Fatores de Riscos que Influenciam em uma Infraestrutura de Data Center utilizando o método TEMAC

Risks Factors that Influence a Data Center Infrastructure through the TEMAC method

Fábio G. F. Tabosa, Daniel A. da Silva, Rafael T. de Sousa Jr, Flavio Elias G. de Deus, Rafael Rabelo Nunes
Universidade de Brasília, Departamento de Energia Elétrica
Campus Universitário Darcy Ribeiro, Brasília, Brasil
fabio.tabosa@gmail.com, daniel.alves@redes.unb.br, {desousa, flavioelias, rafaelrabelo}@unb.br

Resumo — **O trabalho apresenta uma análise dos fatores de riscos que influenciam uma infraestrutura de Data Center, por meio da Teoria do Enfoque Meta Analítico Consolidado (TEMAC). Após pesquisa bibliométrica nos repositórios da Web of Science e Scopus, foram encontrados 96 resultados relevantes. Para análise de co-autoria, co-citação e acoplamento bibliográfico, foram produzidos mapas de calor para facilitar a visualização para facilitar a visualização de autores e obras relevantes. Já na análise da frequência das palavras chaves dos artigos selecionados, foram extraídos termos com grande frequência nas duas bases de dados, tais como: segurança; rede; risco; energia; gerenciamento; virtual e serviço. Como resultado foram obtidos 11 artigos de alta relevância que apresentaram 10 fatores de riscos que influenciam na avaliação de acordo com os identificadores exclusivos de 3 funções e 8 categorias do Framework Segurança Cibernética do NIST, sendo: i) governança; ii) gerenciamento de riscos da cadeia de suprimento; iii) gerenciamento de identidade e controle de acesso; iv) segurança de dados; v) processos e procedimentos de proteção da informação; vi) tecnologia protetora; vii) anomalias e incidentes; viii) monitoramento contínuo de segurança.**

Palavras Chave – Data Center; Risco; Gestão de Risco; Ameaças Cibernéticas; Framework Segurança Cibernética.

Abstract — **The paper presents an analysis of the risk factors that influence a data center infrastructure, by means of the Theory of Meta-Analytic Consolidated Approach (TEMAC). After bibliometric research in the Web of Science and Scopus repositories, 96 relevant results were found. For the analysis of co-authorship, co-citation and bibliographic coupling, heat maps were produced to facilitate the visualization of relevant authors and works. As for the analysis of the frequency of the keywords in the selected articles, terms with high frequency in the two databases were extracted, such as: security; network; risk; energy; management; virtual and service. As a result, 11 highly relevant articles were obtained that presented 10 risk factors that influence the evaluation according to the unique identifiers of 3 functions and 8 categories of the NIST Cybersecurity Framework, being: i) governance; ii) supply chain risk management; iii) identity management and access control; iv) data security; v) information protection processes and procedures; vi) protective technology; vii) anomalies and incidents; viii) continuous security monitoring.**

Keywords – Data Center; Risk; Risk Management; Cyber threats; Cybersecurity Framework.

I. INTRODUÇÃO

Os rápidos avanços na área de tecnologia da informação e comunicação e o avanço da digitalização de serviços, vem impulsionando o intenso uso do espaço cibernético na cadeia produtiva e por consequência nas mais variadas atividades adjacentes por todo o mundo. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade [1]. A evolução dos requisitos para computação onipresente, acesso imediato e análises de dados criaram novas demandas por informações com alta disponibilidade, o que afeta diretamente a operação dos Data Centers [2].

Assim, para melhorar o nível de proteção da infraestrutura de um Data Centers é necessário entender quais são os fatores de risco de segurança da cibernética, e para isso é preciso identificá-los na literatura científica. Deste modo, o objetivo desta pesquisa é realizar uma análise referente aos fatores de riscos que influenciam em uma infraestrutura de Data Center, fazendo uso da Teoria do Enfoque Meta Analítico Consolidado - TEMAC [3] e após a pesquisa bibliométrica, correlacionar os resultados de acordo com uma estrutura de orientação de Segurança Cibernética para infraestruturas críticas como o *Cybersecurity Framework* (CSF) do National Institute of Standards and Technology (NIST).

