ARTIGO DE REVISÃO

OLIVEIRA, Igor Antônio Magalhães de ^[1], DRUMOND, Geisa Meirelles ^[2], MÉXAS, Mirian Picinini ^[3]

OLIVEIRA, Igor Antônio Magalhães de. DRUMOND, Geisa Meirelles. MÉXAS, Mirian Picinini. Governança De Segurança Da Informação Na Indústria De Energia Elétrica: Revisão Bibliográfica. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 15, pp. 64-88. Abril de 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/tecnologia/governanca-de-seguranca>, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/governanca-de-seguranca

Contents

- RESUMO
- 1. INTRODUÇÃO
- 2. CONCEITOS SOBRE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO
- 3. MÉTODO DA PESQUISA
- 4. RESULTADOS
 - 4.1 ANÁLISE POR ANO DE PUBLICAÇÃO
 - 4.2 ANÁLISE POR PUBLICAÇÃO EM PERIÓDICO
 - 4.3 ANÁLISE DESCRITIVA DOS ARTIGOS SELECIONADOS
- 5. CONCLUSÃO
- REFERÊNCIAS

RESUMO

Nos últimos anos, a governança da segurança da informação (GSI) vem ganhando importância na estratégia empresarial das organizações. Entretanto, a indústria de energia, por ter alta relevância social e econômica, precisa de investimentos, a fim de mitigar riscos oriundos de dentro e fora da organização. A partir dessa situação problema surge a seguinte questão: Quais os achados na literatura sobre a Governança de SI na área de energia elétrica? Sendo assim, este estudo tem como objetivo identificar o que a literatura menciona

sobre governança de segurança da informação relacionada à indústria de energia elétrica. Através da metodologia da pesquisa foi realizada uma pesquisa na base de dados SCOPUS, via portal de periódicos Capes. Como resultado, foram selecionados 43 artigos, sendo que poucos eram relacionados à energia elétrica e também se observa um crescimento de artigos publicados nos últimos anos. Espera-se que esta pesquisa possa contribuir para a elevação de maturidade da segurança da informação na indústria de energia, pois cada vez mais as organizações serão impactadas pela falta de uma Governança de SI bem estruturada.

Palavras-chave: Segurança da informação, Energia elétrica, Governança de SI.

1. INTRODUÇÃO

Cada vez mais observa-se que os ataques cibernéticos estão sendo mais sofisticados e complexos, levando empresas a um colapso financeiro e degradação da sua imagem. De acordo com Alencar et al. (2018), áreas como Segurança da Informação (SI) passam a ter, cada vez mais, um papel crucial na estratégia corporativa da organização.

A SI com o passar dos anos deixou de ter uma visão apenas técnica, necessitando de uma abordagem mais voltada para o negócio e integrada a gestão estratégica, a fim de atingir toda organização com normas e políticas bem estruturadas (CARCARY et al., 2016).

Além disso, os riscos enfrentados pelas organizações pela falta de uma Governança de Segurança da Informação são notórios quando ataques ao sistema de automação, vazamento de informações e perdas financeiras são bem-sucedidos (KURE; ISLAM; RAZZAQUE, 2018). Essa governança é um conjunto de normas, políticas, ferramentas de conscientização e treinamentos sobre segurança da informação (NAZARETH; CHOI, 2015)

Vale ressaltar que a indústria de energia elétrica, por tratar de algo essencial na vida do ser humano, conter dados sigilosos dos clientes e oferecer confiabilidade no fornecimento de energia, deve manter um sistema bem estruturado de governança de SI, visando mitigar riscos oriundos da própria organização e fora dela (MARTINS et al., 2019).

A vulnerabilidade em sistemas de automação vem causando impactos sociais e econômicos

em âmbito global. Em 23/12/2015, uma empresa Ucraniana de distribuição de energia elétrica sofreu um ataque ao sistema SCADA (*Supervisory Control and Data Acquisition*), deixando mais de 80 mil clientes sem luz por 3 horas. Pode-se citar, também, como exemplo, um *malware* que, em 25/01/2003, desativou o sistema de segurança de uma empresa nuclear nos Estados Unidos, Ohio, impossibilitando o controle de indicadores dos sensores de medição de temperatura (RODOFILE; RADKE; FOO, 2019).

Dentro deste contexto, esse estudo tem como objetivo identificar o que a literatura menciona sobre governança de segurança da informação relacionada à indústria de energia elétrica, fornecendo informações diferentes sobre o tema. Como contribuição, espera-se que estudos futuros possam esclarecer ainda mais a importância do tema no âmbito corporativo, visando a adequação deste trabalho às melhores práticas de Governança de Segurança da Informação, pois cada vez mais as organizações serão impactadas pela falta de maturidade que a área necessita.

Além desta introdução, na seção 2, apresenta-se o conceito sobre Governança de Segurança da Informação; a seção 3 descreve o método de pesquisa utilizado; na seção 4, são apresentados os resultados da revisão bibliográfica; e finalmente, na seção 5, encontra-se a conclusão.

2. CONCEITOS SOBRE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Em ambientes organizacionais, onde as interconexões de dados aumentam a cada dia que passa, a informação torna-se um ativo como qualquer outro da empresa, precisando de proteção adequada, por conta da alta exposição de ameaças e vulnerabilidades (VALENCIA-DUQUE; OROZCO-ALZATE, 2017). Desde modo, SI é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o seu risco, maximizar o retorno sobre os investimentos e as oportunidades de negócio (KIM; LEE; LIM, 2017).

Governança de SI consiste em um ferramental para a especificação de direitos, decisão e responsabilidade, visando encorajar comportamentos desejáveis no uso da segurança de informação. Atualmente, negócios estão cada dia mais dependentes de suas infraestruturas de segurança de informação, isso faz com que seja necessária a implementação da

governança de segurança da informação nas empresas para garantir a continuidade do negócio (YAOKUMAH, 2014).

O principal objetivo da governança de SI é alinhar a segurança de informação aos requisitos do negócio, considerando solução de apoio ao negócio, assim como a garantia de continuidade dos serviços e a minimização da exposição do negócio aos riscos. A governança pode ser motivada por vários fatores, porém um dos mais importantes é a transparência na administração da segurança de informação e a disponibilidade da infraestrutura de segurança de informação. Prover segurança e disponibilidade da infraestrutura de segurança de informação, atualmente, é um desafio para as organizações, pois essas práticas garantem a disponibilidade do negócio (GEORG, 2017).

