# PRODUÇÃO DE ARTIGOS CIENTÍFICOS SOBRE SEGURANÇA CIBERNÉTICA NO SETOR PÚBLICO: UM ESTUDO EM BASES DE DADOS ACADÊMICAS

[1]GUILHERME DE OLIVEIRA NOLETO, [1]CARLOS ANDRÉ DE MELO ALVES

[1]Universidade de Brasília (UNB)
<olinoleto@gmail.com> <carlosandre@unb.br>
DOI: 10.21439/conexoes.v19.3865

**Resumo.** A segurança cibernética é tema de atenção entre pessoas, organizações e governos, despertando interesses em diferentes setores, tanto privado quanto público. A presente pesquisa busca investigar a produção científica sobre a segurança cibernética no setor público de 2018 a 2023. Trata-se de estudo descritivo com abordagens quantitativa e qualitativa. Efetua-se uma revisão de literatura, selecionando-se 70 artigos da amostra com base no método PRISMA. Os artigos da amostra foram coletados nas bases de dados *Scopus e Web of Science* (WoS). O tratamento dos dados empregou a análise de conteúdo para classificar os artigos por níveis de análise, segundo Oliveira e Abib (2023), complementado pelo emprego da nuvem de palavras. Os principais resultados permitiram identificar artigos em níveis de análise 'Organizacional' (47,14%), 'Ambiental' (38,57%) e 'Individual' (14,29%). Apurou-se 57,14% dos artigos publicados entre 2022 e 2023. Constataram-se 45 filiações acadêmicas na Europa, 42 filiações na região Ásia-Pacífico e 35 nas Américas. Verificou-se 65,71% dos artigos produzidos com até 3 autores. A abordagem qualitativa esteve presente em 62,86% dos artigos da amostra. Este estudo busca contribuir para reflexões de pesquisadores, gestores públicos e demais partes interessadas, trazendo subsídios para delinear oportunidades de pesquisas futuras sobre segurança cibernética no setor público.

**Palavras-chave:** segurança cibernética; espaço cibernético; governo; setor público; produção científica.

# PRODUCTION OF SCIENTIFIC ARTICLES ON CYBERSECURITY IN THE PUBLIC SECTOR: A STUDY IN ACADEMIC DATABASES

**Abstract.** Cybersecurity is of great interest to people, organizations, and governments, arousing interests in different sectors, both public and private. This article aims to investigate the scientific production of cybersecurity in the public sector between 2018 and 2023. It is a descriptive study with quantitative and qualitative approaches. The literature review identified 70 articles for the sample using the PRISMA method. The sample's articles were collected on Scopus and Web of Science (WoS) databases. Concerning the data treatment, content analysis was employed for the classification of the articles on Individual, Organizational, and Environmental levels, according to Oliveira and Abib (2023), complemented by the use of the word cloud. The main results allowed identifying the articles on 'Organizational' (47,14%), 'Environmental' (38,57%), and 'Individual' (14,29%) analysis levels. 57.14% of the sample's articles were published between 2022 and 2023. Was found 45 academic affiliations in Europe, 42 affiliations in the Asia-Pacific region, and 35 in the Americas. In addition, 65.71% of articles were produced with up to 3 authors. The qualitative approach was present in 62.86% of the articles in the sample. This study seeks to contribute to the reflections of researchers, public managers, and other interested parties, providing support to outline opportunities for future research on cybersecurity in the public sector.

**Keywords:** cybersecurity; cybernetic space; government; public sector; scientific production.

## 1 INTRODUÇÃO

A Segurança Cibernética, em inglês *Cyber Security ou Cybersecurity*, é um tema que abrange atenção de pessoas, na proteção de suas liberdades e direitos no espaço cibernético, de empresas, para a gestão e proteção de dispositivos, sistemas e infraestruturas de rede, por exemplo, e de governos, para a segurança nacional, proteção de infraestruturas críticas, governo eletrônico e demais motivações de interesse tanto público quanto privado (Al-Zahrani, 2020; Shackelford, 2019).

À medida em que as interações por meio do espaço cibernético se expandiram e alcançaram implicações para as atividades de pessoas e de organizações, concomitantemente houve o aumento da preocupação com os riscos e incidentes cibernéticos (Rutkowski, 2011). Em razão disso, atualmente, incluir a segurança cibernética na agenda pública tornou-se necessário e relevante para governos em diferentes jurisdições.

No Brasil, existem esforços para normatizar a segurança cibernética em nível nacional no setor público, cabendo desde dezembro de 2023 à Política Nacional de Cibersegurança (PNCiber) orientar a atividade de segurança cibernética no País (Brasil, 2023). No cenário internacional, há uma variedade de formas de conduzir a segurança cibernética, sendo que as principais referências para a manutenção da segurança de espaços cibernéticos podem ser encontradas na *International Organization for Standardization* (ISO) e *The International Electrotechnical Commission* (IEC) (ISO/IEC, 2023), na *International Telecommunication Union* (ITU) (ITU, 2021) e no *framework* de segurança cibernética do *National Institute for Standards and Technology* (NIST) (NIST, 2024).

Assim, o estudo da produção científica sobre segurança cibernética no setor público é um tema de interesse acadêmico. A partir do exame da produção científica sobre o tema é possível, empregando técnicas bibliométricas, melhor entender características atuais da literatura em âmbitos como principais autores e filiações, palavras-chaves mais recorrentes e principais abordagens metodológicas. Esse exame, também, ajuda a entender as práticas relativas à segurança cibernética, para uso em organizações públicas, por permitir identificar temas relevantes por meio da nuvem de palavras-chaves.

O objetivo deste estudo é investigar a produção científica sobre a segurança cibernética no setor público de 2018 a 2023. Trata-se de pesquisa descritiva com abordagem qualitativa e quantitativa, em que se coletou uma amostra de 70 artigos, empregando-se o método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA).

Justifica-se o presente estudo porque contribui para preencher lacuna de estudos com a observação da produção científica sobre segurança cibernética no setor público sob um prisma sistêmico, baseado na classificação Nível Organizacional, de Oliveira e Abib (2023), buscando trazer reflexões sob a perspectiva prática para partes interessadas como pesquisadores, gestores e demais agentes públicos relacionados à segurança cibernética na área pública, trazendo subsídios para delinear oportunidades de pesquisas futuras sobre o tema.

## 2 REFERENCIAL TEÓRICO

### 2.1 Segurança cibernética e o setor público

A Segurança Cibernética é um termo de definição difusa. A evolução de sua caracterização acompanhou a evolução das Tecnologias de Informação e Comunicação (TIC) ou *Information and Communication Technologies* (ICT), em inglês, inaugurando o desenvolvimento e consolidação do que se entende atualmente por espaço cibernético ou *cyberspace* (Rutkowski, 2011). Sem prejuízo desse fato, são exibidos nesta subseção elementos que buscam melhor delimitar o referido termo.

