Revista Ibero-Americana de Estratégia
Iberoamerican Journal of Strategic Management

e-ISSN: 2176-0756
https://doi.org/10.5585/2023.23846
Recebido: 15 fev. 2023 / **Aprovado:** 16 jun. 2023
Processo de Avaliação: Double Blind Review
Editora Chefe: Heidy Rodriguez Ramos
Coeditor: Ivano Ribeiro
Editora de Seção: Dra. Nairana Radtke Caneppele
Editor Assistente: Leandro Rodrigues de Oliveira

ANÁLISE BIBLIOMÉTRICA DAS PUBLICAÇÕES SOBRE RISCOS CIBERNÉTICOS NO SETOR DE SERVIÇOS

Marcia C. Rossi [1] **Gilberto Perez** [2]

Objetivo: Explorar o avanço da produção científica sobre os riscos cibernéticos que permeiam o setor de serviços, identificando pesquisadores e instituições relevantes no tema, medindo o impacto e identificando tendências, contribuições e lacunas de conhecimento. Além disso, o estudo busca utilizar achados bibliométricos para trazer contribuições acadêmicas e gerenciais para o tema.
Metodologia: Estudo bibliométrico, utilizando o método de organização e sistematização da informação (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), cuja estrutura seguiu as premissas das leis de Bradford, Lotka e Zipf, utilizando as bases de dados científicas da WoS - Web of Science. O estudo bibliométrico possibilitou a realização de pesquisa exploratória e descritiva sem recorte temporal, resultando na identificação de 115 publicações (dezembro de 1995 a fevereiro de 2023), o que permitiu mensurar e apresentar as características e o perfil das publicações analisadas.
Originalidade: O estudo revelou potencial para explorar o tema Riscos Cibernéticos no setor de Serviços, considerando a escassez de produção científica. Também permitiu a identificação de tendências emergentes e clusters nas atividades do setor de serviços e a criação de um modelo conceitual com base nas conclusões das publicações analisadas.
Principais resultados: As análises revelaram quais setores da economia de serviços são mais abordados em publicações relacionadas ao tema dos riscos cibernéticos. Essas análises foram organizadas em dez áreas, com a seguinte ordem de relevância (frequência) de publicação: Ciência da Computação, Sistemas de Informação, Engenharia, Negócios, Finanças e Gestão, Telecomunicações, Métodos da Teoria da Ciência da Computação e Inteligência Artificial da Ciência da Computação. Os achados bibliométricos permitiram a criação do modelo conceitual de Riscos Cibernéticos em Serviços, que propõe uma abordagem de melhoria cíclica e contínua para lidar com vulnerabilidades, ameaças cibernéticas e consequências. Isso inclui identificar e avaliar as vulnerabilidades existentes, implementar medidas de mitigação e monitorar constantemente as ameaças e suas consequências.
Contribuições teóricas: O modelo conceitual de Riscos Cibernéticos em Serviços pode ser uma referência para pesquisadores em diversas áreas de atuação, considerando a amplitude do setor de serviços e a natureza interdisciplinar da mitigação de riscos digitais.
Contribuições gerenciais: A compreensão dos riscos cibernéticos apóia a capacidade da organização de responder a eles, fortalecendo sua postura de segurança e protegendo seus ativos e informações críticas de ameaças cibernéticas.

Palavras-chave: Bibliometria. Riscos Cibernéticos. Setor de Serviços.

BIBLIOMETRIC ANALYSIS OF PUBLICATIONS ON CYBER RISKS IN THE SERVICES SECTOR

Objective: To explore the progress of scientific production on cyber risks that permeate the service sector, identifying relevant researchers and institutions on this theme, measuring the impact, and identifying trends, contributions, and knowledge gaps. In addition, the study seeks to use bibliometric findings to bring academic and managerial contributions to the subject.
Methodology: Bibliometric study, using the method of organization and systematization of information (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), whose structure followed the premises of the laws of Bradford, Lotka, and Zipf, using the scientific databases of the WoS - Web of Science. The bibliometric study enabled the performance of exploratory and descriptive research without the temporal cut, resulting in the identification of 115 publications (December 1995 to February 2023), which allowed measuring and presenting the characteristics and profile of the publications analyzed.
Originality: The study revealed a potential for exploring the theme of Cyber Risks in the Services sector, considering the scarcity of scientific production. It also enabled the identification of emerging trends and clusters in service sector activities and the creation of a conceptual model based on the findings of the analyzed publications.
Main results: The analyses revealed which sectors of the service economy are most frequently approached in publications related to the theme of cyber risks. These analyses were organized into ten areas, with the following order of relevance (frequency) of publication: Computer Science, Information Systems, Engineering, Business, Finance and Management, Telecommunications, Computer Science Theory Methods, and Computer Science Artificial Intelligence. The bibliometric findings enabled the creation of the conceptual model of Cyber Risks in Services, which proposes a cyclical and continuous improvement approach to deal with vulnerabilities, cyber threats, and consequences. This includes identifying and assessing existing vulnerabilities, implementing mitigation measures, and constantly monitoring threats and their consequences.
Theoretical contributions: The conceptual model of Cyber Risks in Services can be a reference for researchers in various fields of action, considering the breadth of the services sector and the interdisciplinary nature of digital risk mitigation.
Managerial contributions: Understanding of cyber risks supports the ability of the organization to respond to them, strengthening its security posture and protecting its critical assets and information from cyber threats.

Keywords: Bibliometry, Cyber Risks. Services Sector.

ANÁLISIS BIBLIOMÉTRICO DE PUBLICACIONES SOBRE CIBERRIESGOS EN EL SECTOR SERVICIOS

Objetivo: Explorar el avance de la producción científica sobre los ciberriesgos que permean el sector servicios, identificando investigadores e instituciones relevantes en la materia, así como medir el impacto e identificar tendencias, aportaciones y lagunas de conocimiento. Además, el estudio pretende utilizar los resultados bibliométricos para aportar contribuciones académicas y de gestión sobre el tema.
Metodología: Estudio bibliométrico, utilizando el método de organización y sistematización de la información (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), cuya estructura siguió las premisas de las leyes de Bradford, Lotka y Zipf, utilizando las bases de datos científicas de WoS - Web of Science. El estudio bibliométrico permitió la realización de una investigación exploratoria y descriptiva sin corte temporal, resultando en la identificación de 115 publicaciones (diciembre de 1995 a febrero de 2023), lo que permitió medir y presentar las características y el perfil de las publicaciones analizadas.
Originalidad: El estudio reveló un potencial para explorar el tema del Ciberriesgo en el sector Servicios, dada la escasez de producción científica. Además, permitió identificar tendencias y clusters emergentes en las actividades del sector servicios y crear un modelo conceptual a partir de las conclusiones de las publicaciones analizadas.
Principales resultados: Los análisis revelaron qué sectores de la economía de servicios se abordan con mayor frecuencia en las publicaciones relacionadas con el tema de los ciberriesgos. Estos análisis se organizaron en diez áreas, con el siguiente orden de relevancia (frecuencia) de publicación: Informática, Sistemas de Información, Ingeniería, Negocios, Finanzas y Gestión, Telecomunicaciones, Métodos Teóricos de la Informática e Inteligencia Artificial de la Informática. Los resultados bibliométricos permitieron crear el modelo conceptual de Ciberriesgos en los Servicios, que propone un enfoque cíclico y de mejora continua para hacer frente a las vulnerabilidades, las ciberamenazas y sus consecuencias. Esto incluye la identificación y evaluación de las vulnerabilidades existentes, la implementación de medidas de seguridad para mitigarlas y el monitoreo constante de las amenazas y sus consecuencias.
Aportes teoricos: El modelo conceptual de Riesgos Cibernéticos en los Servicios puede ser una referencia para los investigadores en diversos campos de actividad, teniendo en cuenta la amplitud del sector servicios y la naturaleza interdisciplinaria de la mitigación del riesgo digital.
Aportes gerenciales: Comprensión de los riesgos cibernéticos ayuda a la organización a responder a ellos, reforzando su postura de seguridad y protegiendo sus activos e información críticos frente a las ciberamenazas.

Palabras clave: Bibliometría. Ciberriesgos. Sector Servicios.

.

Cite as / Como citar

American Psychological Association (APA)

Rossi, M. C., & Perez, G. (2023). Análise bibliométrica das publicações sobre riscos cibernéticos no setor de serviços. *Iberoamerican Journal of Strategic Management (IJSM), 22*(1), 1-25, e23846. https://doi.org/10.5585/2023.23846

(ABNT – NBR 6023/2018)

ROSSI, Márcia. C.; PEREZ, Gilbetto. Análise bibliométrica das publicações sobre riscos cibernéticos no setor de serviços. *Iberoamerican Journal of Strategic Management (IJSM),* v. 22, n. 1, p. 1-25, e23546, 2023. https://doi.org/10.5585/2023.23846

[1] Pesquisadora em Recursos e Desenvolvimento Empresarial. Mestre em Controladoria Empresarial. Professora dos cursos de especialização em Controladoria Financeira e MBA em Gestão Estratégica Empresarial na Universidade Prebisteriana Mackenzie. São Paulo/SP – Brasil. contato@marciarossi.com (Contato principal para correspondência).
[2] Livre Docente pela Universidade de São Paulo (USP/FEA, 2022). Professor Adjunto do programa de Pós-Graduação Stricto Sensu em Administração (PPGA) na Universidade Presbiteriana Mackenzie. São Paulo/SP - Brasil. gperez@mackenzie.br

1 Introdução

Os processos de digitalização da economia e da sociedade têm sido importantes para o crescimento e continuidade das empresas, com impacto potencialmente significativo na prosperidade global. As tecnologias de informação e comunicação aumentaram suas taxas de compartilhamento, armazenamento e processamento de informações pessoais em um nível exponencial (Conger, Pratt, & Loch, 2012; Saridakis, Benson, Ezingeard, & Tennakoon, 2016). Incidentes como riscos cibernéticos têm trazido implicações econômicas e sociais relevantes, além dos impactos significativos para a segurança pública (Mantha & Soto, 2020).

O impacto da digitalização nos processos de negócios tem incentivado os mercados de transformação a criarem ou aprimorarem produtos, serviços e modalidades relacionais (Barile, Grimaldi, Loia, & Sirianni, 2020). Ao mesmo tempo, outra frente ativa tem explorado progressivamente novos modelos de negócios, impulsionada por empresas que buscam novos substitutos e adotam estratégias que atendam às necessidades de seus clientes.