Além disso, a Governança de SI tem a responsabilidade de controlar, dirigir e supervisionar processos que são necessários para proteger as informações de uma organização, a fim de garantir a disponibilidade, confidencialidade, integridade e manter o alinhamento com a gestão estratégica do negócio (REBOLLO et al., 2015).

3. MÉTODO DA PESQUISA

Segundo Marconi e Lakatos (2010), uma pesquisa exploratória visa prover ao pesquisador maior conhecimento sobre o tema ou problema de pesquisa em perspectiva, sendo o foco deste estudo uma análise exploratória e pesquisa bibliográfica sobre a Governança de Segurança da Informação na indústria de energia elétrica.

Nesta seção, mostra-se toda a trajetória percorrida para a elaboração da revisão da bibliográfica. O trabalho buscou, para a fundamentação da revisão da literatura, focar na base referencial SCOPUS. Há alguns anos, visando atender à comunidade acadêmica, a CAPES oferece a base SCOPUS para pesquisar em áreas, como: Ciências Humanas, Ciências Sociais, Ciências Exatas e Ciências Biológicas.

Para ser mais específico, foram adotados termos de busca de maneira isolada, a fim de ter maior assertividade na pesquisa. Foram utilizadas, então, as seguintes palavras-chave: *"information security management"*, *"information security governance"*, *"management strategy"* AND *"information security"*, *"information security"* AND *"energy"* e *"SCADA"* AND

“security”. A seguir, encontram-se tabelas demonstrativas dos artigos encontrados, com seus respectivos filtros, que serviram como formulação para o referencial teórico.

Os resultados encontrados na pesquisa relacionados na Tabela 1, foram satisfatórios, pois desde a década de 80, profissionais da área já possuíam preocupações em relação à segurança em sistemas de computadores. As palavras-chave “information security management” OR “information security governance” foram usadas para elaborar conteúdo referente à governança de segurança da informação, totalizando 1424 artigos. Contudo, a partir dos resultados, filtros foram elaborados com o intuito de refinar a pesquisa, restando 345 artigos, como demonstrado na Tabela 1. Após o resultado obtido com este filtro, foi feita uma análise do título e do resumo, onde sobraram apenas 137 artigos. Os demais artigos (208) foram descartados por não estarem aderentes ao tema central da pesquisa. Após essa análise, para contribuir com a pesquisa, 24 artigos foram selecionados entre os anos de 2009 e 2019.

Tabela 1 – Palavras-chave, filtros e seus respectivos resultados encontrados na base SCOPUS

Palavras-Chave	SCOPUS	
	Registros Encontrados	
“information security management” OR “information security governance”	1424	
<i>Document Type = Article or Review</i>		
<i>Article title, Abstract, Keywords</i>		
<i>Source Type = Limit to Journal</i>	345	
<i>Year = Limit to: 2009 a 2019</i>		
Total de artigos utilizados na pesquisa	24	

Fonte: Elaboração própria (2019)

Na Tabela 2 foram usadas as palavras-chave “management strategy”, totalizando 506 artigos. Contudo, a partir dos resultados, filtros foram elaborados com o intuito de refinar a pesquisa, restando 178 artigos. Após o resultado obtido desse filtro, foi feita uma análise do

título e do resumo, onde sobraram apenas 117 artigos. Os 61 artigos restantes foram descartados por não estarem aderentes ao tema central da pesquisa. Com exceção de Porter, Mintzberg, Taylor e Ansoff, que são artigos citados frequentemente em Gestão estratégica, apenas 7 artigos oriundos da pesquisa foram selecionados nesta etapa.

Tabela 2 – Palavras-chave, filtros e seus respectivos resultados encontrados na base SCOPUS

Palavras-Chave	SCOPUS
	Registros Encontrados
"management strategic"	506
<i>Document Type = Article or Review</i>	
<i>Article title, Abstract, Keywords</i>	178
<i>Source Type = Limit to Journal</i>	
<i>Year = Limit to: 2009 a 2019</i>	
Total de artigos utilizados na pesquisa	7

Fonte: Elaboração própria (2019)

Os resultados encontrados na pesquisa, relacionada às Tabelas 3 e 4, foram satisfatórios, pois refletem a importância da segurança da informação na indústria de energia. As palavras-chave "information security" AND "energy" e "scada" AND "security" foram usadas para elaborar conteúdo referente à Governança de TI em Usinas de Geração de Energia Elétrica e SI na Indústria de Energia Elétrica Brasileira, totalizando 2714 (507 + 2207) artigos. Contudo, a partir dos resultados, filtros foram elaborados com o intuito de refinar a pesquisa, restando 514 (147 + 367) artigos, como mostrado nas Tabelas 3 e 4. Após o resultado obtido desse filtro, foi feita uma análise do título e do resumo, onde sobraram apenas 177 (78 + 99) artigos. Os 337 artigos restantes foram descartados por não estarem aderentes ao tema central da pesquisa. Após essa análise, para contribuir com a pesquisa, 8 artigos foram selecionados.

Tabela 3 – Palavras-chave, filtros e seus respectivos resultados encontrados na base SCOPUS

Palavras-Chave	SCOPUS
	Registros Encontrados

"information security" AND "energy"	507
<i>Document Type = Article or Review</i>	
<i>Article title, Abstract, Keywords</i>	147
<i>Source Type = Limit to Journal</i>	
<i>Year = Limit to: 2009 a 2019</i>	
Total de artigos? utilizados na pesquisa	3

Fonte: Elaboração própria (2019)

Tabela 4 - Palavras-chave, filtros e seus respectivos resultados encontrados na base SCOPUS

Palavras-Chave	SCOPUS
	Registros Encontrados
"scada" AND "security"	2207
<i>Document Type = Article or Review</i>	
<i>Article title, Abstract, Keywords</i>	367
<i>Source Type = Limit to Journal</i>	
<i>Year = Limit to: 2009 a 2019</i>	
Total de artigos utilizados na pesquisa	5

Fonte: Elaboração própria (2019)

