XXIV SEMEAD
Seminários em Administração

novembro de 2021
ISSN 2177-3866

TERMINOLOGIAS ADOTADAS PARA GERENCIAMENTO DE RISCOS CIBERNÉTICOS: um estudo bibliométrico

DANIEL SATHLER SILVA
UNIVERSIDADE FUMEC (FUMEC)

FÁBIO PIRES DE OLIVEIRA
UNIVERSIDADE FUMEC (FUMEC)

JUREMA SUELY DE ARAUJO NERY RIBEIRO
UNIVERSIDADE FUMEC (FUMEC)

JULIANA CALDEIRA BICALHO RIBEIRO
UNIVERSIDADE FUMEC (FUMEC)

TERMINOLOGIAS ADOTADAS PARA GERENCIAMENTO DE RISCOS CIBERNÉTICOS: um estudo bibliométrico

1 INTRODUÇÃO

A informação tornou-se o ativo mais importante para diferentes tipos de organizações. Dados sobre clientes, fornecedores, parceiros, competidores, finanças, dentre outros, são comumente hospedados por sistemas computadorizados que, por sua vez, estão sujeitos a diversos tipos de ameaças, o que resulta em riscos para esses sistemas e, consequentemente, para a organização. A identificação, a avaliação e a minimização de riscos de ativos informacionais são pontos que devem ser observados pelas organizações em seus processos de gerenciamento de riscos corporativos (RAHMAN; DONAHUE, 2010).

Os riscos e ameaças modificam-se todos os dias. As práticas de segurança da informação das organizações devem adotar uma abordagem de gerenciamento de risco, o qual é benéfico para a governança de tecnologia da informação (TI), visto que a governança deve garantir a continuidade do negócio contra interrupções e falhas, bem como a conformidade com aspectos legais ou regulatórios.

Diante da evolução tecnológica, diferentes termos vêm sendo utilizados para referir-se a temas relacionados ao gerenciamento de riscos de ativos informacionais. Conforme apontado por Andronache e Althonayan (2018), variações na terminologia podem gerar confusão e ocasionar o uso indevido de termos por autores. Já a falta de padronização e de definição dificulta a organização e a aplicação de conceitos da temática citada. Os termos mais usados, embora não sejam necessariamente sinônimos, são: *information technology security*, *information assurance*, *information security*, *computer security*, *digital security*, *Internet security*, *electronic security* ou *cybersecurity* (ANDRONACHE; ALTHONAYAN, 2018).

Além da presente seção introdutória, este trabalho é composto pelo item 2, correspondendo à apresentação do problema de pesquisa e o objetivo. O item 3 apresenta o referencial teórico, já a metodologia utilizada é apresentada na seção 4. Por sua vez, os resultados quantificados em gráficos são apresentados na seção 5. Por fim, as conclusões estão dispostas no item 6.

2 PROBLEMA DE PESQUISA E OBJETIVO

Diferentes definições e significados podem existir para os termos relacionados ao gerenciamento de riscos, o que resulta em inconsistência e discrepâncias na terminologia empregada para a área de segurança cibernética. É com esse argumento que surge a motivação deste estudo: quais são os termos utilizados na literatura científica internacional em trabalhos relacionados ao gerenciamento de riscos cibernéticos?

Este artigo, a partir de uma metodologia de caráter bibliométrico, busca explorar quais são os termos empregados por autores em artigos científicos que possuem a temática de gerenciamento de riscos, incluindo a avaliação do período, países e os respectivos continentes de publicação desses trabalhos. Diante do cenário apresentado, quatro hipóteses foram formuladas: i) a maior parte das publicações relacionadas ao gerenciamento de riscos faz o uso dos termos *cybersecurity* ou *information security*; ii) o termo *information security* é amplamente utilizado, ao longo do tempo, por trabalhos da área de gerenciamento de riscos; iii) há o aumento do uso do termo *cybersecurity* por trabalhos da área de gerenciamento de riscos cibernéticos; iv) o maior número de publicações utilizando o termo *cybersecurity* é observado na Europa.

3 FUNDAMENTAÇÃO TEÓRICA

A seção de fundamentação teórica encontra-se dividida em quatro subseções, a saber: (3.1) governança de TI, (3.2) gerenciamento de riscos, (3.3) segurança da informação e (3.4) *cybersecurity*.

3.1 Governança de TI

Grembergen (2004) destaca que a governança de TI é a capacidade organizacional exercida pela cúpula diretiva e pela gerência executiva para controlar a formulação e a implementação de sua estratégia, de forma a assegurar o alinhamento da TI com a organização.

É o mecanismo de controle das atividades de TI, consistindo em um processo contínuo de tomada de decisão que considera a monitoração e a melhoria contínua do seu desempenho, garantindo o alinhamento com a governança corporativa (MOLINARO; RAMOS, 2011).

A governança de TI não é somente a implantação de modelos de melhores práticas. Deverá promover também o alinhamento da TI ao negócio em relação a aplicações e à infraestrutura de TI, deverá possibilitar a implantação de mecanismos que garantam a continuidade do negócio contra interrupções e falhas, bem como atuar juntamente com áreas de controle interno, de conformidade e de gestão de riscos, realizando o alinhamento da TI com normas regulatórias (FERNANDO; ABREU, 2014). No próximo tópico, serão abordados os conceitos relacionados ao gerenciamento de riscos.

3.2 Gerenciamento de Riscos

O gerenciamento de riscos apoia a investigação e a análise do ambiente de TI, para verificar se a organização atende aos requisitos regulatórios e de negócios considerados prioritários (MOLINARO; RAMOS, 2011).

Risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. Pode ser uma oportunidade ou uma ameaça aos objetivos da organização, sendo que uma afeta negativamente e a outra, positivamente os objetivos do projeto (MONTEIRO, 2017).