Nesse sentido, os desafios da servitização têm chamado cada vez mais a atenção das empresas do setor industrial, que buscam no planejamento, a estratégia de atendimento integral, cuja categoria de serviço expõe inúmeras oportunidades com perspectivas positivas, na mesma medida em que os riscos são conjuntamente negligenciados (Fang, Palmatier & Steenkamp, 2008; Nordin, Kindström, Kowalkowski, & Rehme, 2011; Rajapathirana & Hui, 2018; Raddats, Kowalkowski, Benedettini, Burton, & Gebauer, 2019).

O ciberespaço não é apenas a internet, incluindo hardware, software e sistemas de informação, mas também envolve pessoas e suas interações em redes de computadores, sejam elas comerciais ou não (Klimburg, 2012; Silva & Nogueira, 2019). A presença do cliente como participante do processo de serviço requer atenção ao projeto da instalação, que até recentemente, não era opcional para as operações tradicionais de manufatura (Fitzsimmons & Fitzsimmons, 2014).

Uma lacuna teórica entre os riscos cibernéticos e o setor de serviços reside na falta de um modelo ou estrutura abrangente que integre as especificidades dos riscos cibernéticos com os desafios enfrentados pelo setor de serviços. Embora existam discussões sobre segurança cibernética e várias estruturas e modelos para avaliar e mitigar riscos digitais, a aplicação desses conceitos ao setor de serviços pode ser complexa e desafiadora. A economia de serviços não se limita a uma única entidade, mas abrange uma ampla gama de serviços com diversos modelos de negócios. Engloba várias atividades que oferecem serviços variados, cada uma com suas particularidades quanto à forma como operam, competem e são reguladas (Gallouj, 2023; Metters, 2023).

Diante desse cenário, propõe-se explorar a literatura e os trabalhos desenvolvidos sobre o tema. Esta pesquisa visa responder a seguinte questão: **Qual é o perfil da produção científica que tem abordado os riscos cibernéticos no setor de serviços?** Para responder à questão proposta, foi realizado um estudo bibliométrico utilizando o método de organização e sistematização da informação proposto

por Chueke e Amatucci (2015). A estrutura da pesquisa seguiu as premissas das leis de Bradford, Lotka e Zipf, utilizando as bases de dados científicas da Web of Science (WoS). Além disso, este estudo busca utilizar os achados bibliométricos como base para a construção de um modelo conceitual que amplie a compreensão da área de pesquisa.

É necessário explorar as discussões sobre riscos cibernéticos no setor de serviços, que desempenha um papel crucial ao permear a oferta de produtos e mercadorias. Compreender o risco cibernético não apenas auxilia as empresas a garantir e gerenciar a conformidade em seus processos, evitando possíveis penalidades financeiras, danos a terceiros e danos à reputação, mas também traz contribuições acadêmicas ao preencher uma lacuna de conhecimento sobre os desafios específicos enfrentados pelo setor de serviços neste contexto. A análise dos riscos cibernéticos no setor de serviços no nível político-legal pode apoiar a formulação de políticas e regulamentos apropriados para proteger dados confidenciais e garantir a segurança cibernética. Além disso, esse entendimento contribui para aumentar a conscientização sobre a importância da proteção da privacidade, confiança do consumidor e inclusão digital, promovendo uma abordagem holística para abordar os impactos sociais e éticos da digitalização e automação no setor de serviços.

Para atingir o objetivo proposto, este artigo está organizado em cinco seções. Distinguindo a introdução e a conclusão, a Seção Dois começa explorando os conceitos de risco cibernético, destacando as ameaças e vulnerabilidades que as organizações têm enfrentado: estratégias de gerenciamento de risco, proteção de dados e segurança cibernética são abordadas neste contexto. Também é abordado o setor de serviços e sua relevância na economia. Estratégias para crescimento, inovação e satisfação do cliente (e participação) nesta indústria em constante evolução são expostas. Combinar esses dois tópicos visa fornecer uma compreensão abrangente de um cenário em que as organizações enfrentam desafios cibernéticos e buscam um equilíbrio adequado entre inovação e segurança nos serviços. A terceira seção apresenta o percurso metodológico adotado para o desenvolvimento deste estudo. A quarta seção apresenta os resultados obtidos, incluindo os setores de serviços identificados na análise dos artigos. As palavras-chave mais utilizadas ajudarão a destacar a tendência do setor para enfrentar os riscos digitais, os artigos e autores mais citados e os países de origem das publicações, que ajudam a visualizar o foco de desenvolvimento e investimentos em pesquisas sobre o tema. A quinta seção, que antecede a seção de Considerações Finais, discute os resultados obtidos, conjugando-os com a fundamentação teórica.

2 Referencial Teórico

Dada a crescente dependência de tecnologias digitais em atividades relacionadas aos serviços, entender a natureza e as implicações dos riscos cibernéticos tornou-se fundamental para pesquisadores e gerentes. Antes de explorar o perfil da produção científica que aborda os riscos cibernéticos no setor de serviços por meio da bibliometria, este referencial teórico buscou fornecer uma compreensão abrangente do conhecimento existente nessa área por meio de uma revisão da literatura. Esta revisão permitiu uma breve exploração dos conceitos relacionados aos riscos cibernéticos e ao setor de serviços.

2.1 Riscos Cibernéticos

Cibernética tem origem grega, significando a "arte do piloto" (Abbagnano, 2007), levando ao entendimento de controle e direção. O termo se destacou durante os trabalhos e experimentos relacionados à Segunda Guerra Mundial do matemático Norbert Wiener, que lhe renderam a publicação intitulada "Cibernética: ou controle e comunicação no animal e na máquina", em 1948 (Wiener, 2017). Este trabalho desenvolve e apresenta as hipóteses desse tema, decorrentes da pesquisa e da interação multidisciplinar com outros grupos científicos, formados por matemáticos, físicos, engenheiros e cientistas sociais.

A cibernética é uma área pluralista e interdisciplinar do conhecimento científico (Kim, 2004; Kandjani, Wen & Bernus, 2012). No entanto, Wiener descobriu tardiamente que Ampère já havia usado a mesma palavra sobre ciência política (Wiener, 1984). O desenvolvimento da cibernética induziu os cientistas a desenvolver novos e complexos modelos matemáticos para expandir o sistema homem-máquina. Palavras comumente citadas com o prefixo ciber, como ciberespaço, devem sua origem à cibernética, que inaugurou muitos desenvolvimentos (Kandjani et al., 2012).

Pierre Lévy (2000) considerou o estudo do ciberespaço como uma ciência da informação e comunicação, entendendo que o ciberespaço é um meio de comunicação decorrente da rede global de computadores interconectados, não especificamente a estrutura física da comunicação digital, mas seu uso pelas pessoas que buscam, promovem e retroalimentam uma infinidade de informações por meio desse mecanismo. Essa perspectiva reforça um dos principais pontos atribuídos à cibernética: não há descontinuidade entre máquinas e homens, cuja troca depende da compatibilidade funcional (Kim, 2004).

O risco cibernético é considerado um subrisco dos riscos operacionais para ativos de informação e tecnologia e pode afetar a confidencialidade, disponibilidade e integridade da informação ou sistema (Cebula & Young, 2010). Os riscos podem assumir duas formas: a) uma natureza estática ou pura, caracterizada pelo risco de perda; b) de natureza especulativa ou dinâmica, que envolve a possibilidade de perda de uma das partes, enquanto a outra ganha algum ganho (Powers, 2006; Durak, 2020).

Para Neghina e Scarlat (2012), as organizações devem defender a transição de uma abordagem baseada principalmente na segurança para uma abordagem mais próxima da avaliação de riscos, abordando assim as vulnerabilidades no planejamento e nos métodos de gerenciamento de riscos.

Paralelamente, a alta competitividade no mercado tem forçado as organizações a melhorarem seu posicionamento em relação à inovação e às tecnologias emergentes, e os pesquisadores têm se desdobrado em explorar, analisar e conceituar o tema, conforme estudos listados na Tabela 1:

Tabela 1

Principais conceitos de Riscos Cibernéticos

Autores	Conceito	Foco
Bewer (2000)	A vulnerabilidade pode ser medida pela multiplicação da ameaça versus o valor do ativo.	Medição, ameaça e valor de ativos
NIST (2006)	Impacto negativo no funcionamento da organização, envolvendo elementos informais baseados na missão, imagem e reputação, em que os recursos e o capital intelectual são os "meios" de utilização do sistema de informação.	Potencial, operações e ativos organizacionais
Fórum Econômico Mundial (2012)	É uma combinação da probabilidade de um evento nos sistemas de informação da rede e os efeitos desse evento nos ativos e na reputação de uma organização.	Combinação de probabilidade, evento, ativos
Nieuwesteeg, Visscher & de Waard (2018)	Aquele que causa danos físicos ou impacta prejuízos financeiros quando há mau funcionamento do ambiente digital ou quando os dados são negligenciados ou compartilhados ilegalmente.	Danos físicos, perdas financeiras, ilegalidades
Biener, Eling & Wirfs (2015)	O risco pode ser definido como uma função de três parâmetros: 1) Impacto expressa o nível de dano que um determinado risco pode causar. 2) Ameaça expressa se um risco específico é provável. 3) Vulnerabilidade expressa se as medidas de segurança da informação são efetivas ou não.	Nível de dano, ameaça expressa e vulnerabilidade
NAIC (2018)	Risco relacionado a um evento eletrônico malicioso que pode causar descontinuidade de negócios e perdas financeiras. Pode ser considerada aquela que cobre todos os demais riscos associados à atividade online, como o armazenamento de dados pessoais e transações que podem resultar em danos à imagem, prejuízos financeiros e adversidades na vida e nos negócios.	Descontinuidade de negócios, evento malicioso, adversidades na vida e nos negócios
Böhme, Laube & Riek (2018)	Dois aspectos podem destacar os riscos cibernéticos: 1) técnico: fluxo do processo, comportamento reprogramável e ameaça global dinâmica; e 2) econômico: assimetria de informação, externalidades e fatores de risco comuns na operacionalização.	Aspectos técnicos e econômicos
Egan *et al.* (2019)	O risco depende das ameaças maliciosas (ou não maliciosas) que a organização enfrenta e como ela mitiga os riscos por meio de decisões estratégicas e de negócios.	Ameaça, decisões e estratégias de negócios
Strupczewski (2021) See More	Os riscos cibernéticos estão ligados à segurança das empresas: trabalho remoto, teletrabalho, acesso a informações estratégicas e sensíveis e uso descuidado de equipamentos como notebooks e smartphones.	Trabalho remoto, recursos sincronizados com os sistemas da empresa e descuido
Liu *et al.*, 2022	[…] aproveitando as vulnerabilidades induzidas pela tecnologia, sistemas hiperconectados, erros humanos e organizações despreparadas para prevenir ou combater tais ataques.	Erros hiperconectados ativados por humanos

Fonte: Com base na literatura pesquisada (2023).