Os resultados encontrados na pesquisa, relacionada à Tabela 5, foram satisfatórios, pois refletem a escassez de documentos referentes à governança de TI. Ao acessar a palavra-chave "information technology governance" encontraram-se 245 artigos. Contudo, a partir dos resultados, filtros foram elaborados com o intuito de refinar a pesquisa, restando 74 artigos, como demonstrado na Tabela 5. Após o resultado obtido desse filtro, foi feita uma análise do título e do resumo, onde sobraram apenas 37 artigos. Dos 37 artigos selecionados, apenas 4 foram utilizados. Os 37 artigos restantes foram descartados por não estarem aderentes ao tema central da pesquisa

Tabela 5 - Palavras-chave, filtros e seus respectivos resultados encontrados na base SCOPUS

Palavras-Chave	SCOPUS
	Registros Encontrados

"information technology governance"	245
<i>Document Type = Article or Review</i>	
<i>Article title, Abstract, Keywords</i>	74
<i>Source Type = Limit to Journal</i>	
<i>Year = Limit to: 2009 a 2019</i>	
Total de artigos utilizados na pesquisa	4

Fonte: Elaboração própria (2019)

Para uma melhor visualização dos artigos usados e suas respectivas palavras-chave, a Tabela 6 demonstra uma compilação dos 43 artigos selecionados.

Tabela 6 - Compilação dos artigos selecionados na base SCOPUS por palavras-chave

Palavras-Chave	SCOPUS	
	Registros Encontrados	
"information security management" OR "information security governance"	24	
"management strategic"	7	
"information security" AND "energy"	3	
"scada" AND "security"	5	
"information technology governance"	4	
Total de artigos utilizados na pesquisa	43	

Fonte: Elaboração própria (2019)

4. RESULTADOS

O objetivo da seção é demonstrar os resultados obtidos na pesquisa, agrupando os 43 artigos pesquisados de acordo com a seguinte premissa: (1) análise por ano de publicação; (2) análise por publicação em periódico; e (3) análise descritiva dos artigos selecionados.

4.1 ANÁLISE POR ANO DE PUBLICAÇÃO

O Gráfico 1 traz um apanhado dos registros encontrados na pesquisa por ano de publicação. Nota-se a importância do tema pelo aumento significativo nas publicações dos periódicos ao longo dos anos, tendo uma maior ocorrência em 2018. Vale lembrar que a pesquisa foi feita até maio de 2019, o que justifica uma menor quantidade em 2019.

Gráfico 1 - Ilustração gráfica com a quantidade dos periódicos e seus respectivos anos

Fonte: Elaboração própria (2019)

4.2 ANÁLISE POR PUBLICAÇÃO EM PERIÓDICO

A fim de aprimorar a pesquisa, foi realizada uma análise dos periódicos mais publicados.

Como mostrado na Tabela 7, dentre os 43 artigos selecionados entre os anos de 2009 e 2019, 6 periódicos foram citados mais de uma vez, mostrando a relevância do tema, sendo o *Information and Computer Security* o mais citado. Os demais 30 periódicos estão relacionados a apenas um artigo, totalizando 36 periódicos diferentes referentes aos 43 artigos.

Tabela 7 – Lista de periódicos mais publicados entre 2009 e 2019

Nome do Periódico	Quantidade	Ano de publicação
<i>Information and Computer Security</i>	3	2015, 2018, 2019
<i>KSII Transactions on Internet and Information Systems</i>	2	2017, 2018
<i>Kerntechnik</i>	2	2015, 2017
<i>British Journal of Management</i>	2	2016
<i>Applied Sciences (Switzerland)</i>	2	2018
<i>Journal of Computer Science</i>	2	2018

Fonte: Elaboração própria (2019)

4.3 ANÁLISE DESCRITIVA DOS ARTIGOS SELECIONADOS

Como apresentado a seguir no Quadro 1, foram analisados os 43 artigos selecionados no referencial teórico, a fim de levantar a importância do tema durante os anos e seus respectivos periódicos. Para enriquecer a análise, foi feito um resumo de todos os artigos mencionados na pesquisa.

Quadro 1 – Lista de periódico, ano, autor e título

Ano de publicação	Autor	Título	Periódico	
2009	JOHNSTON, A. C.; HALE, R	<i>Improved security through information security governance</i>	<i>Communications of the ACM</i>	

Governança De Segurança Da Informação Na Indústria De Energia Elétrica: Revisão Bibliográfica

Ano de publicação	Autor	Título	Periódico	
2009	GONÇALVES, H. S.	<i>Proposal of a strategy model planning aligned to the balanced scorecard and the quality environments</i>	<i>TQM Journal</i>	
2009	ELMUTI, D.; JIA, H.; GRAY, D.	<i>Customer relationship management strategic application and organizational effectiveness: An empirical investigation</i>	<i>Journal of Strategic Marketing</i>	
2009	HÖNE, K.; ELOFF, J. H. P.	<i>Information security governance: Business requirements and research directions</i>	<i>Corporate Ownership and Control</i>	
2010	SÁNCHEZ, L. E. et al.	<i>Managing security and its maturity in small and medium-sized enterprises.</i>	<i>Journal of Universal Computer Science</i>	
2013	KIM, J.; TONG, L	<i>On topology attack of a smart grid: Undetectable attacks and countermeasures</i>	<i>IEEE Journal on Selected Areas in Communications</i>	
2014	YAOKUMAH, W.	<i>Information security governance implementation within Ghanaian industry sectors an empirical study</i>	<i>Information Management and Computer Security</i>	

Governança De Segurança Da Informação Na Indústria De Energia Elétrica: Revisão Bibliográfica

Ano de publicação	Autor	Título	Periódico	
2014	ISMAM, J. N.; ISMAIL, Z.	<i>Sustainable construction waste management strategic implementation model.</i>	<i>WSEAS Transactions on Environment and Development</i>	
2014	TUOMIKANGAS, N.; KAIPIA, R.	<i>A coordination framework for sales and operations planning (S&OP): Synthesis from the literature</i>	<i>International Journal of Production Economics</i>	
2014	CHOLEZ, H.; GIRARD, F	<i>Maturity assessment and process improvement for information security management in small and medium enterprises</i>	<i>Journal of software: Evolution and Process</i>	
2015	MISHRA, S.	<i>Organizational objectives for information security governance: A value focused assessment.</i>	<i>Information and Computer Security</i>	
2015	THIYAGARAJAN, P. et al.	<i>Shamir secret sharing scheme with dynamic access structure (SSSDAS): Case study on nuclear power plant</i>	<i>Kernttechnik</i>	
2015	NAZARETH, D. L.; CHOI, J.	<i>A system dynamics model for information security management.</i>	<i>Information and Management</i>	

