RISCO EM SEGURANÇA DA INFORMAÇÃO

Bruno Yuiti Mitsuda Inomata[1]

bruno.inomata@fatec.sp.gov.br
Faculdade de Tecnologia de São Paulo

Carlos Hideo Arima

charima@uol.com.br
Faculdade de Tecnologia de São Paulo

1. Introdução

De acordo com [3], é por meio da compreensão dos riscos que as pessoas puderam ver que podem não apenas entender o futuro como também se planejarem e orientarem os futuros eventos.

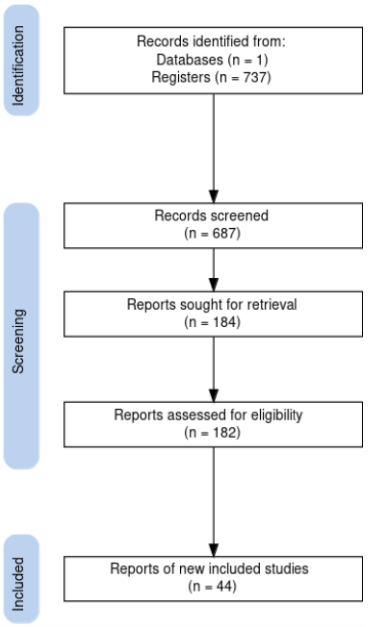
Na área da segurança da informação essa necessidade de se entender os riscos também existe. Assim, foram criados diversos métodos para se administrá-los: desde a descoberta dos riscos aos seus tratamentos. Porém, não há um consenso sobre qual o estado da arte destes modelos, o que dificulta a adoção de medidas em relação aos riscos, prejudicando a segurança da informação.

Portanto, este trabalho busca encontrar os modelos de gestão de risco mais utilizados em segurança da informação atualmente, de forma a facilitar a escolha de um modelo, assim como identificar as lacunas que podem ser exploradas futuramente nesta temática.

2. Metodologia

Para orientação do processo de revisão sistemática, seguiu-se o protocolo PRISMA-P. Onde são definidas etapas para o processo de seleção dos artigos para revisão sistemática (Figura 01).

Figura 01 –Protocolo PRISMA-P



Fonte: Resultado da pesquisa.

Devido à necessidade de se encontrar artigos relevantes, foram utilizados alguns critérios para as pesquisas, conforme apresentado (Tabela 01).

Tabela 01 – Critérios de Busca.

Base de Pesquisa	OpenAlex
Período	2018 - 2024
Idioma	Inglês
Publicação	Artigos de periódicos
Acesso	Aberto

Fonte: Resultado da pesquisa.

Foi feito um levantamento e análises de termos relevantes à temática através de uma nuvem de palavras da obra [8] e pesquisas em obras relacionadas como [12]. Assim, foram definidos duas strings para pesquisas na base de dados (Tabela 02).

Tabela 02 – Termos de buscas.

String de Busca	Número de Resultados
security AND risk AND (assessment OR analysis OR management)	474

(((information OR cyber OR technology OR system OR "IT") AND security) AND risk AND (assessment OR analysis OR management))	263

Fonte: Resultado da pesquisa.

Com os critérios de busca e termos definidos, foram feitas diversas pesquisas bibliográficas em uma nova base de dados chamada OpenAlex [10]. Esta base foi escolhida pelo número abundante de trabalhos catalogados, acesso livre para pesquisas, restrições mínimas, compatibilidade com softwares de bibliometria e interface compreensível.

Os resultados das pesquisas tiveram seus abstracts revisados a respeito da pertinência ao tema para se formar uma lista de artigos que foram revisados sistematicamente e utilizados em uma análise bibliométrica.

3. Resultados

Neste trabalho, notou-se que a maioria dos artigos analisados discutem sobre assuntos específicos populares atualmente: tecnologias e conceitos em desenvolvimento e início de sua aplicação por empresas e organizações, e que, portanto, necessitam de uma gestão de riscos apropriada para que se possa compreender quais as novas vulnerabilidades e ameaças, e, além disso, quais são, como avaliar, e como lidar com estes novos riscos. Estes conceitos são, principalmente: IoT, sistemas ciberfísicos, blockchain, cidades inteligentes e inteligência artificial.

Dos 737 resultados obtidos nas pesquisas, após o processo PRISMA-P, foram selecionados 38. Destes, a média de citações é de 145, a maioria dos artigos são de

2019, e enquanto alguns abordam especificamente sobre gestão e análise de riscos, a maioria discute sobre tecnologias e assuntos emergentes (Figura 02).

Figura 02 –Temas mais abordados nos artigos

Fonte: Resultado da pesquisa.

