INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO – CAMPUS FLORESTA
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

KALLYNE NUNES NASCIMENTO

A RELEVÂNCIA DA CIBERSEGURANÇA EM MEIO A CONSTANTE EVOLUÇÃO TECNOLÓGICA: UM MAPEAMENTO SISTEMÁTICO DA LITERATURA

FLORESTA – PE
2024

KALLYNE NUNES NASCIMENTO

A RELEVÂNCIA DA CIBERSEGURANÇA EM MEIO A CONSTANTE EVOLUÇÃO TECNOLÓGICA: UM MAPEAMENTO SISTEMÁTICO DA LITERATURA

Trabalho de Conclusão de Curso apresentado a Coordenação do curso de Gestão de Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, campus Floresta, como requisito parcial à obtenção do título de Gestor(a) em Tecnologia da Informação.

Orientador(a): Prof. Danilo da Costa Pereira.

FLORESTA - PE

2024

Dados Internacionais de Catalogação na Publicação (CIP)

N244 Nascimento, Kallyne Nunes.

A relevância da cibersegurança em meio a constante evolução tecnológica: um mapeamento sistemático da literatura / Kallyne Nunes Nascimento. - Floresta, 2024.
49 f. : il.

Trabalho de Conclusão de Curso (Gestão de T.I.) -Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, Campus Floresta, 2024.
Orientação: Prof. Msc. Danilo da Costa Pereira.

1. Segurança da Informação. 2. Cibersegurança. 3. Mapeamento sistemático da literatura. 4. Indústria. I. Título.

CDD 658.472

Gerado automaticamente pelo sistema Geficat, mediante dados fornecidos pelo(a) autor(a)

KALLYNE NUNES NASCIMENTO

A RELEVÂNCIA DA CIBERSEGURANÇA EM MEIO A CONSTANTE EVOLUÇÃO TECNOLÓGICA: UM MAPEAMENTO SISTEMÁTICO DA LITERATURA

Trabalho de Conclusão de Curso apresentado a Coordenação do curso de Gestão de Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, campus Floresta, como requisito parcial à obtenção do título de Gestor(a) em Tecnologia da Informação.

Aprovado em: 11 de setembro de 2024

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
DANILO DA COSTA PEREIRA
Data: 27/09/2024 23:00:21-0300
Verifique em https://validar.iti.gov.br

_____
Orientador: Prof. Danilo da Costa Pereira
IF Sertão PE – Campus Floresta

gov.br Documento assinado digitalmente
TASSIO JOSE GONCALVES GOMES
Data: 16/10/2024 10:13:20-0300
Verifique em https://validar.iti.gov.br

_____
Prof. Tássio José Gonçalves Gomes
IF Sertão PE – Campus Floresta

gov.br Documento assinado digitalmente
BRENO LEONARDO GOMES DE MENEZES ARAUJ
Data: 25/10/2024 18:05:08-0300
Verifique em https://validar.iti.gov.br

_____
Prof. Breno Leonardo Gomes de Menezes Araújo
IF Sertão PE – Campus Floresta

FLORESTA - PE

2024

Dedico esse trabalho aos meus pais, que sempre estiveram comigo, me apoiando durante toda essa trajetória no curso de Gestão de Tecnologia da Informação.

AGRADECIMENTOS

Agradeço primeiramente a minha família, em especial aos meus pais Liliana Nunes Nascimento e Wilsomar do Nascimento, por me incentivarem a caminhar nesta jornada e pelo apoio e consideração a mim prestados.

Aos colegas e professores do curso de Gestão de Tecnologia da Informação por me proporcionarem boas memórias, experiências e conhecimentos que levarei comigo, mesmo fora da instituição. Suas presenças tornaram esse processo de aprendizado ainda mais valoroso.

Um agradecimento especial ao meu orientador, o Prof. Danilo da Costa, pela sua disponibilidade em sanar minhas dúvidas, oferecendo assistência e sugestões que me permitiram a construção desse trabalho.

RESUMO

O presente Trabalho de Conclusão de Curso (TCC), apresenta um Mapeamento Sistemático da Literatura (MSL) direcionado a área de cibersegurança, buscando expor a sua relevância em meio ao desenvolvimento tecnológico. No referencial teórico ambos os conceitos de cibersegurança e do MSL são apresentados mais profundamente. Quanto a metodologia aplicada, o MSL se caracteriza como um apanhado de estudos disponíveis em determinada área, esse processo se dá através de algumas etapas, sendo elas: planejamento, condução e resultados. Durante o planejamento, foram definidos todos os tópicos a serem seguidos, bem como os critérios necessários para classificar a relevância dos artigos. Assim, na fase de condução do MSL, 38 estudos foram selecionados para desenvolvimento deste trabalho. Sendo a busca direcionada para identificar, a relação entre evolução tecnológica e a necessidade do uso da cibersegurança, quais as ameaças cibernéticas e mecanismos de defesa mais utilizados no meio digital, assim como quais serão as expectativas para o uso da cibersegurança no futuro, especialmente no meio industrial. Logo, mediante essa pesquisa, foi possível constatar como o aumento do uso da tecnologia influência no crescimento dos ataques cibernéticos, conforme observado em situações como o surgimento da Internet of Things (IoT) e a recente pandemia do COVID-19. Ademais, o estudo permitiu mapear as principais ameaças e métodos de proteção utilizados no meio digital, onde se observa também a possibilidade do uso de tecnologias como Machine Learning (ML) e Deep Learning (DL) para proteção contra ciberataques, além disso, a pesquisa demonstrou como conceitos tal como indústria 4.0 e 5.0 refletem o futuro da tecnologia atrelada a indústria, onde a cibersegurança será fator crucial, vendo-se a possibilidade do uso de tecnologias como IA e Blockchain para contribuir com a segurança digital.

Palavras-chave: Cibersegurança. Mapeamento Sistemático da Literatura. Indústria.

ABSTRACT

This Course Completion Work (CCW) presents a Systematic Mapping Study (SMS) aimed at the area of cybersecurity, seeking to expose its relevance in the midst of technological development. In the theoretical framework, both the concepts of cybersecurity and SMS are presented in more depth. As for the methodology applied, the MSL is characterized as a collection of studies available in a given area, this process takes place through some stages, namely: planning, conduction and results. During planning, all topics to be followed were defined, as well as the criteria necessary to classify the relevance of the articles. Thus, in the SMS conduction phase, 38 studies were selected to develop this work. The search is aimed at identifying the relationship between technological evolution and the need to use cybersecurity, which cyber threats and defense mechanisms are most used in the digital environment, as well as what the expectations will be for the use of cybersecurity in the future, especially in the industrial environment. Therefore, through this research, it was possible to verify how the increased use of technology influences the growth of cyber attacks, as observed in situations such as the emergence of the Internet of Things (IoT) and the recent COVID-19 pandemic. Furthermore, the study made it possible to map the main threats and protection methods used in the digital environment, where the possibility of using technologies such as Machine Learning (ML) and Deep Learning (DL) to protect against cyberattacks is also observed, in addition, the research demonstrated how concepts such as industry 4.0 and 5.0 reflect the future of technology linked to industry, where cybersecurity will be a crucial factor, seeing the possibility of using technologies such as AI and Blockchain to contribute to digital security.

Keywords: Cybersecurity. Systematic Mapping Study. Industry.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADL	Adversarial Machine Learning
CE	Critérios de Exclusão
CI	Critérios de Inclusão
DDoS	Distributed Denial of Service
DL	Deep Learning
IA	Inteligência Artificial
IDS	Intrusion Detection System
IoT	Internet of Things
ML	Machine Learning
MSL	Mapeamento Sistemático da Literatura
Q1	Questão 1
Q2	Questão 2
Q3	Questão 3

SUMÁRIO

1 INTRODUÇÃO

A tecnologia tornou-se parte da sociedade. Seu uso se expandiu entre setores como saúde, política, comércio, educação, dentre outros, se transformando em um aspecto essencial do cotidiano. Como resultado dessa expansão, a digitalização ampliou seus horizontes para além do que é possível tocar, migrando dados, operações para o meio virtual, tudo isso contribuiu para o desenvolvimento do ciberespaço, caracterizado por Ottis e Lorents (2010) como um espaço artificial, um conjunto que depende de sistema de informações interconectados e dos usuários que utilizam esses sistemas. Cada vez mais esse conceito tem se desenvolvido, crescendo junto a tendências como Machine Learning, Inteligência Artificial e Big Data. Fato é que, a tecnologia facilita e agiliza a realização de certos processos, porém também traz uma preocupação relativa a segurança, afinal até que ponto os dados estão seguros no meio digital.

Segundo Gouveia (2021), a cibersegurança, também chamada de segurança cibernética, se caracteriza pela proteção do ciberespaço contra as ameaças que estão presentes no meio digital. Como ao longo dos anos, a propensão é de que a tecnologia continue progredindo, a cibersegurança tem ganhado cada vez mais relevância, pois a digitalização dos processos e dados traz uma necessidade de manter a integridade dos mesmos. Logo, a cibersegurança é indiscutivelmente importante não somente para grandes organizações, mas também para que em uso pessoal se mantenham os princípios de privacidade e segurança. Conforme exposto por Nunes (2012), a necessidade de mecanismos de proteção e defesa, criados para garantir o livre uso da internet, tem feito com que os Estados busquem aprofundar-se no conceito de cibersegurança, através da criação de políticas e estratégias de combate aos ataques virtuais.

Assim, esse trabalho tem como propósito discutir sobre cibersegurança e como sua importância é influenciada pela evolução tecnológica, para tal utilizando da metodologia de mapeamento sistemático da literatura, a fim de coletar estudos que estejam alinhados com o tema.

1.1 Problema

A tecnologia é algo que facilita diversos aspectos presenciados diariamente, porém como com qualquer mecanismo, ela pode conter vulnerabilidades a serem exploradas por pessoas mal-intencionadas, principalmente ao se constatar uma convergência do mundo real com o digital, é necessário pensar em medidas de segurança para prevenir e solucionar problemas advindos do ambiente virtual.