Ano de publicação	Autor	Título	Periódico	
2015	REBOLLO, O. et al.	<i>Empirical evaluation of a cloud computing information security governance framework</i>	<i>Information and Software Technology</i>	
2016	HAUFE, K. et al.	<i>A process framework for information security management.</i>	<i>International Journal of Information Systems and Project Management</i>	
2016	GERARD MACHADO, T. et al.	<i>Methodology for Identifying the Cybersecurity Maturity Level of Smart Grids.</i>	<i>IEEE Latin America Transactions</i>	
2016	BOWMAN, G	<i>The Practice of Scenario Planning: An Analysis of Inter- and Intra-organizational Strategizing</i>	<i>British Journal of Management</i>	
2016	SHAWYUN, T.	<i>Strategic planning as an essential for quality assurance</i>	<i>Journal of Institutional Research South East Asia</i>	
2016	PARDO, C.; PINO, F. J.; GARCIA, F	<i>Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards</i>	<i>International Journal of Software Engineering and its Applications</i>	
2016	CARCARY, M. et al.	<i>A Framework for Information Security Governance and Management</i>	<i>IT Professional</i>	

Ano de publicação	Autor	Título	Periódico	
2016	DHILLON G., SYED R., PEDRON C	<i>Interpreting information security culture: An organizational transformation case study</i>	<i>Computers and Security</i>	
2016	YANG, T.-H.; KU, C.-Y.; LIU, M.-N	<i>An integrated system for information security management with the unified framework</i>	<i>Journal of Risk Research</i>	
2017	GEORG, L	<i>Information security governance: pending legal responsibilities of non-executive boards</i>	<i>Journal of Management and Governance</i>	
2017	MILOSLAVSKAYA N.G., TOLSTOY A.I.	<i>Visualization of information security management processes</i>	<i>Scientific Visualization</i>	
2017	KRISHNAN, R. B. et al.	<i>Font Attributes based Text Steganographic algorithm (FATS) for communicating images: A nuclear power plant perspective</i>	<i>Kerntechinik</i>	
2017	KIM, H.; LEE, K.; LIM, J	<i>A study on the impact analysis of security flaws between security controls: An empirical analysis of K-ISMS using case-control study</i>	<i>KSII Transactions on Internet and Information Systems</i>	

Ano de publicação	Autor	Título	Periódico	
2017	VALENCIA-DUQUE, F. J.; OROZCO-ALZATE, M.	<i>A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards</i>	<i>RISTI – Revista Iberica de Sistemas e Tecnologias de Informacao</i>	
2018	KALOGERAKEI, E.-M. et al.	<i>A novel risk assessment methodology for SCADA maritime logistics environments.</i>	<i>Applied Sciences (Switzerland)</i>	
2018	ALENCAR, G. D. et al	<i>An Adaptable Maturity Strategy for Information Security.</i>	<i>Journal of Electrical Engineering and Technology</i>	
2018	EL GHORFI, R. et al.	<i>Valuating IT governance strategies with real options in a decision making framework.</i>	<i>International Journal of Information Systems in the Service Sector</i>	
2018	AJAYI, B. A.; HUSSIN, H	<i>Conceptualizing Information Technology Governance Model for Higher Education: An Absorptive Capacity Approach</i>	<i>Bulletin of Electrical Engineering and Informatics</i>	
2018	JAMI POUR, M.; KOUCHAK ZADEH, Z.; AHMAD ZADEH, N	<i>Designing an integrated methodology for knowledge management strategic planning: The roadmap toward strategic alignment.</i>	<i>VINE Journal of Information and Knowledge Management Systems</i>	

Ano de publicação	Autor	Título	Periódico	
2018	LAURETT, R.; FERREIRA, J. J.	<i>Strategy in Nonprofit Organisations: A Systematic Literature Review and Agenda for Future Research</i>	<i>Voluntas</i>	
2018	KURE, H. I.; ISLAM, S.; RAZZAQUE, M. A.	<i>An integrated cyber security risk management approach for a cyber-physical system</i>	<i>Applied Sciences (Switzerland)</i>	
2018	NICHO, M.	<i>A process model for implementing information systems security governance.</i>	<i>Information and Computer Security</i>	
2018	HAQAF, H.; KOYUNCU, M	<i>Understanding key skills for information security managers</i>	<i>International Journal of Information Management</i>	
2018	CHINYEMBA, M. K.; PHIRI, J.	<i>An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector</i>	<i>Journal of Computer Science</i>	
2018	YOU, Y. et al.	<i>Advanced approach to information security management system utilizing maturity models in critical infrastructure</i>	<i>KSII Transactions on Internet and Information Systems</i>	

Ano de publicação	Autor	Título	Periódico	
2018	WOO, P. S.; KIM, B. H	<i>Establishment of cyber security countermeasures amenable to the structure of power monitoring & control systems</i>	<i>Transactions of the Korean Institute of Electrical Engineers</i>	
2019	RODOFILE, N. R.; RADKE, K.; FOO, E	<i>Extending the cyber-attack landscape for SCADA-based critical infrastructure</i>	<i>International Journal of Critical Infrastructure Protection</i>	
2019	EVANS, M. et al. HEART-IS	<i>A novel technique for evaluating human error-related information security incidents</i>	<i>Computers and Security</i>	
2019	QASSIM, Q. S. et al.	<i>A review of security assessment methodologies in industrial control systems</i>	<i>Information and Computer Security</i>	
2019	MARTINS, R. J. et al	<i>Specialized CSIRT for Incident Response Management in Smart Grids</i>	<i>Journal of Network and Systems Management</i>	

Fonte: Elaboração própria (2019)

A seguir, segue a análise feita dos 43 artigos, mencionando o objetivo principal de cada trabalho.

