InterSciencePlace
International Scientific Journal – ISSN: 1679-9844
Volume 19, Article nº 01, January/December 2024
D.O.I: http://dx.doi.org/10.6020/1679-9844/v19a1
Accepted: 10/04/2023 Published: 18/06/2024

SEGURANÇA CIBERNÉTICA NAS UNIVERSIDADES: UMA REVISÃO SISTEMÁTICA DA LITERATURA SOBRE A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO ENSINO SUPERIOR

CYBERSECURITY IN UNIVERSITIES: A SYSTEMATIC LITERATURE REVIEW ON INFORMATION SECURITY MANAGEMENT IN HIGHER EDUCATION

Olivia Tozzi Bittencourt
PÓS - GRADUAÇÃO LATO SENSU EM SISTEMAS DE TELECOMUNICAÇÕES
E-mail: oliviatozzibittencourt@gmail.com
Orcid: https://orcid.org/0009-0001-0287-6132

Rafael Lima de Carvalho
Doutorado em Engenharia de Sistemas e Computação.
E-mail: rafael.lima@uft.edu.br
Orcid: https://orcid.org/0000-0002-5296-8641

Gentil Veloso Barbosa
Doutorado em Engenharia de Sistemas e Computação.
E-mail: gentil@uft.edu.br
Orcid: https://orcid.org/0000-0001-5622-516X

George França do Santos
Doutorado em Educação
E-mail: geroge.f@uft.edu.br
Orcid: https://orcid.org/0000-0003-2760-3373

Resumo – A pesquisa atual tem revelado o papel cada vez mais crucial que a segurança da informação desempenha nas organizações contemporâneas, e a educação superior não fica à margem desse contexto. Com incidentes graves de violação de dados já ocorridos e a perspectiva de possíveis recorrências caso não haja um gerenciamento adequado de riscos, torna-se imperativo abordar essa questão de forma proativa. Este

artigo apresenta uma revisão sistemática de artigos publicados entre 2012 e 2022 com o objetivo de analisar a segurança da informação nas Instituições de Ensino Superior. A principal conclusão advinda desta investigação é a escassez de pesquisa empírica sobre riscos de cibersegurança no ambiente do ensino superior, evidenciando notáveis lacunas na literatura. Apesar dessa lacuna, é notável encontrar um elevado grau de convergência nas fontes revisadas quanto às questões de cibersegurança.

Palavras-chave: Gestão da segurança da Informação, Ensino Superior, Cibersegurança.

Abstract - Current research has revealed the increasingly crucial role that information security plays in contemporary organizations, and higher education is not exempt from this context. With serious data breach incidents having already occurred and the prospect of potential recurrences if proper risk management is not in place, it becomes imperative to address this issue proactively. This article presents a systematic review of articles published between 2012 and 2022 with the aim of analyzing information security in Higher Education Institutions. The primary conclusion drawn from this investigation is the scarcity of empirical research on cybersecurity risks in the higher education environment, highlighting notable gaps in the literature. Despite this gap, it is noteworthy to find a high degree of convergence in the reviewed sources regarding cybersecurity issues.
Keywords*:* Information Security Management, Higher Education, Cybersecurity.

Introdução

A era digital trouxe consigo uma revolução sem precedentes na forma como as informações são coletadas, armazenadas, processadas e compartilhadas. Nesse cenário de constante evolução tecnológica, a privacidade e a proteção de dados pessoais tornaram-se temas de preocupação crescente tanto para indivíduos quanto para organizações. A promulgação da Lei Geral de Proteção de Dados (LGPD) marcou um marco importante no Brasil, estabelecendo um conjunto abrangente de regulamentos e diretrizes para garantir a segurança e a privacidade dos dados pessoais dos cidadãos impactará a gestão das IES que deverão instaurar programas de adequação e conformidade e nomear responsáveis pelo tratamento e fiscalização (STELZER, [s.d.]).

