IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

IDENTIFICAÇÃO DE CRITÉRIOS PARA A UTILIZAÇÃO DE ANÁLISE MULTICRITÉRIO NO TRATAMENTO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0

IDENTIFICATION OF CRITERIA FOR THE USE OF MULTICRITERIA ANALYSIS IN THE TREATMENT OF INFORMATION SECURITY VULNERABILITIES IN INDUSTRY 4.0

RODRIGO SILVA SOTOLANI
CENTRO PAULA SOUZA

ISABELLA DE ARAUJO CIONINI MENEZES
CENTRO PAULA SOUZA

NAPOLEÃO VERARDI GALEGALE
CENTRO PAULA SOUZA

MARCELO DUDUCHI FEITOSA
CENTRO PAULA SOUZA

Nota de esclarecimento:
Comunicamos que devido à pandemia do Coronavírus (COVID 19), o IX SINGEP e a 9ª Conferência Internacional do CIK (CYRUS Institute of Knowledge) foram realizados de forma remota, nos dias **20, 21 e 22 de outubro de 2021.**

Agradecimento à orgão de fomento:
Pesquisa realizada no programa de mestrado do Centro Paula Souza - CEETEPS

IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

IDENTIFICAÇÃO DE CRITÉRIOS PARA A UTILIZAÇÃO DE ANÁLISE MULTICRITÉRIO NO TRATAMENTO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0

Objetivo do estudo
O estudo apresentado nesse artigo teve como objetivo identificar e apresentar quais são os critérios apontados pela literatura que podem ser empregados em um método de análise multicritério para a priorização no tratamento de vulnerabilidades de segurança da informação na indústria 4.0.

Relevância/originalidade
O progresso da Indústria 4.0 e Internet of Things também faz aumentar as vulnerabilidades de segurança da informação, tornando mais complexo priorizá-las e tomar decisões. Um método de análise multicritério como o Analytic Hierarchy Process (AHP) é uma proposta de solução.

Metodologia/abordagem
Pesquisa bibliométrica nas bases SCOPUS e Web of Science, entre 2011 e 2020, relacionando as palavras-chaves “industry 4.0”, “security vulnerability” e “multicriteria analysis”, identificou nos resultados os critérios e subcritérios relacionados a vulnerabilidades de segurança da informação na indústria 4.0.

Principais resultados
O resultado da pesquisa identificou oito critérios e 34 subcritérios relacionados ao tratamento das vulnerabilidades de segurança da informação da indústria 4.0 que poderiam ser avaliados para aplicação de um método de análise multicritério, como o AHP, auxiliando a gestão da segurança.

Contribuições teóricas/metodológicas
Os resultados encontrados permitem conduzir novas pesquisas para a validação, acréscimo ou remoção dos critérios e subcritérios identificados na literatura através de survey e também a demonstração da aplicação prática do método AHP com os critérios e subcritérios identificados neste artigo.

Contribuições sociais/para a gestão
Os critérios encontrados na literatura podem ter papel importante em auxiliar a tomada de decisão em ambientes complexos com múltiplos critérios das vulnerabilidades de segurança, ressaltando a importância do olhar da gestão na parte de segurança dos projetos da indústria 4.0.

Palavras-chave: análise multicritério, vulnerabilidade de segurança, Indústria 4.0, priorização, gestão de segurança da informação

IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

IDENTIFICATION OF CRITERIA FOR THE USE OF MULTICRITERIA ANALYSIS IN THE TREATMENT OF INFORMATION SECURITY VULNERABILITIES IN INDUSTRY 4.0

Study purpose
The study presented in this article aimed to identify and present the criteria indicated in the literature that can be used in a multi-criteria analysis method for prioritizing the treatment of information security vulnerabilities in industry 4.0.

Relevance / originality
The progress of Industry 4.0 and Internet of Things also increases information security vulnerabilities, making them more complex to prioritize and make decisions. A multicriteria analysis method such as the Analytic Hierarchy Process (AHP) is a proposed solution.

Methodology / approach
Bibliometric research in SCOPUS and Web of Science databases, between 2011 and 2020, relating the keywords "industry 4.0", "security vulnerability" and "multicriteria analysis", identified in the results the criteria and sub-criteria related to information security vulnerabilities in industry 4.0.

Main results
The research result identified eight criteria and 34 sub-criteria related to the treatment of information security vulnerabilities in Industry 4.0 that could be evaluated for the application of a multi-criteria analysis method, such as AHP, helping the security management.

Theoretical / methodological contributions
The results allow further research conduction for the validation, addition or removal of criteria and sub-criteria identified in the literature through a survey and also the demonstration of the practical application of the AHP method with the criteria and sub-criteria identified.

Social / management contributions
The criteria found in the literature can play an important role in assisting decision-making in complex environments with multiple criteria of security vulnerabilities, highlighting the importance of the management perspective in the security part of industry 4.0 projects.

Keywords: multi-criteria analysis, security vulnerability, Industry 4.0, priorization, information security management

1 Introdução

O número de artigos sobre Indústria 4.0 tem crescido muito nos últimos anos. Somente na base de dados da SCOPUS, de 2016 a 2020, o número de artigos produzidos sobre este tema saltou de cerca de mil para quase dezesseis mil artigos. O rápido desenvolvimento da quarta revolução industrial, Internet das Coisas (IoT) e computação em nuvem, permitiu uma revolução sem precedentes nos sistemas ciber-físicos e seus usuários. Segundo o Annual & Report (2018), o número de dispositivos interconectados chegará a mais de 29 bilhões em 2023, com uma estimativa de cerca de três vezes mais que a população mundial.