Nesse contexto, este trabalho tem como principal contribuição identificar e avaliar quais são as áreas críticas quanto a segurança cibernética em Data Centers a partir da utilização de um framework de segurança para o fortalecimento de ações de defesa cibernética.

O trabalho está organizado da seguinte forma: além desta introdução, a seção 2 apresenta o referencial teórico onde serão discorridos os conceitos da Data Centers e as recomendações para a gestão desses riscos; em seguida, tem-se uma seção 3 com detalhamento da metodologia utilizada no trabalho; a seção 4

2021 16th Iberian Conference on Information Systems and Technologies (CISTI)
23 – 26 June 2021, Chaves, Portugal
ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.

apresenta os resultados e sua análise; seção 5 é feita a correlação dos fatores de risco influenciadores; por fim, apresentar-se a conclusão.

II. Referência Teórico

O sucesso das operações de negócios depende da proteção da confidencialidade, integridade, disponibilidade das informações processadas, armazenadas e transmitidas por esses sistemas. As ameaças aos sistemas de informação incluem falhas de equipamentos, interrupções ambientais, erros humanos ou de máquinas, e ataques intencionais que muitas vezes são sofisticados, disciplinados, bem organizados e bem financiados. [4].

A. Infraestrutura de Data Centers

Data Center é uma instalação física dentro de uma organização, a qual está encarregada de centralizar as operações e os equipamentos de TI focados no processamento, armazenamento, gerenciamento e disseminação de dados de apoio a uma ou várias organizações [5]. Na época das grandes operações de TI centralizadas, esse departamento e todos os sistemas residiam em um único local físico, daí o nome data center [6].

Com os métodos de computação mais distribuídos de hoje, sites únicos de data center ainda são comuns e os gastos com infraestrutura global de data center devem chegar a US $ 200 bilhões em 2021, um aumento de 6% a partir de 2020, de acordo com a última previsão do Gartner, Inc. Apesar de um declínio de 10,3% nos gastos com data center em 2020 devido à restrição fluxo de caixa durante a pandemia COVID-19, o mercado de data center ainda deve crescer ano a ano até 2024 [6].

Indisponibilidades em um Data Center podem paralisar uma ou várias organizações. Os crimes cibernéticos são a segunda causa em todo o mundo, e a que mais cresce, das indisponibilidades de data centers [7].

B. Gestão de Riscos de Segurança e Privacidade

De acordo com o NIST [8], a gestão dos riscos de segurança e privacidade relacionados ao sistema de informação é um processo complexo que requer o envolvimento de toda a organização.

A gestão de riscos é um componente primário da governança, servindo de referência para a definição e a implantação de medidas mitigadoras para organização, nesse sentido, o NIST criou o *Cybersecurity Framework* (CSF) [8] que é uma abordagem baseada em risco para gerenciar os riscos de segurança cibernética e é composta de três partes:

- Estrutura Básica (*Core*).
- Níveis de Implementação (*Tiers*).
- Avaliações da Estrutura (*Profile*).

O CSF se concentra no uso de indicadores de negócios para orientar as atividades de segurança cibernética e considera os riscos de segurança cibernética como parte dos processos de gerenciamento de riscos da organização.

III. Metodologia

A metodologia utilizada foi a pesquisa bibliográfica por meio da Teoria do Enfoque Meta Analítico Consolidado – TEMAC, que é dividida em 3 etapas: i) preparação da pesquisa; ii) apresentação e inter-relação dos dados; iii) detalhamento, modelo integrador e validação por evidências. Como resultado, combinam-se bases de dados diferentes, apresentando um conjunto de material confiável. Portanto, o enfoque meta-analítico visa oferecer uma técnica objetiva de escolha da literatura para respaldar uma pesquisa [3]. Este método permite integrar as exigências atuais da literatura a respeito de trabalhos científicos com precisão, robustez, validade, funcionalidade, tempo e custos [9].

A primeira etapa consiste na construção da *string* de busca com palavras-chave que abordem o tema de pesquisa de forma mais apropriada, bem como as áreas de conhecimento que serão utilizadas.

Após a obtenção dos resultados nas bases de dados com a utilização da *string* de busca definida, é iniciada a segunda etapa que consiste na apresentação e inter-relação entre os registros, dentre esses temos: análise de revistas mais relevantes; análise de revistas que mais publicaram sobre o tema; evolução do tema ano a ano; documentos mais citados; países que mais publicaram; conferências que mais contribuíram; universidades que mais publicaram; agências que mais financiam a pesquisa; áreas que mais publicam; e frequência de palavras-chave.