No contexto das instituições de ensino superior, essas preocupações ganham relevância significativa. Estas instituições se tornaram alvos lucrativos para ataques cibernéticos e já sofreram múltiplos incidentes de alto impacto (TISSIR; EL

KAFHALI; ABOUTABIT, 2021). Elas gerenciam grandes quantidades de pesquisas valiosas e dados pessoais sensíveis, o que as torna alvos atrativos para criminosos cibernéticos, espionagem e hackers em geral.

Sydow (2020, p. 12) ainda aprofunda o conceito:

> Os crimes virtuais podem envolver uma multiplicidade de sujeitos. Pode-se tomar, como exemplo, a conduta de um hacker que é contratado por alguém para roubar segredos corporativos de um concorrente. Nesse caso, o hacker irá utilizar-se de seus conhecimentos em explorar falhas de segurança em um sistema. A princípio, os sujeitos envolvidos seriam o sujeito que contratou, o hacker e a vítima (concorrente) Entretanto, suponha que o hacker precise se dirigir à uma “lan house” para acessar o sistema, e, ao invés de se utilizar de uma falha na segurança da empresa hackeada, prefira enviar um e-mail à algum funcionário solicitando algum tipo de informação. Esse funcionário irá passar para um responsável que confiará no funcionário anterior (e assim por diante) até que alguém instale um programa oculto que permita ao hacker invasão ao sistema informático. Nesse caso, teríamos uma multiplicidade de sujeitos ativos e vítimas

É crucial ressaltar que os criminosos cibernéticos estão ampliando suas habilidades de forma contundente. Apenas no ano de 2019, o FBI recebeu diariamente cerca de 1.300 denúncias de crimes perpetrados através da internet nos Estados Unidos. No Brasil, somente em 2020, foram registradas mais de 8 bilhões de tentativas e ameaças de ataques cibernéticos. Dentro desse cenário, os desafios no campo da cibersegurança são incessantes, demandando soluções em constante atualização para mitigar o impacto do crime cibernético.

O centro de prevenção, tratamento e resposta a incidentes cibernéticos de governo – CTIR Gov disponibiliza as estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. Conforme podemos ver no gráfico 1

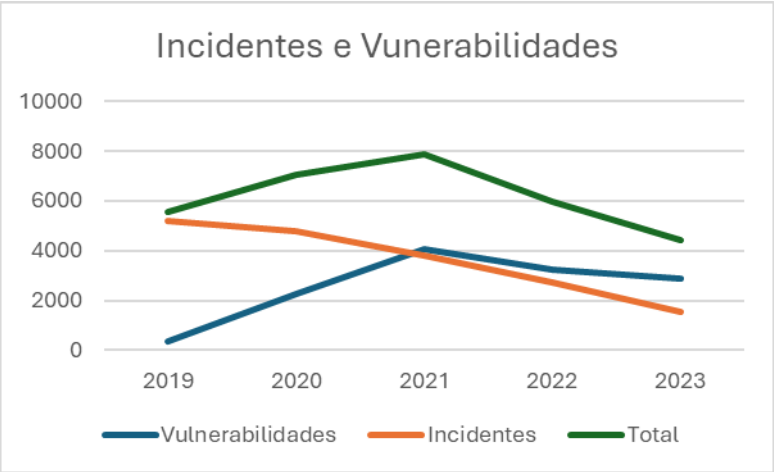

Gráfico 1 – Estatística de Incidentes no Brasil. Fonte: CTIR Gov. Acesso em 15 de ago.

Os dados apontados no gráfico 1 mostram o número de vulnerabilidades e incidentes de segurança cibernética ao longo dos anos de 2019 a 2023. Ao observar o total de vulnerabilidades e incidentes, podemos notar que houve um aumento geral de 2019 a 2021, seguido por uma redução em 2022 e 2023. Isso pode sugerir uma variação natural na segurança cibernética ao longo do tempo.