Outra motivante para este trabalho é a importância dos dados. Atualmente qualquer usuário da internet tem informações pessoais em algum banco de dados, seja em sites ou plataformas como redes sociais, bancos digitais e carteiras digitais. Isso adiciona uma camada de complexidade na proteção dessas informações, pois algumas não pertencem puramente ao indivíduo. Portanto, dado o contexto organizacional, a importância do emprego da cibersegurança se torna ainda maior, pois toda uma estrutura e preparação é necessária para lidar com os dados de clientes e terceiros. Visto que, comprometê-los fere tanto a privacidade dos indivíduos como a imagem da empresa.

É evidente que não é possível prever quando, como e porquê uma ameaça ou um ataque virtual podem aparecer. Mas através da cibersegurança, é possível se preparar para tal cenário. Como Nunes (2012) afirma em seu trabalho, as ameaças cibernéticas podem surgir tanto iniciadas por indivíduos isolados, como hackers e crackers, quanto por grupos organizados ou até mesmo Estados. Logo, aderir a cibersegurança é uma forma de preservar e assegurar a segurança dos conteúdos no meio digital estejam seguros e permitindo que as pessoas possam usufruir da tecnologia sem demais preocupações.

Considerando isso, se desperta a seguinte questão na qual este trabalho foi baseado: a cibersegurança tem se tornado mais relevante se considerado o avanço tecnológico?

1.2 Objetivos

1.2.1 Objetivo Geral

Realizar um mapeamento sistemático sobre a cibersegurança, a fim de entender sua importância frente aos desafios tecnológicos atuais e futuros.

1.2.2 Objetivos Específicos

- Elaborar as questões de pesquisa.
- Realizar um levantamento dos trabalhos presentes na área estudada.
- Selecionar os trabalhos que atendem aos critérios predefinidos.
- Analisar e discutir os resultados obtidos.

1.3 Justificativa

A escolha do tema surge principalmente devido ao contexto atual da tecnologia, visto que há uma crescente aderência a inovações tecnológicas e o uso de métodos digitais faz com que a maioria das informações e processos trabalhados diariamente estejam de alguma forma ligados ao meio virtual. O processo evolutivo da tecnologia é constante e acelerado, por consequência, o ideal é que a cibersegurança esteja alinhada com esse desenvolvimento pois se observa que a dependência das ferramentas tecnológicas se tornou algo natural na era digital. Logo, na situação atual, a cibersegurança desempenha um papel essencial no meio virtual, garantindo que o acesso a dispositivos e redes seja feito de forma segura.

Portanto, o presente trabalho foi realizado com o intuito de explorar o que a literatura documenta em relação a cibersegurança atualmente através de um mapeamento sistemático da literatura, para assim discutir detalhadamente como sua importância e necessidade estão relacionadas com o desenvolvimento da tecnologia.

1.4 Estruturação do trabalho

A distribuição deste TCC é composta por cinco tópicos principais, a introdução sendo o primeiro. No segundo tópico será apresentado o referencial teórico, o terceiro explicara a metodologia utilizada, mostrando detalhadamente o processo do mapeamento sistemático, o quarto tópico expõe os resultados obtidos no MSL e o último apresenta a conclusão do trabalho.

2 REFERENCIAL TEÓRICO

Nessa seção será apresentado o referencial teórico, no qual serão expostos os principais temas utilizados neste trabalho, são eles: cibersegurança e Mapeamento Sistemático da Literatura.

2.1 Cibersegurança

A cibersegurança, também conhecida por segurança cibernética, pode ser descrita como, “o conjunto de medidas que procuram garantir o bem-estar e o regular funcionamento da ação de um estado e das suas populações no ciberespaço e fora dele, desde que derivado de ações diretamente a ele acometidas.” (MILITÃO, 2014). Segundo Caldas et al. (2013), “no essencial, as questões/soluções de cibersegurança devem ter o seu ponto de partida no valor da informação, mais do que nos aspetos tecnológicos que, embora sendo de tratamento obrigatório e não dispensáveis, são subsequentes.”. Um ponto significativo a ressaltar quando se trata da cibersegurança, é a diferença entre ela e a segurança da informação, pois são conceitos que apesar de carregarem fins semelhantes, não se englobam na mesma definição, Silva (2023) explica que “A cibersegurança verifica as informações digitais entre sistemas que estão conectados no ciberespaço. Por sua vez, a segurança da informação não está restrita aos meios digitais, mas também aos meios físicos, como papel.”.

Sendo assim, como forma de diferenciar os atuantes nas duas áreas, Silva (2023) detalha ainda que:

> “os profissionais de cibersegurança são treinados para lidar especificamente com as ameaças persistentes avançadas, em inglês, *advanced persistent threats*. Por outro lado, a segurança de informação está calculada na segurança dos dados e profissionais dessa área são treinados para priorizar os recursos antes de erradicas ameaças e ataque.”

Dito isso, é necessário também compreender do que se trata o ciberespaço, pois se trata do ambiente cuja proteção cabe a cibersegurança. À vista disso, o ciberespaço se caracteriza pela internet e o espaço imaterial que ela gera, onde ocorrem trocas desterritorializadas, em uma velocidade que abole qualquer noção

de distância (VILLOTA, 2017). Por consequência, Nunes (2012) esclarece que, “As ameaças podem surgir de qualquer local e ter efeitos assimétricos e fortemente disruptivos. Sendo necessário o uso da cibersegurança para manter a ordem no que tange a tal ambiente”.

Conforme exposto por Barata (2023), quando se observa o desenvolvimento mundial nos últimos anos, a tecnologia certamente é um fator de destaque, a internet já era acessível em 1994, de forma mais limitada do que atualmente, ainda sim a cibersegurança já era um fator de discussão. No decorrer dos anos, a cibersegurança tem conquistado ainda mais espaço para debate, uma prova recente disso no cenário brasileiro é a declaração da Política Nacional de Cibersegurança (PNCiber), sob decreto de n° 11.856, que tem o propósito trazer orientações das atividades relativas cibersegurança em âmbito nacional. Nessa perspectiva, com a expansão do uso do ciberespaço, surgiu consequentemente um aproveitamento ilícito do que esse espaço oferecia, assim, a atividade criminosa no ciberespaço despertou de diversas formas e em vários contextos, como a violação de confidencialidade e dados pessoais, falsidade informática, acesso ilegítimo, dano e sabotagem, entre outros (MILITÃO, 2014). Logo, Fornasier et al. (2020) observa que, se baseando nessa perspectiva e na escalabilidade das novas tecnologias, hoje criminosos navegam nas redes buscando subtrair dados e cometer fraudes que podem gerar prejuízos de grande proporção, isso torna a cibersegurança um tema cada vez mais relevante, pois a indústria do crime digital movimenta grandes quantidades de dinheiro no mundo, advindo dessas atividades ilícitas.

Assim, Nolasco e Marciel (2022) destacam que,

> “Em suma, a cibersegurança requer a atenção de empresas e de governos para com a segurança da informação, através de investimentos em sistemas de proteção, a fim de atenuar os riscos e os efeitos dos crimes virtuais, mas também o cuidado pessoal de cada cidadão para com suas informações particulares, sejam elas utilizadas no âmbito de trabalho ou nas redes sociais.”

Portanto, observando o cenário mundial atual Barboza (2020) explica que a Internet traz muitas comodidades e benefícios, o que desperta o desejo de conectar ambientes domésticos, corporativos e industriais à Internet, no entanto tal conexão aumenta o número de vulnerabilidades a serem exploradas por criminosos.

O mesmo autor expressa ainda que “conectar tais sistemas na Internet é quase inevitável, sendo assim é necessário pensar em contramedidas para reduzir os riscos de ciberataques nestes ambientes.”.

2.2 Mapeamento Sistemático da Literatura

Conforme explicado por Kitchenham e Charters (2007), o mapeamento sistemático é um tipo de revisão que se integra ao conceito revisão sistemática da literatura, sua natureza se dá como um tipo de apanhado que busca identificar os estudos disponíveis sobre uma determinada área de pesquisa ou eixo temático. Já Petersen et al. (2008) explica que o mapeamento sistemático tem como objetivo apresentar uma visão geral de uma determinada área de pesquisa, ao mesmo tempo em que são identificados tipos de pesquisa e tendências de publicação na área. Os estudos que incorporam o desenvolvimento de um MSL, como declara Proença e Silva (2016), podem ser encontrados em fontes indexadas (como Portal de Periódicos), bancos de dados e serviços de bibliotecas.

Para construção de tal metodologia, Kitchenham e Charters (2007) definem três etapas obrigatórias, sendo elas: planejar, conduzir e relatar a revisão, onde cada fase possui seus subtópicos específicos. Enquanto Petersen et al. (2008) explica que a construção do MSL é caracterizada pela definição das questões de pesquisa, realização da busca, triagem dos artigos, classificação dos resumos por palavra-chave e a extração e mapeamento de dados, sendo essas etapas, parte das fases de planejamento, condução e relato que norteiam o MSL. Kitchenham e Charters (2007) destacam ainda que, a atividades mais importantes de serem realizadas antes do processo de condução do MSL são a definição das questões de pesquisa, e a criação de um protocolo de revisão, que nada mais é do que um plano que documenta todos os procedimentos básicos a serem realizadas na revisão.