Na terceira etapa são realizadas análises mais profundas que permitam compreender melhor o tema, como a identificação de co-autoria e co-citação, as principais abordagens, linhas de pesquisas, validação via evidências e entrega do modelo integrador por meio de comparação dos resultados das diferentes fontes [3] [9].

Foram escolhidas para a pesquisa as bases de dados Web of Science (WoS) e Scopus por serem base de dados consolidadas e de reconhecida qualidade. A busca nas bases foi realizada em janeiro de 2021. Para análise de co-autoria, co-citação e acoplamento bibliográfico foi utilizado o software VOSviewer [10], gerando-se mapas de calor para facilitar a visualização de autores e obras relevantes, e para análise de frequência de palavras foi utilizada a ferramenta TagCrowd [11].

IV. Revisão através do TEMAC e resultados

A. Etapa 1: Preparação da pesquisa

Para construção da *string* de pesquisa foram utilizadas palavras em inglês que refletissem o tema, envolvendo expressões relacionadas a Data Center e Riscos quanto a Segurança Cibernética no corpo do título dos documentos, conforme Tabela I.

TABELA I. STRINGS DE PESQUISA

Base de dados	String
WoS	TI= ("Data Center" OR "Datacenter") AND TI= ("Risk" OR "Security" OR "Cyber" OR "Cybersecurity" OR "Attack") AND PY= (2016-2020) AND WC= (engineering electrical electronic or telecommunications or computer science theory methods or computer science information systems)

2021 16th Iberian Conference on Information Systems and Technologies (CISTI)
23 – 26 June 2021, Chaves, Portugal
ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.

Base de dados	String
Scopus	TITLE ("Data Center" OR "Datacenter") AND TITLE ("Risk" OR "Security" OR "Cyber" OR "Cybersecurity" OR "Attack") AND PUBDATETXT (2016 OR 2017 OR 2018 OR 2019 OR 2020) AND SUBJAREA (comp OR engi)

Para mapear o desenvolvimento do tema foi adotada a delimitação temporal de artigos que contemplasse os últimos 5 anos, de 2016 a 2020, sem limitação espacial. Na WoS os resultados foram filtrados por quatro categorias: Engineering Electrical Electronic, Telecommunications, Computer Science Information Systems, Computer Science Theory Methods, sendo encontrado 33 resultados. Já na base Scopus, foram filtradas as áreas de Engineering e Computer Science, e encontrando 92 resultados.

B. Etapa 2: Apresentação e inter-relação dos dados

Após análise dos resultados foram identificados e removidos resultados duplicados entre as duas bases de dados, bem como livros e ao final restaram 96 documentos únicos. Dentre os mais citados na WoS e Scopus, respectivamente temos o W. Hou [12] com 52 e 57 citações, o segundo foi o de C. Buragohain [13] com 43 citações na base Scopus apenas, o terceiro foi o de K. S. Sahoo [14] com 28 e 40 citações e o quarto foi Z. Li [15]. O estudo de W. Hou [12] foca no risco de segurança em redes de ambientes virtuais em Data Centers distribuídos geograficamente, C. Buragohain [13] e K.S. Sahoo [14] abordam as questões de segurança dos Data Centers baseados em SDN e suas vulnerabilidades, enquanto Z. Li [13], trata do custo da energia como um problema de segurança, o qual atrai muita atenção e traz questões de gerenciamento de otimização energética.

Os autores com mais publicações na base *Scopus* foram 2 e tiveram 4 artigos publicados cada um sobre o tema: M.A. Islam e S. Ren [16], seus estudos abordam temas sobre a capacidade energética de um Data Center e um conjunto de possíveis estratégias de defesa para proteger a infraestrutura contra ataques de energia (consumo excessivo de energia elétrica e até superior a capacidade disponível) que podem ser explorado por clientes mal intencionados que hospedam seus equipamentos de TI no formato de *colocation*. Já na base WoS foram 2 também, porém, autores diferentes da base *Scopus*, M. Levy e D. Raviv [19], ambos com 3 artigos publicados sobre o tema, onde se propõe uma metodologia com objetivo padronizar um processo para ajudar a avaliar a localização física de um Data Center e compará-los entre si, ou comparar diferentes cenários onde o Data Center opera.