A probabilidade de ocorrência e de impacto que o risco exerce sobre os objetivos organizacionais é o que o define. Portanto, quanto maior for a probabilidade e o impacto, maior será o nível desse risco para a organização. Enquanto a probabilidade está associada às chances de o evento acontecer, o impacto está associado ao efeito que o evento ocorrido exerce sobre os objetivos, ou seja, a materialização do risco (FRAPORTI e BARRETO, 2018).

A gestão da segurança de ativos informacionais deve contemplar o gerenciamento de riscos visto que possibilita a minimização do impacto de eventos potencialmente negativos. O próximo tópico abordará os conceitos relacionados à segurança da informação.

3.3 Segurança da Informação

A segurança da informação (SI) tem como propósito proteger os ativos informacionais. Um ativo de informação é qualquer objeto que retém partes da informação da empresa, nas suas mais diversas formas de representação e armazenamento: impressas em papel, armazenadas em discos rígidos de computadores, armazenadas na nuvem ou, até mesmo, retidas em pessoas (CORREA JUNIOR, 2011).

Segundo Kim e Solomon (2014), a maioria das pessoas concorda que informações privadas devem ser seguras. Para garantir essa segurança, a informação deverá satisfazer três princípios fundamentais, ou propriedades de informação, que são a disponibilidade, a integridade e a confidencialidade.

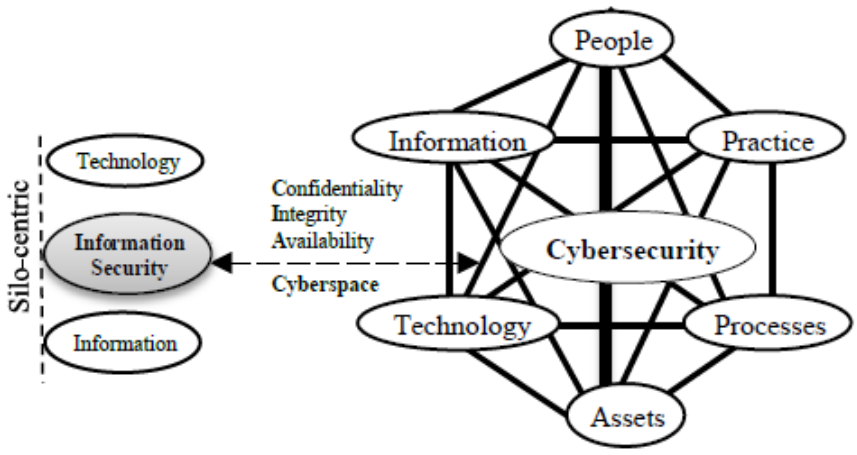
Correa Junior (2011) define confidencialidade como a garantia que usuários não autorizados não acessem determinados dados ou sistemas; integridade como a garantia que a informação seja alterada somente de forma autorizada; e disponibilidade como garantia que os sistemas estejam disponíveis o maior tempo possível.

3.4 *Cybersecurity*

Cibersegurança é a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente e a organização cibernética e os ativos dos usuários (ANDRONACHE; ALTHONAYAN, 2018). A Figura 2 enfatiza a distinção de enfoque e significados, junto com a correlação da segurança da informação em contraste com a segurança cibernética.

De acordo com Andronache e Althonayan (2018), a segurança cibernética é uma abordagem mais ampla para proteger não apenas os ativos de informação, mas também a tecnologia, ativos, processos, pessoas, organização e práticas com variáveis confiáveis semelhantes. Ainda de acordo com os autores, a estratégia da cibersegurança demonstra uma abordagem holística aos riscos da organização como um todo, enquanto a SI permanece uma abordagem em silos que protege os ativos de informação e os sistemas de informação. O contraste entre os princípios da segurança da informação e os da cibersegurança pode ser observado na Figura 1.

Figura 1 – Contraste dos Princípios de SI com os Princípios de Cibersegurança e seus Componentes.



Fonte: Andronache e Althonayan, 2018.

A Figura 1 ilustra que a cibersegurança incorpora um número maior de componentes para proteger a organização, comparada à abordagem de SI, o que inclui informações, pessoas, práticas, processos, ativos, tecnologia. Por sua vez, os componentes citados se relacionam para o atingimento do objetivo em comum, que é a proteção da organização contra ameaças cibernéticas.

4 METODOLOGIA

O presente trabalho é parte de um estudo desenvolvido entre os meses de junho e julho de 2021. Foram buscados, em relevantes bases de dados, artigos científicos sobre a temática proposta, conforme descrição apresentada no Quadro 1. A metodologia apresenta caráter bibliométrico, uma vez que tem como objetivo, a partir de exploração preliminar, identificar e quantificar temas e tendências no material (RODRIGUES; TAVAR; NOGUEIRA; LIBRELOTTO, 2016).

Quadro 1 – Descrição metodológica.

Critério	Descrição
Descritores pesquisados	A expressão utilizada é composta por dois termos, unidos pelo operador "AND": 1. Título: a. "Computer Security" OR "IT Security" OR "Electronic Security" OR "Digital Security" OR "Internet Security" OR "IT Risk Management" OR "Data Security" OR "Information Security" OR "Information Assurance" OR "Information Security Management Systems" OR "Cyber Threat Management" OR "Cybercrime Security" OR "Cyber Security" OR "Cybersecurity" OR "Cybersecurity Risk Management" OR "Cybersecurity Management" b. "Risk Management" OR "Risk Assessment"
Categoria	Artigos científicos publicados em periódicos.
Idiomas	Qualquer.
Bases de dados	Scopus e Scielo.
Critérios de exclusão	Artigos não disponíveis para download.
Contexto	Diferentes termos vêm sendo utilizados para referir-se a temas relacionados ao gerenciamento de riscos cibernéticos.
Justificativa	Inconsistência e discrepâncias na terminologia empregada para a área de segurança cibernética devido a diferentes definições e significados para os termos utilizados de maneira indiscriminada.