De acordo com Johnston e Hale (2009), a governança da segurança da informação tem papel fundamental no planejamento estratégico da empresa, buscando um investimento eficaz, a fim de mitigar os riscos na organização. Desse modo, o executivo da companhia é de suma importância para o sucesso de uma estrutura de gestão da segurança da informação.

O artigo, segundo Gonçalves (2009), tem o objetivo de propor um modelo de planejamento estratégico com alinhamento ao sistema de gestão da qualidade dentro das organizações. Esse modelo foi desenvolvido visando a inserção da qualidade contida no planejamento estratégico, com base nas perspectivas do *Balanced scorecard* (BSC). Desse modo, a qualidade alinhada ao planejamento estratégico tem impacto direto na segurança da informação. Contudo, o planejamento estratégico, governança de TI e governança de SI precisam estar totalmente alinhados, a fim de elevar o nível de maturidade tecnológica e de segurança na organização.

O artigo, de acordo com Elmuti, Jla e Gray (2009), tem o objetivo de identificar *gaps* que possam afetar o gerenciamento de relacionamento com o cliente dentro de uma abordagem estratégica organizacional.

Com mudanças constantes no cenário tecnológico, de acordo com Hone e Eloff (2009), a governança da segurança da informação vem exigindo uma atenção especial da alta administração da organização. Com isso, as empresas precisam adotar medidas de proteção cada vez mais sofisticadas e alinhadas a estratégia da organização.

De acordo com Sanchez et al. (2010), a segurança da informação tem passado por transformações organizacionais devido ao alto consumo e dependência da sociedade perante essas informações. Nesse contexto de proteger cada vez mais a informação do negócio, o sistema de gestão da segurança da informação apoia processos e tomada de decisão para mitigação de riscos.

De acordo com Kim e Tong (2013), mecanismos de defesa voltados para rede *smart grid* são fundamentais para evitar comportamentos indesejáveis ou anomalias oriundas da própria organização. Por se tratar de algo essencial à vida do ser humano, a indústria de energia elétrica padece de uma governança de segurança da informação efetiva dentro da organização. Com isso, contramedidas são necessárias para evitar paradas em seu sistema elétrico.

De acordo com Yaokumah (2014), níveis de implementação de Governança de segurança da informação nas indústrias Ganenses, que identificam melhorias em seus processos de maturidade e adequação tecnológica, foram fundamentais na elevação de maturidade nas

organizações. Com isso, detectou-se que as organizações com mais potencial na governança de SI foram as indústrias do setor financeiro, onde a maioria já possuía uma maturidade elevada no que diz respeito à segurança da informação.

De acordo com Ismam e Ismail (2014), todas as partes interessadas em um planejamento estratégico devem participar ativamente dos processos na organização, visando sempre a sua melhoria contínua. Desse modo, foi desenvolvido um modelo para a implementação da gestão sustentável de resíduos.

Tuomikangas e Kaipia (2014) propõem um modelo de alinhamento da estratégia do negócio voltado a vendas e cadeia de suprimentos, junto com o planejamento operacional da organização, visando a perspectiva de estilo e cultura de liderança dentro das organizações. A ligação estratégica dessas áreas com a governança de Segurança da informação diminui o risco de projetos não estruturados fora da TI. Desse modo, a segurança é envolvida em todos os contextos do planejamento organizacional.

Cholez e Girard (2014) propõem um modelo voltado para pequenas e médias empresas, a fim de fazer uma primeira avaliação de maturidade em sua governança de segurança da informação, identificando riscos e processos dentro da organização.

Por falta de controles apropriados e processos cada vez mais sofisticados, Mishra (2015) propõe desenvolver diretrizes claras de governança de segurança da informação organizacional, pois em muitos casos, a organização não conhece os objetivos da segurança da informação. Com isso, alguns objetivos foram desenvolvidos, tais como: estabelecer estratégia de controle corporativo; estabelecer estrutura punitiva; estabelecer um processo de desenvolvimento de controle; garantir a funcionalidade de avaliação do controle formal e maximizar a coesão do grupo.

Devido ao impacto que a falta de segurança vem causando em usinas de energia nuclear, Thiagarajan et al. (2015) propõem um algoritmo voltado à concessão de acesso dinâmico dentro da organização, a fim de mitigar riscos dentro das plantas de automação. Com isso, acessos ao ambiente de automação precisam ser devidamente monitorados durante todo o ciclo de vida da concessão.

Nazareth e Choi (2015) propõem um modelo alternativo de governança de segurança da informação, com o propósito de fornecer aos gerentes uma melhor tomada de decisão no orçamento da área. Desse modo, fica mais factível investir em tecnologias que irão agregar valor para o negócio.

O serviço de computação em nuvem, segundo Rebollo et al. (2015), vem se tornando cada vez mais essencial dentro da organização. Contudo, problemas relacionados à segurança da informação também se tornam mais graves nesses ambientes. Este trabalho tem por objetivo a elaboração de uma governança de segurança da informação voltada para o ambiente em nuvem.

Haufe et al (2016) propõem um Sistema de gestão de segurança da informação que sirva para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação de uma organização. Com isso, o artigo tem o objetivo de elaborar uma estrutura de processos baseados em *frameworks* e normas como: ISO27000, COBIT e ITIL, visando aumentar a maturidade da segurança da informação.

A segurança da informação para redes inteligentes, segundo Gerard Machado et al. (2016), depende de uma combinação nos sistemas de TI, da disponibilidade da rede de comunicação e dos equipamentos da rede elétrica. Com isso, o artigo objetiva aumentar o nível de maturidade da segurança da informação em redes inteligentes.

Algumas ferramentas, de acordo com Bowman (2016), são usadas para estruturas estratégicas organizacionais. Entretanto, existe uma falta de entendimento sobre o real impacto dessas ferramentas dentro da organização. Com isso, um modelo foi desenvolvido para a construção de artefatos dentro da estratégia inter e intraorganizacional. Esse tipo de modelo ajuda, também, no direcionamento linear entre o planejamento estratégico e a segurança da informação, mantendo um alinhamento mais próximo dessas áreas.

Para Shawyun (2016), a Gestão da qualidade e o planejamento não podem mais trabalhar separadamente. Portanto, foi elaborado um Sistema de gestão de desenvolvimento estratégico que aborda a gestão da qualidade, da informação e do planejamento. Desse modo, a qualidade no serviço da segurança da informação depende, também, de um bom planejamento estratégico. Com isso, riscos de qualquer natureza são mitigados dentro desse

sistema.