Buscando uma delimitação mais abrangente, admite-se a seguinte definição para segurança cibernética:

> (...) refere-se à proteção de sistemas de informação (incluindo *hardware, software* e infraestruturas relacionadas), os dados e os serviços neles providos, seja do acesso não autorizado, danos ou uso indevido. Isso inclui danos causados intencionalmente pelo operador do sistema, ou acidentalmente, como resultado da falha em seguir os procedimentos de segurança (Government, 2016, p. 15)

O supracitado conceito é consonante com o conceito da ISO/IEC 27032 (2023), que considera ainda outras formas de manipulação de dados, informações e sistemas, como vazamento, interrupção, modificação e destruição, abrangendo ainda a análise de risco para a prevenção e proteção da confidencialidade, integridade e disponibilidade da informação e dos sistemas. Ademais, para além do âmbito informacional, a segurança cibernética, também,

envolve coisas físicas e digitais, que não são propriamente informações (Evesti; Kanstrén; Frantti, 2017), como aplicações, sistemas e infraestruturas (digitais ou físicas).

O *The Cybersecurity Body of Knowledge* (CyBOK), num esforço de consolidação da segurança cibernética enquanto campo de estudo multidisciplinar, detalha a pertinência da segurança cibernética nas seguintes áreas: Aspectos Humanos, Organizacionais e Regulatórios; Ataques e Defesas; Segurança de Sistemas; Segurança de *Software* e Plataformas; e Segurança de Infraestruturas (Cybok, 2021).

Em termos de aplicação da segurança cibernética em organizações públicas ou privadas, existem variadas iniciativas, abrangendo normas e *frameworks* que visam descrever a segurança cibernética em diferentes áreas (Syafrizal; Selamat; Zakaria, 2020). A título de exemplo, a Tabela 1 apresenta exemplos dessas iniciativas.

**Tabela 1:** Exemplos de iniciativas aplicadas à segurança cibernética.

| Iniciativa | Descrição |
|---|---|
| **ISO/IEC 27032:2023** | É uma norma que visa tratar aspectos abrangentes relativos à segurança cibernética, tais como avaliação e tratamento de riscos cibernéticos; preparação, prevenção, detecção, monitoramento e resposta a ataques e ameaças; definição de partes interessadas, responsabilidades, políticas, métodos e processos. Também, define diversos controles técnicos aplicáveis, por exemplo, voltados a controles de acesso, educação, conscientização e treinamento, gestão de incidentes de segurança, gestão de vulnerabilidades, gestão da mudança, uso de criptografia, identificação de requisitos legais e de *compliance*, etc. Sua aplicação deve observar outras normas pertinentes da família ISO/IEC 27000. |
| **NIST *Cybersecurity Framework* - CSF** | Trata-se de um *framework* de segurança cibernética de caráter genérico, isto é, aplica-se à indústria, governos, agências e outras organizações, com a finalidade de gerenciar os riscos cibernéticos. Ademais, visa um melhor entendimento, avaliação, priorização e comunicação dos esforços em segurança cibernética, independentemente do tamanho, setor ou maturidade da organização. O CSF parte das funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar, que se subdividem em Categorias e Subcategorias para permitir a identificação de ações a serem feitas no âmbito da segurança cibernética. |

Fonte: adaptada de ISO/IEC (2018, 2023) e NIST (2024).

A segurança cibernética configura-se como um campo de estudo extenso, permeando aspectos e fenômenos nas interações homem-máquina, máquina-máquina, bem como nas sociedades, empresas e, com maior enfoque neste trabalho, nos governos (Cybok, 2021).

Quanto ao setor público, para os fins deste trabalho, diz respeito a todas as atividades e setores em que atua o Estado em razão da finalidade e interesse públicos, do desenvolvimento nacional, setor militar, infraestrutura, saúde, educação, suas relações institucionais, público-privadas e internacionais, dentre outros (Eu, 2016).

A literatura científica pertinente cita a segurança cibernética como uma atribuição pública do Estado sob diferentes justificativas, por exemplo, em aspectos legais e regulatórios (Cybok, 2021), segurança nacional (Garibaldi; Deane, 2023), digitalização do governo e serviços públicos (Al-Zahrani, 2020), direito fundamental (Shackelford, 2019) e proteção de sistemas e infraestruturas críticas (Weiss; Biermann, 2023).

Partindo de variadas justificativas, muitos são os desdobramentos da segurança cibernética abrangendo as organizações públicas, e uma forma possível de entender esses desdobramentos é segmentando o tema por níveis organizacionais. Uma forma possível de segmentar o estudo em diferentes níveis é empregando a classificação descrita por Oliveira e Abib (2023), exibida na Tabela 2, que considera três níveis. Os autores baseiam a referida classificação no estudo de Jilke *et al*. (2019), que indica a Administração Pública como tendo dimensões Micro, Meso e Macro, assumidas respectivamente como níveis Individual, Organizacional e Ambiental. Os diferentes níveis descritos na Tabela 2, inclusive, podem ser aproveitados para segmentar publicações científicas sobre o tema "segurança cibernética no setor público".

**Tabela 2:** Descrição da classificação Nível Organizacional.

| Nível Organizacional | Descrição |
|---|---|
| **Individual** | O nível de análise Individual trata de aspectos cognitivos dos indivíduos na tomada de decisões e seu comportamento perante as situações de riscos e incertezas. Considera-se também temas sobre preparação, percepção, propensão, aversão, tolerância a riscos e demais aspectos psicológicos como também demográficos, de gestores e funcionários públicos, cidadãos e demais agentes humanos dentro da organização, no caso, a administração e setor públicos. |
| **Organizacional** | Trata de toda a gama de políticas, instituições, práticas representantes e atores que trabalham para promover a integridade das instituições públicas, com muita atenção à forma como esses elementos do sistema apoiam ou prejudicam entre si, e também sob o ponto de vista das estratégias, falhas internas, uso de recursos, operações, atos administrativos e demais características próprias da natureza organizacional ou do Estado. Este nível de análise compreende os diferentes escopos do setor público, podendo tratar-se dele como um todo, apenas partes como a saúde pública e forças armadas, ou de uma única instituição pública ou governo em específico. |
| **Ambiental** | Do ponto de vista sistêmico, enquanto os demais níveis de análise envolvem o ambiente interno ou controlável do setor público, o nível Ambiental diz respeito a agentes, fenômenos e fatores externos não pertencentes ou controláveis pelo Estado. Busca compreender como as externalidades influenciam nos níveis Individual e Organizacional, como guerras, crises climáticas, acordos e cooperações internacionais, etc. Também envolve temas sobre terceirização, parcerias público-privadas e redes de colaboração. |

Fonte: Adaptado de Oliveira e Abib (2023).

### 2.2 Estudos bibliométricos

A Bibliometria pode ser entendida como técnica, método ou, de forma mais abrangente, uma metodologia para a medição principalmente quantitativa e estatística do conhecimento científico (Araújo, 2006; Donthu *et al*., 2021). O campo da bibliometria foi mais precisamente definido no início do século XX, com a consolidação de três leis fundamentais: a Lei de Produtividade de Autores de *Lotka*, a Lei de Dispersão de Periódicos de *Bradford*, e a Lei de Frequência de Palavras de *Zipf* (Araújo, 2006).

Apesar de inicialmente voltada ao ofício bibliotecário, a análise bibliométrica passou a ganhar espaço em outros campos de estudo por permitir observar diferentes camadas do conhecimento científico, como sua historicidade ao avaliá-la num dado período de tempo. Essa análise bibliométrica permite, também, identificar elementos entendidos como núcleos da produção científica específica analisada (principais autores, filiações acadêmicas, revistas científicas, países ou continentes, etc), interseções com dimensões qualitativas, dentre outros (Araújo, 2006).

