em serviços. Utilizou-se a *bibliometria* para análise, com um modelo predominantemente qualitativo, com uso das bases *Scopus* e *Web of Science*. O estudo apresenta os principais fatores relacionados à *cibersegurança* em serviços e as necessidades de ações em todas as frentes, incluindo o setor financeiro, serviços digitais, saúde, *cibersegurança*, serviços essenciais e *stakeholders*.

Palavras-chave: *Cibersegurança*, Serviços, Riscos Cibernéticos.

Cybersecurity in Services: A Bibliometric Study

Abstract: The digital economy is based on modern technologies. The availability of web services is changing the way humans rely on data and computing resources in general. An additional effort to ensure security and privacy in services is emerging. Thus, the problem of research is to identify the literature that involves cybersecurity in services. Bibliometric was used for analysis, with a predominantly qualitative model, using the Scopus and Web of Science databases. The study presents key factors related to cybersecurity in services and the needs of actions on all fronts, including the financial sector, digital services, health, cybersecurity, essential services, and stakeholders.

Keywords: Cybersecurity, Services, Cyber-risk.

Data da Submissão: 31/07/2022 **Data de aceitação**: 30/11/2022

https://doi.org/10.51359/2317-0115.2022.256796

1. Introdução

A economia digital se fundamenta nas novas tecnologias. Em geral, segundo Lettieri (2021), constitui-se de 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 do 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 por meio de interfaces digitais.

A resposta aos riscos está dividida em 4 categorias: evitar, reduzir, compartilhar e aceitar; evitar os riscos está ligado a descontinuação da atividade que gera riscos. Reduzir ou minimizar os riscos está ligado a medidas que tem por finalidade a redução da probabilidade de sua ocorrência e/ou impactos destes. Compartilhar riscos, também atua na linha da redução do impacto, mas neste caso, pelo do compartilhamento destes, como por exemplo a contratação de apólices de seguros. Quanto a aceitar os riscos, neste caso nenhuma medida é tomada para redução de probabilidade ou impacto, o risco é aceito como parte da atividade (COSO, 2007).

Utilizando como base a categoria de minimizar os riscos relacionados a ataques pela Internet, a organização deve desenvolver a melhor abordagem possível e mais econômica para a segurança cibernética (MADNICK et al., 2017). Além disso, segundo Madnick *et al.* (2017) à medida que as organizações evoluem para empresas estendidas, mais amplas em sua cadeia de valores, o que inclui laços com fornecedores, clientes e outros parceiros, há um aumento significativo no número de agentes e uma gama mais ampla de complicações e requisitos de segurança.

Entretanto, muitas empresas vêm investindo em diferentes plataformas para escalar rapidamente seus negócios, mas não investem adequadamente em um dos fatores primordiais no mundo atual: a segurança cibernética (LETTIERI, 2021).

Da mesma forma, Ambore *et al*. (2016) defendem que os avanços na computação móvel podem ser uma grande oportunidade de fornecer serviços para metade da população mundial. No entanto, as preocupações com a segurança cibernética no ecossistema de computação móvel formam uma barreira na adoção dos serviços digitais.

A disponibilidade de serviços da *web* está mudando a forma como os humanos dependem de dados e recursos de computação em geral. As infraestruturas em nuvem deram impulso adicional ao uso de serviços, exigindo um esforço adicional para a garantia da segurança e da privacidade do serviço de computação, ou seja, que a tecnologia funcione como pretendido. Existe uma necessidade amplamente aceita de metodologias para verificar a segurança e privacidade dos serviços. Um serviço típico requer dados do usuário e os disponibiliza pela Internet independentemente das plataformas de acesso ou localização do usuário, mas o leigo raramente está ciente dos riscos envolvidos e raramente age com cautela. O sistema combinado humano-tecnologia é complexo: ele entrelaça os protocolos técnicos que estabelecem as propriedades técnicas de segurança e privacidade, com os protocolos sociais que regulam as atitudes e o comportamento humano com os computadores (BELLA et al., 2014).

Outra dinâmica relevante para o presente estudo está associada ao aumento do foco que as empresas colocam em oferecer experiências diferenciadas aos clientes. Isso parece sugerir um papel maior para a segurança cibernética nas maneiras pelas quais as empresas constroem confiança e lealdade com seus clientes. Além disso, a segurança é percebida cada vez mais

como uma jornada, na qual transações e pontos de contato podem representar vulnerabilidades exploráveis (BONGIOVANNI, 2020).

No contexto da pandemia do COVID-19, não apenas se intensificou a transição para formas remotas de atendimento em várias esferas da sociedade, como também se agravou o problema da vulnerabilidade dos serviços virtuais e, principalmente, dos serviços oferecidos pelos bancos (DUDIN et al., 2021). Neste sentido, Elsayed e Zulkernine (2018) apresentam a possibilidade de fornecer a segurança cibernética como um serviço, minimizando a crescente expansão do cenário de ameaças no contexto interno e externo e a crescente escassez de recursos de segurança cibernética, como ferramentas e habilidades, uma lacuna premente nas organizações.

Assim, com este estudo, se propõe identificar a literatura que aborda questões relacionadas com a *cibersegurança* em serviços, principalmente diante do contexto apresentado. A questão de pesquisa para a qual as respostas são buscadas neste estudo é: qual é o perfil da produção científica sobre a *cibersegurança* em serviços?

O principal objetivo deste estudo é investigar a produção científica envolvendo *cibersegurança* em 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 de Zipf (ZIPF, 1949). Assim, os objetivos específicos estão relacionados à identificação da base de conhecimento dos estudos pesquisados, 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 futuros de pesquisadores e profissionais interessados.