Fonte: Elaborado pelos autores (2021).

Conforme apontado pelos autores Andronache e Althonayan (2018), diferentes termos vêm sendo utilizados para referir-se a temas relacionados à segurança cibernética e incluem: *Computer Security; IT Security; Electronic Security; Digital Security; Internet Security; IT Risk Management; Data Security; Information Security; Information Assurance; Information Security Management Systems; Cyber Threat Management"; Cybercrime Security; Cyber Security; Cybersecurity; Cybersecurity Risk Management* ou *Cybersecurity Management.* Os termos citados foram utilizados na construção da expressão de busca. Além disso, *Risk Management* e *Risk Assessment* foram adicionados a *string* de busca com o objetivo de filtrar os trabalhos relacionados ao gerenciamento de riscos.

A base de dados Scopus apresentou-se como a mais importante fonte de informações deste trabalho, uma vez que indicou 567 trabalhos na busca do campo título dos trabalhos, após aplicar o filtro de tipo de documento *article*, obteve-se 181 resultados e, após aplicar o filtro *Open Access,* foram encontrados 53 artigos científicos para *download*. Não foram adicionados filtros para a data de publicação e o artigo mais antigo encontrado foi publicado em 2004. A busca pela *string* foi realizada também na base de dados Scielo, porém não retornou nenhum resultado.

O *software* Microsoft Excel foi utilizado para a categorização dos 53 trabalhos da amostra resultante. Cada artigo foi identificado por um número, sendo explorados e registrados os seguintes metadados: autores, título, ano de publicação e palavras-chaves.

Foram realizadas análises de conteúdo com o objetivo de identificar e quantificar tendências nas publicações, servindo de base para inferências, conforme apresentado na seção de resultados. A partir dos termos aplicados na *string* de busca, foi realizada a categorização dos trabalhos conforme a nomenclatura utilizada pelos autores. Além disso, foram identificados o período, os países e os respectivos continentes de publicação.

5 DISCUSSÃO

O resultado da busca realizada encontra-se apresentado no Quadro 2, no qual é apresentado o total de 53 artigos.

Quadro 2 – Artigos analisados.

N°	Ano	Autores	Título
1	2004	Lenstra, A., Voss, T.	Information security risk assessment, aggregation, and mitigation
2	2009	ZAWIŁA-NIEDŹWIECKI, J., Byczkowski, M.	Information Security Aspect of Operational Risk Management
3	2010	Romanov, A., Tsubaki, H., Okamoto, E.	An approach to perform quantitative information security risk assessment in IT landscapes
4	2010	Beebe, N.L., Rao, S.V.	Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process
5	2011	Bolle, S.R., Hasvold, P., Henriksen, E.	Video calls from lay bystanders to dispatch centers - Risk assessment of information security
6	2011	Saleh, M.S., Alfantookh, A.	A new comprehensive framework for enterprise information security risk management
7	2011	Fenz, S., Ekelhart, A., Neubauer, T.	Information security risk management: In which security solutions is it worth investing?
8	2012	Song, J.-G., Lee, J.-W., Lee, C.-K., Kwon, K.-C., Lee, D.-Y.	A cyber security risk assessment for the design of L&C systems in nuclear power plants
9	2012	Shameli-Sendi, A., Shajari, M., Hassanabadi, M., Jabbarifar, M., Dagenais, M.	Fuzzy multi-criteria decision-making for information security risk assessment
10	2013	Liu, L., Bao, T., Yuan, J., Li, C.	Risk assessment of information security based on grey incidence and D-s theory of evidence
11	2013	Bojanc, R., Jerman-Blažič, B.	A quantitative model for information-security risk management
12	2014	Xiangmo, Z., Ming, D., Shuai, R., Luyao, L., Zongtao, D.	Risk assessment model of information security for transportation industry system based on risk matrix
13	2014	Lai, L.K.H., Chin, K.S.	Development of a failure mode and effects analysis based risk assessment tool for information security
14	2014	Webb, J., Maynard, S., Ahmad, A., Shanks, G.	Information security risk management: An intelligence-driven approach
15	2014	Markovic-Petrovic, J.D., Stojanovic, M.D.	An improved risk assessment method for SCADA information security
16	2014	Coronado, A.J., Wong, T.L.	Healthcare cybersecurity risk management: Keys to an effective plan
17	2015	Herland, K., Hmminen, H., Kekolahti, P.	Information security risk assessment of smartphones using bayesian networks
18	2015	Henshel, D., Cains, M.G., Hoffman, B., Kelley, T.	Trust as a Human Factor in Holistic Cyber Security Risk Assessment
19	2015	Chaitanya Krishna, B., Subrahmanyam, K., Kim, T.-H.	A dependency analysis for information security and risk management