Picos em 2021: O ano de 2021 se destacou com o maior número de vulnerabilidades relatadas (4081) em comparação com os anos anteriores. Isso pode indicar um aumento na identificação e notificação de vulnerabilidades nesse período. É interessante notar que, embora o número de vulnerabilidades tenha diminuído de 2021 para 2022 e 2023, o número de incidentes permaneceu relativamente alto em 2022 e 2023. Isso pode sugerir que as vulnerabilidades identificadas ainda são exploradas por cibercriminosos, destacando a importância da resposta a incidentes de segurança.

Neste artigo, o objetivo foi abordar as seguintes perguntas de pesquisa:

1. Quais são os principais tópicos explorados em pesquisas sobre gerenciamento de segurança da informação no ensino superior?
2. Como é investigada a gestão da segurança da informação no ensino superior na literatura? Quando? Onde? Que amostra, focos, formatos e metodologias são adotadas?
3. Por que a gestão de segurança da informação no ensino superior é considerada um tema relevante?
4. Quais padrões de segurança da informação são adotados?

O artigo está organizado da seguinte forma: próxima seção, será apresentada uma revisão abrangente da literatura, onde serão explorados os principais tópicos e pesquisas relevantes sobre segurança da informação no ensino superior. As metodologias usadas na investigação, incluindo informações sobre quando, onde e como esses estudos foram conduzidos serão detalhadas.

Na terceira seção, será discutida a relevância da gestão de segurança da informação no ensino superior, destacando as razões pelas quais esse tema é de grande importância. E na última seção, analisaremos os padrões de segurança da informação amplamente adotados nas instituições de ensino superior.

A estrutura foi projetada para oferecer uma visão completa e detalhada da pesquisa e das práticas relacionadas à segurança da informação no ensino superior.

Materiais e métodos

A abordagem adotada para este artigo consiste em cinco etapas (WOLFSWINKEL et al., 2013): planejamento, execução, codificação dos resultados, caracterização das publicações e análise dos resultados, complementada com uma etapa preliminar, desenvolver (Paré et al., 2015) para aumentar a sistematicidade e a transparência.

Quando são adequadamente conduzidas, as revisões representam poderosas fontes de informação para pesquisadores, bem como profissionais que buscam evidências existentes para orientar suas tomadas de decisão e práticas (PARÉ et al., 2015).

A pesquisa foi desenvolvida no período de junho a agosto de 2023 por meio de artigos obtidos nas seguintes bases de pesquisa: Scopus, Springer Link e Web of Science, utilizando palavras-chave elaboradas durante o planejamento da revisão, com base nos artigos já estudados sobre a temática e a pesquisa foi restrita à área de ciência da computação.

Durante a pesquisa foi limitado a busca por artigos que tenham sido publicados entre 2012 e 2022. Pois é necessário que qualquer pessoa que queira repetir o processo de busca consiga encontrar os mesmos resultados e chegue nos mesmos artigos. Por este motivo artigos publicados em 2023 não foram

considerados, visto que ainda estamos no ano vigente e esse número poderia aumentar.

Um plano de revisão em torno do tema deste estudo foi desenvolvido e um conjunto de questões de pesquisa formuladas para guiar a investigação (PAPAIOANNOU et al., 2016):

1. Quais são os principais tópicos explorados em pesquisas sobre gerenciamento de segurança da informação no ensino superior?

2. Como é investigada a gestão da segurança da informação no ensino superior na literatura? Quando? Onde? Que amostra, focos, formatos e metodologias são adotadas?

3. Por que a gestão de segurança da informação no ensino superior é considerada um tema relevante?

4. Quais padrões de segurança da informação são adotados?

A pesquisa foi restrita à área de Ciência da Computação e realizou-se uma busca em banco de dados, utilizando palavras-chave elaboradas durante a fase de planejamento da revisão, com base no conhecimento pessoal da literatura e uma revisão de artigos-chave (SCHATZ e BASHROUSH, 2017). Na tabela a seguir podemos observar as strings de pesquisa que foram utilizadas para cada base de dados.