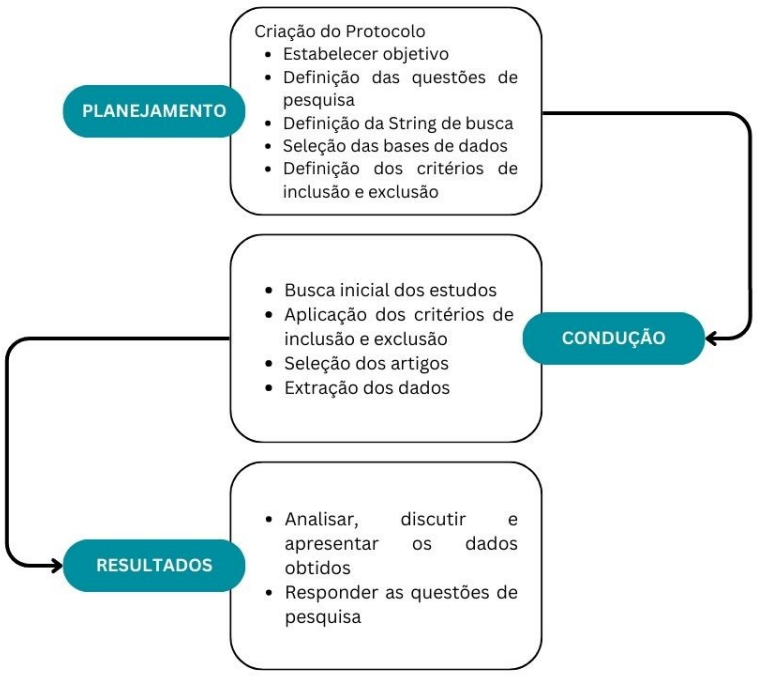
3 METODOLOGIA

Nesse tópico será exposto detalhadamente como ocorreu o processo de pesquisa utilizando o Mapeamento Sistemático da Literatura.

3.1 Planejamento do mapeamento sistemático da literatura

Na etapa inicial, ocorre o planejamento da revisão, onde se estabelece o protocolo que será utilizado para guiar o mapeamento sistemático da literatura, representado na figura 1. O protocolo detalha as etapas que deverão ser exploradas durante a pesquisa, permitindo que o planejamento do MSL seja desenvolvido de forma organizada e consistente durante sua condução.

Figura 1 – Protocolo de Mapeamento



Fonte: elaborado pela autora (2024)

3.1.1 Objetivo do mapeamento

O objetivo da realização desse mapeamento está diretamente alinhado ao

objetivo do trabalho. Logo, ele busca reunir informações de estudos relacionados à cibersegurança, buscando destacar sua relevância atual e discutir como o seu grau de importância está relacionado ao desenvolvimento tecnológico.

3.1.2 Questões de pesquisa

A questão de pesquisa pode ser considerada parte fundamental do processo de mapeamento sistemático, visto que todo o processo de coleta e análise dos dados terá ela como base. Para desenvolvimento deste trabalho, foram definidas três questões de pesquisa, onde todas derivam do tema central deste trabalho, assim, as seguintes questões foram levantadas:

- Q1 – Por que a evolução tecnológica digital aumenta a necessidade do uso da cibersegurança?

- Q2 – Quais são as ameaças digitais e mecanismos de defesa mais utilizados na execução e combate a ciberataques?

- Q3 – Quais são as expectativas futuras para aplicação da cibersegurança, especialmente se observado o desenvolvimento da indústria ao longo dos anos?

3.1.3 String de busca

A string de busca, também referida como termo de pesquisa, é um conjunto de palavras e termos com os quais a pesquisa será conduzida nas ferramentas de busca. A princípio a string desse mapeamento foi definida como (“cybersecurity” OR “cibersegurança”), esses dois termos foram utilizados pois a pesquisa tinha como foco utilizar principalmente artigos nos idiomas inglês e português. No entanto, essa string logo foi reformulada, pois retornava uma quantidade elevada de dados. Ainda que segundo Petersen et al. (2008), uma quantia maior de artigos possa ser considerada no caso de um MSL devido a análise dos estudos se dar de forma menos detalhada, ainda com a filtração desses resultados, haviam estudos demais

para serem observados manualmente, portanto, com o intuito de deixar os retornos mais objetivos a string foi redefinida como a seguinte:

- ("cybersecurity" OR "cibersegurança") AND (("cyber attack" OR "ciberataque") OR ("industry 4.0" OR "industria 4.0") OR ("mechanism" OR "mecanismo"));

A razão para a escolha dos termos ("cyber attack" OR "ciberataque") e ("mechanism" OR "mecanismo"), foi a fim de alinhar os retornos da busca com a questão de pesquisa de número dois, presente na seção 3.1.2, trazendo assim, trabalhos que contribuíssem para responder tal questionamento. Já a menção a ("industry 4.0" OR "industria 4.0"), ocorre por ser um termo recorrente quando explorada a questão da cibersegurança no meio industrial, assim o tornando relevante para resolução da questão de pesquisa três.

Para ligação entre os termos da string, foram utilizados os operadores OR para palavras que possuíam o mesmo sentido e estavam apenas em um idioma diferente, e o AND para unir os termos que deveriam ser encontrados juntos dentro dos estudos retornados. Os termos adicionados a essa nova string surgiram de palavras-chaves que apresentavam alguma relação com o necessário para responder às questões de pesquisa, dessa forma, a busca se tornou mais precisa e específica, facilitando a possibilidade de encontrar materiais relevantes para colaborar com o estudo. Vale ressaltar que a string precisou ser adaptada em algumas das plataformas de pesquisa, contudo não houve alteração em relação aos termos utilizados, apenas da forma em que os operadores ou parênteses eram utilizados.

Os termos ‘cibersegurança’ e ‘cybersecurity’ foram pesquisados como requisito de título, enquanto os restantes poderiam ser de título, palavra-chave ou resumo do artigo.

3.1.4 Fontes de busca

As fontes de busca definem quais sites serão utilizados para o levantadamente dos trabalhos que serão utilizados na pesquisa. Por conseguinte, a tabela 1 exibe quais foram as bases de dados selecionadas para a condução desse mapeamento.

Tabela 1 – Fontes de busca

Fonte de Busca	URL
Science Direct	https://www.sciencedirect.com/
Periódicos Capes	https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?
Scielo	https://www.scielo.br/
ACM Digital Library	https://dl.acm.org/

Fonte: elaborado pela autora (2024)

3.1.5 Critérios de inclusão e exclusão

Com isso, foram definidos então os critérios de exclusão e inclusão, conforme a tabela 2. Resumidamente, os critérios são métricas utilizadas para determinar o que um estudo deve ou não possuir em sua estrutura, a fim de ser relevante para a construção do mapeamento. Estes delimitam os estudos que são retornados nas fontes de busca, de forma que esteja apenas aquilo que se caracteriza como escolha do autor para a sua pesquisa. Dito isso, os seguintes critérios foram definidos para este estudo:

Tabela 2 – Critérios de inclusão e exclusão

Critérios de Inclusão (CI)	Critérios de Exclusão (CE)
CI 1. Devem estar escritos em português ou inglês	CE 1. Artigos duplicados (ex: mesmo artigo identificado em duas bases diferentes)
CI 2. Pelo menos uma das palavras-chave do artigo devem ter relação com os termos levantados nas questões de pesquisa	CE 2. Artigos cujo tema fuja de algo relacionado às questões de pesquisa

CI 3. O título deve estar relacionado a cibersegurança	CE 3. Possuir acesso restrito
	CE 4. Não se enquadrar como artigo (ex: livros, relatórios...)

Fonte: elaborado pela autora (2024)

3.2 Condução do mapeamento

Na etapa de condução é onde de fato se inicia o processo de revisão, executando o MSL baseado nos critérios anteriormente definidos durante a etapa de planejamento.

3.2.1 Busca e seleção dos artigos

Seguindo o protocolo, neste tópico se inicia a fase de condução. Durante a aplicação da pesquisa, os resultados obtidos durante essa etapa proveram das fontes de busca citadas seção 3.1.4, utilizando para tal a string também definida na etapa de planejamento.

Conforme pode ser visualizado na tabela 3, depois de retornados os resultados, houve a aplicação de um primeiro filtro sob os artigos retornados, que consistia na aplicação dos critérios de inclusão e exclusão para limitação dos artigos. Essa filtração foi realizada através das ferramentas disponíveis nos sites, definindo quais elementos eram necessários como acesso livre, tipo de publicação e idioma. Todavia, devido a limitação que algumas plataformas possuíam, a exemplo, a Scielo, que não dispunha da limitação por idioma ou a ACM Digital Library que não possuía a opção de limitar apenas a artigos de acesso aberto, foi necessário realizar uma segunda filtragem nos resultados.

A segunda filtragem foi realizada manualmente através da análise dos títulos e resumos, assim classificando se o artigo se encaixava nos critérios de inclusão e exclusão. Assim, os artigos resultantes da segunda filtragem foram baixados para que seus textos fossem analisados a fundo, sem se restringir apenas a resumos, e destes foram selecionados aqueles cujo conteúdo colabora para responder às questões de pesquisa.

Tabela 3 – Condução da pesquisa

Fonte de Busca	Busca inicial	1° Filtro	2° Filtro	Aplicados na Resolução do MSL
Science Direct	9.428	55	34	15
Periódicos Capes	7.026	326	53	23
Scielo	30	12	2	0
ACM Digital Library	3.062	179	34	0

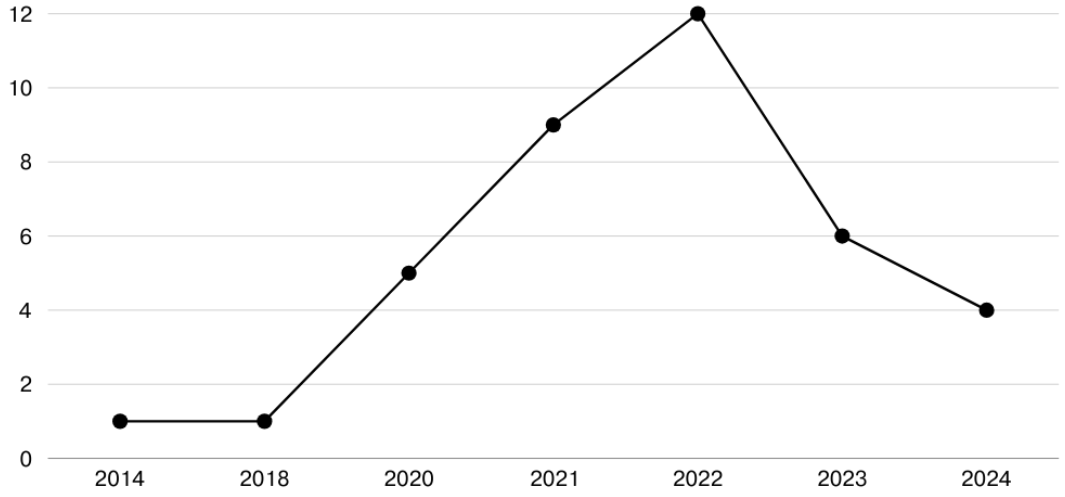
Fonte: elaborado pela autora (2024)

3.2.2 Extração dos dados

A fase de extração dos dados pode ser definida como uma etapa de classificação ou categorização, cujo intuito é realizar a classificação dos artigos que possuem detalhes suficientes para responder às questões de pesquisa (Kitchenham e Charters, 2007). Assim, nesse tópico serão apresentadas algumas tendências identificadas em relação aos estudos coletados sobre a área temática da cibersegurança.