O risco cibernético é uma discussão científica recente, e sua diversidade e complexidade têm caracterizado uma mudança exponencial na segurança cibernética e nas ameaças cibernéticas. Inclusive, ganhou foco com a digitalização acelerada da economia e das interações no ambiente cibernético (Strupczewski, 2021).

A vulnerabilidade pode ser medida multiplicando a ameaça pelo valor dos ativos, representando o potencial impacto negativo na operação de uma organização e expressando se as medidas de segurança da informação são eficazes. Esse impacto engloba elementos tangíveis e intangíveis, como reputação, utilização de recursos e o capital intelectual envolvido (Brewer, 2000; Biener et al., 2015; Liu et al., 2022).

Os aplicativos e serviços da Internet estão cada vez mais vulneráveis a ataques ou roubo de informações (Ghorbani & Ahmadzadegan, 2017). A preocupação com ameaças digitais em riscos cibernéticos tem permanecido em segundo plano na agenda de CEOs ao redor do mundo - essa constatação é reforçada em estudos, entre eles uma pesquisa realizada pela Marsh em parceria com a Microsoft, que envolveu 168 empresas brasileiras em um total de 600 empresas globais, cujos resultados revelaram que 61% dessas empresas não faziam seguro com risco cibernético cobertura. Enquanto 22% não souberam responder se a empresa investe nesse tipo de seguro (Funke, 2021).

As empresas têm enfrentado ataques de grupos sofisticados, que implantaram malware, um tipo de software malicioso direcionado contra sistemas e indivíduos projetados para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável (McAfee, 2021).

Avaliar os danos causados por ataques cibernéticos impôs desafios colossais e globais para empresas e governos. Sabe-se que os ataques causam interrupções catastróficas de serviços em cascata que causaram bilhões de dólares em perdas financeiras para organizações e infraestrutura crítica em todo o mundo (Pal et al., 2021). Em 2020, os valores enviados e recebidos de atividades ilícitas chegaram a 10 bilhões de dólares, representando 0,34% de toda a operação global com moedas digitais (ChainAnalysis, 2020). Rosati, Gogolin e Lynn (2022) apontam deficiências no controle organizacional interno, cujas falhas de segurança cibernética são consideradas fatores de risco significativos que afetam negativamente os resultados financeiros das empresas.

Nesse sentido, os riscos cibernéticos incluem aspectos técnicos, como fluxo de processos, comportamento reprogramável, ameaças globais dinâmicas e aspectos econômicos, como assimetria de informações, externalidades e fatores de risco operacional compartilhados (Böhme et al., 2018). A gravidade desses riscos depende da capacidade da organização em mitigá-los por meio de decisões estratégicas e operacionais (Egan et al., 2019).

Como agravante, a pandemia do COVID-19 expôs novas dificuldades, além das enfrentadas pela área da saúde, como os desafios causados pela flexibilização da segurança de dados e informações, quando, devido ao trabalho remoto adotado pela maioria das empresas , o clima organizacional estendeu-se ao ambiente doméstico dos indivíduos. Merece destaque também a expansão da demanda por serviços por meio de aplicativos, que cresceu 149% em 2020 (Saraiva, 2021). Isso demonstra que os consumidores têm recorrido cada vez mais à solicitação e utilização de produtos e serviços por meio digital.

Os riscos cibernéticos estão relacionados à segurança da empresa, incluindo trabalho remoto, teletrabalho, acesso a informações estratégicas e confidenciais e uso responsável de dispositivos como

laptops e smartphones (Strupczewski (2021). Esses riscos exploram vulnerabilidades induzidas por tecnologia, sistemas interconectados, humanos erro e despreparo das organizações para prevenir ou lidar com tais ataques (Liu et al., 2022).

Os gerentes devem estar cientes das várias fontes de risco cibernético e seu impacto potencial, garantindo que o negócio esteja suficientemente preparado contra tais eventos por meio da conscientização de segurança de entidades de infraestrutura crítica por meio de confidencialidade, disponibilidade e integridade dos serviços oferecidos (Egan et al., 2019; Amanowicz & Kamola, 2022).

2.2 Setor de Serviços

O setor de serviços é uma nomenclatura reconhecida mundialmente, baseada em um segmento representado pela força de trabalho desde a revolução industrial, configurando-se como a coprodução de valores por pessoas, tecnologia, sistema de atendimento interno e externo e informações compartilhadas (Fitzsimmons & Fitzsimmons, 2014).

Stoshikj Kryvinska e Strauss (2016, p. 214) resumem o setor como uma "ciência de serviços composta por sistemas de serviços holísticos, como cidades, universidades e hospitais – e que podem ser descritos como sistemas de sistemas, como alimentação, água, energia, saúde, educação, transporte" - uma vez que as empresas têm competido em algum grau com base em serviços (Zeithaml, 2017).

Além dos conceitos e especificidades trazidas pela literatura do setor de serviços, a pluralidade, a intangibilidade (não estocagem, a intransportabilidade e, sobretudo, a intransferibilidade) e o consumo simultâneo traduzem um formato praticamente unânime de atuação do setor (Gallouj, 1997; Mittal, 1999; Fitzsimmons & Fitzsimmons, 2014; Rajapathirana & Hui, 2018).

No Brasil, a representatividade do setor de serviços na economia pode ser destacada pela participação de 74% das atividades de serviços no Produto Interno Bruto (PIB) em 2020 (Agência Brasil, 2020). Numa perspectiva global, Rubalcaba e Solano (2023) expuseram os indicadores que refletem a participação percentual dos serviços no valor adicionado total nas regiões em desenvolvimento do mundo, que chega a aproximadamente 76%. Além disso, globalmente, esses serviços representam cerca de 51% dos empregos.

Nesse conteúdo, o setor se destaca na Agenda 2030 para o Desenvolvimento Sustentável, expondo a economia e o comércio de serviços com grande aptidão para induzir transformações estruturais e desenvolvimento sob o entendimento de que "políticas nacionais e esforços regulatórios, bem como políticas comerciais , multilaterais, regionais e cooperativos devem reconhecer o potencial para o desenvolvimento de serviços" (Conferência das Nações Unidas, 2017).

Em larga escala, "a economia como um todo pode ser interpretada como um enorme sistema de serviços, contendo uma variedade de entidades e subsistemas inter-relacionados" (Stoshikj et al., 2016, p. 212). Ainda, cada vez mais, a terceirização tem sido percebida como uma atividade complementar nas organizações para que elas possam se dedicar ao seu negócio principal (Gorla & Somers, 2014).

Barile et al. (2020) relatam que as transações de serviços estão evoluindo, e a sua natureza emergente aumentou a complexidade e incerteza, tornando-se cada vez mais imprevisível no ambiente de negócios. No entanto, os pesquisadores estão preocupados com a lacuna de inovação na pesquisa de serviços, apontando, como fatores significativos o investimento enxuto em iniciativas de pesquisa e desenvolvimento (Gallouj & Djellal, 2011; Rajapathirana & Hui, 2018) e o caráter menos tecnológico e dinâmico, quando em comparação com a indústria (Kubota, 2006).

Os estudos que analisam a inovação em serviços vêm crescendo em ritmo lento. Uma das motivações está assentada na tradicional investigação em inovação, que promove novas tecnologias e artefactos tangíveis, enquanto o setor dos serviços raramente formaliza iniciativas de Pesquisa & Desenvolvimento (P&D) ou as produz (Gallouj & Djellal, 2011).

Cenários de risco podem ser potencializados e acelerados em processos e modelos de negócios no segmento de serviços, inclusive levando empresas a sofrerem interrupção de atividades, incorrendo em altos custos, e enfrentando a possibilidade de litígio em desacordo com a existência do setor de serviço como solução de problemas para os clientes (Gadrey, Gallouj & Weinstein, 1995; Mcleod & Dolezel, 2018) .

3 Procedimentos Metodológicos

A bibliometria foi utilizada para investigar as publicações sobre a temática. A abordagem qualitativa possibilitou examinar e mensurar as publicações e suas particularidades para fornecer subsídios mais significativos para a análise dos resultados gerados.

A análise descritiva (Gil, 2002) considerou um levantamento quantitativo das publicações. Nesta etapa, explorou-se a evolução do número de artigos publicados por ano para identificar a tendência de interesse pelo tema “riscos cibernéticos no setor de serviços” na literatura de gestão empresarial sem desconsiderar o conteúdo existente em outras áreas de pesquisa. A cibernética é uma área interdisciplinar com base no conhecimento existente (Kim, 2004; Kandjani et al., 2012), e o setor de serviços é percebido como plural, intangível e compartilhável (Fitzsimmons & Fitzsimmons, 2014).

Além disso, este estudo utilizou o método de organização e sistematização das informações apresentado por Chueke & Amatucci (2015), cuja estrutura seguiu as premissas das leis de Bradford, Lotka e Zipf, utilizando as bases de dados científicas da plataforma Web of Science da CAPES, como mostrado na Tabela 2:

Tabela 2

Leis bibliométricas

Autor	Lei	Foco	Descrição	
Samuel C. Bradford	Lei de Bradford	Periódicos	A(r) = a + b.log (r)	A(r) = número cumulativo de artigos sobre o mesmo assunto publicados por periódicos diferentes r = *classificação cumulativa* a e b = constantes
Alfred J. Lotka	Lei de Lotka	Autores	$Y = C/X^2$	X = número de publicações Y = número de autores com x publicações C = constante
George K. Zipf	Lei de Zipf	Palavras	f(n) = K/n	f(n) = frequência de ocorrências de uma palavra n = ordem de frequência K = constante

Fonte: Guedes & Borschiver (2015); Chueke & Amatucci (2015)

A Lei de Bradford foi aplicada para identificar os periódicos científicos mais proeminentes que publicam estudos sobre riscos cibernéticos em serviços. Analisar a distribuição dos artigos científicos sobre o tema em diferentes periódicos permite identificar quais publicações têm se destacado e quais fornecem uma sólida base de conhecimento.