Base	String de Pesquisa
Scopus	*security OR cybersecurity AND information AND management AND high OR higher AND education OR university*
Springer Link	*Cybersecurity AND High AND Education AND Management*
Web of Science	*security OR cybersecurity AND information AND management AND high OR higher AND education OR university*

Tabela 1 – Strings de Pesquisa

Devido às diferentes opções de busca em bancos de dados, alguns ajustes foram feitos nos termos de busca. Sempre que possível, o título, o resumo e as palavras-chave foram pesquisados para garantir consistência com o escopo da pesquisa. Para garantir a sistematicidade (Paré et al., 2015), apenas artigos foram incluídos na busca, independentemente de subcategorias como classificação de periódicos, métodos de pesquisa ou região geográfica. O idioma inglês também foi selecionado como filtro para os artigos pesquisados.

Bases	Filtros aplicados	N° de artigos encontrados
Scopus	2012-2022 Subject area: Computer Science Document type: Article Language: English Keywords: Information Management, Higher Education, Network Security, Cybersecurity Information Security, Cyber Security, Risk Managemen, Higher Education Institutions, Risk Assessment	76 documentos
Springer Link	Realizando a busca avançada: With all of the words: Cybersecurity AND High AND Education AND Management Where de title contains: Cybersecurity 2012 -2022 Aplicando os filtros: Filtros aplicados (springer): Content Type: Article	62 documentos
Web of Science	Selecionando a aba RESUMO e limitando a data de 01/01/2012 a 31/12/2022 Filtros: artigos de revisão, anos da publicação (de 2012 a 2022), idioma (inglês), área de pesquisa (computer science), categoria da web of science (computer science information systems), tópicos de citação principal (security systems) e Microtópicos de citação (Phishing, malware e differential privacy)	122 documentos

Tabela 2 – Filtros Aplicados

Após a aplicação dos filtros elencados na tabela 2, todos os 260 artigos foram exportados para uma única tabela e gerado o gráfico 1, onde Podemos notar o expressivo crescimento de artigos publicados de 2012 a 2022, reiterando a importância do assunto no contexto da pesquisa científica.

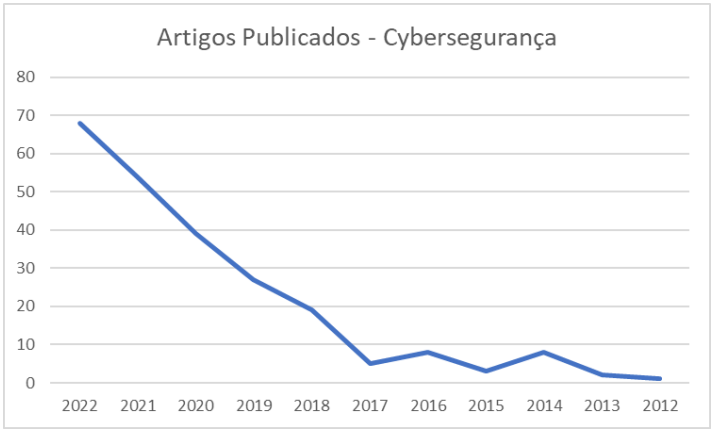

Gráfico 2 – Artigos publicados na última década. Fonte: elaboração dos próprios autores

Dentro dos 260 artigos, apenas 1 estava duplicado e por este motivo foi removido, restando 259 artigos. E para finalizar foram mantidos apenas os artigos que possuíam a palavra security no seu título e também higher education ou university. Restando portanto apenas 14 artigos (um deles de 2009 que foi removido por estar fora da data estipulada).