O gráfico 1 apresenta uma relação entre os anos e o número de publicações, desse ponto de vista, fica evidente o quanto a cibersegurança tem ganhado destaque e importância, pelo menos se considerados os artigos selecionados durante o MSL. Nos anos seguintes a 2014 não houve publicações, mas de 2018 a 2022 houve uma crescente, diminuindo no ano de 2023. E considerando a data de realização deste trabalho é possível que o número de publicações de 2024 em diante possa aumentar.

Gráfico 1 – Publicações ao longo dos anos

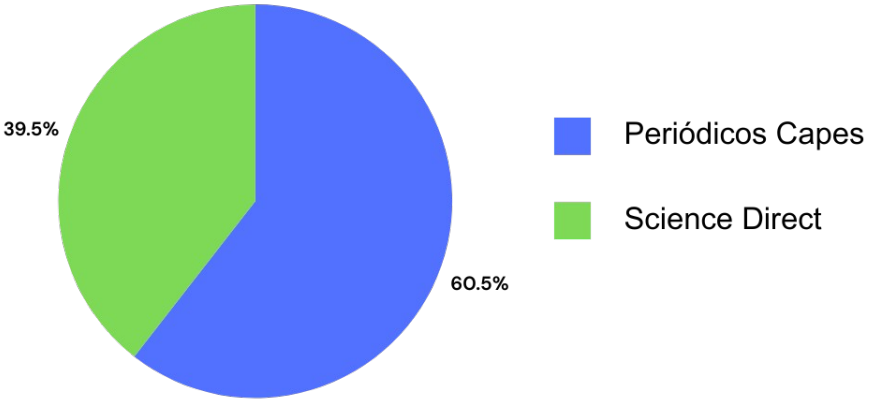


Fonte: elaborado pela autora (2024)

Mesmo tendo em vista que o processo de extração se aplica somente aos artigos escolhidos, os demais trabalhos não considerados demonstram que ainda assim, considerando os números, a cibersegurança tem sido uma área discutida, porém para princípios de praticidade e grau de relevância para a pesquisa apenas 38 artigos foram selecionados para o MSL.

Outro ponto observado foi a relação entre quantia de artigos coletados das fontes de busca, exposta no gráfico 2. Dos artigos escolhidos, vinte e três (23) foram do portal Periódicos Capes e quinze (15) do Sciente Direct. As fontes de busca Scielo e ACM Digital Library acabaram não entregando artigos cujo conteúdo fosse relevante para as questões de pesquisa e portanto seus resultados não fizeram parte do total coletado.

Gráfico 2 – Porcentagem por fonte de busca



Fonte: elaborado pela autora (2024)

As áreas abordadas nos artigos variaram bastante, desde aplicação da cibersegurança em setores como governo, saúde, educação, economia, cotidiano, entre outros, até o trabalho com conceitos mais voltados ao meio digital como a Internet of Things (IoT), ameaças digitais e o ciberespaço nos quais a cibersegurança já é fator fundamental. Essa variedade é compreensiva, já que a cibersegurança não é algo que se limite a um só ramo. Percebe-se também que houve uma predominância do idioma inglês em relação aos artigos. Já que a maioria dos resultados retornados nas fontes de busca estavam nessa linguagem e aqueles restantes após a aplicação dos critérios também estão em língua inglesa.

Dos artigos que foram baixados após a realização do segundo filtro, trinta e oito (38) foram escolhidos para compor o MSL seguindo os critérios de inclusão e exclusão. A tabela 4 detalha os títulos e autores desses artigos, bem como para quais questões estes foram relevantes.

Tabela 4 – Artigos selecionados

Autor(es)	**Título**	**Relevante para a questão**		
		Q1	**Q2**	**Q3**
Park, C. et al.	A BN driven FMEA approach to assess maritime cybersecurity risks		X	
Rudenko, R. et al.	A Brief Review on Internet of Things, Industry 4.0 and	X	X	X

	Cybersecurity			
Flor-Unda, O. et al.	A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America	X	X	
Alawida, M. et al.	A deeper look into cybersecurity issues in the wake of Covid-19: A survey	X	X	
Al-Quayed, F. et al.	A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0		X	X
Torbacki, W.	A Hybrid MCDM Model Combining DANP and PROMETHEE II Methods for the Assessment of Cybersecurity in Industry 4.0		X	
Mullet, V. et al.	A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0		X	X
Jang-Jaccard, J. et al.	A survey of emerging threats in cybersecurity		X	X
Gatica-Neira F. Et al.	Adoption of Cybersecurity in the Chilean Manufacturing Sector: A First Analytical Proposal		X	X
Mehmood, A. et al.	Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques	X	X	
Kianpour, M. et al.	Advancing the concept of cybersecurity as a public good	X		
Anthi, E. et al.	Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems		X	
Czeczot, G. et al.	AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes		X	X
Akhtar, M. S. et al.	An overview of the applications of Artificial Intelligence in Cybersecurity		X	
Alharbi, A. et al.	Analyzing the Impact of Cyber Security Related Attributes for		X	

	Intrusion Detection Systems			
Abdiyeva-Aliyeva, G. et al.	Application of classification algorithms of Machine learning in cybersecurity		X	
Mishraa, A. et al.	Attributes impacting cybersecurity policy development: An evidence from seven nations	X		
Shulha, O. et al.	Banking Information Resource Cybersecurity System Modeling		X	
Nobles, C.	Botching Human Factors in Cybersecurity in Business Organizations	X	X	
Alcaide, J. I. et al.	Critical infrastructures cybersecurity and the maritime sector		X	
Bouramdane, A.	Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process		X	
Sulich, A. et al.	Cybersecurity and Sustainable Development	X		
Sarker, I. et al.	Cybersecurity data science: an overview from machine learning perspective		X	
Raimundo, R. et al.	Cybersecurity in the Internet of Things in Industrial Management	X	X	X
Ahsan, M. et al.	Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review		X	
Loishyn, A. et al.	Development of the Concept of Cybersecurity of the Organization	X	X	
Alshaikh, O. et al.	Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach		X	
Zeadally, S. et al.	Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity	X	X	X
Toussaint, M. et al.	Industry 4.0 data security: A cybersecurity frameworks review			X

El-Bably, Amar Yasser	Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management	X	
Alqudhaibi, A. et al.	Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations	X	X
Hoffmann, R. et al.	Risk based approach in scope of cybersecurity threats and requirements	X	X
Fernández-Caramés, T. et al.	Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases	X	
Alshaibi, A. et al.	The Comparison of Cybersecurity Datasets	X	
Tao, F. et al.	The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey	X	X
Medoh, C. et al.	The Future of Cybersecurity: A System Dynamics Approach	X	
Clim, A. et al.	The Need for Cybersecurity in Industrial Revolution and Smart Cities	X	X
Bahassi, H. et al.	Toward an exhaustive review on Machine Learning for Cybersecurity	X	

Fonte: elaborado pela autora (2024)

Com o fim de analisar quais instituições têm buscado discutir sobre a cibersegurança, a tabela 5 apresenta ainda um levantamento das organizações com as quais os autores dos artigos estão associados, seja como alunos, profissionais ou colaboradores. Vale ressaltar que, devido a alguns artigos possuírem mais de um autor, a quantidade de instituições se excede ao número de artigos.

Tabela 5 – Artigos e suas instituições

Instituições	Artigos Associados
Academia de Bucharest de Estudos Econômicos	1

Academia de Polícia Egípcia	1
Academia Nacional de Ciências do Azerbaijan	1
Airbus	1
Centro de Direito e Informação Bancária (CPBil)	1
Centro de Organização de Pesquisa Científica e Industrial da Comunidade (CSIRO)	1
Colégio Universitário de Molde	1
Instituto Bancário de Warsaw (WIB)	1
Instituto de Economia e Previsões da Academia Nacional de Ciências da Ucrânia	1
Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)	1
Instituto Superior de Educação e Ciências (ISEC Lisboa)	1
Instituto Superior Tecnológico Bolivar	1
Laboratório Integrativo de Fisiologia e Metabolismo (iPAM)	1
Universidade Americana do Oriente Médio	1
Universidade Atilim	1
Universidade Babasaheb Bhimrao Ambedkar	1
Universidade Babu Banarasi Das	1
Universidade da Coruña	1
Universidade de Trás-os-Montes e Alto Douro	1
Universidade de Abu Dhabi	2
Universidade COMSATS Islamabad	1
Universidade de Abuja	1
Universidade da Beira Interior	1
Universidade de Cadiz	1
Universidade de Cardiff	1
Universidade de Ciência e Tecnologia de Wroclaw	1
Universidade de Cranfield	1
Universidade de Defesa Nacional da Ucrânia (NDUU)	1
Universidade de East Stroudsburg	1
Universidade de Economia e Negócios de Wroclaw	1
Universidade de Georgetown	1
Universidade de Glasgow	1
Universidade de Huddersfield	1
Universidade de Johannesburg	1
Universidade de Kazimierz Wielki	1