A Lei de Lotka foi utilizada para investigar a produtividade dos autores, identificando aqueles que são prolíficos e suas respectivas contribuições. Essa análise não apenas apoia a entender as perspectivas e abordagens adotadas no campo do risco cibernético no setor de serviços, mas também auxilia na identificação de autores cuja pesquisa pode ser relevante para o estudo.

E por último, a aplicação da Lei de Zipf na análise de estudos sobre riscos cibernéticos em serviços permite explorar a distribuição das palavras-chave mais frequentes encontradas na literatura científica. Analisar a frequência desses termos permite obter clareza sobre os principais riscos, ameaças e até mesmo ações mitigadoras que permeiam os modelos de negócios.

Essa análise busca um direcionamento fundamentado para o estudo, permitindo identificar com mais precisão as lacunas do conhecimento que merecem maior atenção. Adicionalmente, este estudo utilizará ferramentas como o VOSviewer para ampliar esta análise. Ao visualizar os dados da pesquisa, o VOSviewer permite identificar conexões e padrões entre os termos e temas mais recorrentes na literatura, contribuindo para a compreensão do campo de estudo dos riscos cibernéticos em serviços.

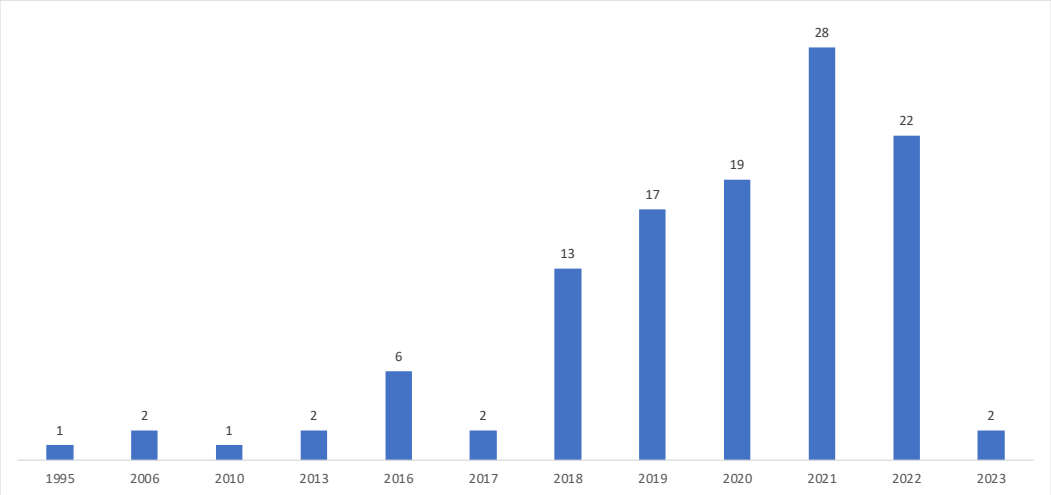
4 Apresentação e Análise de Resultados

A bibliometria foi aplicada para identificar, coletar e analisar os dados relevantes na literatura científica relacionados aos riscos cibernéticos em serviços. Com o objetivo de analisar as características das publicações sobre o tema, a metodologia procedeu primeiramente à coleta de dados utilizando os termos “riscos cibernéticos” e “serviços*” sem qualquer recorte temporal. Utilizando as bases de dados científicas da Web of Science (WoS), optou-se por buscar as publicações por "tópico" para alcançar a funcionalidade de busca de ocorrências nos termos indicados pelo título, resumo e palavras-chave trazidas pelos autores.

No processo de seleção dos artigos, adotou-se como critério-chave a pertinência do conteúdo referente à questão de pesquisa. O objetivo foi selecionar artigos que abordassem diretamente o tema em questão e estabelecessem relação, ou mesmo que de forma indireta com o objetivo e a questão delineada para esta pesquisa. Ao aplicar esse critério, buscamos garantir a inclusão dos estudos mais pertinentes, contribuindo para a qualidade e validade da pesquisa. Os critérios de exclusão adotados consideraram artigos que não enfocavam o objetivo da pesquisa e aqueles que não foram revisados por pares. Os estudos sobre riscos cibernéticos em serviços aumentaram significativamente nos últimos cinco anos, como pode ser observado no gráfico 1.

Gráfico 1

Produção científica anual sobre Riscos Cibernéticos em Serviços



Fonte: Dados da Pesquisa

Os resultados permitiram coletar publicações de dezembro de 1995 a fevereiro de 2023, chegando ao total de 624. Após a análise dessas publicações, um novo filtro foi aplicado, restringindo a busca. Como resultado, foram obtidos 115 artigos com foco no tema da pesquisa e revisados por pares.

Os resultados mostram que o tema tem crescido em importância, com o aumento das publicações a partir de 2018. É possível identificar uma lacuna desde 1995, em que o primeiro artigo sobre o tema

preconizava os "bancos do amanhã", apontando as oportunidades e os riscos do ambiente bancário digital.

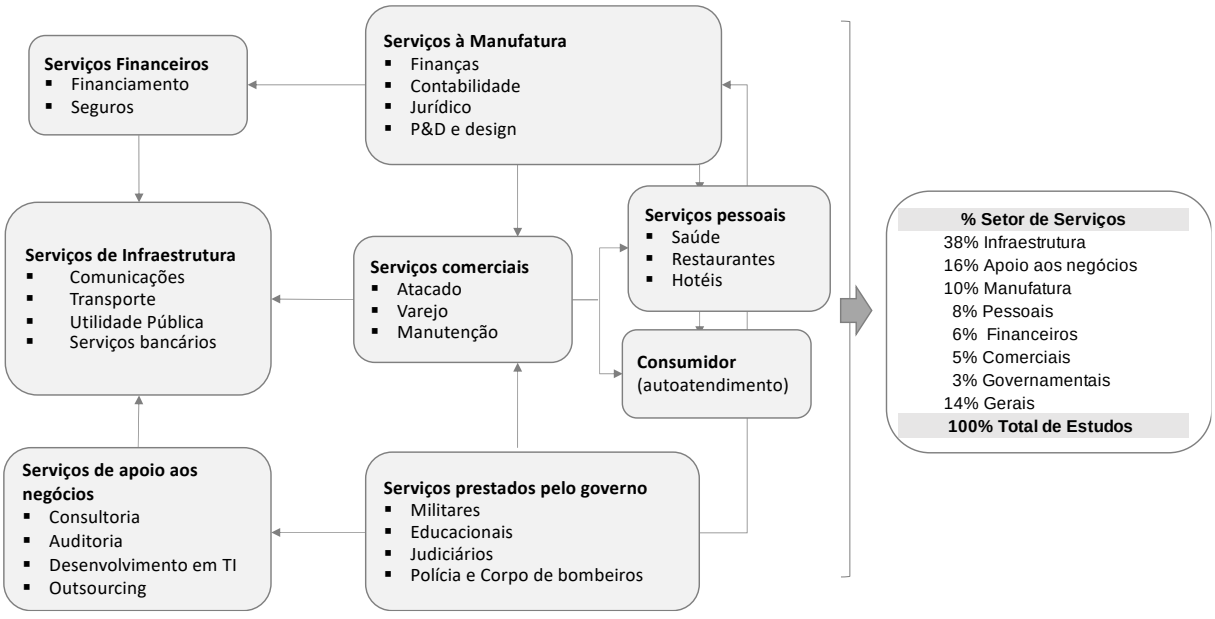
4.1 Organização das Publicações Científicas por Área de Pesquisa e Setor de Serviços

Na base de dados WoS - Web of Science, as publicações foram agrupadas de acordo com a área de pesquisa e o setor da área de serviço para o qual os estudos foram direcionados. Inicialmente, as publicações foram organizadas em dez áreas, com a seguinte ordem de relevância de publicação: Ciência da Computação e Sistemas de Informação (58%), Engenharia (35%), Negócios, Finanças e Gestão (29%), Telecomunicações (26%) e, Métodos de Teoria da Ciência da Computação, Inteligência Artificial da Informática (estes três últimos com 5%).

Ao explorar a produção científica sobre riscos cibernéticos no setor de serviços, buscou-se identificar em quais setores os estudos focaram o tema. A exploração incluiu a leitura e análise dos 115 artigos, permitindo sua classificação segundo os setores de serviços. Além disso, foram quantificados e observados, a partir do modelo proposto por Fitzsimmons & Fitzsimmons (2014), conforme mostra a Figura 1.

Figura 1

Riscos cibernéticos no setor de Serviços



Fonte: Adaptado de Fitzsimmons & Fitzsimmons (2014)

Na análise, destacaram-se os estudos em torno da infraestrutura (38%), o que pode ser justificado pela funcionalidade da complexa economia que compõe esses tipos de serviços, que funcionam como meio de distribuição para os clientes, constituindo um setor essência para a indústria (Fitzsimmons & Fitzsimmons, 2014).

Knowledge-Intensive Business Services (KIBS), ou Serviços Empresariais Intensivos em Conhecimento são serviços e operações de negócios fortemente dependentes de conhecimento profissional, comumente reconhecidos como serviços de suporte de negócios. A estatística (16%) apresentada para esses tipos de serviços segue em linha com a constatação de Desmarchelier, Djellal e Gallouj (2013), que afirmam que a fonte do aumento da produtividade do trabalho deslocou-se da indústria para os serviços, ainda que o motor do processo de terceirização continua sendo os setores industriais, dependentes de KIBS.

Na sequência, vem a área de serviços fabris (10%), composta por tomadas de decisão e controles internos das empresas. Considerou-se fundamental destacar o item "Geral" (14%), composto por estudos que abordam o setor de serviços, porém, de forma genérica, como Internet das coisas, estudos de caso e discussões sobre cibersegurança. Ao identificar as áreas de pesquisa com maior concentração do tema proposto, os resultados obtidos podem abrir a oportunidade de avaliar profundamente outros setores da área de serviços, como os setores pessoal, comercial e financeiro.

No que diz respeito à ação do governo, a oportunidade pode estar em medidas coercitivas e consequências legais para lidar com crimes cibernéticos cometidos contra empresas e indivíduos. A esse respeito, Mcleod e Dolezel (2018) entendem que as leis federais devem impor penalidades pesadas para as instalações cuja negligência contribua para violações de dados.

4.2 Expressões-chave mais usadas

Seguindo os critérios da Lei de Zipf, após revisão da literatura, foram obtidas as expressões-chave mais recorrentes que favorecem a busca pelo tema "Riscos Cibernéticos" e "Serviços", utilizados em conjunto por quase três décadas. No entanto, essas expressões também passaram a contribuir para outros resultados de busca.