Este estudo é composto por esta introdução, conceitos, que aprofunda a teoria relevante para o trabalho, o detalhamento da metodologia, resultados e conclusão.

2. Apresentação dos conceitos

Esta seção dedica-se a introduzir os conceitos de suporte à pesquisa.

2.1 *Cibersegurança*

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). Em seguida, Ware (1970) apresenta um relatório sobre controles de segurança para sistemas de computador e enfatiza que o design de um sistema seguro deve fornecer proteção contra os vários tipos de vulnerabilidades, como divulgação acidental, penetração deliberada, infiltração ativa e ataque físico (LECHNER, 2017).

Na literatura atual, 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 furto 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 *cibersegurança* tenham sido aprimoradas, para Andrade e Yoo (2019), é necessário considerar o estabelecimento 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 e ataques remotos.

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).

2.2 Segurança cibernética em serviços

Uma grande parte dos setores de serviços é dominada por fornecedores, incluindo serviços públicos e sociais, como saúde, educação, administração pública, serviços pessoais (hotéis e restaurantes, domésticos, manutenção) e serviços de distribuição. As características desses setores, amplamente heterogêneos em termos de tamanho das empresas, dependem principalmente da tecnologia adotada no setor (GALLOUJ; SAVONA, 2009).

Recentemente, os avanços na computação móvel apresentaram uma grande oportunidade de fornecer serviços para metade da população mundial que atualmente não tem acesso a este tipo de serviço, por exemplo, o serviço móvel financeiro. No entanto, as preocupações com a segurança cibernética no ecossistema de computação móvel desaceleraram este interesse (AMBORE et al., 2016).

No contexto da pandemia do COVID-19, não apenas se intensificou a transição para formas remotas de atendimento em várias esferas da sociedade, como também se agravou o

problema da vulnerabilidade dos serviços virtuais e serviços oferecidos por Bancos (DUDIN; SHKODINSKII; USMANOV, 2021).

Entretanto, a indústria da Internet das Coisas (IoT) cresce rapidamente devido a sua característica de serviços críticos de negócios. A adoção da IoT gera dois tipos de desafios: riscos de segurança cibernética e preocupações com a privacidade (FELTUS et al., 2018).

A atividade *cibercriminosa* está representando grande ameaça à perda de informações confidenciais e apresentando grandes desafios às empresas e organizações. As empresas de serviços financeiros são os principais alvos e essas empresas têm sofrido perdas significativas. Esse cenário mundial merece um olhar mais atento sobre o comportamento dos *cibercriminosos*, a fim de averiguar possíveis intervenções e medidas preventivas tratadas como segurança cibernética em serviços (NAGURNEY, 2015).

3. Procedimentos Metodológicos

Nesta seção apresentam-se 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. 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 literatura de *cibersegurança* em serviços (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. Definem-se os critérios de pesquisa, seleção de artigos e, por fim, avaliação de estudos. Toda a análise principal foi construída com o apoio do pacote *bibliométrico* chamado Bibliometrix® 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® 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* e *Scopus*, por considerar que as bases são amplas o suficiente para o estudo desenvolvido. As pesquisas ocorreram em agosto de 2022.

A definição dos critérios de pesquisa utiliza as palavras-chave: *cybersecurity* e *service*, realizando a busca por tópicos na base *Web of Science*. Em seguida, realizando a busca por título, abstract, palavras-chave, limitado a cp (*conference paper*) e ar (artigos), entre outros, para a base *Scopus*, uma vez que o resultado da busca apresentava títulos divergentes em sua plenitude para o estudo em levantamento. O termo de pesquisa foi elaborado com as fórmulas apresentadas na tabela 1.

A tabela 1 apresenta os totais da busca em cada etapa do processo, sendo a unificação das bases *WoS e Scopus* totalizam 3.624 documentos, com a eliminação das duplicidades, restam 2.612 documentos na base unificada, utilizando os recursos do *software* R. O filtro (1) e o filtro (2) foram aplicados à base de dados unificada. O filtro (1) tratou da eliminação de títulos que não tenham relação com a pesquisa ou qualquer relação com o objetivo do estudo por meio da leitura individual. O objetivo era identificar a *cibersegurança* em serviços e títulos com abordagens locais ou estritamente técnicos, como *Privacy concerns in China's smart city campaign the deficit of China's cybersecurity law* e *Securing pinbased authentication in smartwatches with just two gestures* foram desconsiderados, antes mesmo da leitura dos resumos. O filtro (2) tratou da análise dos resumos de cada um dos artigos restantes, totalizando 37 documentos ao final do processo.

Tabela 1: Quantidades de estudos.

Bases científicas	**Termos de pesquisa**	**Quantidade**
WoS	TS=(cybersecurity) AND TS=(service*)	1.333
Scopus	(TITLE-ABS-KEY (cybersecurity) AND TITLE-ABS-KEY (service*)) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "MATH") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "PHYS") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "MATE") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "MULT")) AND (LIMIT-TO (LANGUAGE , "English"))	2.291
Duplicidades eliminadas		-1.012
	Subtotal	*2.612*
Filtro (1): Análise de títulos		-2.523
Filtro (2): Análise de Resumos		-52
	Total final	**37**

Fonte: Autores (2022).

As principais informações identificadas sobre o acervo total analisado, utilizando o Bilbiometrix® estão resumidas na tabela 2. O período em que foram encontradas publicações vai de 1999 a 2022. Não foram utilizados filtros relacionados a períodos nas buscas nas bases de dados utilizadas.