Em relação às revistas e conferências onde foram publicados os estudos sobre o tema, caso fossem agregados os registros por organizações publicadoras, sem considerar o nome completo da revista e/ou a edição do evento, temos a organização Institute of Electrical and Electronics Engineers (IEEE) com a maior concentração de documentos, 30,2%, ou seja, 29 resultados do total de 96 artigos, sendo deste, 24 artigos de conferências mundiais do IEEE.

Os dez países que mais publicaram sobre o tema são apresentados na Tabela II. O Brasil está localizado na 7º posição, com a mesma quantidade de publicações com a Malásia, Portugal e Arábia Saudita, em um ranking de 18 nações que possuem artigos que abordam o tema do presente estudo.

TABELA II. PAÍSES COM MAIOR NÚMERO DE PUBLICAÇÕES

País	Publicações	%
1º Estados Unidos	21	21,9%
2º China	20	20,8%
3º India	14	14,6%
4º Inglaterra	7	7,3%
5º Russia	5	5,2%
6º Italia	4	4,2%
7º Brasil	3	3,1%
7º Malásia	3	3,1%
7º Portugal	3	3,1%
7º Arábia Saudita	3	3,1%
Outros	13	13,5%
Total	96	100%

No Brasil, as pesquisas sobre o tema, foram a respeito de segurança em redes com o uso da tecnologia de *Software Defined Networks* (SDN) [14] [17] e a avaliação da maturidade dos centros de dados [18].

A Fig. 1 mostra a evolução das publicações sobre o tema nas bases WoS e Scopus, e possui um crescimento a partir do ano de 2018. Quanto aos números de citações, verifica-se a evolução, onde se nota o mesmo comportamento em ambas as bases com um crescimento ano após ano.

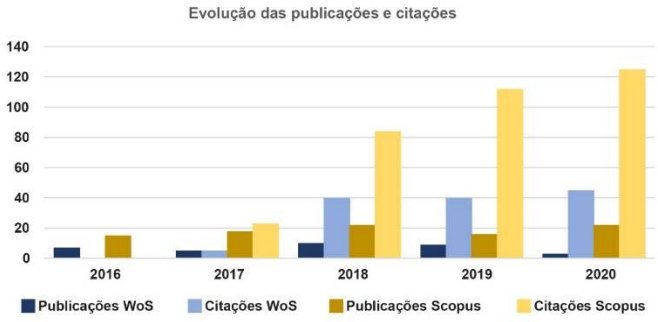


Figura 1. Evolução do tema ano após ano na WoS e Scopus

Em relação a frequência de palavras-chave [11], é apresentado na Fig. 2 o *"word cloud"* elaborado pelas as palavras-chave dos artigos excluindo, as palavras Data, Center e Datacenter. É possível observar as seguintes palavras em destaques na ordem decrescente, superior a 18 de frequência, de amostragem: *security; network; risk; energy; management; virtual e service.*

C. Etapa 3: Detalhamento, modelo integrador e validação por evidências

Com base nos dados extraídos da WoS e Scopus, foram criados mapas de calor [10], de forma a facilitar a visualização da análise sobre o rumo da pesquisa dos fatores de riscos que influenciam em uma infraestrutura de Data Center. Esses mapas usam cores mais quentes e fontes em negrito para enfatizar conceitos que são frequentemente utilizados, enquanto palavras

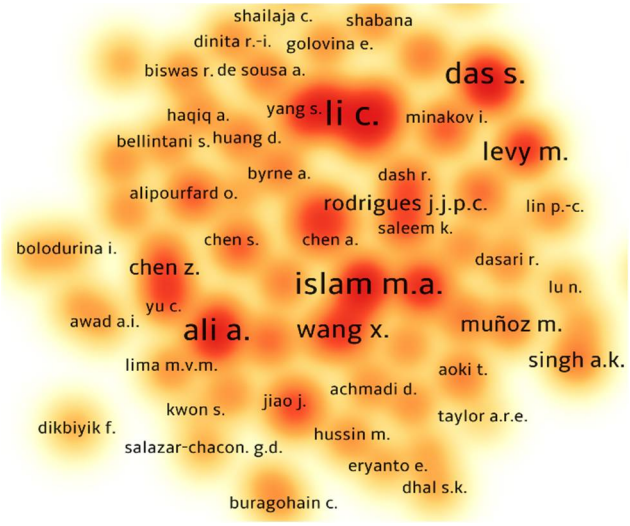
ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.

que são usadas apenas esporadicamente são mostradas em cores mais frias e fontes menores [20].