Para além de sua aplicabilidade, a bibliometria demonstra-se pertinente e relevante por aspectos tecnológicos, com softwares atualmente que permitem a fácil e precisa utilização das técnicas bibliométricas. Também, denota-se sua utilidade para lidar com grandes volumes de dados científicos, para a elaboração de um panorama da literatura pesquisada, para a identificação de lacunas de conhecimento e para a geração de novas ideias para investigação (Donthu *et al*., 2021).

Ainda conforme Donthu *et al*. (2021), a análise bibliométrica possui uma variedade de técnicas. Entre essas técnicas citadas, podem ser lembradas a distribuição das publicações segundo número de autores e coautores, produção de artigos por ano de publicação, por filiação acadêmica, nuvem indicativa de frequência de palavras-chaves, dentre outras. Também, é possível efetuar análise de coautoria (Uddin *et al*., 2012), capaz de representar, em um esquema de rede (*network analysis*), a colaboração de autores, instituições ou países entre um ou mais artigos. Em complemento, pode-se empregar a análise de co-ocorrência de palavras-chaves, a qual é capaz de indicar a força de ligação das palavras-chaves umas com as outras (Mcallister; Lennertz; Mojica, 2022). A análise de co-ocorrência pode contribuir, inclusive, para demonstrar a presença de palavras-chaves variadas em estudos abordando a temática da segurança cibernética (Bolbot *et al*., 2022).

Análises bibliométricas, inclusive, já foram estudadas juntamente com emprego da análise de conteúdo, para

investigar a produção científica no setor público, com foco em benefícios e riscos do uso da computação em nuvem no referido setor (David *et al*., 2022).

Por fim, é possível o emprego da análise bibliométrica concomitante à aplicação do método PRISMA, citado na introdução deste estudo. O referido método traz um conjunto de etapas para orientar a seleção e análise de artigos numa revisão de literatura e já foi empregado no âmbito do setor público por Moura, Brauner e Janissek-Muniz (2020). Este método, inclusive, foi empregado neste trabalho para a identificação, seleção, eleição e inclusão adequada de artigos, conforme descrito na metodologia desta pesquisa.

## 3 METODOLOGIA

Esta pesquisa é descritiva, pois presume a observação sem interferência do pesquisador no fenômeno, o registrando, analisando, classificando e interpretando. Quanto à abordagem, é tanto quantitativa quanto qualitativa (Prodanov; Freitas, 2013).

A população desta pesquisa abrange publicações científicas disponíveis nas bases de dados *Scopus e Web of Science*, indexadas ao Portal de Periódicos da Capes (2024), relacionadas à segurança cibernética no setor público. A amostra de artigos é do tipo não probabilística (Sampieri; Collado; Lucio, 2013).

Para se chegar à amostra de artigos, empregou-se o método PRISMA, que indica a seleção sistemática de artigos em etapas de Identificação, Seleção, Elegibilidade e Inclusão, cada uma com seus próprios critérios de exclusão ou inclusão (Moher *et al*., 2015), conforme ilustra a Figura 1. A sistematização proporcionada pelo PRISMA permite a seleção adequada de obras que indiquem características próprias das literaturas pesquisadas, inclusive daquelas específicas dentro do próprio campo da segurança cibernética (Bolbot *et al*., 2022; Uchendu *et al*., 2021). Em razão disso, justifica-se seu uso no presente trabalho.

Os critérios de identificação envolveram a busca de artigos completos publicados e avaliados por pares em periódicos científicos, entre 2018 e 2023, a partir dos descritores *cybersecurity* ou *cyber security* associados a algum dos seguintes termos: *public sector*, *public administration*, *public management* ou *government*. A partir dos descritores, obteve-se 1019 documentos, em que, excluindo a duplicidade de artigos entre as bases, restaram 720, conforme ilustra a Figura 1.

Na seleção, os critérios de exclusão foram: ser artigo retratado, entendido como obra que, após a publicação, foi reanalisada por pares e considerada imprecisa ou com erros críticos; ter acesso pago ou restrito; não ser artigo científico, não ser completo ou não ter sido revisado por pares; não estar em inglês, português ou espanhol; e não ter palavras-chaves ou resumo. Nesta etapa, foram excluídos 286 artigos, restando 434, segundo mostra a Figura 1.

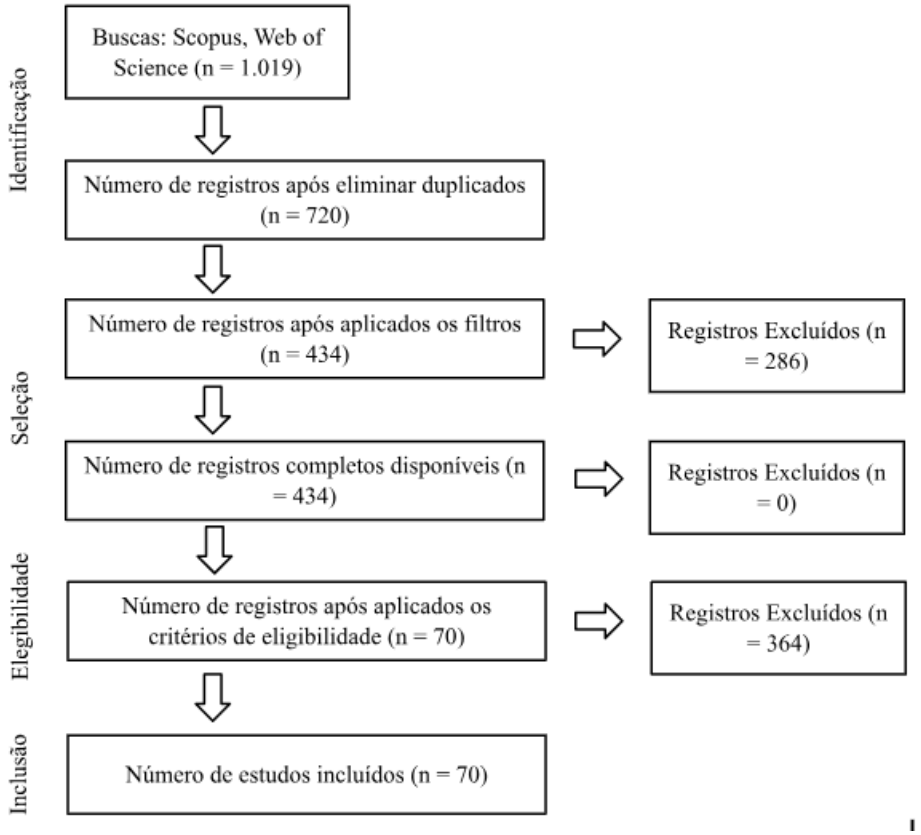
Os critérios de exclusão da etapa de elegibilidade são: não ocorrência dos descritores utilizados na Identificação, necessariamente no resumo e nas palavras-chaves, bem como não possuir a relação entre segurança cibernética e setor público como objeto principal de pesquisa. Após essa etapa, excluíram-se 364 artigos.