Tabela 2: Principais informações do acervo

Item	**Informação**
Período pesquisado	1999:2022
Revistas	34
Documentos	37
Crescimento médio anual de publicações	22,28 %
Autores	116
Palavras-chave dos autores	132

Item	Informação
Referências	493
Idade média dos documentos	2,44
Média de citações por documento	4,865

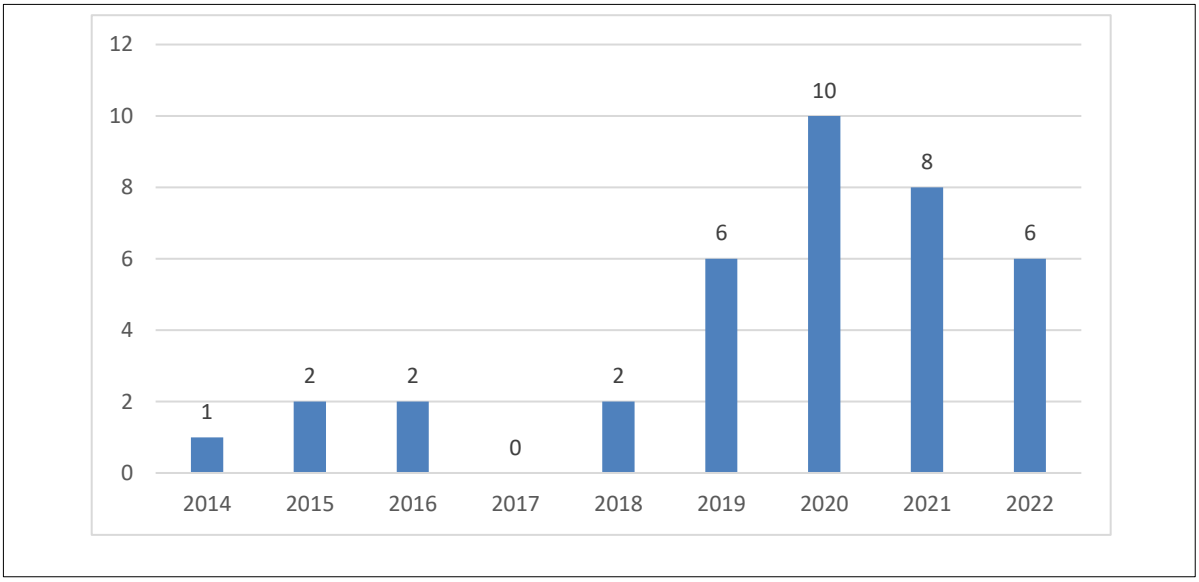
Fonte: Autores (2022).

A idade média dos documentos, apresenta a informação de que a literatura é relativamente recente. 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. Resultados

Analisando-se a produção científica entre os anos de 1999 e 2022, pode-se identificar que os termos *cibersegurança* e serviços evoluíram de forma mais acentuada após o ano de 2019, conforme a figura 1. Entretanto, o maior crescimento ocorre no ano de 2020, demonstrando que o tema é relativamente novo e que apresenta grandes oportunidades de crescimento. O ano de 2022 apresenta dados parciais no período de coleta, considerando a data de elaboração.

Figura 1: Evolução da produção científica (1999 a 2022).

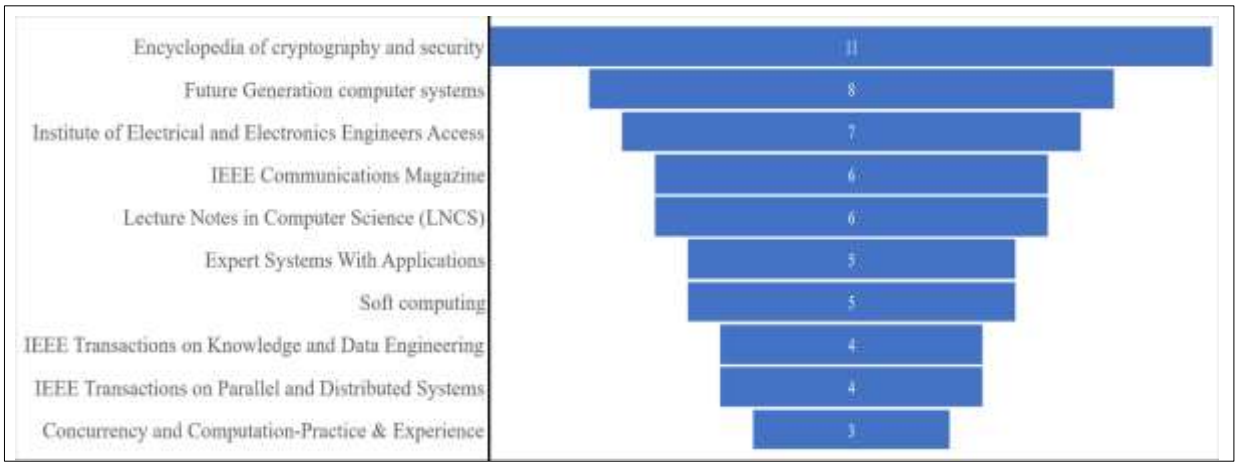


Os periódicos são os meios em que os artigos são publicados. Foram avaliados os principais periódicos relacionados aos temas de pesquisa em segurança cibernética e serviços. O periódico de destaque citado localmente é a *Encyclopedia of cryptography and security* com 11 citações e a *Future generation computer systems* com 8 citações no período, demonstradas na figura 2.

Em relação à frequência de palavras, a figura 3 exibe a rede de palavra-chave *plus* usando o mapa de *coocorrência*. As palavras-chave *plus* consistem em palavras e frases colhidas dos títulos, resumos e palavras-chave dos artigos citados (JOSHI, 2016). Dentro da palavra-chave *plus*, o termo *cybersecurity* foi mencionado 10 vezes, *security of data* - 5 vezes, *ecossystems* – 3 vezes, *finance* - 3 vezes e *cyber-attacks* - 2 vezes.