Fígura 2. Word cloud com as palavras chaves de todos os 96 artigos.

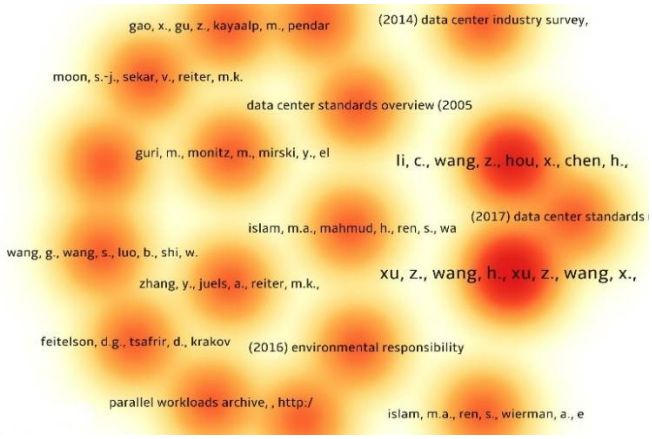
As análises de co-autoria que é a colaboração entres autores com formação de redes de pesquisadores, são apresentadas na Fig. 3.



Fígura 3. Mapa de calor de co-autoria de todos os 96 artigos.

De um total de 252 autores presentes nos 96 artigos, é possível observar ao analisar a Fig. 3 que existem 2 clusters de co-autoria, sendo o primeiro de Z. Li e C. Li cada um desses autores possui 2 artigos, onde os mesmos trabalharam em conjunto e esses autores são da Nanjing University, Nanjing, China, o segundo cluster é formado por M. A. Islam e X. Wang cada um desses autores com 4 artigos sem nenhum trabalho em conjunto, porém o autor L. Yang realizou dois trabalhos, sendo um artigo com cada um desses autores o que viabilizou esse elo entre eles, onde os Islan é da University of California, Riverside, United States e Wang do Northeastern Univ, Liaoning, Peoples R China, mostrando que é comum a co-autoria entre autores da mesma nacionalidade ou pais residente, bem como entre nações.

Na análise de co-citação, no mapa de calor apresentado na Fig. 4, é possível observar uma proximidade entre os artigos citados de C. Li [23] e Z. Xu mostrando que esses artigos apresentam assuntos semelhantes.



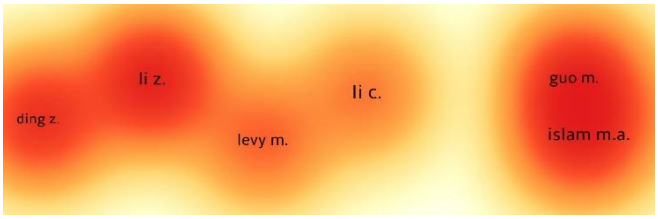
Fígura 4. Mapa de calor de co-citação de todos os 96 artigos.

Dentre o total de co-citação foram identificadas 2.128 referências nos 96 artigos analisados, desses, a Tabela III lista os 4 mais referenciados.

TABELA III. OS 4 ARTIGOS MAIS REFERÊNCIADOS

Referência	# Citações nos 96
Z. Xu, H. Wang, Z. Xu, and X. Wang, “Power attack: An increasing threat to data centers,” 2014.	5
C. Li, Z. Wang, X. Hou, H. Chen, X. Liang, and M. Guo, “Power attack defense: Securing battery-backed data centers,” 2016.	4
J. Stanley, and J. Koomey. "The Science of Measurement: Improving Data Centre Performance with Continuous Monitoring and Measurement of Site Infrastructure." 2009.	3
X. Meng, V. Pappas, and L. Zhang, “Improving the scalability of data center networks with traffic-aware virtual machine placement,” 2010.	3

Na Fig. 5 é apresentado a análise do acoplamento bibliográfico, que é quando artigos possuem citações em comum, logo abordam assuntos semelhantes. Observa-se três manchas avermelhada concentrada nos estudos de Z. Ding [21], Z. Li [35] [22] e M. A. Islam [16]. A primeira mancha é centrada no estudo de Z. Ding [21] que trata de eficiência energética em Data Centers.