A etapa de inclusão, por fim, ressalta os artigos que sobraram após todos os critérios de exclusão, totalizando 70 artigos que constituem a amostra de artigos deste estudo, conforme citado na Figura 1.

Para o tratamento dos dados foram empregadas análise bibliométrica e análise de conteúdo. A análise bibliométrica empregada, considerando Donthu *et al*. (2021) e Araújo (2006), empregou as seguintes métricas: quantidade de artigos por ano de publicação, quantidade de autores por artigo, quantidade de palavras-chaves expressa por meio de nuvem de palavras, quantidade de artigos por periódico científico, e quantidade de filiações acadêmicas juntamente da classificação quanto ao continente de origem. Tais análises exibem frequências acompanhadas de percentuais e estão exibidas em gráficos e em tabelas elaborados no *Google*® Planilhas. A nuvem de palavras foi gerada por meio do *software* NVivo® 14 e foram consideradas as palavras-chaves contidas nos artigos que estivessem presentes em pelo menos dois artigos da amostra, conforme Mcallister, Lennertz e Mojica (2022). Realizaram-se, também, análises de coautoria e de co-ocorrência de palavras-chaves. Conforme citado na Subseção 2.2, a análise de coautoria descreve, em um esquema de rede, a colaboração de autores em um ou mais artigos e a análise de co-ocorrência de palavras-chaves indica a força de ligação dessas palavras-chaves umas com as outras.

Por sua vez, a análise de conteúdo baseou-se nas recomendações de Bardin (1977), examinando-se a presença de elementos nos textos dos artigos que permitissem a classificação desses artigos sob duas perspectivas: 1. a abordagem metodológica predominante do artigo (quantitativa, qualitativa, ou quali-quantitativa), conforme descrito por Prodanov e Freitas (2013); 2. o nível organizacional predominante no teor do artigo (Individual, Organizacional, ou Ambiental), conforme a Tabela 2 deste estudo, baseada em Oliveira e Abib (2023). A respeito da

**Figura 1:** Aplicação do método PRISMA.




Fonte: os autores, adaptado de dados da pesquisa, considerando Moher *et al.* (2015).

classificação segundo o nível organizacional predominante, o texto de cada artigo foi analisado buscando identificar elementos descritos na Tabela 2, permitindo categorizar um nível organizacional predominante evidenciado no conteúdo do texto de cada artigo. Para realizar as referidas análises, empregou-se de forma auxiliar o *software Microsoft Excel*.

## 4 RESULTADOS E DISCUSSÃO

### 4.1 Quantidade de artigos publicados por ano de publicação

Inicialmente apresenta-se a evolução cronológica do número de artigos da amostra. O recorte temporal da amostra, entre 2018 e 2023, após aplicação da recomendação PRISMA, indicou 70 artigos distribuídos da seguinte forma na Tabela 3.

A Tabela 3 mostra que o ano de 2018 teve 3 artigos, correspondendo a 4,29% em relação ao total da amostra, enquanto que em 2023 constataram-se 19 artigos, igual a 27,14% da amostra. O ano de 2022, com 21 artigos, correspondendo a 30% de participação, juntamente do ano de 2023 representam mais de 50% da amostra. Tais resultados indicam, de forma geral, que o número de publicações evoluiu com o passar dos anos. Tal evolução é condizente com o estudo de Kail *et al.* (2023) que, por meio de gráficos, sinalizaram a Segurança Cibernética como domínio de interesse progressivo.

### 4.2 Periódicos científicos conforme quantidade de artigos

A Tabela 4 apresenta os periódicos científicos e a quantidade de artigos por periódicos encontrados nas bases de dados *Scopus* e *WoS*. A análise bibliométrica de periódicos, que pode ser efetuada a partir de diferentes variáveis,

**Tabela 3:** Frequência anual de pesquisas da amostra.

| Ano | Frequência | (%) |
|---|---|---|
| 2018 | 3 | 4,29% |
| 2019 | 6 | 8,57% |
| 2020 | 10 | 14,29% |
| 2021 | 11 | 15,71% |
| 2022 | 21 | 30,00% |
| 2023* | 19 | 27,14% |
| **Total** | **70** | **100,00%** |

Fonte: os autores, a partir de dados da pesquisa.

* A coleta no ano de 2023 corresponde aos artigos publicados até setembro.

**Tabela 4:** Periódicos científicos e suas participações por quantidade de artigos.

| Periódicos | Quantidade de artigos por periódico | Quantidade total de artigos* | (%) |
|---|---|---|---|
| *International Journal of Computer Science and Network Security* (IJCSNS) / *Information and Computer Security* (ICS) | 5 | 10 | 14,29 |
| *Government Information Quarterly* (GIQ) | 4 | 4 | 5,71 |
| *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI) | 3 | 3 | 4,29 |
| Demais 9 periódicos | 2 | 18 | 25,71 |
| Demais 35 periódicos | 1 | 35 | 50,00 |
| **Total** | | **70** | **100,00** |

Fonte: os autores, a partir de dados da pesquisa.

* A coluna 'Quantidade total de artigos' traz o resultado da multiplicação entre a quantidade de periódicos citados na coluna 'Periódicos' e os dados da coluna 'Quantidade de artigos por periódico'.

é relevante para identificar periódicos mais produtivos (Araújo, 2006), neste caso relacionados à quantidade de artigos publicados.

Na Tabela 4, os periódicos com 3 artigos ou mais representam 1/4 da amostra. Tanto o IJCSNS quanto o ICS tiveram 5 ocorrências cada, juntos correspondendo a 14,29% da amostra. O GIQ apresenta 4 artigos, uma participação de 5,71%, e a RISTI, com 3 artigos, contribui com 4,29% da amostra. Em complemento, constataram-se 9 periódicos com duas publicações cada e outros 35 periódicos com um artigo cada. Esses resultados sinalizam fragmentação na publicação de artigos da amostra em diferentes periódicos, evidência que coincide em certo grau com os resultados de Bolbot *et al*. (2022).

### 4.3 Classificação de artigos conforme quantidade de autores

Observar a quantidade de autores de uma certa literatura viabiliza a análise da sua rede de autores, que indica as características daquele conjunto de autores que colaboram para a pesquisa de determinado tema (Uddin *et al*., 2012). A Tabela 5 descreve a distribuição de artigos sob o critério do número de autores por artigo.

A Tabela 5 mostra que os artigos com coautoria com 4 autores ou mais apresentam 24 publicações, que correspondem a 34,29% dos artigos da amostra. Entretanto, a maior parte da amostra (65,71%) compreende publicações com até 3 autores, resultados próximos daqueles da análise bibliométrica de Makawana e Jhaveri (2018), voltada à bibliografia de aprendizagem de máquina aplicada à segurança cibernética, cuja amostra mostrou-se concentrada

**Tabela 5:** Proporção de artigos por quantidade de autores.

| **Nº de autores** | **Quantidade de artigos** | **(%)** |
|---|---|---|
| 1 autor | 12 | 17,14% |
| 2 autores | 22 | 31,43% |
| 3 autores | 12 | 17,14% |
| 4 autores ou mais | 24 | 34,29% |
| **Total** | **70** | **100,00%** |

Fonte: os autores, a partir de dados da pesquisa.

entre artigos com até 3 autores.