Universidade de Kentucky	1
Universidade de Las Américas	1
Universidade de Littoral Côte d'Opale	1
Universidade de Lorraine	1
Universidade de Maryland	1
Universidade de Nevada	1
Universidade de New South Wales	1
Universidade de San Sebastián	1
Universidade de Sumatra do Norte	1
Universidade de Syracuse	1
Universidade de Tecnologia de Lanzhou	2
Universidade de Tecnologia de Sydney	1
Universidade de Wisconsin – Eau Claire	1
Universidade do Bío-Bío	1
Universidade Deakin	1
Universidade Edith Cowan (ECU)	1
Universidade Estadual de Dakota do Norte	1
Universidade Estadual de Sistemas de Controle e Radioeletrônica de Tomsk	1
Universidade Estadual de Tecnologias Intelectuais e Comunicações	1
Universidade Europeia	1
Universidade Internacional de La Rioja	1
Universidade John Moores de Liverpool	1
Universidade Jouf	1
Universidade Hassan II de Casablanca	1
Universidade Hazara	1
Universidade Internacional de Rabat (UIR)	1
Universidade La Trobe	1
Universidade Macquarie	1
Universidade Marítima de Szczecin	1
Universidade Militar de Tecnologia (WAT)	1
Universidade Nacional de Kharkiv	1
Universidade Nacional de Kyiv	1
Universidade Norueguesa de Ciência e Tecnologia	1
Universidade Pedagógica Nacional Drahomanov	1

Universidade Politécnica de Madrid	1
Universidade Taif	1
Universidade Técnica de Azerbaijan	1

Fonte: elaborado pela autora (2024)

A partir dos dados na tabela 5, nota-se uma evidente variedade de fundações, com apenas a Universidade de Abu Dhabi e a Universidade de Tecnologia de Lanzhou possuindo dois (2) artigos relacionados a cada uma delas. Assim, é notório como a cibersegurança tem ganhado espaço em diversos setores e países, se tornando um tema a ser explorado em qualquer área que a tecnologia esteja envolvida.

4 RESULTADOS

Por fim, nessa etapa haverá o relato do mapeamento. Expondo quais foram os resultados atingidos, e destacando quais as informações coletadas dos artigos que foram essenciais para a discussão e resolução das questões de pesquisa.

4.1 Q1 – Por que a evolução tecnológica digital aumenta a necessidade do uso da cibersegurança?

Como apontado por Mehmood et al. (2024), no cenário atual, onde o mundo tem se tornado cada vez mais acelerado e digitalizado, a cibersegurança se tornou um escudo contra as crescentes ameaças que surgem junto aos avanços tecnológicos. Isso porque boa parte dos dispositivos e sistemas atuais trabalham com um fator em comum, os dados, e a propensão é que com o surgimento de inovações tecnológicas, cada vez mais o armazenamento e manipulação dos dados se torne uma prática comum. Não apenas essa questão, mas a interconectividade entre os dispositivos da era digital, também colabora para o crescente número de ataques virtuais. A importância do investimento em cibersegurança não é apenas uma questão individual, afinal seu campo de atuação envolve tudo aquilo que está no meio digital, a internet, os dispositivos e sistemas, como destaca Kianpour et al (2022) a cibersegurança se tornou uma parte central das decisões que abrangem o âmbito social, político e econômico, devido ao aumento dos riscos e ameaças cibernéticas que acometem indivíduos, organizações e governos.

Um acontecimento recente que demonstrou como a cibersegurança deve ser um aspecto a ser aplicado como fator social, foi a pandemia do COVID-19. As ameaças digitais cresceram em consequência de fatores como a dependência excessiva do mundo digital, o que tornou o cibercrime uma preocupação ainda mais significativa e grave, durante a pandemia da COVID-19 (Mishraa et al., 2022).A necessidade de confinamento e diminuição do contato entre as pessoas acabou resultando em situações como, a aplicação de trabalho remoto e o ensino a distância o que expandiu ainda mais o alcance das tecnologias (Loishyn et al., 2021), pois novos métodos e sistemas foram desenvolvidos e adaptados para atender a necessidade das pessoas, o que aumentou também a quantidade de brechas e vulnerabilidades que poderiam ser exploradas por pessoas mal-

intencionadas na internet. Como constatado por Sulich et al. (2021) e Alawida et al (2022), durante a pandemia houve um aumento significativo de ataques, principalmente nos setores financeiro e de saúde. Sulich et al. (2021) observa ainda que houve uma crescente de 238% em relação a ataques cibernéticos visando o setor financeiro no período de fevereiro a abril de 2020, situação que pode ser explicada devido ao fato da popularização do PIX e também a limitação de atendimento em relação às agências bancárias, o que levou muitos ao uso de bancos digitais e digitalizados. Tais instituições consequentemente acabaram acumulando muitos dados de clientes e transações, o que certamente despertou o interesse de hackers.

Quando se pensa em desenvolvimento tecnológico, um conceito recorrente que demonstra a necessidade da cibersegurança e que reflete a realidade atual e futura do mundo, é a *Internet of Things*. Zeadally et al. (2020), define IoT como um sistema que liga a internet ao mundo físico, usando sensores, hardware, software, os conectando de forma a coletar e trocar dados. Tal cenário condiz bastante com o que é esperado em relação ao desenvolvimento tecnológico, já que o uso de tecnologias como carros automáticos, casas inteligentes e Inteligência Artificial tem ganho cada vez mais popularidade, o que demonstra como cada vez mais o ciberespaço está se misturando com o mundo físico. Flor-Unda et al. (2023) pontua que o impacto dos ataques cibernéticos em dispositivos IoT é tão significativo devido a interconexão entre esses dispositivos, afinal a falta de ação humana nos processos de comunicação entre os sistemas os deixa propensos a ataques. Ao observar a IoT, é perceptível que as ferramentas digitais têm ganhado autonomia, podendo através da coleta de dados personalizar seus serviços e um comportamento, produto ou serviço adequado a necessidade de seu usuário.

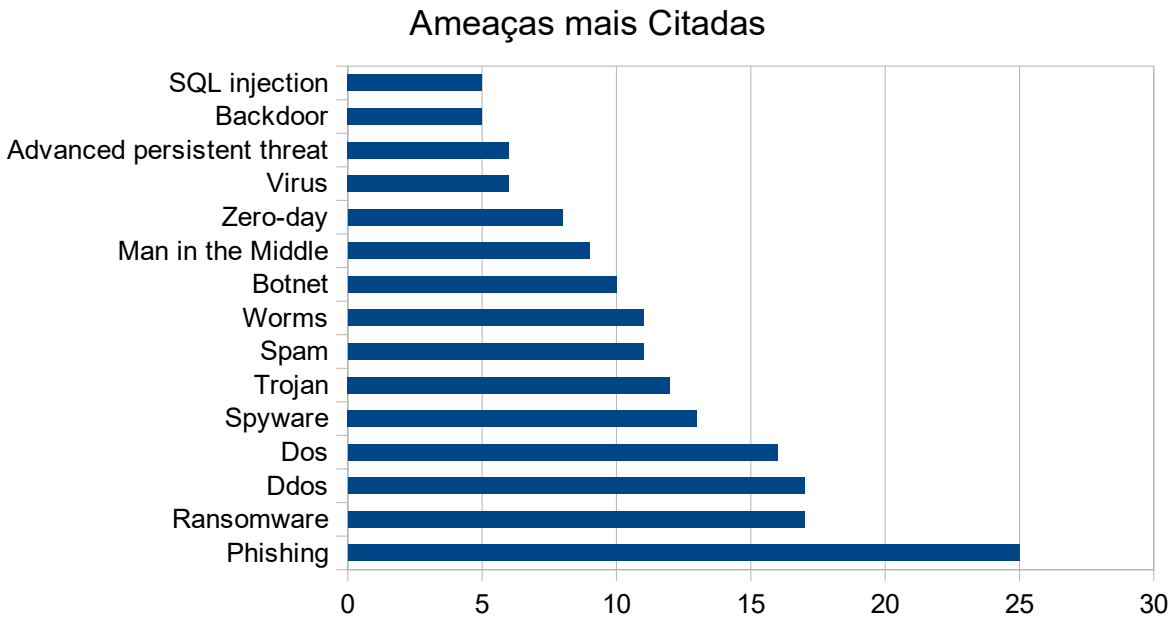
Todos os fatos expostos se alinham em um ponto, o surgimento, conexão e uso das ferramentas tecnológicas. Quanto mais utilizadas, mais o ciberespaço se expande, e portanto, maiores são os riscos. Com o crescimento da necessidade e a dependência da tecnologia, mais entidades e pessoas estarão propensas a sofrerem ataques virtuais, isso não quer dizer que o acesso à internet e a tecnologia deva ser limitado, apenas que é necessário adotar medidas de proteção para que o uso dessas ferramentas seja seguro. Pois como aponta Akthtar et al. (2021), os ataques cibernéticos emergentes serão, cada vez mais sofisticados, de forma que sistemas

convencionais não serão efetivos, abrindo a necessidade de abordagens escaláveis, adaptáveis e flexíveis para lidar com essas novas ameaças.

4.2 Q2 – Quais são as ameaças digitais e mecanismos de defesa/prevenção mais utilizados na execução e combate a ciberataques?

À medida que a tecnologia se desenvolve, é evidente que mais ameaças cibernéticas surgirão, cada vez mais rápidas e inteligentes, da mesma forma, há grande esforço em criar métodos eficazes para mitigar essas ameaças. Os artigos coletados apresentaram uma boa variedade de informações em relação esses aspectos, onde alguns expõem ameaças e mecanismos de defesa já familiares no meio digital, enquanto outros buscam criar abordagens que se adéquem ao contexto atual da tecnologia, trabalhando no refinamento e exploração de ferramentas já conhecidas para desenvolver métodos efetivos no combate às ameaças cibernéticas. Assim, foram categorizados as ameaças cibernéticas e mecanismos de defesa e proteção mais abordados em cada trabalho, destaca-se que boa parte dos artigos apresentam mais de uma ameaça ou ferramenta de proteção comuns ao meio tecnológico. Com isso, o gráfico 3 traz uma relação entre as ameaças cibernéticas mais citadas nos artigos, e o quanto elas foram mencionadas.