ID	Título do Artigo	Ano de Publicação
1.	A Systematic Review of Cybersecurity Risks in Higher Education	2021
2.	Cyber security in university libraries and implication for library and information science education in Nigeria	2023
3.	Cybersecurity Awareness Level: The Case of Saudi Arabia University Students	2021
4.	Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions	2022
5.	Evaluating the explanatory power of theoretical frameworks on intention to	2019

	comply with information security policies in higher education	
6.	Human factor and information security in higher education	2014
7.	Information security policy compliance: a higher education case study	2018
8.	Information security risk management framework for University computing environment	2017
9.	Information security risks management framework – A step towards mitigating security risks in university network	2017
10.	Introducing information security concepts and standards in higher education	2019
11.	Regional Information Management of Higher Education Based on Network Security and Grey Relational Analysis	2022
12.	Should we wear a velvet glove to enforce Information security policies in higher education?	2022
13.	The least secure places in the universe? A systematic literature review on information security management in higher education	2019

Tabela 3 – Artigos utilizados na Revisão

Resultados

A primeira pergunta de pesquisa desta revisão de literatura buscou identificar os principais tópicos explorados por estudiosos que investigam a gestão da segurança da informação em instituições de Ensino superior. Utilizando a codificação aberta, foi estabelecida uma classificação de tópicos.

Entre os artigos revisados, 53% se concentraram principalmente na exploração de estruturas de gerenciamento de riscos e padrões utilizados em instituições de Ensino superior para garantir a gestão da segurança da informação; por outro lado, a análise de risco de sistemas de segurança da informação foi o principal tópico abordado por apenas 23% dos artigos.

Um total de 66 palavras-chave foi gerado a partir de 13 artigos (apenas 1 artigo não tinha palavra-chave). Essas palavras-chave foram limpas, agregadas conforme necessário (por exemplo, formas singulares e plurais, sinônimos) e, em seguida, analisadas. A consistência com os principais tópicos foi enfatizada ao focar

nas palavras-chave mais recorrentes, incluindo "Universidade" (6 artigos), "Ensino Superior" (5), "gestão da segurança da informação" (5), e "vulnerabilidade" (3). A variedade de sub-tópicos abordados nos artigos foi demonstrada pela presença de 15 palavras-chave únicas.

A segunda pergunta de pesquisa explorou ano, local, amostra, foco, formato e metodologias dos 13 artigos na amostra. O gráfico 2 ilustra o aumento no número de publicações acadêmicas sobre gestão da segurança da informação em universidades nos últimos 10 anos. Geograficamente, os estudos exibem uma diversidade significativa. Os Estados Unidos sediaram 3 estudos, seguido por Índia, com 2, e os demais países com apenas 1 artigo cada (Noruega, Nigéria, Arábia Saudita, Malásia, Grécia, Bulgária, China e Reino Unido.

A terceira pergunta de pesquisa teve como objetivo compreender por que a gestão da segurança da informação é um tópico relevante a ser explorado. A análise dos artigos foi fundamental para definir a resposta dessa questão. Os resultados destacaram como a maioria dos artigos (8) ofereceu pouca ou nenhuma justificação para investigar o tópico da gestão da segurança da informação no ensino superior. Os outros 5 artigos exploraram a especificidade da gestão da segurança da informação no ensino superior, justificando sua relevância com base nos seguintes argumentos:

• As universidades produzem documentos legais (por exemplo, diplomas), cuja confidencialidade, integridade e disponibilidade devem ser protegidas;

• Há um número crescente de violações de segurança relatadas nas universidades;

• As universidades são plataformas de inovação abertas e organizações públicas;

• Devido à fragilidade da tecnologia de segurança da informação e ao aumento de seu atrativo para indivíduos mal-intencionados, os sites de universidades e faculdades se tornaram um alvo importante para hackers;

• Tradicionalmente, as universidades são consideradas inseguras do ponto de vista de TIC (por exemplo, seus sites);

• As universidades possuem uma quantidade extensa de materiais em papel que precisam ser protegidos contra ameaças de segurança.