### 4.4 Filiações acadêmicas e classificação quanto ao continente

Foram identificadas 125 filiações acadêmicas associadas a um ou mais autores dos artigos da amostra. Considerando todas as filiações acadêmicas, observa-se 45 filiações na Europa, continente com maior número, seguido de 42 filiações para Ásia-Pacífico, com maioria de filiações da Ásia, o continente das Américas, com 35 filiações, e o continente África, com apenas 3 filiações e todas localizadas na África do Sul. A Tabela 6 destaca as filiações acadêmicas mais recorrentes, com 2 ou mais aparições.

**Tabela 6:** Filiações acadêmicas mais recorrentes em artigos da amostra.

| **Filiações** | **País** | **Continente** | **Número de aparições*** |
|---|---|---|---|
| *Lviv Polytechnic National University* | Ucrânia | Europa | 5 |
| *Arizona State University* | EUA | Américas | 2 |
| *Sungkyunkwan University* | Coréia do Sul | Ásia-Pacífico | 2 |
| *Tallinn University of Technology* | Ucrânia | Europa | 2 |
| *Universidad de Alicante* | Espanha | Europa | 2 |
| *Universiti Teknikal Malaysia Melaka* | Malásia | Ásia-Pacífico | 2 |
| *Uzhgorod National University* | Ucrânia | Europa | 2 |
| *Zhytomyr Polytech State University* | Ucrânia | Europa | 2 |

Fonte: os autores, a partir de dados da pesquisa.

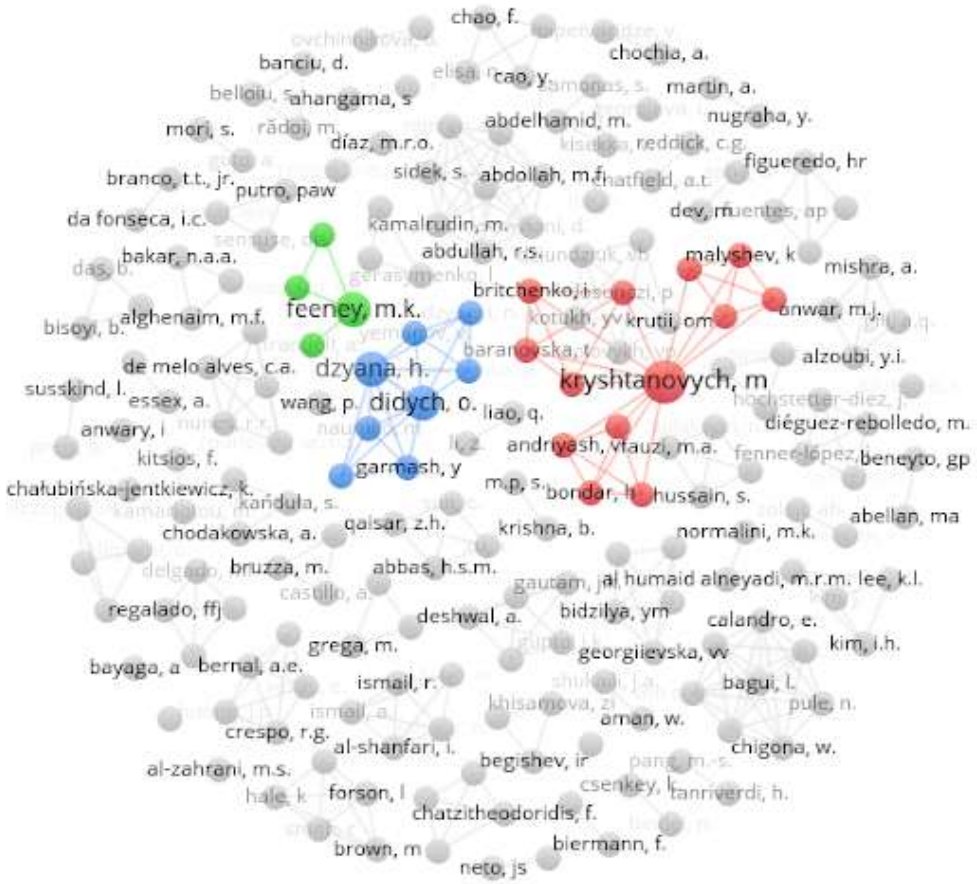
* Observação: De um total de 125 filiações.
Ásia-Pacífico: Compreende os continentes Ásia e Oceania.
EUA: Estados Unidos da América.

Identificar as instituições mais recorrentes é uma das diferentes métricas para analisar o âmbito das publicações sobre determinado tema (Donthu *et al*., 2021). Em termos de participação em número de artigos, a Tabela 6 mostra que *Lviv University* é a mais recorrente, ocorrendo em 5 artigos, as demais filiações ocorreram 2 vezes cada. Denota-se a predominância de filiações acadêmicas da Europa na citada Tabela 6.

### 4.5 Análise de coautoria

A análise de coautoria, lembrada na literatura sobre estudos bibliométricos (Donthu *et al*., 2021), é a representação em rede da colaboração de autores, de instituições ou de países envolvidos na publicação de um ou mais artigos (Mcallister; Lennertz; Mojica, 2022). Mais especificamente, neste trabalho realizou-se uma análise voltada aos 199 autores que foram identificados na amostra de 70 artigos desta pesquisa. Tal análise de coautoria está ilustrada na Figura 2.

**Figura 2:** Análise de coautoria dos artigos da amostra.




Fonte: os autores, a partir de dados da pesquisa.

Com base na Figura 2, evidencia-se que a maior parte da rede de coautoria, destacada em cinza, consiste em coautorias envolvendo dois ou mais autores em um mesmo artigo. As coautorias coloridas são aquelas em que um ou mais autores colaboraram com outros autores em mais de um artigo. *Myroslav Kryshtanovych*, da Ucrânia, é o autor que mais publicou sobre o tema, com 3 artigos publicados, *Halyna Dzyana* e *Oleg Didych*, ambos da Ucrânia, juntos publicaram 2 artigos, e *Mary K. Feeney*, dos EUA, publicou 2 artigos sobre o tema. Denota-se, portanto, que a Ucrânia é a nacionalidade de 3 dos 4 autores que mais publicaram sobre o tema.

### 4.6 Nuvem de palavras-chaves dos artigos

A nuvem de palavras, ou *word cloud*, consiste na visualização mais simplificada da co-ocorrência de palavras-chaves, indicando graficamente os termos mais recorrentes (Donthu *et al*., 2021). No presente trabalho, esta análise foi gerada pelo *VosViewer*, utilizando-se do *Nvivo* 14 para geração da visualização em nuvem, conforme Figura 3.

Conforme citado na metodologia, a elaboração em nuvem considerou termos que ocorreram ao menos duas vezes entre os artigos da amostra. Quanto maior a fonte do termo na Figura 3, maior é a frequência dele nos artigos da amostra. O termo *cybersecurity* ocorreu 62 vezes, por sua vez os termos *information security* e *cybercrime* ocorreram 14 e 12 vezes, respectivamente. O termo *security*, que considera aspectos de segurança mais abrangentes do que o espaço cibernético, aparece 13 vezes. O termo *e-government* ocorre 8 vezes, e os termos *ICTs*, *public administration* e *threat* ocorrem 7 vezes cada. Ademais, outros termos como *risk*, *critical information infrastructure*, *internet of things* e *privacy* demonstram foco dos artigos sobre o desenvolvimento e segurança das tecnologias e espaços cibernéticos públicos.