Fígura 5. Mapa de calor de acoplamento bibliográfico de todos os 96 artigos.

A segunda mancha tem foco em 2 estudos: Z. Li [15] [22] que aborda a eficiência energética em Data Center, como também, no tratamento da segurança da informação de dados sensíveis e o seu armazenamento. E a terceira mancha concentra-se em dois estudos: M. A. Islam [16] que aborda a disponibilidade de Data Center no que tange a vulneráveis a ataques de energia elétrica, mesmo com a aplicação de redundâncias, nesses ambientes; e M. Guo [23] que trata do gerenciamento da capacidade de energia em Data Centers.

ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.

Sendo assim, analisando os artigos que apresentam relevância, será possível obter uma lista de fatores de risco que influenciam na infraestrutura de um Data Center.

V. FATORES DE RISCOS INFLUENCIADORES

O CSF versão 1.1 do NIST possui uma estrutura básica com um conjunto comum de atividades para gerenciar o risco de segurança cibernética [8].

Nesta pesquisa, as atividades (subcategorias do CSF) foram colocadas no contexto de frases declarativas negativa e realizado uma correlação com os artigos relevantes os quais possuem relacionamento direto com ausência de atividades técnicas e/ou de gerenciamento.

Com a revisão bibliométrica foi possível observar 11 artigos relevantes, com maior influência no campo acadêmico e identificados os principais autores que contribuem com o tema, as principais abordagens e os resultados encontrados, utilizando o TEMAC, sendo eles: W. Hou [12], C. Buragohain [13], K. S. Sahoo [14], Z. Li [15], M. A. Islam [16], A.M. Abdelrahman [17], M. V. M. Lima [18], M. Levy [19], Z. Ding [21], Z. Li [22], C. Li [23]. Após análise dos mesmos foi possível identificar 10 fatores de riscos influenciadores em uma infraestrutura de Data Center, de acordo com o CSF, que são observados na Tabela IV.

TABELA IV. FATORES DE RISCOS INFLUENCIADORES

NIST CSF – Subcategoria (Contexto de Negação)	**Referências**										
	[12]	**[13]**	**[14]**	**[15]**	**[16]**	**[17]**	**[18]**	**[19]**	**[21]**	**[22]**	**[23]**
DE.AE-1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas **não** é estabelecida e gerenciada			X			X					
DE.CM-1: A rede **não** é monitorada para detectar potenciais incidentes de segurança cibernética		X	X		X	X			X		X
DE.CM-2: O ambiente físico **não** é monitorado para detectar possíveis eventos de segurança cibernética					X			X			X
ID.GV-2: As funções e responsabilidades de segurança cibernética **não** são coordenadas e alinhadas com funções internas e parceiros externos				X							
ID.SC-1: Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos **não** são identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.				X	X				X		X
PR.AC-5: A integridade da rede **não** é protegida (por exemplo, segregação de rede, segmentação de rede)	X									X	
PR.DS-5: As proteções contra vazamentos de dados **não** são implementadas	X									X	
PR.IP-1: Uma configuração básica de sistemas de tecnologia de informação/controle industrial **não** é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)							X				
PR.PT-4: Redes de comunicação e controle **não** são protegidas	X	X	X		X	X	X				
PR.PT-5: Alguns mecanismos (por exemplo, *fail-safe, load balancing, hot swap*) **não** são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas				X	X				X	X	

Considerando os fatores de riscos identificados após a leitura e a análise dos 11 artigos, para um melhor entendimento, tais fatores de riscos foram classificados de acordo com as subcategorias do CSF que possui um total de 108, distribuídas em 23 categorias de 5 funções [8].

Na Tabela V apresentam-se a quantidade de artigos, de acordo com o seu respectivo fator de risco, constante na Tabela IV, versus a função e categoria do CSF [8] que se endereçam. Observa-se que de um total de 5 funções, apenas 3 são endereçadas (60%), de 23 categorias, apenas 8 são endereçadas (34,7%) e de 108 subcategorias, apenas 10 foram endereçadas (9,2%). As funções de Responder e Recuperar que ao todo possuem 8 categorias e 22 subcategorias não obtiveram nenhum artigo com fator de risco identificado que se aplicasse.