Pardo, Pino e Garcia (2016) propõem o alinhamento entre a ISO 20000 com a ISO 27001 (norma internacional de gestão de segurança da informação), fornecendo uma análise detalhada de como harmonizar essa interação entre ambas as normas.

Carcary et al. (2016) fornecem uma estrutura de maturidade destinada à governança de segurança da informação para ajudar as organizações na identificação de áreas problemáticas. O artigo aborda aspectos técnicos, humanos e de processos, fornecendo caminhos efetivos para implementação de uma governança efetiva.

Quando existe a fusão entre duas empresas, de acordo com Dhilton; Syed, Pedron (2016), as tecnologias, política e segurança da informação e normas acabam entrando em conflito. Dessa forma, as mudanças acabam dificultando o processo de fusão e, inevitavelmente, a segurança é abalada. O objetivo do artigo transita justamente na avaliação de interrupções na cultura de segurança da informação após uma fusão.

Yang, Cu, Liu (2016) resumem a trajetória que a gestão de segurança da informação desempenha na organização, com políticas, normas e metodologias. Entretanto, essas metodologias podem ser complicadas quando tratadas separadamente. O propósito do artigo é elaborar uma metodologia que visa à unificação desses processos e normas de Mercado.

Georg (2017) expõe que, devido à ausência de uma governança de segurança corporativa nas organizações e à falta de conscientização desse processo, muitas vezes os executivos entram em conflito sobre as questões legais e os riscos a serem enfrentados pela segurança da informação.

Miloslavskaya e Tolstoy (2017) remetem à questão da necessidade de processos de segurança da informação que contribuem na tomada de decisão, aspirando a melhoria contínua da área. De acordo com os autores, alguns processos são fundamentais para um bom funcionamento da governança de segurança da informação, quais sejam: planejamento, implementação, controle e melhoria.

Krishinan et al (2017) propõem um novo algoritmo esteganográfico. Esses algoritmos têm a função de ocultar a informação secreta dentro de outro meio de cobertura, de forma

imperceptível, como um texto ou uma imagem.

Kim; Lee e Lim (2017) mencionam a importância e a dificuldade da medição dos níveis de segurança da informação. De acordo com os autores, as pesquisas focam na complexidade em atingir determinados níveis, mas não citam as pesquisas relacionadas aos diferentes tipos de falhas nos controles de segurança, em como afetam uns aos outros e quais falhas são mais críticas por causa desses efeitos.

Valência Duque e Orozco Alzate (2017) propõem uma abordagem metodológica para a implementação de um Sistema de segurança da informação baseado na família ISO 27000, intentando cumprir os requisitos mencionados na norma ISO 27001. De acordo com os autores, os controles de segurança mencionados na ISO 27002, o esquema de risco na ISO 27005 e as etapas mencionadas na ISO 27003 se correlacionam a todo tempo.

Kalogeraki et al. (2018) propõem a elaboração de uma nova metodologia de avaliação de risco, visando abordar especificidades e particularidades na segurança do ambiente SCADA na indústria de logística marítima. O estudo identifica vulnerabilidades e ameaças de ativos para estimar os riscos cibernéticos e seus efeitos em cascata.

Com o intuito de auxiliar na aplicação e priorização de ações de segurança da informação no âmbito corporativo, Alencar et al. (2018) apresentam uma estratégia para medir o nível de maturidade na governança de segurança da informação.

A governança de TI, de acordo com El Ghorfi et al. (2018), é parte fundamental na governança corporativa, e busca controlar a implementação e formulação dos objetivos estratégicos de uma organização. Para avaliar as estratégias de governança, os autores propuseram estender a estrutura tradicional de análise de opção real (ROA).

De acordo com Ajayi e Hussin (2018), para entender o valor de negócios de TI, a governança de tecnologia da informação tem emergido como questão central em muitas organizações. De acordo com os autores, o papel da gestão do conhecimento e dos processos em que se baseia deve ser um dos temas principais na governança de TI.

Hoje, nas organizações, de acordo com Jami, Kouchak e Ahmad (2018), o compartilhamento e extração do conhecimento vêm sendo as prioridades dos gestores. Contudo, o alto

investimento na área de gestão do conhecimento não é suficiente, pois o fracasso também é significativo. Desse modo, a gestão do conhecimento tem impacto direto na segurança da informação, uma vez que a deterioração de tal processo é prejudicial às organizações. O objetivo do artigo é oferecer uma metodologia integrada para o planejamento da gestão do conhecimento.

Laurett e Ferreira (2018) apresentam a evolução e o desenvolvimento das pesquisas realizadas sobre as estratégias aplicadas em organizações sem fins lucrativos, visando, também, a proteção das informações dentro dessas organizações.

De acordo com Kure; Islam e Razzaque (2018), um Sistema cibernético é estruturado com componentes físicos, que possuem uma interconectividade muito estreita. O artigo oferece uma abordagem diferente para gerenciar o risco de segurança cibernética de maneira proativa.

Com ataques cibernéticos cada vez mais frequentes nas organizações devido à falta de controles de TI, de acordo com Nicho (2018), a governança de segurança da informação tem sido adotada massivamente nas empresas. O objetivo do artigo é elaborar um modelo de processo de governança baseado no (PDCA).

Para as empresas que consideram a informação um ativo valioso dentro da organização, o gerenciamento da segurança da informação torna-se atividade prioritária nesse processo. Haqaf e Koyuncu (2018) sugerem um método Delphi, elaborando uma lista de construção de itens, contendo 16 habilidades na segurança da informação.

Os ataques a ativos internos são violações de segurança com direitos de acesso irrestrito aos Recursos que podem ser ou não intencionais. Chinyemba e Phiri (2018) apresentam três empresas na Zambia que investiram em algumas normas internacionais de segurança e governança.

À medida que órgãos, como instituições públicas e infraestrutura crítica medem e avaliam os Recursos de segurança da informação, os níveis de processos se tornam cada vez mais complexos. Com base em informações fornecidas por grupos especialistas em infraestrutura crítica, You et al. (2018) desenvolveram um modelo de maturidade, a fim de medir e

gerenciar ambientes críticos.