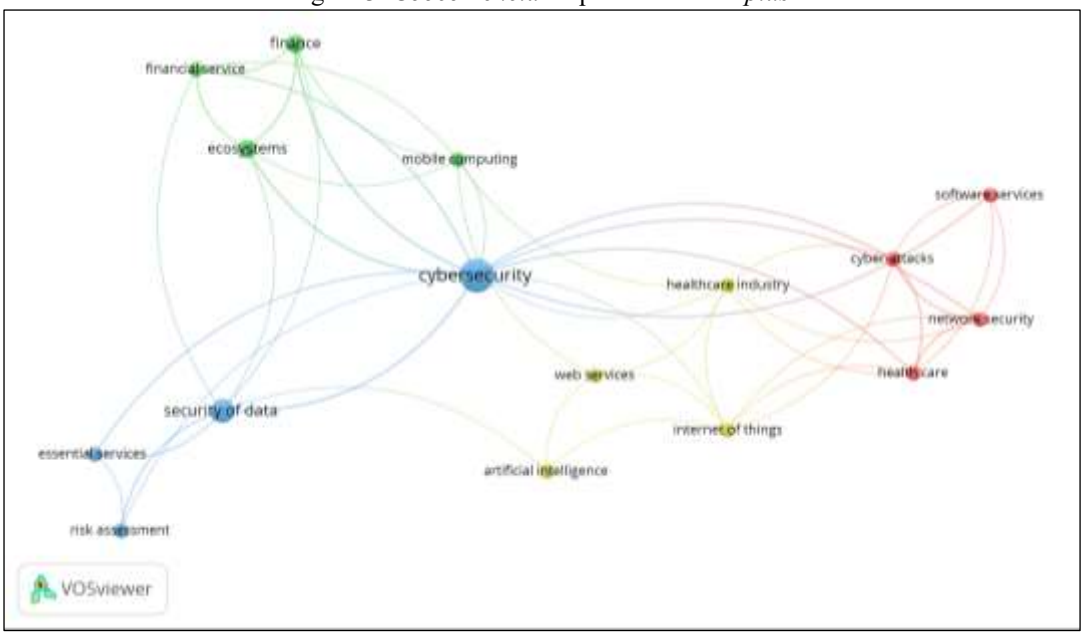
Na figura 3, são identificados 4 *clusters* importantes, sendo o *cluster* central relacionado à segurança cibernética, em seguida, ecossistemas e serviços financeiros, posteriormente, ataques cibernéticos e serviços *web*. Importante destacar que o tema saúde aparece no *cluster* de serviços *web* e no *cluster* de ataques cibernéticos, relacionado a serviços e a questões de segurança, confirmando os dados e importância apresentados na literatura.

Figura 2: Periódicos mais citados localmente.



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

Figura 3: *Coocorrência* de palavras-chave *plus*.



Fonte: Scopus (2022) e Web of Science (2022) em tela do *software* VOSviewer®.

Os 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). Mas, 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).

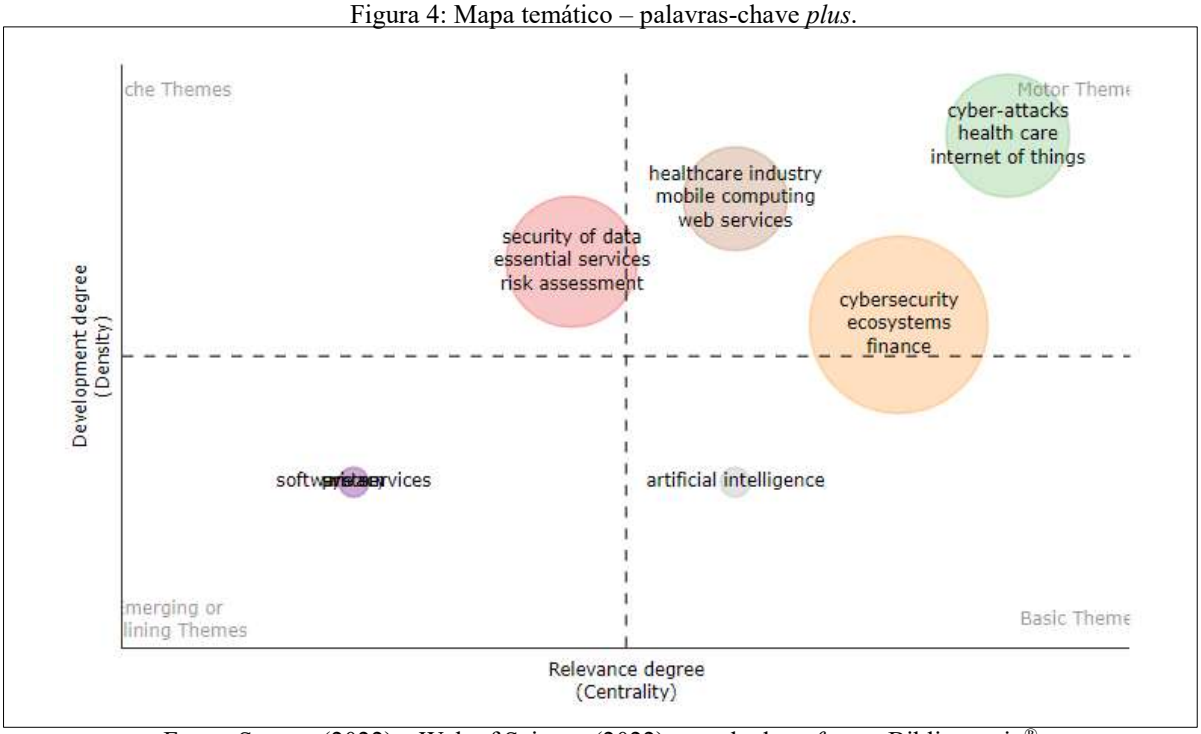
Já a densidade mede o nível de coesão *intra-cluster*, especificando na medida em que as palavras-chave em cada cluster estão conectadas e, portanto, um tema é desenvolvido. Nesse sentido, o quadrante superior direito contém temas com alta centralidade e densidade: temas que podem influenciar o campo 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 palavras-chave *cyber-attacks, health care* e *Internet of Things* possuem forte relacionamento e são considerados temas motores durante o período analisado, na figura 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.