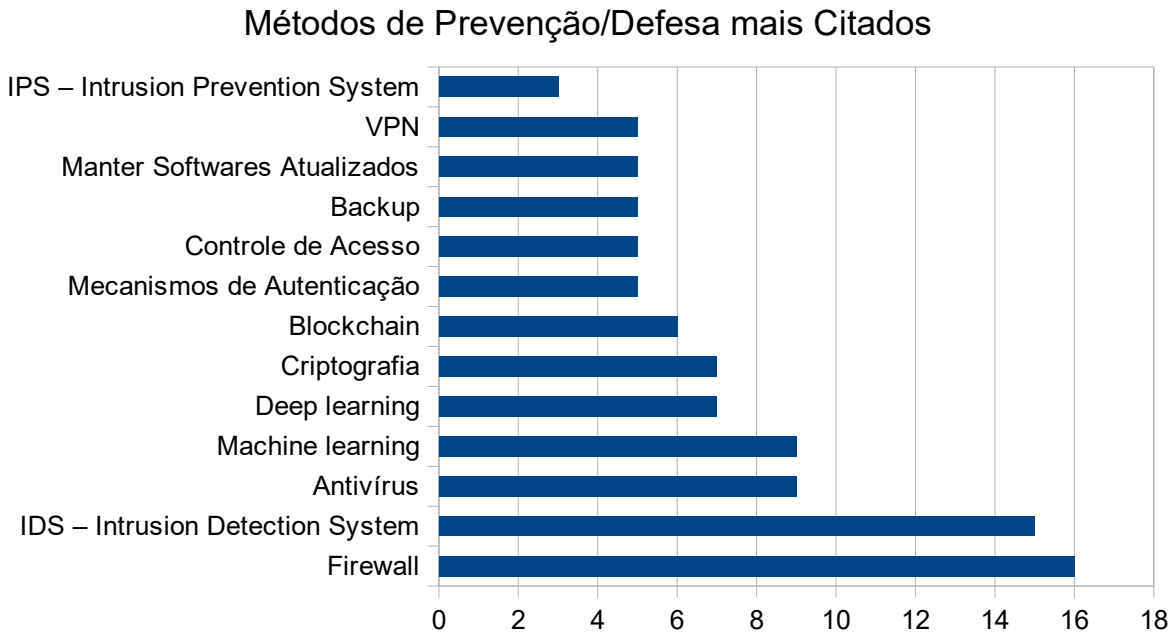
Gráfico 3 – Ameaças cibernéticas mais citadas



Fonte: elaborado pela autora (2024)

Percebe-se que, em relação aos artigos coletados, o Phising acabou sendo o método de ciberataque mais mencionado, seguido pelo Ransonware e Distributed Denial of Service (DDOS). Já em relação as formas de defesa utilizadas contra essas ameaças cibernéticas, o gráfico 4 apresenta os métodos de proteção e prevenção majoritariamente mencionadas nos artigos obtidos.

Gráfico 4 – Métodos de prevenção e defesa mais citados



Fonte: elaborado pela autora (2024)

Em uma comparação entre o gráfico 3 e o gráfico 4, percebe-se que o tema das ameaças cibernéticas é consideravelmente mais abordado em comparação aos métodos de prevenção e defesa, como pode ser visto ao observar seus elementos que possuem mais e menos menções ao longo dos trabalhos. Em consideração a proteção do ciberespaço, fugir do convencional e buscar novas soluções, se tornou atualmente algo necessário, já que os mecanismos de defesa habituais acabarão se tornando defasados para lidar com as ameaças cibernéticas emergentes em decorrência das novas tecnologias. Deixando os números de lado, e pensando numa realidade futura, alguns artigos se aprofundaram em algumas das técnicas citadas no gráfico 4, trabalhadas com métodos que possivelmente serão efetivos na prevenção e proteção de dispositivos e da internet na realidade atual e futura da era

digital. O uso de IA, ou mais especificamente dos seus ramos que compreendem, Machine Learning (ML) e Deep Learning (DL) foram os mais citados como forma de auxílio no futuro da cibersegurança. Czeczot et al. (2023) afirma que um sistema de IA com autoaprendizagem tem mais chance de isolar com maior facilidade e rapidez novos tipos de ataques, bem como criar mecanismos de defesa quase em tempo real. Essa rapidez e precisão de sistemas de IA se torna extremamente importante dado o fato dos cibercriminosos estarem criando novos métodos de ataques cibernéticos que estão cada vez mais refinados (Akhtar et al., 2021).

Como exposto por Alshaikh et al. (2024), o Machine Learning se tornou uma ferramenta essencial para a cibersegurança, isso por ser capaz de identificar e detectar ameaças potenciais consumindo poucos recursos e sem a necessidade de intervenção humana, destaca-se ainda a possibilidade de melhorar métodos de segurança existente, alocando o ML a sistemas como IDS e firewalls. No entanto, o mesmo explica os riscos de seu uso já que os mecanismos de ML podem gerar alarmes falsos ou ignorar ameaças reais se o treinamento dos algoritmos não for feito adequadamente. Dados incompletos, irrelevantes ou inconsistentes podem comprometer a qualidade do processo de aprendizagem, possivelmente prejudicando a funcionalidade dos mecanismos de Machile Learning (Ahsan et al., 2022). Portanto, ao coletar os dados a serem utilizados no aprendizado do mecanismo, é importante conferir sua legitimidade, utilidade e relevância para o resultado comportamental que se deseja obter da máquina.

Já em relação ao Deep Learning, Ahsan et al. (2022) define Deep Learning como um modelo que utiliza redes neurais artificiais, construídas utilizando vários perceptrons que são conectados de forma aleatória no início do treinamento do modelo. Enquanto segundo Sarker et al. (2020), o Deep Learning faz parte do Machine Learning, porém cujo modelo é inspirado nas redes neurais biológicas do cérebro humano. Ambos ML e DL fazem parte de um conjunto abrangente que possui Inteligência Artificial, mas sua principal diferença, como expõe Sarker et al. (2020) é o fato dos algoritmos de DL possuírem um melhor desempenho com grandes volumes de dados, enquanto os mecanismos de ML se adéquam a uma quantia menor de dados. Se trabalhados de forma correta, ambos o ML e DL podem ser eficazes ao lidar com ameaças, já que reúnem dados passados para aprendizado e podem utilizar esse conhecimento para compreenderem o

comportamento das ameaças cibernéticas assim auxiliando na detecção, prevenção e enfrentamento de ciberataques.

Para aumentar a robustez de sistemas como ML e DL, Anthi et al. (2021) sugere o Adversarial Machine Learning (AML), uma técnica que explora os pontos fracos do modelo recém-treinado, encontrando brechas nos dados utilizados no aprendizado, e inserindo pequenas perturbações no algoritmo. Tal ação utilizando o AML permite avaliar se o mecanismo conta com dados completos e relevantes, e se há alguma brecha ou ponto que pode ser melhorado, assim tornando a ferramenta mais desenvolvida e preparada para lidar com ameaças reais.

Outro mecanismo também mencionado que pode ser utilizado no contexto da cibersegurança, foi o Blockchain, uma tecnologia que segundo Zeadally et al. (2020), permite que uma rede de computadores armazene dados criptografados sem a necessidade de uma autoridade central, o que pode ser extremamente útil se considerado o nível de integração com as tecnologias da IoT no futuro, já que os dispositivos tradicionalmente se comunicam de forma centralizada e isso somado a interconexão dos mesmos, os deixa vulneráveis. Conforme Raimundo et al. (2022), a interconectividade de dispositivos inteligentes e uso das redes públicas é uma grande questão quando se pensa em cidades inteligentes, principalmente no que diz respeito a cibersegurança, nesse contexto, a Blockchain contribui para privacidade, segurança e não repúdio dos sistemas IoT, pois oferece segurança ponta a ponta, escalonável e descentralizada que permite que a grande quantidade de dados da IoT e seus dispositivos serem geridos com maior segurança.

Todos os conceitos citados já possuem sua relevância atualmente em diversos setores que fazem o uso da tecnologia, mas no escopo desse MSL estas também são, possivelmente, as tecnologias mais cobiçadas para implementação no ramo da cibersegurança em relação às novas ferramentas digitais que estão por vir.

4.3 Q3 – Quais são as expectativas futuras para aplicação da cibersegurança, especialmente se observado o desenvolvimento da indústria ao longo dos anos?

Conforme Jang-Jaccard et al. (2014), a privacidade se tornou uma questão crucial no desenvolvimento de sistemas de TI nos últimos anos, pois os ciberataques evoluíram com o passar do tempo, aproveitando vantagens decorrentes das novas

tecnologias e dos milhões de usuários ativos na internet. Tal situação significa que é necessário pensar em aspectos como privacidade, proteção de dados e segurança de uma forma nova, adaptando os processos digitais à nova realidade cibernética (Hoffmann et al., 2020).

Observando de um ponto de vista produtivo e econômico. Mullet, et al. (2021) explica que o setor industrial passou por diversas revoluções, sendo a primeira marcada pela mecanização, a segunda pela eletricidade e produção em massa, enquanto a terceira introduziu aspectos como a automação e equipamentos de TI, inicializando a digitalização do setor. Assim, presencia-se o estado atual do ramo industrial, a chamada indústria 4.0. Al-Quayed et al. (2024) explica que a Indústria 4.0 tem seus fundamentos em sistemas de rede, nela, máquinas, sensores, dispositivos e pessoas se comunicam entre si facilitando a transmissão de dados, mas ressalta ainda que lapsos na segurança desse processo de comunicação podem levar a violações de privacidade, criando sérios problemas para indivíduos e empresas. Já Toussaint et al (2024) define a indústria 4.0 como um processo de transformação digital no mundo industrial, essa transição inclui a adoção da IoT, tecnologias de comunicação e padrões novos que incluem a automação e a troca de dados em tempo real. Raimundo et al. (2022) reforça ainda que a indústria 4.0 é um importante subtema relacionado a IoT, sendo também conhecida como Industrial Internet of Things (IIoT), a qual, assim como a IoT, conecta dispositivos a internet tanto no cotidiano das pessoas quanto no ambiente industrial. Sendo assim, a indústria 4.0 se caracteriza pela implementação e uso de novas tecnologias em seus processos, na busca de torná-los mais ágeis, eficientes e menos custosos, mas possuir tantos benefícios têm seus riscos, a aplicar a digitalização nos processos industriais sem pensar na segurança dos mesmos, pode ser um grande erro, já que o comprometimento dessas atividades pode gerar altos prejuízos, sejam monetários ou não. Para solução de tais problemas, Mullet et al. (2021) sugere considerar a gestão da cibersegurança não apenas como uma medida de proteção, mas também como uma estratégia a ser aplicada para benefício dos processos industriais digitalizados. Pensando na cibersegurança Gatica-Neira et al. (2023) recomenda ainda a ISO 27.001 e o framework NIST como regulamentações que podem ser aplicadas para cibersegurança na indústria 4.0. É importante pensar nessas questões pois como explica Raimundo et al. (2022), a quarta revolução industrial

terá consequências econômicas, sociais e políticas a nível global, revolucionando o modo de produção de bens e serviços.