20	2015	Shamala, P., Ahmad, R., Zolait, A.H., Sahib, S.B.	Collective information structure model for information security risk assessment (ISRA)
21	2015	Woo, P.S., Kim, B.H., Hur, D.	Towards cyber security risks assessment in electric utility SCADA systems
22	2016	Zarei, J., Sadoughi, F.	Information security risk management for computerized health information systems in hospitals: A case study of Iran
23	2016	Talabeigi, E., Jalali Naeeini, S.G.	Information security risk management and incompatible parts of organization
24	2016	Pan, L., Tomlinson, A.	A systematic review of information security risk assessment
25	2016	Shedden, P., Ahmad, A., Smith, W., Tscherning, H., Scheepers, R.	Asset identification in information security risk assessment: A business practice approach
26	2017	Wangen, G.	Information Security Risk Assessment: A Method Comparison
27	2018	Wangen, G., Hallstensen, C., Snekkenes, E.	A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF
28	2018	Zhu, Q., Qin, Y., Zhou, C., Gao, W.	Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems
29	2018	Fielder, A., König, S., Panaousis, E., Schauer, S., Rass, S.	Risk assessment uncertainties in cybersecurity investments
30	2018	Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., Hu, B.	A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems
31	2018	Kure, H.I., Islam, S., Razzaque, M.A.	An integrated cyber security risk management approach for a cyber-physical system
32	2018	Öbrand, L., Holmström, J., Newman, M.	Navigating Rumsfeld's quadrants: A performative perspective on IT risk management
33	2018	Musman, S., Turner, A.	A game theoretic approach to cyber security risk management
34	2018	Li, S., Bi, F., Chen, W., Miao, X., Liu, J., Tang, C.	An improved information security risk assessments method for cyber-physical-social computing and networking
35	2018	Hashim, N.A., Abidin, Z.Z., Zakaria, N.A., Ahmad, R., Puvanasvaran, A.P.	Risk assessment method for insider threats in cyber security: A review
36	2018	Alohali, M., Clarke, N., Furnell, S.	The design and evaluation of a user-centric information security risk assessment and response framework
37	2018	Kovácsné Mozsár, A.L., Michelberger, P.	It risk management and application portfolio management [Zarządzanie ryzykiem it i zarządzanie portfelem aplikacji]
38	2018	Xuepeng, H., Wei, X.	Method of information security risk assessment based on improved fuzzy theory of evidence
39	2019	Kure, H.I., Islam, S.	Assets focus risk management framework for critical infrastructure cybersecurity risk management
40	2019	Chen, Y.-T., Huang, C.-C.	Determining information security threats for an iot-based energy internet by adopting software engineering and risk management approaches
41	2019	Mokhor, V., Gonchar, S., Dybach, O.	Methods for the total risk assessment of cybersecurity of critical infrastructure facilities [Myetodi otsinki sumarnogo riziku kibyerbyezpyeki ob'iektiv kritichnoyi infrastrukturi]
42	2019	Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev, S.	Information security risk assessment in critical infrastructure: A hybrid MCDM approach
43	2019	Haji, S., Tan, Q., Costa, R.S.	A hybrid model for information security risk assessment
44	2019	Shang, W., Gong, T., Chen, C., Hou, J., Zeng, P.	Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees

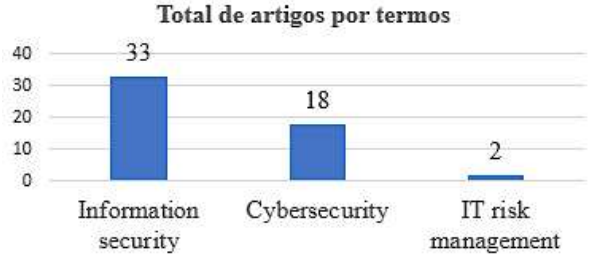
45	2020	Wang, Z., Chen, L., Song, S., Cong, P.X., Ruan, Q.	Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations
46	2020	Brunner, M., Sauerwein, C., Felderer, M., Breu, R.	Risk management practices in information security: Exploring the status quo in the DACH region
47	2020	Maček, D., Magdalenić, I., Ređep, N.B.	A systematic literature review on the application of multicriteria decision making methods for information security risk assessment
48	2020	Wang, J., Neil, M., Fenton, N.	A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model
49	2020	Liu, H.B., Liu, Y., Xu, L.	Dombi Interval-Valued Hesitant Fuzzy Aggregation Operators for Information Security Risk Assessment
50	2021	Yoo, Y., Park, H.-S.	Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship
51	2021	Kalinin, M., Krundyshev, V., Zegzhda, P.	Cybersecurity risk assessment in smart city infrastructures
52	2021	Bhuiyan, T.H., Medal, H.R., Nandi, A.K., Halappanavar, M.	Risk-averse bi-level stochastic network interdiction model for cyber-security risk management
53	2021	Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., Wang, J.	A Systematic Risk Assessment Framework of Automotive Cybersecurity

Fonte: Elaborado pelos autores (2021).

O Quadro 2 apresenta os artigos identificados na busca considerando os respectivos anos de publicação, autores e títulos.

A partir dos termos aplicados na *string* de busca, foi realizada a categorização dos trabalhos, e o resultado encontra-se apresentado na Figura 2.

Figura 2 – Total de Artigos por termos.