**Figura 3:** Nuvem de palavras-chaves dos artigos da amostra.


Fonte: os autores, a partir de dados da pesquisa.

Os termos citados no parágrafo imediatamente anterior, presentes na nuvem de palavras da Figura 3, evidenciam a multidisciplinaridade da temática sobre segurança cibernética. A constatação da segurança cibernética como um campo de estudo multidisciplinar foi lembrada por Cybok (2021), citado na Subseção 2.1 do referencial teórico deste estudo.

### 4.7 Análise de co-ocorrência de palavras-chaves

A análise de co-ocorrência representa a rede de conexões entre as palavras-chaves dos artigos da amostra. Conforme ilustra a Figura 4, quanto maior o tamanho da fonte do termo e o tamanho do círculo que o representa na figura, maior é seu número de ocorrências e de ligações. Em adição, as linhas que conectam os termos são mais finas ou espessas a partir da menor ou maior força de ligações entre estes termos (Mcallister; Lennertz; Mojica, 2022).

Assim como descrito na nuvem de palavras-chaves na Figura 3, a análise de co-ocorrência da Figura 4 demonstra variados termos ligados ao tema, algo também evidenciado por Bolbot *et al*. (2022) ao fazer uma revisão de literatura sobre segurança cibernética. Tal análise contribui para indicar proximidades entre os termos em razão de seus usos e contextos a partir de *clusters* diferenciados por cores.

### 4.8 Classificação dos artigos quanto à abordagem metodológica

A Tabela 7 apresenta a classificação da amostra de artigos segundo a abordagem metodológica. Após a realização da análise de conteúdo dos textos dos 70 artigos da amostra, foi possível obter essa classificação, considerando as abordagens citadas por Prodanov e Freitas (2013).

### 4.9 Classificação dos artigos quanto ao nível organizacional

A Tabela 8 apresenta a classificação dos artigos da amostra de acordo com os níveis organizacionais. A classificação foi realizada considerando três níveis previamente descritos na Tabela 2 do referencial teórico: Individual, Organizacional e Ambiental (Oliveira; Abib, 2023). Os diferentes níveis descritos na citada Tabela 2 foram aproveitados nesta pesquisa para segmentar os artigos da amostra que abordaram o tema 'segurança cibernética no setor

**Tabela 7:** Abordagem metodológica dos artigos da amostra.

| Abordagem Metodológica | Frequência | (%) |
|---|---|---|
| Qualitativa | 44 | 62,86% |
| Quantitativa | 16 | 22,86% |
| Qualitativa e Quantitativa | 10 | 14,29% |
| **Total** | **70** | **100,00%** |

Fonte: os autores, a partir de dados da pesquisa.

público‘.

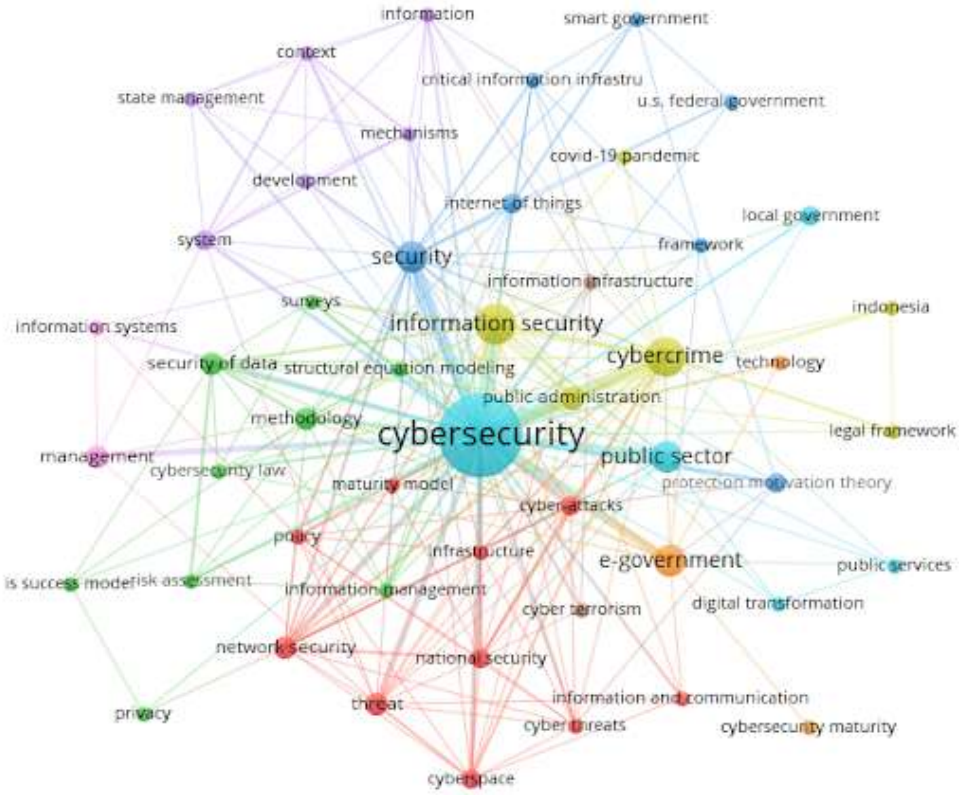
**Tabela 8:** Classificação dos artigos da amostra quanto ao nível organizacional.

| Nível | Frequência | (%) |
|---|---|---|
| Organizacional | 33 | 47,14% |
| Ambiental | 27 | 38,57% |
| Individual | 10 | 14,29% |
| **Total** | **70** | **100,00%** |

Fonte: os autores, a partir de dados da pesquisa.

A Tabela 8 mostra que o nível ‘Organizacional‘ prevaleceu em 33 artigos, correspondendo a 47,14% da amostra. O nível ‘Ambiental‘ prevaleceu em 27 artigos, compreendendo a parcela de 38,57% dos 70 artigos analisados. O

**Figura 4:** Análise de co-ocorrência de palavras-chaves da amostra.




Fonte: os autores, a partir de dados da pesquisa.

nível 'Individual', por sua vez, predominou em 10 artigos, correspondente a 14,29% da amostra. A classificação pelos três níveis de análise é importante, pois deve-se entender os diferentes temas em torno do setor público em todas essas dimensões, em consonância com o estudo de Jilke *et al*. (2019), que inspirou a classificação.

Os resultados citados na Tabela 8 indicam predomínio de artigos da amostra vinculados aos níveis 'Organizacional' e 'Ambiental'. Com maior frequência do que os demais, a classificação no nível 'Organizacional' contemplou pesquisas que visaram analisar questões institucionais, como a gestão da segurança cibernética, o desempenho das organizações públicas e aspectos associados à maturidade e infraestruturas relacionadas com a segurança cibernética.