Apesar de a sociedade ainda estar vivenciando a indústria 4.0, alguns autores já iniciam suas discussões a respeito da próxima revolução industrial, a 5.0. Segundo Czeczot et al. (2023) a próxima fase da revolução industrial trará um novo nível de integração entre pessoas, automação e máquinas. Já Toussaint et al. (2024), aponta que a indústria 5.0 buscará combinar a experiência humana com as máquinas para, em termos de recursos, produzir eficientemente, ultrapassando a indústria 4.0. Ambos os autores discutem ainda em relação ao uso de IA na nova etapa industrial, Toussaint et al. (2024) observa que o uso de Machine Learning, e a convergência da IA com a cibersegurança é fundamental tanto na indústria 4.0 quanto para sua sucessora, e Czeczot et al. (2023), explica que para fazer o uso de tais tecnologias é necessário considerar a possibilidade de ter que processar uma grande quantidade de dados como dados financeiros ou pessoais, áudios, imagens, já que gerenciar ou atualizar esses conjuntos de dados se torna algo cada vez mais complexo à medida que eles crescem em números.

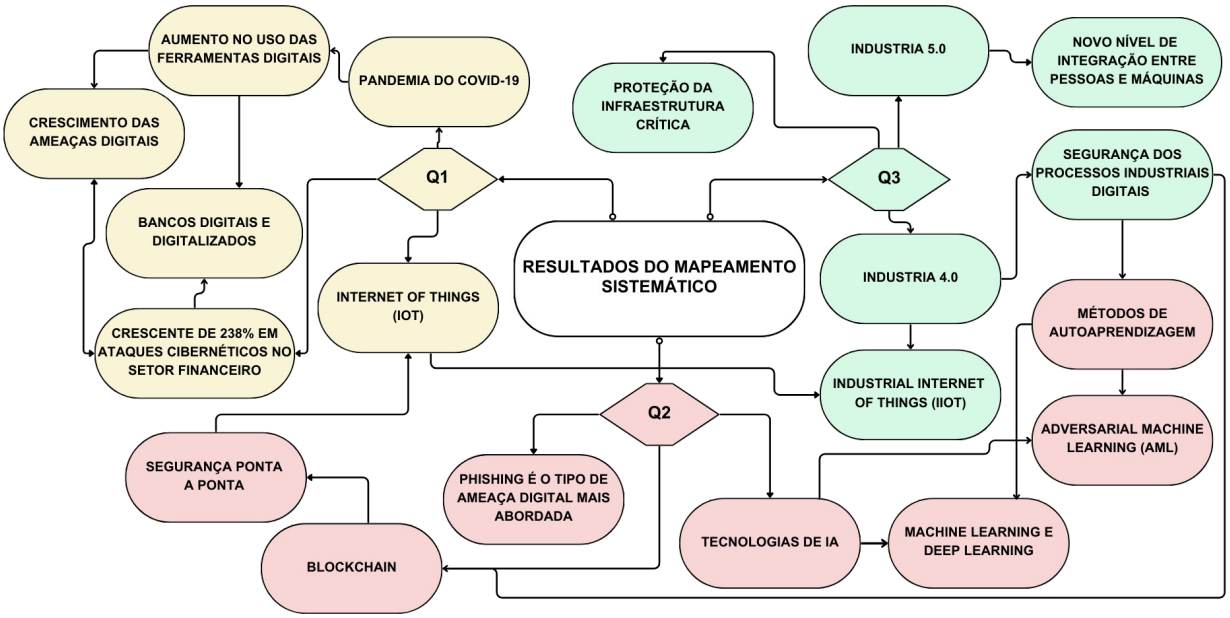
Além disso, é importante mencionar a relação entre a cibersegurança e a infraestrutura crítica e como a junção desses dois elementos será essencial no futuro. Conforme exposto por Alqudhaibi et al. (2023), a infraestrutura crítica tem um papel essencial tanto a nível nacional quanto internacional, já que é necessária para manter as funções sociais essenciais, segurança pública e sustentabilidade econômica. Toda essa infraestrutura é composta por ramos como energia, água, sistemas de controle de tráfego, telecomunicações, sendo assim, de grande importância para as atividades diárias da sociedade, já que as pessoas dependem de sua disponibilidade e integridade (Zeadally et al., 2020). Alqudhaibi et al. (2023) explica ainda que os governos e organizações são incentivados utilizar medidas avançadas de segurança, isso porque muitos modelos de TI são usados para operar as infraestruturas críticas em vários setores, logo tais entidades são incitados a fazer o uso de tecnologias como IA e ML para se antecipar a ataques as infraestruturas críticas. Portanto, evidencia-se que a integração de tecnologias a processos relacionados com as infraestruturas críticas precisam de alto nível de atenção, devendo ser algo cuidadosamente pensado, especialmente devido ao desenvolvimento rápido e avançado da tecnologia, pois se tratam de atividades essenciais para o funcionamento da economia e sociedade.

Como soluções futuras para auxiliar na prevenção e proteção contra ciberataques, Rudenko et al. (2022) acredita que blockchain e aprendizagem automática podem ser úteis na criação de tecnologias de cibersegurança. Tao et al. (2021) presume que mecanismos de IA, especialmente ML e DL, serão técnicas promissoras na mitigação de ameaças cibernéticas. Para a indústria 4.0 e 5.0, Clim et al. (2022) considera o investimento em tecnologias como IoT, IA, blockchain entre outras emergentes como sendo uma forma de melhorar diversas capacidades operacionais, ressalta ainda que o paradigma cibernético é necessário, pois afeta aspectos como saúde, energia, transporte e outros elementos da vida contemporânea. Consequentemente, fica explícito como a cibersegurança será um fator determinante olhando para o futuro a nível global. A digitalização dos processos e expansão do ciberespaço levará a uma maior integração mundo digital com o real, assim, adotar novas medidas de segurança pensadas para a realidade condizente é o ideal para manter os princípios de autenticidade, integridade e disponibilidade que regem a cibersegurança.

4.4 Visão Geral das Questões de Pesquisa e Temas

Por fim, no intuito de sintetizar os tópicos mais expressivos abordados durante a resolução do mapeamento sistemático, a figura 2 apresenta um mapa mental dos resultados atingidos, interligando os temas e abordagens trabalhadas nas questões de pesquisa, possibilitando entender quais assuntos se relacionam entre si.

Figura 2 – Visão geral dos resultados obtidos



Fonte: elaborado pela autora (2024)

5 CONCLUSÃO

Este trabalho teve como foco discutir a cibersegurança e a sua importância em relação ao desenvolvimento tecnológico. Para cumprir com tal propósito, ao longo desse estudo foi desenvolvido um Mapeamento Sistemático da Literatura. O MSL permitiu a obtenção de uma visão de como se encontra o tema da cibersegurança, especialmente em relação a estudos científicos. Através da resolução das questões de pesquisa, foi possível observar como a área de cibersegurança está diretamente relacionada ao desenvolvimento tecnológico, e como a digitalização de diversos processos que movem as atividades cotidianas traz consigo uma necessidade de manter a integridade e segurança dessas atividades. Foi possível também observar que há um esforço evidente em identificar novas metodologias e formas de proteger o ciberespaço e os dispositivos que o compõem, tecnologias de IA como Machine Learning e Deep Learning, além do Blockchain tem sido amplamente consideradas como medidas possivelmente eficientes para se aplicar a cenário atual e futuro da cibersegurança.

Considerando a realidade de uma era marcada pela digitalização. Abordar a cibersegurança e a sua importância no meio digital, será algo cada vez mais necessário, especialmente para aqueles que querem aderir às inovações da tecnologia, seja para uso pessoal, profissional ou comum. Para manter a segurança de tudo que está englobado no ciberespaço, é necessário que a cibersegurança caminhe de forma alinhada com a tecnologia, de forma a preservar a segurança dos processos digitais e assegurar que o uso das inovações tecnológicas seja feito de forma segura. Logo, esse trabalho cumpre seu propósito na exploração desse tema.

Como limitações desse estudo, observou-se após o fechamento dos resultados, a ausência de bases de dados como Scopus e IEEE, que poderiam ter agregado no número de estudos coletados, mas acabaram não fazendo parte das fontes de busca utilizadas na condução do mapeamento sistemático.

Para elaboração de trabalhos futuros voltados a cibersegurança, propõe-se uma discussão mais detalhada de como as tecnologias de Machine Learning, Deep Learning e Blockchain podem ser integradas na área. Outra possibilidade, seria discutir medidas de cibersegurança para assegurar a integridade dos processos de dispositivos da Internet of Things.

REFERÊNCIAS

BACELAR GOUVEIA, J. CyberLaw and CyberSecurity. **Revista Jurídica Portucalense**,[S. l.], p. 59–77, 2021. Disponível em: https://revistas.rcaap.pt/juridica/article/view/24897. Acesso em: 12 mar. 2024.

BARATA, R. P. A. **Procedimentos de resposta a incidentes de cibersegurança no GRA**. [s. n.], 2023. Disponível em: http://hdl.handle.net/10198/28640. Acesso em: 7 mai. 2024.

BARBOZA, R. M. **Monitoramento voltado à cibersegurança em sistemas industriais**. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/26105. Acesso em: 7 mai. 2024.