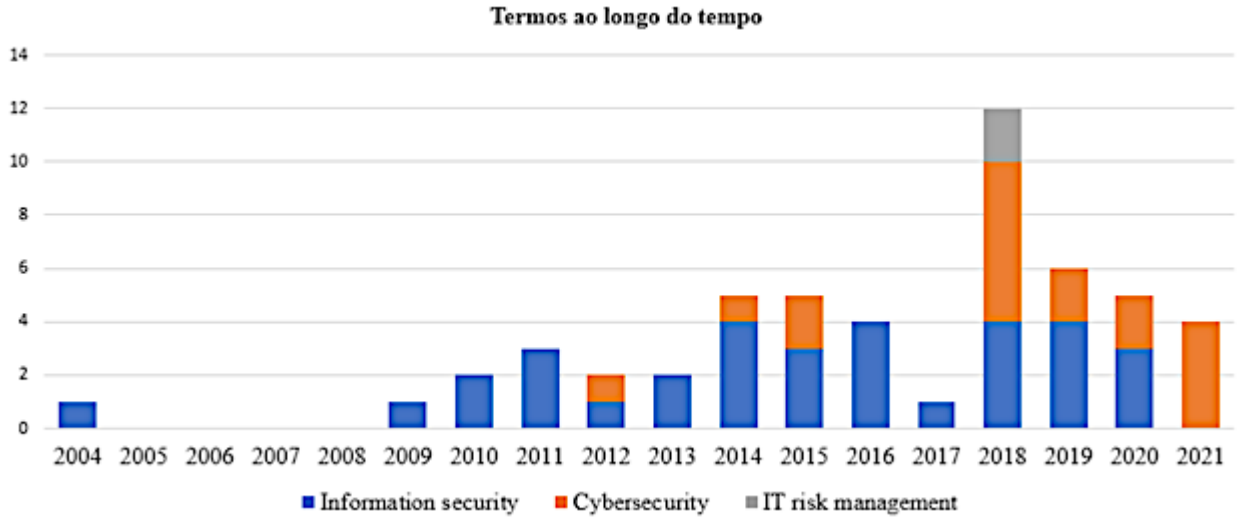


Fonte: Elaborado pelos autores (2021).

É possível observar na Figura 2 que o termo com maior utilização é *information security* com o total de 33 artigos. Em seguida, o termo *cybsersecurity* foi utilizado por 18 trabalhos. Por fim, o termo *IT risk management* foi observado em duas publicações. A análise da figura citada confirma a primeira hipótese proposta para o presente trabalho, uma vez que os principais termos utilizados por trabalhos relacionados ao gerenciamento de riscos cibernéticos são, respectivamente, *information security* e *cybersecurity*.

Já o resultado da classificação dos artigos, considerando os anos de publicação, está apresentado na Figura 3. Lenstra e Voss (2004) abordam o processo de conformidade com a norma *Basel 2*, no qual requisitos de gestão de risco operacional devem ser atendidos por instituições financeiras que, por sua vez, devem definir como lidar com o gerenciamento de riscos. Após a publicação do trabalho citado, não foram localizadas outras publicações nos quatro anos seguintes, sendo que a próxima publicação foi realizada em 2009.

Figura 3 – Utilização de termos ao longo do tempo.



Fonte: Elaborado pelos autores (2021).

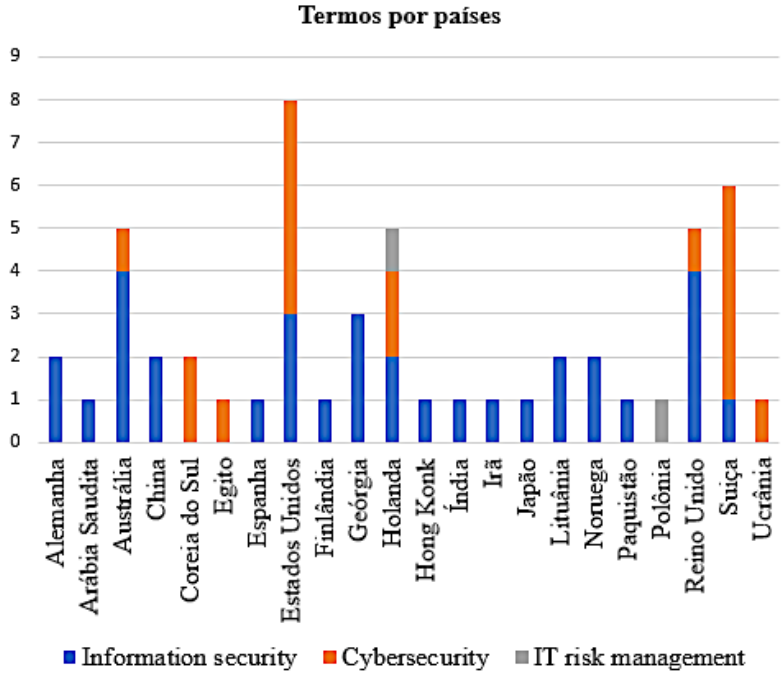
A partir dos dados apresentados na Figura 3, é possível notar que, entre 2009 e 2020, houve a publicação ininterrupta de trabalhos que utilizam o termo *information security*, o que comprova a segunda hipótese proposta neste trabalho.

Por sua vez, houve a publicação constante de artigos com a utilização do termo *cybersecurity* a partir de 2018. Além do uso contínuo do termo, é possível também observar o aumento do número de publicações, visto que 14 artigos (78% do total da amostra do presente trabalho para o termo citado) foram publicados a partir de 2018. A elevação do número de publicações a partir de 2018 com o termo *cybersecurity* comprova a terceira hipótese proposta. Também é válido observar que, no ano de 2021, não foram encontrados artigos publicados com o termo *information security*.

Por fim, o termo *IT risk management* foi observado em publicações apenas do ano 2018. Öbrand, Holmström e Newman (2018) utilizam em seu trabalho o termo citado, no qual são abordados aspectos da teoria de gerenciamento de risco por meio de um estudo de caso, de natureza exploratória, em uma fábrica de papel e celulose, em que foram analisadas as diferentes estratégias empregadas pelos atores envolvidos na organização alvo do estudo. Já Kovácsné Mozsár e Michelberger (2018) apresentam uma nova abordagem para o gerenciamento de riscos de TI baseada na ISO 31000 e fazem o uso do termo *IT risk management*.

O resultado da categorização de artigos por termos, considerando os países de publicação, está apresentado na Figura 4.

Figura 4 – Utilização dos termos por países.