Em complemento, a classificação no nível 'Ambiental', também exibida na Tabela 8, abrangeu pesquisas com maior interesse em compreender aspectos externos à organização ou setor público, como as implicações da Covid-19, ameaças externas como de ciberterrorismo e crimes cibernéticos. Por fim, a classificação no nível 'Individual' contemplou menos pesquisas do que os demais níveis citados na referida Tabela 8, indicando uma oportunidade de agenda de pesquisas sobre aspectos individuais relacionados, por exemplo, ao comportamento, motivação, treinamento, escolaridade, entre outros.

### 4.10 Agenda de pesquisas futuras

Os resultados exibidos nas subseções anteriores podem auxiliar a proposição de uma agenda de pesquisas futuras sobre segurança cibernética no setor público. Inicialmente, em termos geográficos de produção científica, identificou-se na Subseção 4.3 dos resultados que a África possui 3 filiações acadêmicas associadas a autores de 2 artigos da amostra. Esse fato pode indicar uma oportunidade de mais pesquisas envolvendo segurança cibernética no setor público dirigido a instituições e a contextos localizados no continente africano.

Quanto à abordagem metodológica, observou-se na Tabela 7 uma concentração de 62,86% da amostra em abordagem qualitativa, indicando uma oportunidade para produções com outras abordagens, como a quantitativa ou a quali-quantitativa, com vistas a uma maior compreensão sobre os assuntos relacionados à segurança cibernética no setor público.

Quanto à análise de coautoria, observa-se que embora a maioria dos artigos tenham sido elaborados em coautoria, como evidenciou a Subseção 4.3 desta pesquisa, ao observar a Figura 2 mostrou-se reduzido nível de colaboração entre os autores em mais de uma pesquisa, uma vez que dos 199 autores que contribuíram para publicar a amostra de artigos, apenas 4 publicaram mais de uma vez sobre o tema. Isso pode indicar a necessidade de mais iniciativas buscando fomentar grupos de estudo sobre o tema, bem como oportunidades para fomento a uma rede de colaboração maior entre autores dispostos a tratar sobre segurança cibernética no setor público.

A segurança cibernética é campo de estudo multidisciplinar e os achados colhidos da análise de co-ocorrência de palavras-chaves, ilustrada na Figura 4, podem ensejar desenvolvimento de pesquisas que abarquem os termos citados na referida análise de co-ocorrência. Por exemplo, pode ser observada a viabilidade de produção de pesquisas que tratem mais sobre termos combinados, como crimes cibernéticos (*cybercrime*) e legislação em segurança cibernética (*cybersecurity law*), ou que busquem, também, pesquisar sobre a maturidade do setor público em segurança cibernética (*cybersecurity maturity*).

Por fim, a classificação dos artigos segundo níveis de análise, ilustrada na Tabela 8, indicou o nível 'Individual' contemplando 14,29% dos artigos da amostra. Em adição, a nuvem de palavras-chaves, também, mostrou poucos termos ligados ao indivíduo ou ao fator humano. Neste sentido, ao tratar sobre a segurança cibernética no setor público, é possível propor a realização de mais estudos que investiguem aspectos cognitivos, psicológicos, decisórios e comportamentais dos indivíduos atuantes no setor público. Essa proposição pode integrar agenda de pesquisa de interesse de profissionais nas diversas áreas que tenham vínculo com o referido setor, como gestores de riscos, desenvolvedores de *software*, acadêmicos, inclusive atuantes em escolas de governo, dentre outros.

## 5 CONSIDERAÇÕES FINAIS

O objetivo deste artigo foi investigar a produção científica sobre a segurança cibernética no setor público de 2018 a 2023. Este estudo busca contribuir para reflexões de pesquisadores, gestores públicos e demais partes interessadas, trazendo subsídios para delinear oportunidades de pesquisas futuras sobre segurança cibernética no setor público.

Os principais resultados mostraram que os artigos sobre segurança cibernética no setor público estão mais concentrados entre os anos de 2022 e 2023, correspondendo a 57,14% do total. Dentre os 48 periódicos científicos relacionados à amostra, 35 publicaram um único artigo, demonstrando a fragmentação da divulgação destas pesquisas.

No que tange ao número de autores por artigo, apurou-se 65,71% dos artigos produzidos com até 3 autores, enquanto os artigos com coautoria com 4 autores ou mais correspondem a 34,29% dos artigos da amostra. A Europa apresenta a maior quantidade de filiações acadêmicas (45 das 125 identificadas), inclusive as mais recorrentes, que se situam na Ucrânia, enquanto a África, por sua vez, demonstrou a menor participação, com 3 filiações.

A análise de coautoria indicou 4 autores que contribuíram com mais de um artigo e que, ao mesmo tempo, fizeram coautoria com outros autores, sendo: *Myroslav Kryshtanovych*, com 3 artigos publicados, *Halyna Dzyana* e *Oleg Didych*, que juntos publicaram 2 artigos, e Mary K. Feeney, que publicou 2 artigos sobre o tema.

O termo mais recorrente da nuvem de palavras foi *cybersecurity* (62 ocorrências), observando-se para a distinção do termo com *information security* (14), em concordância com a posição da ISO/IEC 27000 (2018) e ISO/IEC 27032 (2023). Os termos citados na nuvem de palavras evidenciaram a segurança cibernética como um campo de estudo multidisciplinar.

Quanto à análise de co-ocorrência de palavras-chaves, além de *cybersecurity*, com 52 ocorrências e 50 ligações, e *information security*, com 14 ocorrências e 25 ligações, outros termos citados foram *cybercrime*, com 12 ocorrências e 25 ligações, *public sector* e *e-government*, ambos com 8 ocorrências e 14 ligações. Ademais, a visualização em rede destacou as palavras-chaves em *clusters*, contribuindo para reflexões de futuras pesquisas e de agentes públicos interessados.

A maioria dos artigos (62,86% da amostra) apresentou a abordagem qualitativa para a condução de suas pesquisas, e sobre os artigos com abordagem quali-quantitativa, correspondem a 14,29% dessa amostra. A presença de artigos vinculados à abordagem qualitativa indica a necessidade da compreensão de aspectos subjetivos ou não quantificáveis pertinentes à segurança cibernética no setor público.

A partir do exame do conteúdo dos textos da amostra de artigos, apurou-se que o nível de análise 'Organizacional' foi vinculado a 47,14% dos artigos da amostra. O nível 'Ambiental' abrangeu 38,57% dos artigos da amostra, e o nível 'Individual' foi vinculado a 14,29% dos artigos da amostra. A classificação dos artigos segundo níveis de análise encontrou respaldo na literatura, na forma descrita na Tabela 2 deste estudo.

Este trabalho investigou um tema cuja relevância é crescente, tecendo contribuições para acadêmicos, ao descrever diferentes características bibliométricas da literatura pesquisada, como também para gestores públicos e outras partes interessadas. Contudo, o tema da segurança cibernética no setor público foi tratado a partir de artigos científicos coletados apenas nas bases de dados *Scopus* e WoS, indicando a possibilidade de maiores dados ao expandir para outras bases. Considera-se também o período escolhido, de 2018 a 2023, e a limitação deste último ano para resultados até o mês de setembro.