Em relação aos modelos de gestão de riscos, não foi possível identificar um consenso ou modelos amplamente utilizados. Alguns autores apresentaram adaptações de modelos já existentes como em [2]; enquanto outros apresentaram uma metodologia de avaliação de riscos nova, como [13] e sua metodologia híbrida entre avaliação quantitativa e qualitativa; [4] utilizou do guia de orientações ETSI; e [5] não utilizou-se de frameworks, baseando-se em análises dos pilares da segurança da informação.

Uma das lacunas identificadas entre os trabalhos foi a exploração de uma metodologia genérica e compreensível que seja aplicável para organizações de todos os tipos, não abordando apenas tecnologias em ascensão como o blockchain ou IoT.

Outra lacuna identificada são as pesquisas com foco no fator humano em segurança da informação, cuja importância é apontada em [11], onde é dito que o ser humano é o elo mais fraco da cadeia de segurança. Dentre as 38 obras selecionadas apenas cinco lidam com esta temática: [6] apresenta um framework de treinamento para operadores que não são especialistas em sistemas de informação que lidam com infraestrutura crítica como enfermeiros e bombeiros; [1] aborda os problemas de se treinar pessoas contra ataques de engenharia social; em [9] é feita uma revisão sistemática da literatura sobre o tema em relação à área da saúde; [11] apresenta técnicas de detecção, prevenção e mitigação dos ataques de engenharia social; e de forma paralela, em [7] é apresentado um jogo como parte do treinamento de pessoas que propõe aumentar a conscientização dos conceitos de cibersegurança em uma organização.

4. Conclusões

Este trabalho buscou identificar um modelo amplamente utilizado entre organizações através de buscas em uma base de dados, análises bibliométricas e revisão sistemática. Algumas das restrições observadas foram as limitações de outras bases de dados exploradas, que dificultavam o acesso a informações das obras necessárias para as etapas seguintes da pesquisa, principalmente sem as credenciais necessárias. As oportunidades de futuras pesquisas identificadas são a de exploração de modelos de gestão de riscos

em cenários mais comuns em organizações, e a de modelos com um maior foco no fator humano para proteção contra engenharia social.

Referências

ALDAWOOD, Hussain; SKINNER, Geoffrey.Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future internet, v. 11, n. 3, p. 73, 2019.

AK, M. Fatih; GUL, Muhammet. AHP–TOPSISintegration extended with Pythagorean fuzzy sets for information security risk analysis. Complex &
Intelligent Systems, v. 5, n. 2, p. 113-126, 2019.

BERNSTEIN, Peter L. Desafio aos deuses: afascinante história do risco. Gulf Professional Publishing, 1997.

BUTUN, Ismail; PEREIRA, Nuno; GIDLUND,Mikael. Security risk analysis of LoRaWAN and future directions. Future Internet, v. 11, n. 1, p. 3, 2018.

DWIVEDI, Ashutosh Dhar et al. A decentralizedprivacy-preserving healthcare blockchain for IoT. Sensors, v. 19, n. 2, p. 326, 2019.

GHAFIR, Ibrahim et al. Security threats to criticalinfrastructure: the human factor. The Journal of Supercomputing, v. 74, p. 4986-5002, 2018. [7] HART, Stephen et al. Riskio: A serious game for cyber security awareness and education. Computers & Security, v. 95, p. 101827, 2020.

MAČEK, Davor; MAGDALENIĆ, Ivan; REĐEP,N. Begičević. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. International Journal of Safety and Security Engineering, v. 10, n. 2, p. 161-174, 2020.

NIFAKOS, Sokratis et al. Influence of humanfactors on cyber security within healthcare organisations: A systematic review. Sensors, v. 21, n. 15, p. 5119, 2021.

PRIEM, Jason; PIWOWAR, Heather; ORR,Richard. OpenAlex: A fully-open index of scholarly works, authors, venues, institutions, and concepts. arXiv preprint arXiv:2205.01833, 2022.

SALAHDINE, Fatima; KAABOUCH, Naima.Social engineering attacks: A survey. Future internet, v. 11, n. 4, p. 89, 2019.

YOKOYAMA, Rodrigo; ARIMA, Carlos Hideo.Análise textual e bibliométrica sobre modelagem de ameaça Textual and bibliometric analysis on threat modeling. Brazilian Journal of Development, v. 8, n. 1, p. 7678-7690, 2022.

ZOGRAFOPOULOS, Ioannis et al. Cyber-physicalenergy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, v. 9, p. 29775-29818, 2021.

Agradecimentos

À instituição Faculdade de Tecnologia de São Paulo pela realização das medições.

[1] Aluno de IC com bolsa PIBIC-CNPq: Processo 105304/2024-07.