No entanto, as palavras-chave *cybersecurity, ecossystems* e *finance*, apesar de menor densidade do que o primeiro bloco, apresentam-se também como temas motores de segunda relevância. Os temas *privacy, systems* e *software services* apresentam-se no quadrante de temas emergentes, com pouca influência em relação aos demais temas.

Figura 4: Mapa temático – palavras-chave *plus*.

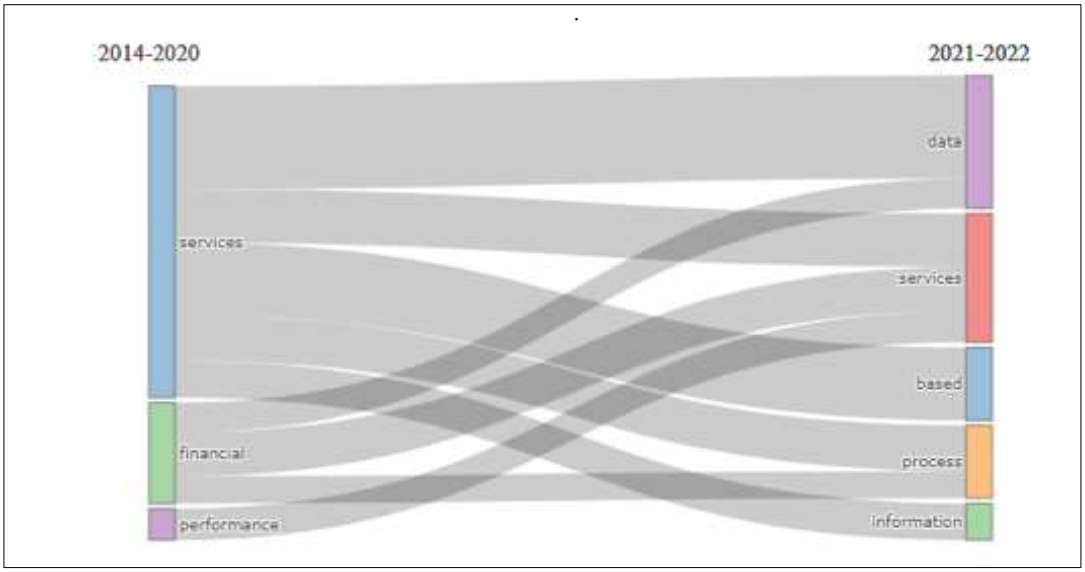


Fonte: Scopus (2022) e Web of Science (2022) em tela do *software* Bibliometrix®.

Na figura 5 apresenta-se a evolução temática das principais palavras encontradas nos *abstracts*, demonstrando tendências e a evolução no período de estudo. O termo *services*

evoluiu dos termos *data, services, based, process* e *information*, com maior relevância que os demais termos.

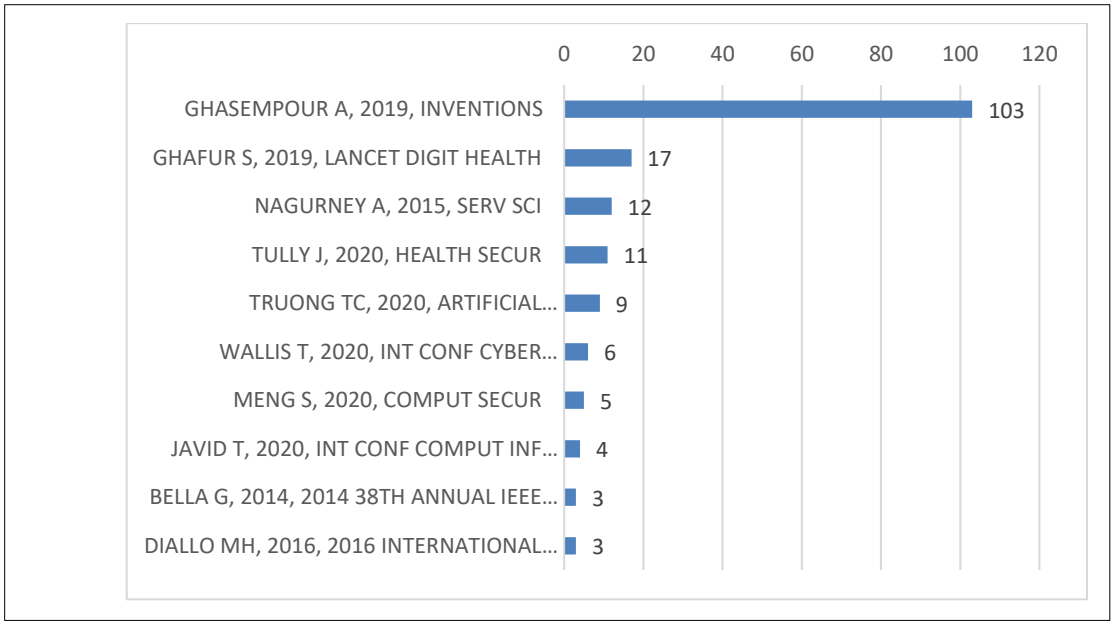
Figura 5: Evolução temática – *Abstracts*



Fonte: Scopus (2022) e Web of Science (2022) em tela do *software* Bibliometrix®.