O surgimento das redes inteligentes, *smart grid*, é uma combinação perfeita de tecnologia da informação no Sistema elétrico. Woo e Kim (2018) propõem uma Análise do Sistema de controle de energia na Coreia, com avaliação e método de contramedida de monitoramento de energia e sistemas de controles, medindo o impacto da segurança da informação nesses ambientes.

A mudança da arquitetura dos sistemas de controles de supervisão e aquisição de dados de serial para IP trouxe riscos cibernéticos de alto impacto para esse ambiente. Rodofile; Radke, Foo (2019) revelam os efeitos de ataques na infraestrutura crítica através da rede de TI.

As organizações continuam a sofrer incidentes de cibersegurança, como por exemplo resultado de erro humano. Em vez de investir em conscientização e treinamento de pessoal, as organizações mantêm a estratégia de focar apenas na parte técnica da segurança da informação. Evans et al. (2019) definem uma nova técnica de avaliação e redução de falha humana.

As práticas comuns de implementação de Sistema e controle industrial moderno abrem portas para riscos cibernéticos. Assim, Qassim et al. (2019) propõem analisar várias metodologias de avaliação de segurança de infraestrutura crítica, a fim de identificar um método consistente de aferição de vulnerabilidade apropriada para esse Sistema.

Com a constante modernização do *smart grid* e sua importância na rede elétrica, um incidente de segurança pode gerar consequências de grande impacto. Martins et al. (2019) definem uma equipe de resposta a incidente para o gerenciamento efetivo dessas anomalias de segurança no *smart grid*.

5. CONCLUSÃO

O presente estudo teve o intuito de realizar uma revisão bibliográfica sobre a Governança da Segurança da Informação na indústria de energia elétrica, através do acesso à base SCOPUS. Ao todo, 43 artigos de 36 diferentes periódicos foram analisados e, em seguida, foi elaborado um esquema de classificação por: evolução cronológica de publicação; publicações de

periódicos e análise descritiva dos 43 artigos selecionados.

Baseado nos resultados da pesquisa, observa-se o aumento significativo nas publicações dos periódicos ao longo dos anos, tendo uma maior ocorrência em 2018. Vale lembrar que a pesquisa foi feita até maio de 2019, o que justifica uma menor quantidade em 2019. Além disso, 6 (seis) dos periódicos que mais publicaram sobre o tema pesquisado foram: *Information and Computer Security*, *KSII Transactions on Internet and Information Systems*, *Kerntechnik*, *British Journal of Management*, *Applied Sciences (Switzerland)* e *Journal of Computer Science*.

Após a análise do objetivo dos 43 artigos, observa-se que 24 artigos mencionam o tema de governança de segurança da informação e sua importância dentro do contexto organizacional. Desse modo, essa governança impacta diretamente no ambiente de automação energética, onde, pelo número de artigos, apenas 8 abordam o tema de segurança, mostrando que a indústria ainda vê como embrionário a área de SI.

Como proposta para pesquisas futuras, sugere-se a realização de uma pesquisa de campo junto a empresas de energia elétrica e profissionais de Segurança da informação visando mapear a percepção desses *stakeholders* no que diz respeito à Governança de Segurança da Informação nessas organizações, e fazer uma comparação sobre o que diz a literatura.

REFERÊNCIAS

AJAYI, B. A.; HUSSIN, H. Conceptualizing Information Technology Governance Model for Higher Education: An Absorptive Capacity Approach. *Bulletin of Electrical Engineering and Informatics*, v.7, n.1, p.117-124, 2018.

ALENCAR, G. D. et al. An Adaptable Maturity Strategy for Information Security. *Journal of Convergence Information Technology (JCIT)*, v. 13, n. 2, p. 1-12, Jun. 2018

ANSOFF, H. Igor. Do planejamento estratégico à administração estratégica. São Paulo: Atlas, 1990.

BOWMAN, G. The Practice of Scenario Planning: An Analysis of Inter- and Intra-organizational

Strategizing. *British Journal of Management*, v.27, n.1, p.77-96, 2016.

CARCARY, M. et al. A Framework for Information Security Governance and Management. *IT Professional*, v.18, n.2, p.22-30, 2016.

CHINYEMBA, M. K.; PHIRI, J. An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector. *Journal of Computer Science*, v. 14, n. 10, p. 1389-1400, 2018.

CHOLEZ, H.; GIRARD, F. Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of software: Evolution and Process*, v. 26, n. 5, p. 496-503, 2014.

DHILLON G., SYED R., PEDRON C. Interpreting information security culture: An organizational transformation case study. *Computers and Security*, v. 53, p. 63-69. 2016.

EL GHORFI, R. et al. Valuating IT governance strategies with real options in a decision making framework. *International Journal of Information Systems in the Service Sector*, v. 10, n.4, p 42-58, 2018.

ELMUTI, D.; JIA, H.; GRAY, D. Customer relationship management strategic application and organizational effectiveness: An empirical investigation. *Journal of Strategic Marketing*, v.17, n.1, p.75-96, 2009.

EVANS, M. et al. HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers and Security*, v. 80, p. 74-89, 2019.

GEORG, L. Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management and Governance*, v. 21, n.4, p. 793-814, 2017.

GERARD MACHADO, T. et al. Methodology for Identifying the Cybersecurity Maturity Level of Smart Grids. *IEEE Latin America Transactions*, v.14, n.11, p.4512-4519, 2016.

GONÇALVES, H. S. Proposal of a strategy model planning aligned to the balanced scorecard and the quality environments. *TQM Journal*. v. 21, n. 5, p. 462-472, 2009.

HAQAF, H.; KOYUNCU, M. Understanding key skills for information security managers. *International Journal of Information Management*, v.43, p.165-172, 2018.

HAUFE, K. et al. A process framework for information security management. *International Journal of Information Systems and Project Management*, v. 4, n. 4, p. 27-47, 2016

HÖNE, K.; ELOFF, J. H. P. Information security governance: Business requirements and research directions. *Corporate Ownership and Control*, v. 7, n. 1 C CONT. 2, p. 309-317, 2009.