TABELA V. FATORES DE RISCOS INFLUENCIADORES VERSUS O FUNÇÕES E CATAGORIAS DO CSF

Id. subcategoria do NIST CSF	**Funções e Categorias do NIST CSF [8] (# de artigos)**		
	Identificar	**Proteger**	**Detectar / Diagnostic ar**
	Governança	**Ger. de Riscos da Cadeia de Suprimento**	**Ger. de identidade e controle de acesso**	**Segurança de Dados**	**Processos e Procedimentos de Proteção da Informação**	**Tecnologia Protetora**	**Anomalias e Incidentes**	**Monitoramento Contínuo de Segurança**
DE.AE-1							2	
DE.CM-1								6
DE.CM-2								3
ID.GV-2	1							
ID.SC-1		4						
PR.AC-5			2					
PR.DS-5				2				
PR.IP-1					1			
PR.PT-4						6		
PR.PT-5						4		

VI. CONCLUSÕES

Neste estudo foram analisados os artigos com maior influência no âmbito acadêmico e identificado os principais autores que contribuem com o tema, as principais abordagens e

ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.

os resultados encontrados, utilizando a Teoria do Enfoque Meta-analítico Consolidado (TEMAC). É necessário entender os fatores de risco que influenciam em uma infraestrutura de Data Center, para incentivar e aperfeiçoar estudos voltados para o tema, uma vez que essas infraestruturas são ambientes de missão críticas os quais sustentam serviços de tecnologias que estão cada dia mais sendo requisitado por todo o tipo de usuário e serviços.

Com os resultados obtidos pelos índices bibliométricos de co-autoria, co-citação e acoplamento bibliográfico, foi possível identificar 11 artigos relevantes que auxiliaram a levantar 10 fatores de riscos influenciadores em uma infraestrutura de Data Center nos últimos 5 anos.

Não obstante, é fato que a crescente digitalização dos serviços, sejam eles públicos ou privados, impõem grandes desafios no que tange a segurança cibernética, pois além de garantir a disponibilidade desses serviços é necessário também garantir a confidencialidade e integridade dos dados pessoais e de negócios que trafegam e são armazenados nos Data Centers que hoje mais do que nunca, são responsáveis por prover infraestrutura para o desenvolvimento e guarda de todo conhecimento cientifico produzido. A partir das análises dos dados extraídos das duas bases de dados, percebeu-se um interesse pelo tema, porém não tão abrangente quanto aos riscos possíveis que envolve um Data Center como esperado se comparado com *Cybersecurity Framework* [8].

Como trabalhos futuros, a adição da expressão *cloud* à *string* de busca nas bases da Web of Science e Scopus, poderá apresentar uma variedade e quantidade de fatores de risco maior se comparado ao atual, uma vez que nos últimos anos o serviço de computação em nuvem vem ganhando espaço devido aos seus benefícios em relação as infraestruturas de TI tradicionais, porém, ambas dependentes de infraestruturas de Data Centers.

AGRADECIMENTOS

Este trabalho de pesquisa conta com o suporte do Ministério da Cidadania representado pela Secretaria Nacional de Assistência Social (TED SNAS/MC 01/2019) e do Ministério da Justiça e Segurança Pública representado pela Diretoria de Tecnologia da Informação e Comunicação (TED DTIC/SE/MJSP 01/2019). Agradecem também às agências de pesquisa e inovação brasileiras CAPES, CNPq e FAPDF.

VII. REFERÊNCIAS BIBLIOGRÁFICA

[1] Brasil, "DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 - Aprova a Estratégia Nacional de Segurança Cibernética" Gov.br. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 20 jan. 2021.

[2] H. E. Miller and K. J. Engemann, "Business continuity management in data center environments," Int. j. inf. technol. syst. approach, vol. 12, no. 1, pp. 52–72, 2019, doi: 10.4018/ijitsa.2019010104.

[3] A. M. Mariano and M. S. Rocha, "Revisão da Literatura: Apresentação de uma Abordagem Integradora." XXVI Congreso Internacional de la Academia Europea de Dirección y Economía de la Empresa (AEDEM), v. 26, n. September, p. 427–443, 2017.