Por fim, na figura 6, identificaram-se os documentos mais citados localmente, sendo que Ghasempour (2019) com 103 citações vem a ser o documento que mais contribuiu para os estudos identificados globalmente, Ghafur *et al.* (2019) com 17 citações, Nagurney (2015) com 12 citações e Tully *et al.* (2020) com 11 citações são os mais relevantes.

Figura 6: Documentos mais citados globalmente.



Fonte: Scopus (2022) e Web of Science (2022) em tela do *software* Bibliometrix®.

Com base nos dados da pesquisa, foi elaborado o quadro 1, no qual se apresenta uma classificação dos serviços identificados, sendo indicados em ordem de maior para menor impacto nos estudos de *cibersegurança*.

Quadro 1: Classificação dos serviços identificados

Classificação	Serviços
Financeiro	Serviços financeiros, serviços bancários e serviços de pagamentos digitais
Serviços digitais	Digitalização, serviços de Internet, nuvem, serviços eletrônicos, serviços tecnológicos, serviços 5G, serviços IoT, Inteligência Artificial, *Machine Learning* e *Smart cities*
Serviços de saúde	Informações de saúde, dados de saúde, sistemas de saúde, acesso a sistemas críticos de saúde
Cibersegurança	A própria segurança cibernética como um serviço
Serviços essenciais	Energia, cadeia de suprimentos, serviços públicos, fornecimento de água etc.
Stakeholders	*Stakeholders* na prestação de serviços, fornecedores de infra, prestação de serviços de *software*, entre outros relacionados

O quadro 2, utiliza como base as classificações adotadas e apresentadas no quadro 1, que demonstra as principais referências analisadas no estudo e suas relações com a *cibersegurança,* de forma conceitual, facilitando o entendimento e a visão geral dos levantamentos.

Quadro 2: Relação das principais referências analisadas com a *cibersegurança.*

Classificação	Referência	Abordagem
Financeiro	Nagurney (2015)	A atividade *cibercriminosa* está representando grandes ameaças à perda de informações financeiras e outras e apresentando grandes desafios às empresas e organizações. As empresas de serviços financeiros e seus produtos, em particular, de dados de cartão de crédito a informações pessoais, são os principais alvos e essas empresas têm sofrido perdas significativas
Financeiro	Pendley (2015)	A proposta é adicionar um conjunto de controles de TI e segurança cibernética aos controles financeiros, segurança física, controles gerais e segregação de funções. Os controles devem abranger a prevenção de violações de dados, a eliminação da perda de dados e o cumprimento às leis e regulamentos de *cibersegurança* e privacidade
Financeiro	Ambore *et al.* (2016)	Os avanços na computação móvel apresentaram uma grande oportunidade de fornecer Serviços Financeiros Móveis. O uso de abordagens de fator humano ajudou na identificação dos principais objetivos para mitigar as preocupações e riscos de segurança cibernética nas interações entre as infraestruturas complexas e o comportamento humano
Financeiro	Berdyugin e Revenkov (2019)	As divisões de risco das organizações financeiras e de crédito devem incluir especialistas que são capazes de avaliar os riscos cibernéticos, devendo o suporte metodológico, utilizado para auditar e resolver questões de nivelamento das possíveis consequências da realização do RCa (risco de *cyber-ataque*) no *hardware* e *software* dos sistemas automatizados bancários, deve ser atualizado em tempo hábil

Classificação	Referência	Abordagem
Financeiro	Bongiovanni (2020)	Instituições participantes em vários graus concordaram com o pressuposto de que o setor bancário/financeiro, e não a segurança cibernética, é seu *core business*. Ao mesmo tempo, todos concordaram com a importância da segurança cibernética como um complemento necessário para suas ofertas de serviços
Financeiro	Spagnoletti (2020)	Os crimes cibernéticos financeiros buscam lucro por meio da apropriação indevida de valor no ecossistema de serviços financeiros. Tal apropriação indébita é realizada pelo uso malicioso de tecnologias digitais
Financeiro	Dudin *et al.* (2021)	Os processos de digitalização da economia estão penetrando em todos os aspectos da sociedade e do sistema socioeconômico, mudando tanto a atitude mental em relação às tecnologias eletrônicas e virtuais que entraram em nossa realidade, quanto a percepção devido aos motores da competitividade, otimização e conforto ao setor bancário
Financeiro	Wilusz (2021)	Interações humano-computadores reais e onipresentes exigem processos de pagamento que precisam ser instantâneos, convenientes e interoperáveis. No entanto, esses requisitos funcionais estão em oposição a um dos requisitos não funcionais mais significativos: a segurança do processo de pagamento
Serviços digitais	Bella *et al.* (2014)	A computação de serviço está intimamente ligada à interação humana. O problema de segurança e privacidade adquire então mais facetas do que o problema técnico típico
Serviços digitais	Feltus *et al.* (2018)	A indústria da Internet das Coisas (IoT) cresce rapidamente e se torna progressivamente mais dedicada a serviços críticos de negócios. A adoção da IoT gera dois tipos de desafios: riscos de segurança cibernética e preocupações com a privacidade
Serviços digitais	Ghasempour (2019)	Internet das Coisas (IoT) é uma conexão de pessoas e coisas a qualquer hora, em qualquer lugar, com qualquer pessoa e qualquer coisa, usando qualquer rede e qualquer serviço. Assim, a IoT é uma enorme infraestrutura de rede global dinâmica de entidades habilitadas para Internet com serviços da *web*
Serviços digitais	Meng *et al.* (2020)	O rápido desenvolvimento de sistemas de IoT (Internet das Coisas) e técnicas de nuvem abriu o caminho para sistemas de recomendação para facilitar a vida diária dos usuários. No entanto, os riscos de segurança cibernética associados, como ataques ambientais e ataques de *software*, não devem ser ignorados
Serviços digitais	Robberechts *et al*. (2020)	O principal objetivo das cidades inteligentes é a busca de qualidade na vida das pessoas, provendo serviços usando a tecnologia da informação junto aos componentes das cidades
Financeiro e serviços digitais	Mahalakshmi *et al*. (2022)	A adoção de tecnologias avançadas aumenta a qualidade, a eficiência e a produtividade de uma indústria. A inteligência artificial e o aprendizado de máquina estão trazendo automação no trabalho e nos serviços financeiros profissionais. Além disso, o relatório revela as várias funções da incorporação dessas tecnologias nas indústrias financeiras. Uma das funções mais significativas avaliadas é detectar atividades de fraude e simplificar o processo geral
Serviços de saúde	Ghafur *et al.* (2019)	À medida que a tecnologia moderna se torna indispensável nos cuidados de saúde, as vulnerabilidades às ameaças cibernéticas continuam a aumentar, comprometendo as informações de saúde e a segurança de milhões de pessoas. Essa ameaça pode ocorrer de várias maneiras: dados podem ser furtados; os dados podem ser excluídos ou corrompidos de uma forma que não é óbvia até anos mais tarde; e dispositivos médicos podem ser *hackeados*, causando danos diretos aos pacientes
Serviços de saúde	Ganai *et al.* (2022)	Garantir a segurança dos pacientes, a confidencialidade e a confiabilidade exigem o uso da segurança cibernética. Mais recursos e esforços devem ser investidos na proteção da segurança cibernética.