A quarta e última pergunta focou em trazer quais os padrões de segurança são adotados e basicamente três artigos falaram sobre o tema de uma forma mais abrangente e trazendo uma resposta mais completa para essa questão. O primeiro artigo (A Systematic Review of Cybersecurity Risks in Higher Education) apresenta em seu item 8 uma análise das vulnerabilidades no ensino superior baseada na ISO 27005:2018, ficando divida a seção 8 em subcategorias: (Seção 8.1) Administrativa (pessoal e organização), (Seção 8.2) Técnica (incluindo hardware, software e rede) e (Seção 8.3) Física (local).

A segurança da informação engloba a salvaguarda de dados e informações em todas as suas manifestações. O campo da segurança da informação tem sido objeto de crescente pesquisa e interesse educacional ao longo dos anos. Um número considerável de universidades passou a integrar princípios de segurança em seus cursos, sejam eles já existentes ou recém-criados, em conformidade com as diretrizes estabelecidas pela série de normas ISO/IEC 27000.

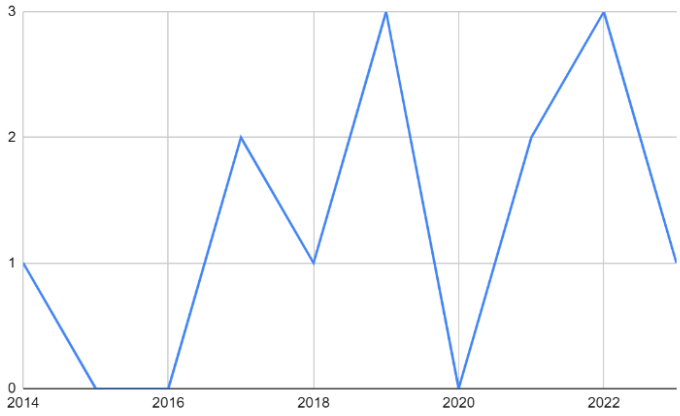

Gráfico 3 – Publicações no últimos anos. Fonte: elaboração dos próprios autores

Conclusão

Ao adotar uma abordagem de teoria fundamentada, ancorada em trabalhos que utilizaram um método destinado a aprimorar a sistematicidade e a transparência (Paré et al., 2015), esta revisão sistemática da literatura produziu contribuições teóricas de várias maneiras.

Primeiramente, ressaltou a complexidade das práticas adotadas pelas universidades ao lidar com a confidencialidade, integridade e acessibilidade das

informações que possuem. Essa análise identificou dois tópicos principais (e vários sub-tópicos) abordados na literatura, abrangendo desde a adoção de estruturas e padrões de gerenciamento de riscos até soluções técnicas para desafios de cibersegurança, além de sistemas de governança eficazes para a gestão da segurança da informação. Além disso, o artigo revelou que a pesquisa nesse campo está em seus estágios iniciais, uma vez que a maioria dos estudos foi publicada após 2018. Isso evidencia um interesse crescente e a necessidade de intensificar os esforços de pesquisa nessa área. Essa tendência também é reforçada pelo número significativo de artigos conceituais e pela falta de estudos quantitativos na amostra, bem como pela ausência de justificativas específicas em muitos dos artigos revisados para investigar a gestão da segurança da informação nas universidades.

Como uma última contribuição teórica, este artigo resumiu áreas para pesquisas futuras nesse campo, incluindo, por exemplo, cultura de segurança da informação e estudos de referência entre o ensino superior e outras indústrias. Apesar de sua natureza predominantemente teórica, uma revisão de literatura também pode oferecer algumas contribuições práticas, e este artigo não é exceção.

Profissionais de tecnologia da informação e comunicação que trabalham em instituições de Ensino superior podem se beneficiar de sua abordagem holística e sintética e expandir sua compreensão do status atual da pesquisa em gestão da segurança da informação.