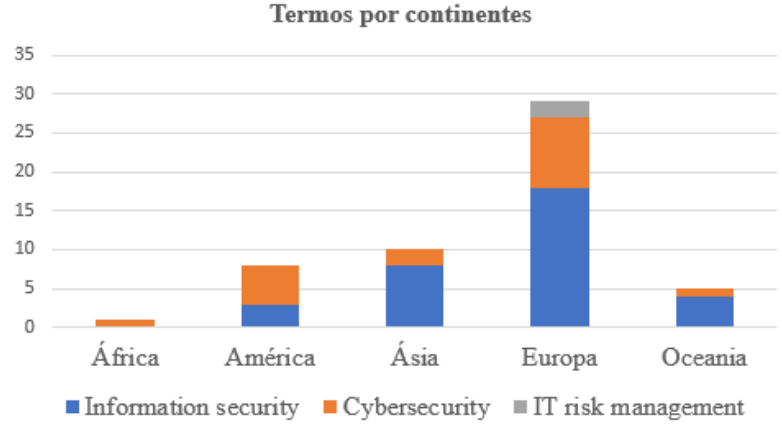


Fonte: Elaborado pelos autores (2021).

É possível notar que os países com maior número de publicações são, respectivamente, Estados Unidos (8), Suíça (6), Austrália, Holanda e Reino Unido (5). Vale ressaltar que o maior uso do termo *cybersecurity* foi observado por artigos dos Estados Unidos e Suíça, ambos com o total de cinco publicações, o que representa a maior parte dos trabalhos publicados nestes dois países.

O resultado da categorização de artigos por termos, considerando os continentes de publicação, está apresentado na Figura 5.

Figura 5 – Utilização dos termos por continentes



Fonte: Elaborado pelos autores (2021).

O maior número de publicações ocorreu na Europa, o que comprova a quarta hipótese proposta no presente trabalho. Vale ressaltar que, no continente citado, foi criada, em 2004, a *European Union Agency for Cybersecurity* (ENISA). Trata-se de uma agência que coopera com os Estados-membros e o setor privado para melhorar as capacidades de defesa contra os ataques cibernéticos (IAVICH; GNATYUK; IASHVILI; FESENKO, 2019). Além da Europa, os continentes que possuem maior volume de publicação são, respectivamente, Ásia, América, Oceania e África.

6 CONCLUSÃO / CONTRIBUIÇÃO

Diante da evolução tecnológica, diferentes termos vêm sendo utilizados para referir-se a temas relacionados ao gerenciamento de riscos de ativos informacionais, o que pode resultar em inconsistências e discrepâncias na terminologia empregada para a área citada. O presente trabalho teve como objetivo explorar quais termos vêm sendo empregados por autores de artigos científicos relacionados ao tema de gerenciamento de riscos cibernéticos. Para isso, foi realizada a busca nas bases de dados Scopus e Scielo utilizando uma *string* construída a partir dos termos comumente utilizados para referir-se à temática proposta.

O objetivo proposto para o presente trabalho foi cumprido a partir da identificação dos termos, período, países e continentes das publicações. Vale ressaltar que a primeira hipótese foi comprovada a partir da análise da Figura 2, visto que os principais termos utilizados por trabalhos relacionados ao gerenciamento de riscos cibernéticos são, respectivamente, *information security* e *cybersecurity*.

Já a segunda e terceira hipótese foram confirmadas por meio da análise da Figura 3. O termo *information security* é amplamente utilizado, entretanto é notável o aumento de publicações utilizando o termo *cybersecurity* a partir de 2018, o que sugere uma mudança na terminologia empregada para o gerenciamento de riscos de ativos informacionais. Por sua vez, a quarta hipótese foi comprovada por meio do levantamento do número de publicações por continentes, no qual foi possível observar que a maior quantidade de trabalhos foi desenvolvida pelo continente europeu. O continente citado possui uma agência que coopera com os Estados-membros e o setor privado para melhorar as capacidades de defesa contra os ataques cibernéticos.

O presente trabalho possui como limitação a utilização de duas bases de dados e pode ser expandido com o uso de outras bases para realização das buscas. Além disso, como trabalho futuro, sugere-se a realização de pesquisas empíricas com o objetivo de avaliar possíveis impactos nas organizações decorrentes da falta de padronização da terminologia empregada para o gerenciamento de riscos cibernéticos. Outra sugestão para trabalhos futuros é refazer a busca, após o período de um ano, para verificar se a tendência de utilização do termo *cybersecurity* permanece ativa.

REFERÊNCIAS BIBLIOGRÁFICAS

ALOHALI, M., CLARKE, N., FURNELL, S. **The design and evaluation of a user-centric information security risk assessment and response framework.** 2018. International Journal of Advanced Computer Science and Applications, 9 (10), pp. 148-163.

ANDRONACHE, Alina; ALTHONAYAN, Abrahim. **Shifting From Information Security Towards A Cybersecurity Paradigm.** 2018. Disponível em: <www.researchgate.net/publication/326400825>. Acesso em: 17 jul. 2021.

BEEBE, N.L., RAO, S.V. **Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process**. 2010. Communications of the Association for Information Systems, 26 (1), pp. 329-358.

BHUIYAN, T.H., MEDAL, H.R., NANDI, A.K., HALAPPANAVAR, M. **Risk-averse bi-level stochastic network interdiction model for cyber-security risk management**. 2021. International Journal of Critical Infrastructure Protection, 32, art. no. 100408.

BOJANC, R., JERMAN-BLAŽIČ, B. **A quantitative model for information-security risk management**. 2013. EMJ - Engineering Management Journal, 25 (2), pp. 25-37.

BOLLE, S.R., HASVOLD, P., HENRIKSEN, E. **Video calls from lay bystanders to dispatch centers - Risk assessment of information security.** 2011. BMC Health Services Research, 11, art. no. 244.

BRUNNER, M., SAUERWEIN, C., FELDERER, M., BREU, R. **Risk management practices in information security: Exploring the status quo in the DACH region**. 2020. Computers and Security, 92, art. no. 101776.

CHAITANYA KRISHNA, B., SUBRAHMANYAM, K., KIM, T.-H. **A dependency analysis for information security and risk management**. 2015. International Journal of Security and its Applications, 9 (8), pp. 205-210.