Classificação	Referência	Abordagem
Serviços de saúde	Tully *et al.* (2020)	A segurança cibernética refere-se à proteção da tecnologia baseada em computador contra interrupção deliberada ou inadvertida por meio da manipulação de *software, hardware* ou conexões de rede subjacentes
Cibersegurança	Elsayed e Zulkernine (2018)	*Security as a service* simplesmente gira em torno do provisionamento de soluções de segurança entregues, mantidas e gerenciadas como serviços na nuvem por meio de assinatura ou sob demanda
Serviços essenciais	Markopoulou e Papakonstantinou (2021)	A digitalização do setor de água está avançando em ritmo acelerado, com sistemas inteligentes de gerenciamento de água sendo implantados por um número cada vez maior de fornecedores de água e operadores de rede. No entanto, tornar a gestão da água inteligente, pelo uso de dispositivos inteligentes, como medidores inteligentes e redes de água inteligentes, tem um preço, a segurança cibernética
Stakeholders	Rashid *et al.* (2019)	A utilização de informações de segurança cibernética para melhorar a postura de segurança de uma organização resultou na evolução dos ecossistemas de compartilhamento de informações de segurança cibernética. Três partes interessadas foram analisadas, os provedores de soluções de segurança cibernética, provedores de informações e usuários finais. Seus valores dependem da inter-relação entre eles e são baseados em diversos parâmetros de valor

O aumento do uso da Internet e a potencialização do uso do meio digital fortalecem a necessidade de especial atenção aos serviços para os temas de *cibersegurança,* considerando o volume de dados transitados, os riscos de um *cyber-attack* e a necessidade de privacidade. Observa-se que a literatura trata em primeiro lugar dos serviços financeiros ou bancário, com forte impacto em vulnerabilidades e em segundo lugar os serviços digitas, como *IoT* e uso do 5G, que potencializam o volume de dados e a velocidade das transações.

5. Conclusão

A análise *bibliométrica* mostrou uma oportunidade que permeia os conceitos de *cibersegurança* e serviços e que merece um estudo profundo, com benefícios para todos os agentes envolvidos.

Para Bongiovanni (2020), é preciso construir uma linguagem comum em torno da segurança da informação para funcionários e clientes. Para isso, vários caminhos são possíveis: por exemplo, mapear a experiência dos clientes em suas interações com os serviços que as empresas oferecem e considerar a segurança cibernética como um componente dessa experiência.

Na parte técnica, é necessária a inclusão de sistemas de detecção de ameaças cibernéticas, detecção de intrusão, prevenção de intrusão e indicadores de engajamento cibernético (DIALLO et al., 2016).

No campo da saúde, a confidencialidade deve ser incorporada ao serviço desde o início, em vez de ser uma reflexão tardia. A *cibersegurança* deve ser incorporada à mentalidade de segurança do paciente. Problemas adicionais de privacidade e segurança se desenvolveram como resultado do aumento do uso de tecnologias de *IoT* na área da saúde (GANAI et al., 2022).

Adicional aos levantamentos, foi possível identificar nas análises *bibliométricas* a divisão em *clusters* da literatura que envolve o tema abordado, podendo, como oportunidade, aumentar seu nível de relacionamento e compartilhamento de soluções, envolvendo todo o

ecossistema de forma ampla. O estudo apresentou os principais fatores relacionados à *cibersegurança* em serviços, fortalecendo as necessidades de ações em todas as frentes, incluindo o setor financeiro, serviços digitais, saúde, *cibersegurança*, serviços essenciais e *stakeholders*, com diferentes particularidades, mas ações e soluções muito similares. Aprofundar cada uma das frentes ou outras não abordadas neste estudo, com foco em *cibersegurança* em serviços, nas questões organizacionais e individuais, como proposta de valor para a sociedade, pode ser a maior oportunidade apresentada por este estudo.

Referências

AGRAFIOTIS, I. et al. 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.