Referências

ALJOHNI, WEJDAN; ELFADIL, NAZAR; JARAJREH, MUTSAM; GASMELSIED, Mwahib. Cybersecurity awareness level: The case of Saudi Arabia University students. International Journal of Advanced Computer Science and Applications, v.12, n.3, p.427-437, 2021.

ALSHARE, KHALED A.; LANE, PEGGY L.; LANE, MICHAEL R. Information security policy compliance: a higher education case study. Information & Computer Security, v.26, n.1, p.91-108, 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: [https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm]. Acesso em: 31 de ago. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 de ago. 2023.

BONGIOVANNI, I. The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, v.86, p.350–357, 2019.

GANESEN, RACHEL; ABU BAKAR, ASMIDAR; RAMLI, RAMONA; ABDUL RAHIM, FIZA; ZAWAWI, MD NABIL AHMAD. Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions. International Journal of Advanced Computer Science and Applications, v.13, n.8, 2022.

HWEE-JOO KAM, DAN J. KIM & WU HE. Should we wear a velvet glove to enforce Information security policies in higher education?, Behaviour & Information Technology, v.41, n.10, p.2259-2273, 2022. DOI: 10.1080/0144929X.2021.1917659

IGBINOVIA, MAGNUS OSAHON; ISHOLA, BOLANLE CLIFFORD. Cyber security in university libraries and implication for library and information science education in Nigeria. Digital Library Perspectives, 2023.

ISO/IEC 27002:2013. Information Technology–Security Techniques–Information Security Risk Management; Standard; International Organization for Standardization: Geneva, Switzerland, 2018.

JOSHI, CHANCHALA; SINGH, UMESH KUMAR. Information security risks management framework–A step towards mitigating security risks in university network. Journal of Information Security and Applications, v.35, p.128-137, 2017.

METALIDOU, E.; POLYCHRONAKI, M.; GIANNAKAS, G.; DOUKIDIS, G. Human factor and information security in higher education. Journal of Systems and Information Technology, v.16, n.3, p.210-221, 2014.

OROZOVA, DANIELA; KALOYANOVA, KALINKA; TODOROVA, MAGDALINA. Introducing information security concepts and standards in higher education. TEM Journal, v.8, n.3, p.1017, 2019.

PAPAIOANNOU, DIANA; SUTTON, ANTHEA; BOOTH, ANDREW. Systematic approaches to a successful literature review. Systematic approaches to a successful literature review, 336p., 2016.

GUY PARÉ; MICHAEL ALAVI; DANIEL D. MCCARTHY; DAVID J. MILLER. Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, v.52, n.2, p.183-199, 2015.

SYDOW, SPENCER TOTH; SPÍNOLA, LUÍZA MOURA COSTA. A viabilidade de aplicação da justiça restaurativa nos crimes de sextorsão e pornografia de vingança. Revista Direitos Culturais, v.15, n.36, p.329-355, 2020.

SCHATZ, DANIEL; BASHROUSH, RABIH; WALL, JULIE. Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, v.12, n.2, p.8, 2017.

SHEN, LING; WANG, GUANGMING; GAO, HAIWEI . Regional Information Management of Higher Education Based on Network Security and Grey Relational Analysis. Security and Communication Networks, v.2022, 2022.

SINGH, UMESH KUMAR; JOSHI, CHANCHALA. Information Security Risk Management Framework for University Computing Environment. **International Journal of Network Security**, v.19, n.5, p.742-751, 2017.

ULVEN, JOACHIM BJØRGE; WANGEN, GAUTE. A systematic review of cybersecurity risks in higher education. Future Internet, v.13, n.2, p.39, 2021.

WOLFSWINKEL, JOOST F.; FURTMUELLER, ELFI; WILDEROM, CELESTE PM. Using grounded theory as a method for rigorously reviewing literature. European journal of information systems, v.22, n.1, p.45-55, 2013.