Após a análise dos 624 artigos, que resultaram em 115 para este estudo, utilizamos o VOSviewer para aprimorar a visualização das informações. Ao carregar os arquivos de texto extraídos do WoS para o VOSviewer, optou-se por utilizar a funcionalidade "criar um mapa baseado em dados de texto". Em seguida, foi escolhida a opção "Título e campos do resumo" no campo "escolher arquivos" para incluir os campos título e resumo na análise. Na seção da "escolha o método de contagem", a "contagem binária" foi selecionada como o método de contagem. A contagem binária atribuiu o valor de "ocorrências" ao número de documentos em que um termo ocorre pelo menos uma vez. Um limite mínimo de cinco ocorrências foi definido no campo "número mínimo de ocorrências de um termo" em "escolher limite." Esses procedimentos ampliaram os critérios da Lei de Zipf, permitindo uma melhor visualização das expressões-chave no VOSviewer. Com o mapa resultante, obtivemos uma representação mais explícita e abrangente dos principais temas e interconexões nos artigos analisados.

No cálculo, palavras-chave foram identificadas pela WoS para representar os artigos do tema da pesquisa. A palavra mais frequente é "processo", obtida 37 vezes, seguida dos termos "internet" com

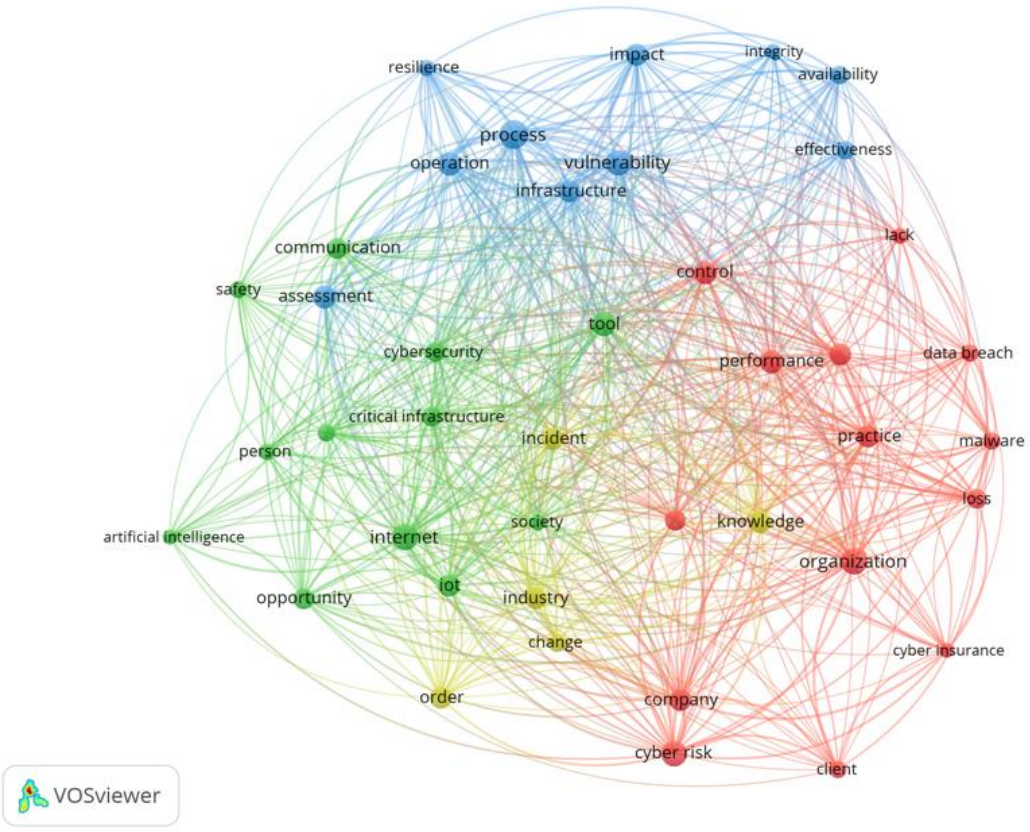
36, e “vulnerabilidade” 33 vezes. Além disso, foram identificados e descartados termos que não possuem um conceito específico aderente ao tema da pesquisa, palavras como "estudo", "caso" e "publicação".

Para melhor compreender a interação das expressões críticas obtidas pelos clusters que destacaram pontos de análise alusivos aos riscos cibernéticos no setor de serviços, a Figura 2 apresenta os termos obtidos pela técnica de visualização da densidade de citações por meio de cada ponto (cluster).

Cada ponto na exibição de densidade de itens tem uma cor correspondente, que indica a densidade dos itens naquele ponto. Por padrão, na visualização, a relação entre as cores e a distância das palavras-chave indica que quanto mais próximas estiverem, mais forte será a relação entre elas. O tamanho da imagem representada no cluster demonstra sua densidade, enquanto o círculo maior reflete a representatividade do item na amostra (Van Eck & Waltman, 2020).

Figura 2

Análise de rede



Fonte: Research Data / VOSviewer 1.6.19

Na figura 2, o cluster vermelho conglomera termos ligados a fatores mitigadores que podem caracterizar ameaças no ambiente cibernético, como atividades e desempenho de controle, conhecimento e segurança cibernética que permeiam os processos de uma organização, seja pela

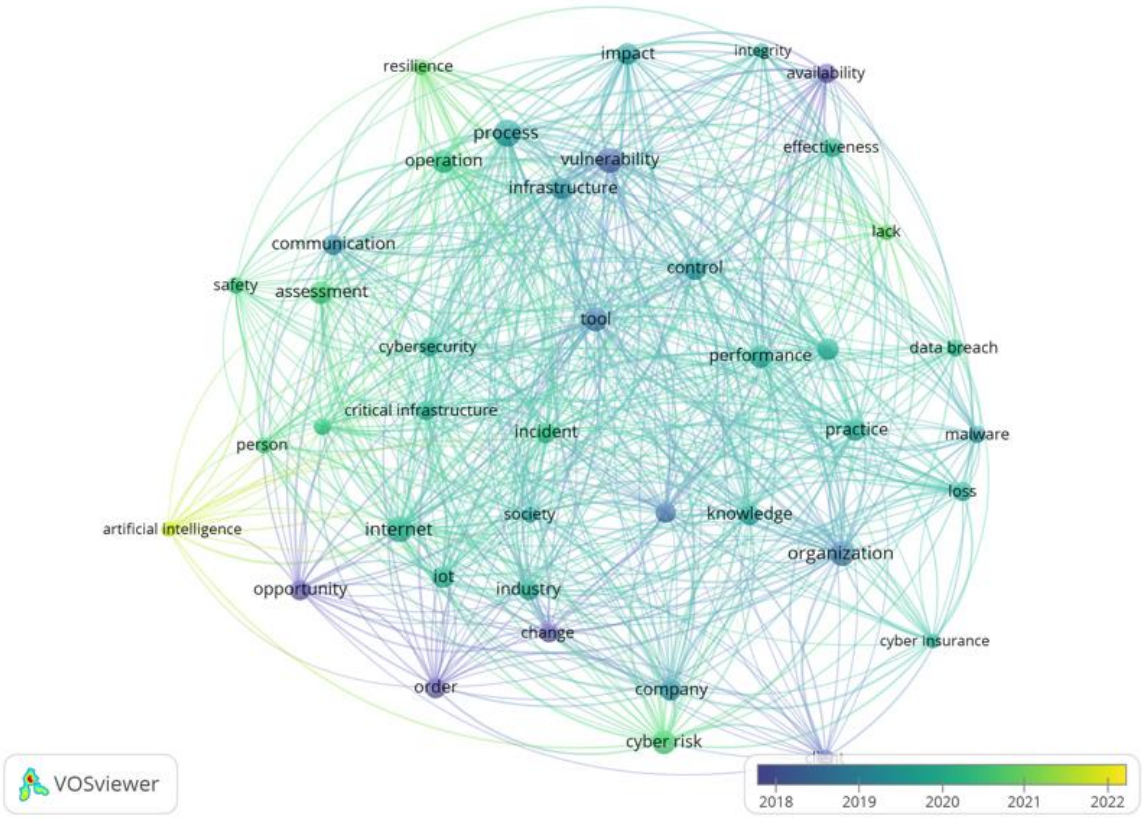
identificação de ataques, violações de dados, perdas (financeiro, operacional e reputacional) ou falta de conhecimento.

Em seguida, o cluster azul (figura 2) representa os estudos dedicados à compreensão do risco cibernético usando a Internet das coisas. Destacam-se os termos "vulnerabilidade" e "infraestrutura", em que a literatura destaca ataques, danos e subtração de informações do usuário. Termos como avaliação, eficácia, integridade e resiliência representam ações para enfrentar riscos relacionados a eventos futuros e incertos, exigindo um conhecimento mais profundo dos processos para gerenciá-los.

Enquanto o cluster verde destaca a Internet das coisas (IoT) e a Inteligência Artificial como elementos inseridos na literatura de risco cibernético, o cenário trazido pelo cluster verde é, de certa forma, absorvido pelo cluster vermelho, destacando fatores como incidentes, mudança , conhecimento, indústria e, consequentemente, pedidos (compras). Na literatura pesquisada também são destacados termos como infraestrutura crítica, comunicação e segurança, vinculados às informações dos clientes (empresa ou pessoa física) que realizam suas transações tecnológicas no Internet. É preciso considerar a relevância das ameaças e riscos nos últimos anos, a partir de 2018, com o aumento de publicações relacionadas a temas de discussão recentes, conforme o Gráfico 1 e a Figura 3.

Figura 3

Tópicos de discussão recentes



Fonte: Research Data / VOSviewer 1.6.19

Na Figura 3, analisando os temas discutidos a partir de 2018, pelo cluster azul, termos como vulnerabilidade, ferramenta, disponibilidade, mudança e oportunidade demonstram a preocupação com os riscos cibernéticos na infraestrutura organizacional, pois os pesquisadores começaram a voltar sua atenção para esses termos desse período em diante, como mostra o Gráfico 1.

O cluster amarelo representa estudos mais recentes abrangendo empresas de serviços sobre inteligência artificial, um campo de conhecimento que vem sendo estudado e aplicado aos setores de serviços, privados ou públicos, essenciais para o funcionamento da sociedade e da economia, o que confirma as estatísticas obtidas neste área de pesquisa (Figura 1).

Após expor os tipos de publicações, além das palavras-chave mais frequentes e recentes relacionadas aos riscos cibernéticos no setor de serviços, a análise da produção científica foi ampliada para identificar as fontes primárias de impacto, autores e os artigos mais relevantes e colaboração em pesquisas entre os países sobre este tema.