AMBORE, S. et al. A "Soft" Approach to Analysing Mobile Financial Services Socio-Technical Systems. **PROC INT BCS HUM COMPUT INTERACT CONF., HCI**, 2016.

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, M., & CUCCURULLO, C. bibliometrix: An R-tool for comprehensive science mapping analysis. **Journal of Informetrics**, v. 11, n. 4, p. 959–975, 2017.

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.

BELLA, G. et al. **A socio-technical methodology for the security and privacy analysis of services**. Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014. **Anais**...Institute of Electrical and Electronics Engineers Inc., 18 set. 2014.

BERDYUGIN, A. A.; REVENKOV, P. V. **Approaches to measuring the risk of cyberattacks in remote banking services of Russia**. CEUR Workshop Proceedings. **Anais**...CEUR-WS, 2019.

BONGIOVANNI, I. Designing User-Centric Information Security Management Systems in Financial Services Organisations. **2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)**, 2020.

BRADFORD, S. C. Sources of information on specifc subjects. **Engineering**, v. 137, p. 85–86, 1934.

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

COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. 2007. **Gerenciamento de Riscos Coorporativos** – Estrutura Integrada, Sumário Executivo. v. 2, set. 2007.

DIALLO, M. H. et al. **AutoMigrate: A Framework for Developing Intelligent, Self-Managing Cloud Services with Maximum Availability**. Proceedings - 2016 International Conference on Cloud and Autonomic Computing, ICCAC 2016: Co-located with the 10th IEEE International Conference on Self-Adaptive and Self-Organizing Systems, SASO 2016. **Anais**...Institute of Electrical and Electronics Engineers Inc., 5 dez. 2016.

DUDIN, M. N.; SHKODINSKII, S. V.; USMANOV, D. I. Key trends and regulations of the development of digital business models of banking services in industry 4.0. **Finance: Theory and Practice**, v. 25, n. 5, p. 59–78, 2021.

ELSAYED, M.; ZULKERNINE, M. **A taxonomy of security as a service**. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). **Anais**...Springer Verlag, 2018.

FELTUS, C. et al. **Towards a standard-based security and privacy of IoT system's services**. Proceedings - 2018 International Conference on Computational Science and Computational Intelligence, CSCI 2018. **Anais**...Institute of Electrical and Electronics Engineers Inc., 1 dez. 2018.

GALLOUJ, F.; SAVONA, M. Innovation in services: A review of the debate and a research agenda. **Journal of Evolutionary Economics**, v. 19, n. 2, p. 149–172, abr. 2009.

GANAI, P. T. et al. **A Detailed Investigation of Implementation of Internet of Things (IOT) in Cyber Security in Healthcare Sector**. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). **Anais**...IEEE, 28 abr. 2022. Disponível em: <https://ieeexplore.ieee.org/document/9823887/>

GHAFUR, S. et al. **The challenges of cybersecurity in health care: the UK National Health Service as a case study**. **The Lancet Digital Health**. Elsevier Ltd, 1 maio 2019.

GHASEMPOUR, A. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions. **MDPI Multidisciplinary Digital Publishing Institute**, 1 mar. 2019.

HOFSTETTER, M. et al. **Applications of AI in cybersecurity**. Proceedings - 2020 2nd International Conference on Transdisciplinary AI, TransAI 2020. **Anais**...Institute of Electrical and Electronics Engineers Inc., 1 set. 2020.

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.

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

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

LOTKA, A. J. The frequency distribution of scientific productivity. **Journal of the Washington Academy of Sciences**, v. 16, n. 12, p. 317–323, 1926.

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.

MAHALAKSHMI, V. et al. The Role of implementing Artificial Intelligence and Machine Learning Technologies in the financial services Industry for creating Competitive Intelligence. **Materials Today: Proceedings**, v. 56, p. 2252–2255, 1 jan. 2022.

MARKOPOULOU, D.; PAPAKONSTANTINOU, V. Digitalisation of water services and the water services and the water sector cyber threat landscape: Is the EU regulatory framework adequate? **Journal of Water Law**, v. 27, n. 4, p. 119–133, 1 jan. 2021.

MENG, S. et al. **Security-Driven Hybrid Collaborative Recommendation Method for Cloud-based IoT Services**.

NAGURNEY, A. **A Multiproduct Network Economic Model of Cybercrime in Financial Services. Service Science**.

PENDLEY, J. A. Information Security and Cloud-Based Computing: Tools for the Corporate Treasurer. **Journal of Corporate Accounting and Finance**, v. 26, n. 3, p. 27–30, 1 mar. 2015.

RASHID, Z.; NOOR, U.; ALTMANN, J. **Network externalities in cybersecurity information sharing ecosystems**. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). **Anais**...Springer Verlag, 2019.

ROBBERECHTS, J. et al. **A Novel Edge-To-Cloud-As-A-Service (E2CaaS) Model for Building Software Services in Smart Cities**. Proceedings - IEEE International Conference on Mobile Data Management. **Anais**...Institute of Electrical and Electronics Engineers Inc., 1 jun. 2020.

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

SPAGNOLETTI, P.; CECI, F.; SALVI, A. **Adversarial Evolution: Competing dynamics and reactive institutional forms in financial services ecosystem**.

TULLY, J. et al. Healthcare Challenges in the Era of Cybersecurity. **Health Security**, v. 18, n. 3, p. 228–231, 1 maio 2020.

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.

WILUSZ, D.; WÓJTOWICZ, A. Security Analysis of Transaction Authorization Methods for Next Generation Electronic Payment Services. **Lecture Notes in Computer Science**, v. 12788, 2021.

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

ZIPF, G. K. Human behavior and the principle of least effort. In Addison-Wesley, 1949.