CHEN, Y.-T., HUANG, C.-C. **Determining information security threats for an iot-based energy internet by adopting software engineering and risk management approaches**. 2019. Inventions, 4 (3), art. no. 53.

CORONADO, A.J., WONG, T.L. **Healthcare cybersecurity risk management: Keys to an effective plan**. 2014. Biomedical Instrumentation and Technology, 48, pp. 26-30.

CORREA JUNIOR, H. E. **Segurança de sistemas: conceitos básicos: material adaptado da Academia Latino-Americana de Segurança - Microsoft**. 2011. Disponível em: <pt.scribd.com/document/84971695/aula1>. Acesso em: 16 jul. 2021.

FERNANDO, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços.** 4 ed. Rio de Janeiro: Brasport, 2014.
FIELDER, A., KÖNIG, S., PANAOUSIS, E., SCHAUER, S., RASS, S. **Risk assessment uncertainties in cybersecurity investments**. 2018. Games, 9 (2), art. no. 34.

FRAPORTI, Simone; BARRETO, Jeanine dos Santos. **Gerenciamento de riscos.** Porto Alegre: SAGAH EDUCAÇÃO S.A., 2018.

FENZ, S., EKELHART, A., NEUBAUER, T. **Information security risk management: In which security solutions is it worth investing?** 2011. Communications of the Association for Information Systems, 28 (1), pp. 329-356.

GREMBERGEN, W. V. **Strategies for information technology governance.** Hershey, PA: Idea Group Publishing, 2004.

HAJI, S., TAN, Q., COSTA, R.S. **A hybrid model for information security risk assessment**. 2019. International Journal of Advanced Trends in Computer Science and Engineering, 8 (1).

HASHIM, N.A., ABIDIN, Z.Z., ZAKARIA, N.A., AHMAD, R., PUVANASVARAN, A.P. **Risk assessment method for insider threats in cyber security: A review**. 2018. International Journal of Advanced Computer Science and Applications, 9 (11), pp. 126-130.

HERLAND, K., HMMINEN, H., KEKOLAHTI, P. **Information security risk assessment of smartphones using bayesian networks**. 2015. Journal Cyber Security and Mobility,4, p.65-86.

HENSHEL, D., CAINS, M.G., HOFFMAN, B., KELLEY, T. **Trust as a Human Factor in Holistic Cyber Security Risk Assessment**. 2015. Procedia Manufacturing, 3, pp. 1117-1124.

IAVICH M., GNATYUK S., IASHVILI G., FESENKO, A. **Cyber security European standards in business**. 2019. Scientific and Practical Cyber Security Journal(SPCSJ)3(2):36- 39.

KALININ, M., KRUNDYSHEV, V., ZEGZHDA, P. **Cybersecurity risk assessment in smart city infrastructures**. 2021. Machines, 9 (4), art. no. 78.

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação.** 1. Ed. Rio de Janeiro: LTC, 2014.

KOVÁCSNÉ MOZSÁR, A.L., MICHELBERGER, P. **It risk management and application portfolio management [Zarządzanie ryzykiem it i zarządzanie portfelem aplikacji]**. 2018. Polish Journal of Management Studies, 17 (2), pp. 112-122.

KURE, H.I., ISLAM, S. **Assets focus risk management framework for critical infrastructure cybersecurity risk management**. 2019. IET Cyber-Physical Systems. 4 (4), pp. 332-340.

KURE, H.I., ISLAM, S., RAZZAQUE, M.A. **An integrated cyber security risk management approach for a cyber-physical system.** 2018. Applied Sciences (Switzerland), 8 (6), art. no. 898.

LAI, L.K.H., CHIN, K.S. **Development of a failure mode and effects analysis based risk assessment tool for information security**. 2014. Industrial Engineering and Management Systems, 13 (1), pp. 87-100.

LI, S., BI, F., CHEN, W., MIAO, X., LIU, J., TANG, C. **An improved information security risk assessments method for cyber-physical-social computing and networking**. 2018. IEEE Access, 6, pp. 10311-10319.

LIU, L., BAO, T., YUAN, J., LI, C. **Risk assessment of information security based on grey incidence and D-s theory of evidence**. 2013. Journal of Applied Sciences, 13(10), p. 1740-1745.

LIU, H.B., LIU, Y., XU, L. **Dombi Interval-Valued Hesitant Fuzzy Aggregation Operators for Information Security Risk Assessment**. 2020. Mathematical Problems in Engineering, 2020, art. no. 3198645.

LENSTRA, A., VOSS, T. **Information security risk assessment, aggregation, and mitigation**. 2004. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3108, pp. 391-401.

MAČEK, D., MAGDALENIĆ, I., REĐEP, N.B. **A systematic literature review on the application of multicriteria decision making methods for information security risk assessment**. 2020. International Journal of Safety and Security Engineering, 10 (2), pp. 161-174.

MARKOVIC-PETROVIC, J.D., STOJANOVIC, M.D. **An improved risk assessment method for SCADA information security**. 2014. Elektronika ir Elektrotechnika, 20 (7), pp. 69-72.

MOKHOR, V., GONCHAR, S., DYBACH, O. **Methods for the total risk assessment of cybersecurity of critical infrastructure facilities**. 2019. Nuclear Radiation Safety, 2(82), p. 4-8.

MOLINARO, Luís Fernando Ramos; RAMOS, Karoll Haussler Carneiro**. Gestão de tecnologia da informação: governança de TI: arquitetura e alinhamento entre sistemas de informação e o negócio.** Rio de Janeiro: LTC, 2011.

MONTEIRO, M. S. **A importância da gestão de riscos.** Belém: CONACI, 2017.

MUSMAN, S., TURNER, A. **A game theoretic approach to cyber security risk management**. 2018. Journal of Defense Modeling and Simulation, 15 (2), pp. 127-146.