4.3 Artigos mais citados

Aplicando a Lei de Lotka (Chueke & Amatucci, 2015), a Tabela 3 mostra as publicações mais citadas sobre Riscos Cibernéticos no Setor de Serviços. Os artigos mais citados foram publicados nos últimos cinco anos, reforçando a relevância da divulgação científica diante das ameaças e ataques que empresas e indivíduos têm enfrentado. No entanto, a amostra pode ser considerada pequena, dada a relevância financeira e econômica trazida pelos riscos cibernéticos e ataques que tem ocorrido globalmente.

Tabela 3

Os artigos mais citados

Número Citações	Título	Autores	Periódico	Ano
239	Relationship between innovation capability, innovation type, and firm performance	Rajapathirana, RP Jayani; Hui, Yan	Revista de Inovação e Conhecimento	2018
143	A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services	Stellios, Ioannis; Kotzanikolaou, Panayiotis Psarakis, Mihalis; Alcaraz, Cristina; López, Javier	Pesquisas e tutoriais de comunicações do IEEE	2018
90	TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems	Alsaedi, Abdullah; Mustafá, Nour; Tari, Zahir; Mahmood, Abdun; Anwar, Adnan	Acesso IEEE	2020
86	Cybersecurity in Distributed Power Systems	Li, Zhiyi; Shahidehpour, Mohammad; Aminifar, Farrokh	Anais do IEEE	2017
75	Adaptive Formation of Microgrids with Mobile Emergency Resources for Critical Service Restoration in Extreme Conditions	Che, Liang; Shahidehpour, Mohammad	Sistemas de Energia de Transações IEEE	2019
72	Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach	Ullah, Farhan; Naeem, Hamad; Jabbar, Sohail; Khalid, Shehzad; Latif, Muhammad Ahsan; Al-Turjman, Fadi; Mostarda, Leonardo	Acesso IEEE	2019
51	Data security and consumer trust in FinTech innovation in Germany	Stewart, Harrison; Juerjens, janeiro	Segurança da Informação Informática	2018
55	A Survey of Moving Target Defenses for Network Security	Sengupta, Sailik; Chowdhary, Ankur; Sabur, Abdulhakim; Alshamrani, Adel; Huang, Dijiang; Kambhampati, Subbarao	Pesquisas e tutoriais de comunicações do IEEE	2020
40	Cyber-analytics: Modeling factors associated with healthcare data breaches	McLeod, Alexander; Dolezel, Diane	Sistemas de Suporte à Decisão	2018

Fonte: Dados da Pesquisa.

Ao considerar a importância dos artigos mais citados na comunidade científica, é essencial encontrar um equilíbrio entre o reconhecimento e a validade do estudo. Os artigos analisados (Tabela 3) convergem no reconhecimento dos riscos cibernéticos e na importância da implementação de medidas de segurança adequadas. Os autores destacam a necessidade de proteger organizações e usuários de ameaças cibernéticas para preservar a confidencialidade, integridade e disponibilidade dos sistemas. Além disso, três artigos enfocam os riscos associados à Internet das Coisas (IoT), abordando os desafios enfrentados em infraestrutura crítica e ambientes domésticos. O setor de serviços é identificado como uma área de preocupação, com destaque para setores como seguros, FinTech e distribuição de energia.

Embora compartilhem associações, os artigos diferem quanto a contextos específicos e abordagens propostas. Cada um aborda um contexto específico, como inovação em seguradoras, segurança IoT, segurança cibernética em sistemas elétricos distribuídos, detecção de ameaças em IoT,

confiança do consumidor em FinTech e análise de violação de dados na área da saúde. Essa diversidade de contextos reflete a amplitude dos setores em que os riscos cibernéticos são relevantes. Além disso, os documentos apresentam abordagens distintas para enfrentar os desafios de segurança cibernética. Isso inclui o uso de sistemas de detecção de intrusão, defesa de alvo móvel, técnicas de aprendizado profundo e medidas de segurança adaptáveis. Essas diferentes abordagens destacam a necessidade de uma abordagem abrangente e adaptável para combater as ameaças cibernéticas em constante evolução.

Os demais artigos resultantes da pesquisa, não listados na Tabela 3, abordam a importância da segurança cibernética em setores específicos, como saúde, bancos, e-commerce, petróleo e gás e infraestrutura, demonstrando preocupação em proteger dados sensíveis e sistemas nessas áreas devido aos riscos associados a possíveis violações de segurança. Além disso, há discussões sobre o uso de seguro cibernético para gerenciar riscos, indicando o reconhecimento das organizações sobre a necessidade de proteção contra danos causados por incidentes cibernéticos. Outro destaque é a Internet das Coisas (IoT), mencionada em diversos artigos, que traz desafios de segurança devido à crescente interconectividade de dispositivos e sistemas - isso expande a superfície de ataque e ressalta a importância de abordar adequadamente os riscos cibernéticos no contexto da IoT. Além disso, pontos de discussão comuns são a detecção e prevenção de ataques cibernéticos, como *botnets*, *ransomware* e tráfego de comando e controle, destacando a necessidade de mecanismos eficazes para defender e proteger contra ameaças em evolução.

Uma característica interessante a destacar nos dez artigos mais citados é que pelo menos sete deles são assinados por mais de quatro autores, chegando a oito em um único artigo. O que se pode inferir dessa amostra é o fato de o tema dos riscos cibernéticos no setor de serviços reunir um número mais significativo de pesquisadores devido à complexidade e multiplicidade de temas.

Também fica claro que o IEEE Xplore se destaca de outros periódicos em termos de publicações científicas e técnicas centradas em informática e eletrônica. No entanto, a gestão de riscos também envolve outras áreas do conhecimento, como administração, economia e sociologia.

4.4 Autores Mais Citados

Utilizando as premissas da Lei de Lotka (Chueke & Amatucci, 2015), foram identificados os autores mais relevantes da amostra de dados obtida. Dentre eles, os dez autores mais citados são apresentados na Tabela 4, seguidos da quantidade das respectivas citações e do número de artigos publicados.

Tabela 4

Autores mais citados

Autor	Número citações	Número Publicações
Rajapathirana, RPJ	239	1
Hui, Y.	239	1
Shahidehpour, M	161	2
Stélios, I.	144	2
Kotzanikolaou, P.	144	2
Psarakis, M	143	1
Alcaraz, C.	143	1
Lopes, J.	143	1
Li, Z.	86	1
Che, L.	75	1

Fonte: Dados da Pesquisa

Com os resultados apresentados na Tabela 4, os pesquisadores têm trabalhado recentemente no tema que abrange os riscos cibernéticos no setor de serviços, considerando que a amostra apresentou uma média de uma publicação para os dez autores mais citados.

Embora o artigo " Relationship between innovation capability, innovation type, and firm performance" dos autores Rajapathirana & Hui (2018) tenha recebido destaque significativo por meio de citações, este artigo não explora detalhadamente os riscos cibernéticos em serviços - apenas destaca que estes riscos são uma preocupação relevante para a indústria em relação à capacidade de inovação e desempenho das seguradoras.

As áreas de pesquisa dos demais autores estão ligadas aos desafios e ameaças encontrados no ambiente cibernético e aos serviços prestados neste contexto. Ioannis Stellios concentra em Segurança da Informação, abordando tópicos como criptografia, detecção de intrusão e proteção de informações confidenciais. Panayiotis Kotzanikolaou centraliza sua análise em privacidade, criptografia e infraestruturas críticas. Mihalis Psarakis explora Sistemas Integrados Confiáveis e Teste de Circuitos Integrados, que buscam proteger sistemas em dispositivos médicos, automóveis e equipamentos industriais. Cristina Alcaraz tem foco em Internet das Coisas (IoT) e Segurança de TI. Javier Lopez se concentra em segurança de TI de forma ampla, abordando tópicos como criptografia, segurança de rede e estratégias de defesa. Zhiyi Li pesquisa operações de sistemas de energia, segurança cibernética e cidades inteligentes. Por fim, Liang Che se concentra em operações e controle do sistema de energia. Foi possível obter as respectivas áreas de pesquisa dos autores por meio da WoS (Web of Science), complementando as informações obtidas no estudo bibliométrico. A lista dos autores mais citados pode ajudar a orientar os pesquisadores que desejam explorar no tema de riscos cibernéticos e serviços.

4.5 Publicações por países

Ao identificar a origem dos artigos publicados em uma determinada área de pesquisa, é possível ter uma visão da distribuição geográfica da produção científica e identificar os países ou instituições líderes em riscos cibernéticos no setor de serviços. Pesquisadores dos Estados Unidos lideram o volume de publicações, seguidos pelo Reino Unido, Holanda, Suíça e, na quinta posição, o México. A Tabela 5 apresenta os países com maior número de publicações nas bases de dados investigadas.

Tabela 5

Publicações por países

Posição	Países	Número de publicações
1	Estados Unidos	43
2	Reino Unido	22
3	Holanda, Suíça	13
4	Alemanha	6
5	México	3
7	Espanha, Japão, Romênia e Ucrânia	4
8	China, Colômbia, Croácia, França, Índia, Coreia do Sul, Polônia	3

Fonte: Dados da Pesquisa

É importante destacar que o conjunto de 115 trabalhos analisados foi publicado em 17 países por pesquisadores de 47 nacionalidades diferentes – o que pode demonstrar a forma descentralizada e pulverizada com que se encontra o tema dos riscos cibernéticos nos serviços. No entanto, devido à pluralidade de países e pesquisadores, infere-se que o assunto tornou-se uma preocupação mundial, mesmo com a escassez de publicações.

O Cryptocurrency Crime Report, emitido pela ChainAnalisys (2021), revelou o ranking dos países que receberam os maiores volumes de criptomoedas de endereços ilícitos com base na análise das localizações dos usuários do serviço. Entre as cinco primeiras posições dessa avaliação estão Estados Unidos e Reino Unido, o que pode justificar a liderança desses países em publicações relacionadas a riscos cibernéticos no setor de serviços.

5 Discussão

As 115 publicações identificadas têm em comum o foco em riscos cibernéticos e segurança da informação em diferentes contextos. Embora cada um aborde aspectos específicos, a maioria reconhece a importância de abordar os riscos cibernéticos para proteger os ativos, garantir a confiança do cliente e promover a inovação. Além disso, a maioria dos artigos menciona a Internet das Coisas (IoT) como um

campo em que os riscos cibernéticos são especialmente relevantes. Eles apontam que os dispositivos IoT em infraestrutura crítica e ambientes domésticos podem ser pontos de entrada para ataques cibernéticos, exigindo medidas de segurança apropriadas para proteger a privacidade dos dados e garantir a integridade do sistema.