[4] Joint Task Force Transformation Initiative, "Risk management framework for information systems and organizations:: A system life cycle approach for security and privacy," National Institute of Standards and Technology, Gaithersburg, MD, 2018.

[5] E. O. Diaz and M. Muñoz, "Strategy for performing critical projects in a data center using DevSecOps approach and Risk Management," Int. j. inf. technol. syst. approach, vol. 13, no. 1, pp. 61–73, 2020, , doi: 10.4018/ijitsa.2020010104.

[6] Gartner, Inc., "Gartner says worldwide data center infrastructure spending to grow 6% in 2021," Gartner.com. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2020-10-07-gartner-says-worldwide-data-center-infrastructure-spending-to-grow-6-percent-in-2021. Acesso em: 19 fev. 2021.

[7] T. Aquim, "Data Centers sob ataque: a busca pela segurança," Datacenterdynamics.com, 17-Nov-2017. Disponível em: https://www.datacenterdynamics.com/br/opini%C3%B5es/data-centers-sob-ataque-a-busca-pela-seguran%C3%A7a/. Acesso em: 19 fev. 2021.

[8] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity, version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, 2018, doi: 10.6028/nist.cswp.04162018.

[9] G. Abramo and C. A. D'Angelo, "Evaluating research: from informed peer review to bibliometrics," Scientometrics, vol. 87, no. 3, pp. 499–514, 2011, doi: 10.1007/s11192-011-0352-7.

[10] Centre for Science and Technology Studies, Leiden University, "VOSviewer: Visualizing Scientific Landscapes," ver. 1.6.16. Disponível em: https://www.vosviewer.com/.

[11] D. Steinbock, TagCrowd.com". Disponível em: https://tagcrowd.com/.

[12] W. Hou, Z. Ning, L. Guo, Z. Chen, and M. S. Obaidat, "Novel framework of risk-aware virtual network embedding in optical data center networks," IEEE Syst. J., vol. 12, no. 3, pp. 2473–2482, 2018, doi: 10.1109/jsyst.2017.2673828.

[13] C. Buragohain and N. Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers," in 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016, doi: 10.1109/spin.2016.7566750.

[14] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," Future Gener. Comput. Syst., vol. 89, pp. 685–697, 2018, doi: 10.1016/j.future.2018.07.017.

[15] Z. Li et al., "Energy cost minimization with job security guarantee in Internet data center," Future Gener. Comput. Syst., vol. 73, pp. 63–78, 2017, doi: 10.1016/j.future.2016.12.017.

[16] M. A. Islam, S. Ren, and A. Wierman, "Exploiting a thermal side channel for power attacks in multi-tenant data centers," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, doi: 10.1145/3133956.3133994.

[17] A. M. Abdelrahman et al.,"Software‐defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions,"Int. J. Commun. Syst., 2020, doi: 10.1109/jsyst.2017.2673828.

[18] M. V. M. Lima, R. M. F. Lima, and F. A. A. Lins, "A multi-perspective methodology for evaluating the security maturity of data centers," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, doi: 10.1109/smc.2017.8122775.

[19] M. Levy and D. Raviv, "A framework for data center site risk metric," in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, doi: 10.1109/uemcon.2017.8248970.

[20] I. Zupic and T. Cater, "Bibliometric methods in management and organization: A review," Acad. Manag. Proc., vol. 2013, no. 1, p. 13426, 2013, doi: 10.5465/ambpp.2013.13426abstract..

[21] Z. Ding, L. Xie, Y. Lu, P. Wang, and S. Xia, "Emission-aware stochastic resource planning scheme for data center microgrid considering batch workload scheduling and risk management," IEEE Trans. Ind. Appl., vol. 54, no. 6, pp. 5599–5608, 2018, doi: 10.1109/icps.2018.8369969.

[22] Z. Li and J. Wang, "Security storage of sensitive information in cloud computing data center," International Journal of Performability Engineering, 2019, doi: 10.23940/ijpe.19.03.p32.10231032.

[23] C. Li, Z. Wang, X. Hou, H. Chen, X. Liang, and M. Guo, "Power attack defense: Securing battery-backed data centers," in 2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA), 2016, doi: 10.1109/isca.2016.50.

ISBN: 978-989-54659-1-0

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on January 25,2023 at 15:44:45 UTC from IEEE Xplore. Restrictions apply.