ÖBRAND, L., HOLMSTRÖM, J., NEWMAN, M. **Navigating Rumsfeld's quadrants: A performative perspective on IT risk management**. 2018. Technology in Society, 53, pp. 1-8.

PAN, L., TOMLINSON, A. **A systematic review of information security risk assessment**. 2016. International Journal of Safety and Security Engineering, 6 (2), pp. 270-281.

RAHMAN, Syed (Shawon) M., DONAHUE, Shannon E. **Convergence of Corporate and Information Security**. 2010. International Journal of Computer Science and Information Security,Vol. 7, No. 1.

RODRIGUES, A. R.; TAVAR, C.; NOGUEIRA, G. M.; LIBRELOTTO, R. F. **A bibliometria como ferramenta de análise da produção intelectual: uma análise dos hot topics sobre sustentabilidade**. Biblionline, v. 12, n. 3, p. 34-47, 2016.

ROMANOV, A., TSUBAKI, H., OKAMOTO, E. **Caan approach to perform quantitative information security risk assessment in IT landscapes**. 2010. Journal of Information Processing, 18, pp. 213-226.

SALEH, M.S., ALFANTOOKH, A. **A new comprehensive framework for enterprise information security risk management**. 2011. Applied Computing and Informatics, 9 (2), pp. 107-118.

SHAMALA, P., AHMAD, R., ZOLAIT, A.H., SAHIB, S.B. **Collective information structure model for information security risk assessment (ISRA)**. 2015. Journal of Systems and Information Technology, 17 (2), pp. 193-219.

SHAMELI-SENDI, A., SHAJARI, M., HASSANABADI, M., JABBARIFAR, M., DAGENAIS, M. **Fuzzy multi-criteria decision-making for information security risk assessment**. 2012. Open Cybernetics and Systemics Journal, 6 (1), pp. 26-37.

SHANG, W., GONG, T., CHEN, C., HOU, J., ZENG, P. **Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees**. 2019. Security and Communication Networks, 2019, art. no. 3574675.

SHEDDEN, P., AHMAD, A., SMITH, W., TSCHERNING, H., SCHEEPERS, R. **Asset identification in information security risk assessment: A business practice approach**. 2016. Communications of the Association for Information Systems, 39 (1), art. no. 15, pp. 297-320.

SONG, J.-G., LEE, J.-W., LEE, C.-K., KWON, K.-C., LEE, D.-Y. **A cyber security risk assessment for the design of L&C systems in nuclear power plants**. 2012. Nuclear Engineering and Technology, 44 (8), pp. 919-928.

STEINBERG, Joseph. **Cybersecurity for Dummies.** 1 ed. Rio de Janeiro: Alta Books, 2020.

TALABEIGI, E., JALALI NAEEINI, S.G. **Information security risk management and incompatible parts of organization**. 2016. Journal of Industrial Engineering and Management, 9 (4), pp. 964-977.

TURSKIS, Z., GORANIN, N., NURUSHEVA, A., BORANBAYEV, S. **Information security risk assessment in critical infrastructure: A hybrid MCDM approach**. 2019. Informatica (Netherlands), 30 (1), pp. 187-211.

XIANGMO, Z., MING, D., SHUAI, R., LUYAO, L., ZONGTAO, D. **Risk assesment model of information security for transportation industry system based on risk matrix**. 2014. Applied Mathematics and Information Sciences, 8 (3), pp. 1301-1306.

XUEPENG, H., WEI, X. **Method of information security risk assessment based on improved fuzzy theory of evidence**. 2018. International Journal of Online Engineering, 14 (3), p. 188-196.

YOO, Y., PARK, H.-S. **Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship**. 2021. Journal of Marine Science and Engineering, 9 (6), art. no. 565.

WANG, Z., CHEN, L., SONG, S., CONG, P.X., RUAN, Q. **Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations**. 2020. Alexandria Engineering Journal, 59 (4), pp. 2725-2731.

WANG, J., NEIL, M., FENTON, N. **A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model**. 2020. Computers and Security, 89, art. no. 101659.

WANG, Y., WANG, Y., QIN, H., JI, H., ZHANG, Y., WANG, J. **A Systematic Risk Assessment Framework of Automotive Cybersecurity**. 2021. Automotive Innovation.

WANGEN, G. **Information Security Risk Assessment: A Method Comparison**. 2017. Computer, 50 (4), art. no. 7912273, pp. 52-61.

WANGEN, G., HALLSTENSEN, C., SNEKKENES, E. **A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF**. 2018. International Journal of Information Security, 17 (6), pp. 681-699.

WEBB, J., MAYNARD, S., AHMAD, A., SHANKS, G. **Information security risk management: An intelligence-driven approach**. 2014. Australasian Journal of Information Systems, 18 (3), pp. 391-404.

WOO, P.S., KIM, B.H., HUR, D. **Towards cyber security risks assessment in electric utility SCADA systems**. 2015. Journal of Electrical Engineering and Technology, 10 (3), pp. 888-894.

ZAREI, J., SADOUGHI, F. **Information security risk management for computerized health information systems in hospitals: A case study of Iran**. 2016. Risk Management and Healthcare Policy, 9, pp. 75-85.

ZAWIŁA-NIEDŹWIECKI, J., BYCZKOWSKI, M. **Information Security Aspect of Operational Risk Management**. 2009. Foundations of Management, 1 (2), pp. 45-60.

ZHANG, Q., ZHOU, C., TIAN, Y.-C., XIONG, N., QIN, Y., HU, B. **A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems**. 2018. IEEE Transactions on Industrial Informatics, 14 (6), pp. 2497-2506.

ZHU, Q., QIN, Y., ZHOU, C., GAO, W. **Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems**. 2018. International Journal of Distributed Sensor Networks, 14 (6).