O envolvimento e a importância dos setores de serviços na economia abrangem infraestrutura, serviços empresariais intensivos em conhecimento, manufatura e outros setores, conforme indicado na Figura 1. Esses setores fornecem serviços essenciais à sociedade e estão interligados a outros, desempenhando um papel fundamental na economia em desenvolvimento. No entanto, as publicações reforçam o entendimento de que o setor de serviços também enfrenta riscos cibernéticos que podem comprometer a eficiência, a segurança e a confiabilidade e afetar negativamente as operações comerciais de clientes, fornecedores e governo. As publicações são praticamente unânimes de que a adoção de medidas de segurança e estratégias de gestão de riscos fortaleceria a resiliência desses setores e garantiria a continuidade dos serviços prestados.

Uma lacuna identificada após a revisão das publicações é a falta de modelos ou diretrizes que considerem os riscos cibernéticos em diferentes subsetores do setor de serviços, como serviços financeiros, saúde, turismo, varejo e outros. Com base nos trabalhos publicados, desenvolveu-se um modelo conceitual como ponto de partida para atender às demandas emergentes do setor de serviços. Este modelo fornece uma estrutura abrangente (Figura 4) que aborda de forma eficaz os desafios enfrentados até o momento, ao mesmo tempo em que se esforça para atender às necessidades identificadas na linha de tendência. Ainda, este modelo pode ser estendido a outros setores da economia além do setor de serviços.

Figura 4

Modelo Conceitual de Riscos Cibernéticos em Serviços

Fonte: Elaborado pelos autores (2023)

Esse modelo propõe a adoção de uma abordagem de melhoria contínua e cíclica para lidar com esses três elementos: vulnerabilidades, ameaças cibernéticas e consequências. Isso envolve identificar e avaliar as vulnerabilidades existentes, desenvolver e implementar medidas de segurança apropriadas para mitigar as ameaças identificadas e monitorar constantemente as ameaças e consequências para ajustar e melhorar continuamente as práticas de segurança.

Capacitação e conscientização: este modelo propõe a capacitação e a conscientização no centro da mitigação do risco cibernético no setor de serviços. Partindo do pressuposto de que capacitar e treinar as partes interessadas (além de funcionários, clientes e fornecedores) é fundamental para fortalecer a resiliência de uma empresa à incerteza e ao risco, o treinamento está alinhado para desenvolver habilidades relevantes, adaptar-se à mudança, usar melhor os recursos (sistemas e políticas) e tomar decisões. Dos trabalhos revisados neste estudo, os exemplos incluem desafios relacionados à tecnologia e negócios de comércio eletrônico que exigem enfrentamento orientado pelo conhecimento por parte dos usuários (Liu et al., 2022), desenvolvimento de conhecimento e treinamento para investigadores de crimes cibernéticos (Johnson et al., 2020), além de treinamento para modelos de aprendizado de máquina, segurança de IoT e classificação de tráfego de rede (Guan et al., 2021).

Além disso, combinando capacitação com compliance na gestão de TI, Sipior et al. (2021) expõem a aplicação de um estudo de caso do "mundo real" para fornecer recomendações relacionadas aos riscos operacionais de TI de uma organização em suas operações, relatórios financeiros e conformidade.

Gerenciamento de conformidade de TI: definir responsabilidades por meio de investimentos em seguro cibernético para transferir alguns dos riscos associados a possíveis violações no futuro (Bodin et al., 2018). Ainda, Rifat et al., 2019, destacaram a importância do gerenciamento de riscos cibernéticos, da garantia de conformidade e qualidade dos serviços eletrônicos de impostos (e-tax) no governo digital. Além disso, a conformidade na gestão de TI inclui líderes envolvidos no suporte de transição, focado na melhoria da governança e integração, e suporte transformacional, que envolve a promoção de uma nova mentalidade cultural para resiliência cibernética (Loonam et al., 2022).

Medidas de segurança: a cibersegurança desempenha um papel relevante no setor de serviços. A implementação de medidas de segurança, como o uso de tecnologias avançadas e a formação de microrredes (Li et al., 2017; Che & Shahidehpour, 2019), pode ajudar a mitigar riscos e garantir a continuidade do serviço em desastres ou ataques cibernéticos. A confiança do consumidor e a qualidade do serviço são fatores essenciais na adoção de inovações, como as tecnologias financeiras (Stewart & Jurjens, 2018). Os artigos destacam a necessidade de investir em medidas robustas de segurança cibernética e serviços de alta qualidade para ganhar a confiança do cliente e promover uma adoção mais ampla de inovações tecnológicas - como a computação em nuvem, que conquistou a adesão das empresas devido à sua escalabilidade, estabilidade e alta disponibilidade (Ouedraogo & Mouratidis, 2013; Akinrolabu et al., 2019; Torkura et al., 2020).

Gerenciamento de Incidentes: em relação ao gerenciamento de incidentes, as publicações também enfatizam a necessidade de abordagens inovadoras e adaptativas para segurança cibernética, como o uso de sistemas de detecção de intrusão adaptados para aplicações de Internet das Coisas Industrial (IIoT) e Defesa de Alvo Móvel (MTD)[3]. Essas abordagens visam mitigar os riscos cibernéticos, superando as vantagens dos invasores e adaptando-se continuamente aos ataques (Bruger et al., 2019; Alsaedi et al., 2020; Sengupta et al., 2020).

A revisão da literatura e o estudo bibliométrico permitiram aprofundar a análise de conteúdo das publicações de forma que pudesse trazer um modelo que não apenas representasse e comunicasse os conceitos e relações que envolvem os riscos cibernéticos no setor de serviços, mas que os tornasse mais acessíveis, permitindo uma melhor compreensão do tema para o desenvolvimento de pesquisas futuras.

[3]O objetivo central do MTD é criar um ambiente de computação dinâmico onde os principais elementos do sistema, como endereços IP, portas de rede, protocolos e configurações, são constantemente alterados ou mascarados.

6 Considerações Finais

Ao combinar os dois temas, riscos cibernéticos e setor de serviços, foi possível abordar os desafios específicos que surgem nas transações por meio do comércio eletrônico e as ameaças à confidencialidade e integridade das informações. Além disso, também está incluída a segurança do dispositivo, que envolve os riscos associados aos dispositivos conectados à rede, cujas publicações têm discutido amplamente a IoT.

Muitos serviços atualmente dependem de dispositivos IoT para operar de forma eficiente no setor de serviços. Por exemplo, nos setores de saúde, energia e transporte, a IoT desempenha um papel crucial no monitoramento e controle de sistemas críticos. As empresas de serviços podem tomar medidas de segurança apropriadas para proteger seus sistemas e infraestrutura contra possíveis ataques ao compreender os riscos cibernéticos associados aos dispositivos IoT. Isso pode envolver a implementação de práticas de segurança robustas, como autenticação forte, criptografia de dados e monitoramento contínuo de dispositivos IoT.

Além disso, as publicações abordaram preocupações sobre o ambiente de infraestrutura, onde os riscos cibernéticos estão associados à segurança e operação de sistemas de infraestrutura crítica, como redes elétricas, transporte, água, saúde, telecomunicações e outras instalações críticas. Isso cobre as vulnerabilidades desses dispositivos e um ambiente propenso a fraudes. Isso porque os serviços desenvolvidos no ambiente cibernético envolvem o processamento e armazenamento de informações sensíveis, como dados pessoais e financeiros dos usuários, tornando-os alvos potenciais de ataques cibernéticos.

O tímido número de publicações pode indicar que o tema dos riscos cibernéticos não recebe atenção dos pesquisadores há quase 30 anos. Isso pode resultar de uma menor conscientização sobre os riscos cibernéticos em períodos anteriores ou da falta de interesse acadêmico em explorar o assunto. A presença de muitos autores sobre um tema com poucas publicações sugere que a pesquisa sobre riscos cibernéticos envolve uma abordagem interdisciplinar. Isso porque o risco cibernético é uma área complexa que engloba aspectos técnicos, legais, éticos, sociais e comportamentais. Portanto, a colaboração de diversos especialistas pode ser necessária para entender completamente os desafios associados a esse tópico.

No entanto, outro ponto que contribui para essa perspectiva de que o tema dos riscos cibernéticos não é amplamente discutido ou referenciado na literatura científica é o número de citações. Isso pode resultar de desenvolvimento conceitual insuficiente, pesquisa ou base teórica menos consolidada. Considerando a crescente relevância da segurança cibernética, pode-se inferir que os riscos cibernéticos devem chamar mais atenção dos pesquisadores. Com a rápida evolução da tecnologia e as crescentes ameaças cibernéticas, há uma necessidade crescente de explorar e entender estes riscos em profundidade.

Este estudo adotou como critério para elaboração da amostra analisada no estudo bibliométrico as publicações que continham as palavras-chave "riscos cibernéticos" e "serviços*" mencionadas no item tópico da WoS. Nesta pesquisa, foram apresentadas publicações de destaque que podem ser exploradas com profundidade por pesquisadores do setor de serviços, especialmente os riscos cibernéticos nos setores destacados na Figura 1, o que pode ser uma oportunidade interessante para expandir pesquisas empíricas considerando a pluralidade do tema dos serviços e considerando que quanto maior a conectividade, maior a sujeição da empresa aos riscos cibernéticos.

A revisão da literatura realizada neste estudo ratificou o valor científico dos estudos bibliométricos e as contribuições para a área, considerando que:

(i) A pesquisa revelou o potencial de exploração do tema, na qual foram identificadas as áreas de serviços e sua representatividade nas pesquisas relacionadas aos riscos cibernéticos.

(ii) Possibilitou a organização conceitual dos riscos cibernéticos e seu núcleo/foco de entendimento (Tab. 1).

(iii) Pode identificar tendências emergentes e clusters nas atividades do setor de serviços (Fig. 2 e 3).

(iv) O desenvolvimento do modelo conceitual (Fig. 4) pretende ser uma estrutura inicial, fornecendo subsídios para pesquisas futuras e desenvolvimento contínuo no setor de serviços.

Os achados são considerados relevantes para pesquisadores que desejam se aprofundar em uma determinada atividade de serviços para além de outros setores da economia. Além disso, este estudo buscou despertar o interesse de pesquisadores de diferentes áreas, como administração, tecnologia e sociologia, indo além dos referenciais teóricos e focando na aplicação e operacionalização no contexto organizacional.