BRASIL. Decreto n°11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 20 ago. 2024

CALDAS, A.; FREIRE, V. Cibersegurança: Das Preocupações à Ação. **National Defense Institute of Portugal**, 2013. Disponível em: http://www.jstor.org/stable/resrep19122. Acesso em: 20 ago. 2024.

ENRÍQUEZ, J. A. V.; OGÉCIME, M.; ENRÍQUEZ, M. D. V.; VALENCIA, H. G. Para uma política de informação no ciberespaço: avanços, perspectivas e desafios. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 15, n. 3, p. 736–757, 2017. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8647632. Acesso em: 12 mar. 2024.

FORNASIER, M de O.; SPINATO, T. P.; RIBEIRO, F. L.. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. **Revista Thesis Juris**, [S. l.], v. 9, n. 1, p. 208–236, 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739. Acesso em: 7 mai. 2024.

KITCHENHAM, B.; CHARTERS, S.. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. Keele University and Durham University Joint Report, v. 2, jan. 2007.

MILITÃO, O. P. **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional**. [s. n.], 2014. Disponível em: http://hdl.handle.net/10362/14300. Acesso em: 7 mai. 2024.

NOLASCO, L. G.; MACIEL SILVA, B. D.. Crimes cibernéticos, privacidade e cibersegurança. **Revista Quaestio Iuris**, [S. l.], v. 15, n. 4, p. 2353–2389, 2022. Disponível em: https://www.e-publicacoes.uerj.br/quaestioiuris/article/view/67976.

Acesso em: 7 mai. 2024.

NUNES, P. F. V. A Definição de uma estratégia nacional de cibersegurança. **Instituto da Defesa Nacional**, 2012. Disponível em: http://hdl.handle.net/10400.26/42467. Acesso em: 12 mar. 2024.

OTTIS, R.; LORENTS, P.. Cyberspace: Definition and Implications. **Proceedings of the 5th International Conference on Information Warfare and Security**, p. 267-270, abr. 2010.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATTSSON, M. Systematic Mapping Studies in Software Engineering. **Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering**, v. 17, jun. 2008.

PROENÇA JÚNIOR, D.; SILVA, É. R.. Contexto e processo do Mapeamento Sistemático da Literatura no trajeto da Pós-Graduação no Brasil. **Transinformação**, v. 28, n. 2, p. 233–240, mai. 2016.

SILVA, M. B. F. da. Cibersegurança: uma visão panorâmica sobre a segurança da informação na Internet. **Freitas Bastos**, 2023. Disponível em: https://books.google.com.br/books?id=5MCnEAAAQBAJ. Acesso em: 20 ago. 2024.

APÊNDICE I – REFERÊNCIAS DOS ARTIGOS USADOS NO MSL

ABDIYEVA-ALIYEVA, G.; ALIYEV, J.; SADIGOV, U. Application of classification algorithms of Machine learning in cybersecurity. **Procedia Computer Science**, v. 215, p. 909-919, 2022.

AHSAN, M.; NYGARD, K. E.; GOMES, R.; CHOWDHURY, M. M.; RIFAT, N.; CONNOLY, J. F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. **Journal of Cybersecurity and Privacy**, v. 2, 2022.

AKHTAR, M. S.; FENG, T. An overview of the applications of Artificial Intelligence in Cybersecurity. **EAI Endorsed Transactions on Creative Technologies**, v. 8, p. 172218, 2021.

ALAWIDA, M.; OMOLARA, A. E.; ABIODUN, O. I.; AL-RAJAB, M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. **Journal of King Saud University - Computer and Information Sciences**, v. 34, n. 10, p. 8176-8206, 2022.

ALCAIDE, J. I.; LLAVE, R. G. Critical infrastructures cybersecurity and the maritime sector. **Transportation Research Procedia**, v. 45, p. 547-554, 2020.

ALHARBI, A.; HUSSAIN, A.; ALOSAIMI, W.; ALYAMI, H.; AGRAWAL, A.; KUMAR, R.; KHAN, R. Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems. **Sustainability**, v. 13, p. 12337, 2021.

AL-QUAYED, F.; AHMAD, Z.; MAMOONA, H. A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0. **IEEE Access**, 2024.

ALQUDHAIBI, A.; ALBARRAK, M.; ALOSEEL, A.; JAGTAP, S.; SALONITIS, K. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. **Sensors**, v. 23, 2023.

ALSHAIBI, A.; AL-ANI, M.; AL-AZZAWI, A.; KONEV, A.; SHELUPANOV, A. The Comparison of Cybersecurity Datasets. **Data**, v. 7, p. 22, 2022.

ALSHAIKH, O.; PARKINSON, S.; KHAN, S. Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach. **Computers & Security**, v. 139, p. 103694, 2024.

ANTHI, E.; WILLIAMS, L.; RHODE, M.; BURNAP, P.; WEDGBURY, A. Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. **Journal of Information Security and Applications**, v. 58, p. 102717, 2021.

BAHASSI, H.; EDDDERMOUG, N.; MANSOUR, A.; MOHAMED, A. Toward an exhaustive review on Machine Learning for Cybersecurity. **Procedia Computer Science**, v. 203, p. 583-587, 2022.

BOURAMDANE, A. Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. **Journal of Cybersecurity and Privacy**, v. 3, 2023.

CLIM, A.; TOMA, A.; ZOTA, R. D.; RADU, C. The Need for Cybersecurity in Industrial Revolution and Smart Cities. **Sensors and Materials**, v. 23(1), 2022.

CZECZOT, G.; ROJEK, I.; MIKOLAJEWSKI, D.; SANGHO, B. AI in IIoT Management of Cybersecurity for Industry 4.0 and
Industry 5.0 Purposes. **Eletronics**, v. 12, 2023.

EL-BABLY, A. Y. Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. **Journal of Information Security & Cybercrimes Research**, v. 4, p. 95-102, 2021.

FERNÁNDEZ-CARAMÉS, T.; FRAGA-LAMAS, P. Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. **Sensors**, v. 20, 2020.

FLOR-UNDA, O.; SIMBAÑA, F.; LARRIVA-NOVO, X.; ACUÑA, A.; TIPÁN, R.; ACOSTA-VARGAS, P. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin América. **Informatics**, v.10, p.71, 2023.

GATICA-NEIRA, F.; GALDAMES, P.; RAMOS, M. Adoption of Cybersecurity in the Chilean
Manufacturing Sector: A First Analytical Proposal. **IEEE Access**, 2023.

HOFFMANN, R.; JAROSLAW, N.; TOMASZ, P.; JERZY, S. Risk based approach in scope of cybersecurity threats and requirements. **Procedia Manufacturing**, v. 44, p. 655-662, 2020.

JANG-JACCARD, J.; NEPAL, S. A survey of emerging threats in cybersecurity. **Journal of Computer and System Sciences**, v. 80, n. 5, p. 973-993, 2014.

KIANPOUR, M.; KOWALSKI, S. J.; ØVERBY, H. Advancing the concept of cybersecurity as a public good. **Simulation Modelling Practice and Theory**, v. 116, p. 102493, 2022.

LOISHYN, A.; HOHONIANTS, S.; YA.TKACH, M.; TYSHCHENKO, M.; TARASENKO, N.; KYVLIUK, V. Development of the Concept of Cybersecurity of the Organization. **TEM Journal**, v. 10, p. 1447-1453, 2021.

MEDOH, C.; TELUKDARIE, A. The Future of Cybersecurity: A System Dynamics Approach. **Procedia Computer Science**, v. 200, p. 318-326, 2022.

MEHMOOD, A; SHAFIQUE, A.; ALAWIDA, M.; KHAN, A. Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques.

IEEE Access, 2024.

MISHRAA, A.; ALZOUBI, Y.; ANWAR, M. J.; GILL, A. Attributes impacting cybersecurity policy development: An evidence from seven nations. **Computers & Security**, v. 120, 2022.

MULLET, V.; SONDI, P.; RAMAT, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. **IEEE Access**, 2021.

NOBLES, C. Botching Human Factors in Cybersecurity in Business Organizations. **Holistica**, v. 9, p. 71-88, 2018.

PARK, C.; KONTOVAS, C.; YANG, Z.; CHANG, C. A BN driven FMEA approach to assess maritime cybersecurity risks. **Ocean & Coastal Management**, v. 235, p. 106480, 2023.

RAIMUNDO, R.; ROSÁRIO, A. T. Cybersecurity in the Internet of Things in Industrial Management. **Applied Sciences**, volume 12, 2022.

RUDENKO, R.; PIRES, I.; OLIVEIRA, P.; BARROSO, J.; REIS, A. A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. **Electronics**, v. 11, p. 1742, 2022.

SARKER, I.; KAYES, A. S. M.; BADSHA, S.; ALQAHTANI, H.; WATTERS, P.; NG, A. Cybersecurity data science: an overview from machine learning perspective. **Journal of Big Data**, vol. 7, 2020.

SHULHA, O.; YANENKOVA, I.; KUZUB, M.; MUDA, I.; NAZARENKO, V. Banking Information Resource Cybersecurity System Modeling. **Journal of Open Innovation: Technology, Market, and Complexity**, v. 8, 2022.

SULICH, A.; RUTKOWSKA, M.; KRAWCZYK-JEZIERSKA, A.; JEZIERSKI, J.; ZEMA, T. Cybersecurity and Sustainable Development. **Procedia Computer Science**, v. 192, p. 20-28, 2021

TAO, F.; AKHTAR, M. S.; JIAYUAN, Z. The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. **EAI Endorsed Transactions**, v. 8, 2021.

TORBACKI, W. A Hybrid MCDM Model Combining DANP and PROMETHEE II Methods for the Assessment of Cybersecurity in Industry 4.0. **Sustainability**, v. 13, p.8833, 2021.

TOUSSAINT, M.; KRIMA, S.; PANETTO, H. Industry 4.0 data security: A cybersecurity frameworks review. **Journal of Industrial Information Integration**, v. 39, p. 100604, 2024.

ZEADALLY, S.; ADI, E.; BAIG, Z.; KHAN, I. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. **IEEE Access**, 2020.