Este estudo apresenta uma subseção nos resultados que detalha uma proposta de agenda de pesquisas futuras, indicadas a partir das evidências encontradas nos achados deste trabalho. Tais pesquisas futuras podem considerar as lacunas descritas, como a baixa representatividade de filiações e artigos na África, por exemplo. Ademais, constitui-se fonte oportuna a exploração de termos combinados da nuvem de palavras-chaves apresentada, contendo temas ainda não tão profundamente investigados. Um exemplo dessas possíveis pesquisas abrange o estudo sobre crimes cibernéticos e legislação em segurança cibernética com foco no setor público. Também deve-se considerar a possibilidade de investigação sobre o comportamento e a evolução de redes de colaboração entre pesquisadores atrelados à investigação da segurança cibernética no setor público.

Por fim, os resultados da classificação de artigos da amostra segundo nível de análise, especialmente para o nível individual, também indicam oportunidades para pesquisas futuras, que contribuam para a compreensão de aspectos cognitivos do indivíduo na tomada de decisão e seu comportamento perante as situações de riscos e incertezas abordando a temática da segurança cibernética no setor público.

## REFERÊNCIAS


AL-ZAHRANI, M. Integrating is success model with cybersecurity factors for e-government implementation in the kingdom of saudi arabia. **Ijece**, Indonesia, v. 10, n. 5, p. 4937–4955, 2020.

ARAÚJO, C. A. Bibliometria: Evolução histórica e questões atuais. **Em Questão**, Porto Alegre, v. 12, n. 1, p. 11–32, 2006.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1977. 225 p.

BOLBOT, V.; KULKARNI, K.; BRUNOU, P.; BANDA, O. V.; MUSHARRAF, M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. **Ijcip**, Netherlands, v. 39, p. 1–18, 2022.

BRASIL. **Decreto Nº 11.856, de 26 de dezembro de 2023:** Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

CAPES. **Portal de periódicos da Capes**. Brasília: Capes, 2024. Disponível em: periodicos-capes-gov-br.ezl.periodicos.capes.gov.br.

CYBOK. **The cyber security body of knowledge:** Version 1.1.0. England: Cybok, 2021. 1029 p. Disponível em: cybok.org/media/downloads/CyBOK_v1.1.0.pdf.

DAVID, D. J.; ALVES, C. A. M.; NUNES, R. R.; OLIVEIRA, R. M. Benefícios e riscos do uso da computação em nuvem no setor público: Uma análise baseada em artigos disponibilizados em bases de dados acadêmicas de 2017 a 2021. **Risti**, Portugal, E54, p. 537–549, 2022.

DONTHU, N.; KUMAR, S.; MUKHERJEE, D.; PANDEY, N.; LIM, W. M. How to conduct a bibliometric analysis: An overview and guidelines. **Journal of Business Research**, Usa, v. 133, p. 285–296, 2021.

EU. **Analysis of the value of new generation of e-government services and how can the public sector become an agent of innovation through Ict**. Brussels: European Comission, 2016. 222 p. Disponível em: ec.europa.eu/futurium/...

GARIBALDI, S.; DEANE, F. Cyberspace as a fifth dimension of national security: Trade measure exceptions. **Journal of International Trade Law and Policy**, United Kingdom, v. 22, n. 2, p. 67–88, 2023.

GOVERNMENT, H. **National cyber security strategy 2016–2021**. Uk: His Majesty Government, 2016. 80 p. Disponível em: assets.publishing.service.gov.uk/.

ISO/IEC. **Iso/Iec 27000:2018:** Information technology - Security techniques - Information security management systems - Overview and vocabulary. Iec: Iso, 2018. Disponível em: iso.org/standard/73906.html.

ISO/IEC. **Iso/Iec 27032:2023:** Cybersecurity guidelines for internet security. Iec: Iso, 2023. Disponível em: iso.org/standard/76070.html.

ITU. **Itu cybersecurity programme:** Cirt framework. It: Itu, 2021. 22 p. Disponível em: itu.int/dms_pub/.../D-STR-CYBERSEC-2021-01-PDF-E.pdf.

JILKE, S.; OLSEN, A. L.; RESH, W.; SIDDIKI, S. Microbook, mesobrook and macrobrook. **Perspectives on Public Management and Governance**, Uk, v. 2, n. 4, p. 245–253, 2019.

KAIL, E.; BANATI, A.; FLEINER, R.; MOSAVI, A.; MAKO, C. Machine learning methods for cybersecurity: Review and bibliometric analysis. **Sisy**, Croatia, v. 21, p. 527–536, 2023.

MAKAWANA, P. R.; JHAVERI, R. H. A bibliometric analysis of recent research on machine learning for cyber security. **Intelligent Communication and Computational Technologies**, Singapura, v. 19, p. 213–226, 2018.

MCALLISTER, J. T.; LENNERTZ, L.; MOJICA, Z. A. Mapping a discipline: A guide to using Vosviewer for bibliometric and visual analysis. **Science & Technology Libraries**, v. 41, n. 3, p. 319–348, 2022.

MOHER, D.; LIBERATI, A.; TETZLAFF, J.; ALTMAN, D. G.; PRISMA, G. Principais itens para relatar revisões sistemáticas e meta-análises: A recomendação Prisma. **Epidemiologia e Serviços de Saúde**, Brasília, v. 24, n. 2, p. 335–342, 2015.

MOURA, L. M. F.; BRAUNER, D. F.; JANISSEK-MUNIZ, R. Blockchain e a perspectiva tecnológica para a administração pública: Uma revisão sistemática. **Rac**, Rio Grande do Sul, v. 24, n. 3, p. 259–274, 2020.

NIST. **The Nist cybersecurity framework (Csf) 2.0**. Eua: Nist, 2024. 32 p. Disponível em: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

OLIVEIRA, V. G.; ABIB, G. Risco na administração pública: Uma revisão sistemática focada em uma agenda de pesquisas futuras. **Rap**, Rio de Janeiro, v. 57, n. 6, p. 1–19, 2023.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico:** Métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. 277 p.

RUTKOWSKI, A. Public international law of the international telecommunication instruments: Cyber security treaty provisions since 1850. **Info**, Uk, v. 13, n. 1, p. 13–31, 2011.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. **Metodologia de pesquisa**. 5. ed. Porto Alegre: Penso, 2013. 617 p.

SHACKELFORD, S. J. Should cybersecurity be a human right? Exploring the 'shared responsibility' of cyber peace. **Stanford Journal of International Law**, Eua, v. 55, n. 2, p. 1–46, 2019.

SYAFRIZAL, M.; SELAMAT, S. R.; ZAKARIA, N. A. Analysis of cybersecurity standard and framework components. **Ijcnis**, Uk, v. 12, n. 3, p. 417–432, 2020.

UCHENDU, B.; NURSE, J. R. C.; BADA, M.; FURNELL, S. Developing a cyber security culture: Current practices and future needs. **Computer & Security**, Netherlands, v. 109, p. 1–23, 2021.

UDDIN, S.; HOSSAIN, L.; ABBASI, A.; RASMUSSEN, K. Trend and efficiency analysis of co-authorship network. **Scientometrics**, Hungary, v. 90, p. 687–699, 2012.

WEISS, M.; BIERMANN, F. Cyberspace and the protection of critical national infrastructure. **Journal of Economic Policy Reform**, Uk, v. 26, n. 3, p. 250–267, 2023.