Referências

Abbagnano, N. (2007). *Dicionário de Filosofia*, São Paulo: Martins Fontes.

Amanowicz, M., & Kamola, M. (2022). *Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspac*e. Electronics, 11(22), 3835.

Brazil Agency. (2020). *Serviços avançam e comércio cai como parcela do PIB desde 1947*. Retrieved on february 01, 2023, from https://agenciabrasil.ebc.com.br/economia/noticia/2020-12/servicos-avancam-e-comercio-recua-na-participacao-no-pib-desde-1947 .

Barile, S., Grimaldi, M., Loia, F., & Sirianni, CA (2020). Technology, value Co-Creation and innovation in service ecosystems: Toward sustainable Co-Innovation. *Sustainability*, 12(7), 2759.

Biener, C., Eling, M., & Wirfs, JH (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), 131-158.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544.

Böhme, R., Laube, S., Riek, M. (2018). A fundamental approach to cyber risk analysis. *Variance,* 12 (2), 161–185.

Brewer, D. (2000). *Risk assessment models and evolving approaches.* IAAC Work. Retrieved January 29, 2023, from www.gammassl.co.uk/research/archives/events/IAAC.php .

Cebula, JL, & Young, LR (2010). *A taxonomy of operational cyber security risks.* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Chain Analysis (2021). *The 2021 Crypto Crime Report – Everything you need to know about ransomware, darknet markets, and more.* Retrieved January 28, 2023, from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf .

Chueke, GV., & Amatucci, M. (2015). O que é bibliometria? Uma introdução ao Fórum. *Internext*, *10*(2), 1-5.

Conger, S., Pratt, JH., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401-417.

Desmarchelier, B., Djellal, F., & Gallouj, F. (2013). *Knowledge intensive business services and long term growth.* Structural Change and Economic Dynamics, 25, 188-205.

Durak, T. (2020). Innovation spaces: the new campus risk paradigm. In Challenges *for Health and Safety in Higher Education and Research Organizations,* pp. 304-336. Royal Society of Chemistry.

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acaryya, M., ... & Ang, K. (2019). Cyber operational risk scenarios for insurance companies. *British Actuarial Journal,* 24.

Fang, E., Palmatier, RW, & Steenkamp, JBE (2008). Effect of service transition strategies on firm value. *Journal of Marketing*, 72(5), 1-14.

Fitzsimmons, JA, & Fitzsimmons, MJ (2014). *Service Administration: Operations, Strategy and Information Technology.* Amgh Publisher.

Funke, Martha. (2021). Empresas lançam soluções voltadas para riscos cibernéticos. *Jornal Valor.* Consultado em 28 de janeiro de 2023, em https://valor.globo.com/publicacoes/suplementos/noticia/2021/03/25/empresas-lancam-solucoes-voltadas-a-riscos-ciberneticos.ghtml

Gadrey, J., Gallouj, F., & Weinstein, O. (1995). New modes of innovation: how services benefit industry. International Journal of Service Industry Management.

Gallouj, C. (1997). Asymmetry of information and the service relationship: selection and evaluation of the service provider. International Journal of Service Industry Management.

Gallouj, C. (2023). Information Economy, Knowledge Economy, Intangible and New Economy... What Next? In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), Elgar Encyclopedia of Services (pp. 119-121). Edward Elgar Publishing.

Gallouj, F., & Djellal, F. (Eds.). (2011). The handbook of innovation and services: a multi-disciplinary perspective. Edward Elgar Publishing.

Ghorbani, HR, & Ahmadzadegan, MH (2017, November). Security challenges in internet of things: survey. In *2017 IEEE Conference on Wireless Sensors* (ICWiSe), 1-6. IEEE.

Gil, AC (2002). *Como elaborar projetos de pesquisa*, vol. 4, p. 175. São Paulo: Atlas.

Gorla, N., & Somers, TM (2014). The impact of IT outsourcing on information systems success. *Information & Management*, 51(3), 320-335.

Guan, J., Cai, J., Bai, H., & You, I. (2021). Deep transfer learning-based network traffic classification for scarce dataset in 5G IoT systems. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3351-3365.

Guedes, V. L., & Borschiver, S. (2005). Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *Encontro nacional de ciência da informação*, *6*(1), 18.

ISO/IEC (2014). *ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary*. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). Retrieved January 28, 2023, from https://www.iso.org/standard/63411.html

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, *84*(5), 427-450.

Kandjani, H., Wen, L., & Bernus, P. (2012). Enterprise architecture cybernetics for collaborative networks: Reducing the structural complexity and transaction cost via virtual brokerage. *IFAC Proceedings*, 45(6), pp. 1233-1239.

Kim, J. H. (2004). Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. *Horizontes antropológicos*, *10*, 199-219.

Klimburg, A. (Ed.). (2012). *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence.

Kubota, LC. (2006). Inovação tecnológica das empresas de serviços no Brasil. *In* JA Negri, LC Kubota (Orgs.). *Estrutura e dinâmica do setor de serviços no Brasil*. Indivíduo. 2. Instituto de Pesquisa Econômica Aplicada. Brasília: IPEA, 35-72.

Lévy, P. (2000). *Cibercultura*. 2ª ed. São Paulo: Editora 34.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce, Front. Psychol., 19 October 2022, Sec. Organizational Psychology.

Mantha, B. R., & García de Soto, B. (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management*, *28*(10), 3078-3105.

Melo, H. P. D., Rocha, F., Ferraz, G. T., Di Sabbato, A., & Dweck, R. H. (1998). *O setor serviços no Brasil: uma visão global*-1985/95.

McAfee (2021). *What is malware*? Retrieved January 28, 2023, from https://www.mcafee.com/en-us/antivirus/malware.html

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68.

Metters, R. (2023). Service Operations. In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), *Elgar Encyclopedia of Services* (pp. 183-185). Edward Elgar Publishing.

Mittal, B. (1999). The advertising of services: meeting the challenge of intangibility. *Journal of Service Research*, *2*(1), 98-116.

NAIC (2018). Cybersecurity Risk Management. *National Association of Insurance Commissioners (NAIC)*. Retrieved January 30, 2023, from https://content.naic.org/consumer/cybersecurity.htm.

Neghina, DE, & Scarlat, E. (2012). Managing information technology security in the context of cyber crime trends. *International journal of computers communications & control*, 8(1), 97-104.

Nieuwesteeg, B., Visscher, L., & de Waard, B. (2018). The law and economics of cyber insurance contracts: a case study. *European Review of Private Law*, 26(3).

NIST - National Institute of Standards and Technology (2006). Minimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200. National Institute of Standards and Technology (NIST), Gaithersburg, MD. Retrieved January 30, 2023, from https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf .

Nordin, F., Kindström, D., Kowalkowski, C., & Rehme, J. (2011). The risks of providing services: Differential risk effects of the service-development strategies of customisation, bundling, and range. *Journal of Service Management*, *22*(3), 390-408.

Nonaka, I., o Nonaka, I., Ikujiro, N., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation* (Vol. 105). OUP USA.

Pal, R., Huang, Z., Lototsky, S., Yin, X., Liu, M., Crowcroft, J., ... & Nag, B. (2021). Will catastrophic cyber-risk aggregation thrive in the IoT age? A Cautionary Economics Tale for (Re-)Insurers and Likes. *ACM Transactions on Management Information Systems* (TMIS), 12(2), 1-36.

Powers, M. R. (2006). Pure vs speculative risk: False choice; sham marriage. *The Journal of Risk Finance*, *7*(4), 345-347.

Raddats, C., Kowalkowski, C., Benedettini, O., Burton, J., & Gebauer, H. (2019). Servitization: A contemporary thematic review of four major research streams. *Industrial Marketing Management*, *83*, 207-223.

Rajapathirana, RJ, & Hui, Y. (2018). Relationship between innovation capability, innovation type, and firm performance. *Journal of Innovation & Knowledge*, 3(1), 44-55.

Rifat, A., Nisha, N., & Iqbal, M. (2019). Predicting e-tax service adoption: Integrating perceived risk, service quality and TAM. *Journal of Electronic Commerce in Organizations* (JECO), 17(3), 71-100.

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701-728.

Rubalcaba, L., & Solano, E. (2023). Services Economic Growth. In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), *Elgar Encyclopedia of Services* (pp.92-94). Edward Elgar Publishing.

Saraiva, J. (2021). *Novos hábitos fazem gastos com entrega crescerem 149% em 2020* . Jornal valor. suplementos. Consultado em 28 de janeiro de 2023, em https://valor.globo.com/publicacoes/suplementos/noticia/2021/06/29/novos-habitos-fazem-gastos-com-entregas-crescerem-149-em-2020. ghtml .

Saridakis, G., Benson, V., Ezingeard, JN, & Tennakoon, H. (2016). Individual security information, user behavior and cyber victimization: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320-330.

Silva, W. R., & Nogueira, J. M. (2019). Ataques cibernéticos e medidas governamentais para combatê-los. *O Comunicante*, *9*(1), 42-57.

Sipior, J. C., Lombardi, D. R., & Gabryelczyk, R. (2021). Information Technology Operational Risk: A Teaching Case. *Journal of Computer Information Systems*, *61*(4), 328-344.

Stoshikj, M., Kryvinska, N., & Strauss, C. (2016). Service systems and service innovation: two pillars of service science. *Procedia computer science*, *83*, 212-220.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135, 105143.

United Nations Conference (2017). *The role of the services economy and trade in structural transformation and inclusive development.* Trade and Development Board. Geneva, July 2017. Retrieved January 28, 2023, from https://unctad.org/system/files/official-document/c1mem4d14_en.pdf .

Van Eck, NJ, Waltman, L. (2020). *VOSviewer Manual: Manual for VOSviewer version 1.6.17* . 25 November 2020. Universiteit Leiden/ CWTS. Retrieved January 28, 2023, from https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.16.pdf.

Wiener, N. (1984). *Cibernética e sociedade: o uso humano de seres humanos.* São Paulo: Cultrix, 1984.

Wiener, N. (2017). *Cibernética ou controle e comunicação no animal e na máquina* . Tradução de Gita K. Guinsburgl. 1st ed. São Paulo: Perspective

World Economic Forum. (2012). *Global risks 2012.* Seventh edition, Insight Report, Geneva.

Younan, M., Houssein, EH, & Ali, AA (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, v. 151.

Zeithaml, VA (2017). *Excelência em atendimento.* Saraiva Educação SA.