ISMAM, J. N.; ISMAIL, Z. Sustainable construction waste management strategic implementation model. *WSEAS Transactions on Environment and Development*, v. 10, p. 48-59, 2014.

JAMI, P. M.; KOUCHAK, Z. Z.; AHMAD, N. Designing an integrated methodology for knowledge management strategic planning: The roadmap toward strategic alignment. *VINE Journal of Information and Knowledge Management Systems*. v.48, n.3, p.373-387, 2018.

JOHNSTON, A. C.; HALE, R. Improved security through information security governance. *Communications of the ACM*, v. 52, n. 1, p. 126-129, 2009.

KALOGERAKI, E.-M. et al. A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences (Switzerland)*, v.8, n.9, 2018.

KIM, H.; LEE, K.; LIM, J. A study on the impact analysis of security flaws between security controls: An empirical analysis of K-ISMS using case-control study. *KSII Transactions on Internet and Information Systems*, v. 11, n. 9, p. 4588-4608, 2017.

KIM, J.; TONG, L. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE Journal on Selected Areas in Communications*, v. 31, n. 7, p. 1294-1305, 2013.

KRISHNAN, R. B. et al. Font Attributes based Text Steganographic algorithm (FATS) for communicating images: A nuclear power plant perspective. *Kerntechnik*, v. 82, n. 1, p. 98-111, 2017.

KURE, H. I.; ISLAM, S.; RAZZAQUE, M. A. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, v. 8, n. 6, 2018.

LAURETT, R.; FERREIRA, J. J. Strategy in Nonprofit Organisations: A Systematic Literature Review and Agenda for Future Research. *Voluntas*, v. 29, n. 5, p. 881-897, 2018.

MARCONI, M. A.; LAKATOS, E. M. Fundamentos de metodologia científica. 7. ed. São Paulo: Atlas, 2010.

MARTINS, R. J. et al. Specialized CSIRT for Incident Response Management in Smart Grids. *Journal of Network and Systems Management*, v. 27, n. 1, p. 269-285, 2019.

MILOSLAVSKAYA N. G., TOLSTOY A. I. Visualization of information security management processes. *Scientific Visualization*, v.9, n. 5, p. 117-116. 2017.

MINTZBERG, H. Generic strategies: Towards a comprehensive framework. *In: SHRIVASTAVA, P. (Ed.). Advances in strategic management*. Greenwich, CT: JAI Press, 1988. p. 1-67.

MISHRA, S. Organizational objectives for information security governance: A value focused assessment. *Information and Computer Security*, v.23, n.2, p.122-142, 2015.

NAZARETH, D. L.; CHOI, J. A system dynamics model for information security management. *Information and Management*, v.52, n.1, p.123-134, 2015.

NICHO, M. A process model for implementing information systems security governance. *Information and Computer Security*, v. 26, n. 1, p. 10-38, 2018.

PARDO, C.; PINO, F. J.; GARCIA, F. Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards. *International Journal of Software Engineering and its Applications*, v.10, n.9, p.217-230, 2016.

PORTER, M. E. Competitive advantage: Creating and sustaining superior performance. New York, NY: Free Press, 1985.

QASSIM, Q. S. et al. A review of security assessment methodologies in industrial control

systems. Information and Computer Security, v. 27, n. 1, p. 47-61, 2019.

REBOLLO, O. et al. Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, v. 58, pp. 44-57, 2015.

RODOFILE, N. R.; RADKE, K.; FOO, E. Extending the cyber-attack landscape for SCADA-based critical infrastructure. International Journal of Critical Infrastructure Protection, v.25, p.4-35, 2019.

SÁNCHEZ, L. E. et al. Managing security and its maturity in small and medium-sized enterprises. Journal of Universal Computer Science, v. 15, n. 15, p. 3038-3058, 2010.

SHAWYUN, T. Strategic planning as an essential for quality assurance. Journal of Institutional Research South East Asia, v. 14, n. 1, p. 42-70, 2016.

TAYLOR, B. Strategies for planning. Long Range Planning, Elmsford, p.27-40, Aug. 1975.

THIYAGARAJAN, P. et al. Shamir secret sharing scheme with dynamic access structure (SSSDAS): Case study on nuclear power plant. Kerntechnik, v. 80, n. 2, p. 150-160, 2015.

TUOMIKANGAS, N.; KAIPIA, R. A coordination framework for sales and operations planning (S&OP): Synthesis from the literature. International Journal of Production Economics, v.154, p.243-262, 2014.

VALENCIA-DUQUE, F. J.; OROZCO-ALZATE, M. A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards. RISTI - Revista Iberica de Sistemas e Tecnologias de Informação, n. 22, p. 73-88, 2017.

WOO, P. S.; KIM, B. H. Establishment of cyber security countermeasures amenable to the structure of power monitoring & control systems. Transactions of the Korean Institute of Electrical Engineers, v. 67, n. 12, p. 1577-1586, 2018.

YANG, T.-H.; KU, C.-Y.; LIU, M.-N. An integrated system for information security management with the unified framework. Journal of Risk Research, v.19, n.1, p.21-41, 2 jan. 2016.

YAKUMAH, W. Information security governance implementation within Ghanaian industry sectors an empirical study. *Information Management and Computer Security*, v. 22, n. 3, p. 235-250, 2014.

YOU, Y. et al. Advanced approach to information security management system utilizing maturity models in critical infrastructure. *KSII Transactions on Internet and Information Systems*, v. 12, n. 10, p. 4995-5014, 2018.

[¹] Mestrando em Sistemas de Gestão. Especialização em Gestão Estratégica de TI. Especialização em Segurança em Redes de Computadores. Graduação em Redes de Computadores.

[²] Doutoranda em Sistemas de Gestão Sustentável. Mestre em Sistemas de Gestão. Especialização em Organização e Estratégia. Especialização em Gestão Estratégica e Qualidade. Especialização em Informática na Educação. Graduação em Biblioteconomia e Documentação e Psicologia.

[³] Orientadora. Doutorado em Engenharia Civil. Mestrado em Engenharia de Sistemas e Computação. MBA em Administração de Empresas. Pós-Graduação em PIGEAD (Planejamento, Implementação e Gestão da EaD). Graduação em Matemática (Bacharelado e Licenciatura).

Enviado: Março, 2021.

Aprovado: Abril, 2021.