Uma quantidade tão grande de dispositivos conectados impactará nossas vidas em muitos domínios de aplicação como transporte, saúde, casa, cidades inteligentes e, gerenciamento de energia, entre outros. No entanto, em paralelo ao avanço da IoT, existe a questão de segurança da informação em que qualquer coisa pode se tornar um dispositivo espião a qualquer hora, em qualquer lugar. Desde a última década, o número de *malwares* em dispositivos IoT explodiu. Na primeira metade de 2018, havia mais de cento e vinte mil instâncias de *malwares* IoT detectadas pelo Kaspersky IoT Lab (Phu et al., 2019). A motivação por trás desses ataques geralmente é de ordem financeira, mas também pode ser por razões políticas, por ideologia ou protesto e por espionagem.

O crescimento no número de dispositivos conectados aos Sistemas Cyber-Físicos (CPS) aumenta vulnerabilidades a falhas tecnológicas e expande a superfície de ataque para adversários (Modarresi & Symons, 2020). A maioria desses dispositivos tem vida útil longa e muitos deles não recebem atualizações de segurança suficientes ou nunca são atualizados, resultando em ataques maliciosos que podem ter consequências graves em vidas humanas, produtividade empresarial e segurança nacional (Walker-Roberts et al., 2020).

A adoção da indústria 4.0 exige integridade, interoperabilidade, capacidade de composição e segurança. Atualmente, enquanto a segurança fica limitada ao gerenciamento de riscos como um primeiro passo, os demais itens já são direcionados por abordagens modernas de integração aos sistemas corporativos (Dimitriadis et al., 2020).

Alguns dispositivos da indústria podem ter recursos de computação, comunicação e processamento limitados tornando a aplicação da criptografia de dados clássica e dos protocolos de comunicação seguros impraticáveis (Walker-Roberts et al., 2020).

Assim, torna-se cada vez mais complexo gerenciar as vulnerabilidades existentes, tornando difícil avaliar quais vulnerabilidades priorizar (Galegale et al., 2017). O ambiente cada vez mais complexo envolvendo a indústria 4.0, seus dispositivos, redes, integrações, conexões e fatores humanos, exige a avalição de múltiplos critérios para a tomada de uma decisão. Uma possível solução para apoiar a tomada de decisão na gestão das vulnerabilidades de cyber segurança na indústria 4.0 poderia ser a utilização de análise multicritério.

O *Analytic Hierarchy Process* (AHP), desenvolvido por Thomas L. Saaty no início da década de 70, tem ampla utilização e facilidade de aplicação. Marins, Souza e Barros (2009) Destacam o grande uso do AHP no apoio à tomada de decisão na resolução de conflitos negociados e em problemas com múltiplos critérios.

Dado este cenário, o presente artigo é norteado pela questão de pesquisa "Quais critérios poderiam ser considerados na definição de prioridades no tratamento das vulnerabilidades de segurança da informação na indústria 4.0 por análise multicritério pelo método AHP?" e tem como objetivo identificar e sugerir os principais critérios na literatura para este fim.

2. Referencial teórico

Este capítulo aborda um breve referencial teórico a respeito das vulnerabilidades de segurança da informação, da indústria 4.0 e da análise multicritério, em especial o método AHP.

A abordagem dá destaque aos trabalhos que descreveram os possíveis critérios para o tratamento de vulnerabilidades de segurança da informação na indústria 4.0.

2.1 Vulnerabilidades de segurança da informação

Segundo Sommerville (2011), à medida que mais aplicações se conectam à rede, crescem os ataques qualificados a estes. Sem as devidas precauções de segurança, os atacantes podem se aproveitar de vulnerabilidades para roubar dados confidenciais, fazer mau uso do hardware e causar diversos problemas.

Com a implementação contínua de aplicações de críticas dos Sistemas Ciber-Físicos, os riscos e custos de potenciais ataques de segurança crescem. Os componentes principais de infraestruturas críticas tornaram-se alvo para ataques cibernéticos. Por exemplo, hackers sabotaram o sistema de controle da rede elétrica da Ucrânia, causando queda de energia que afetou cerca de 230 mil pessoas. Sem controles de segurança eficazes, os invasores são potencialmente capazes de causar danos a longas distâncias (Walker-Roberts et al., 2020).

As ameaças à segurança cibernética aos sistemas de controle industrial (ICS) que controlam e operam infraestrutura crítica estão entre os problemas mais significativos e crescentes que os EUA enfrentam. Para aumentar a conscientização sobre os riscos e melhorar a proteção cibernética, a CISA e o FBI lançaram uma campanha em julho de 2021 instando proprietários e operadores de infraestrutura crítica a revisar as publicações, alertas e avisos e aplicar as mitigações (CISA, 2021).

O crescimento exponencial das interconexões da Internet levou a um crescimento significativo de incidentes de ataque cibernético, muitas vezes com consequências desastrosas e graves. O *Malware* é a escolha primária de arma para realizar intenções maliciosas no ciberespaço, seja por exploração de vulnerabilidades existentes ou utilização de características únicas de tecnologias emergentes (Jang-Jaccard & Nepal, 2014).

2.2 Indústria 4.0

Para Almeida (2019) com a evolução tecnológica e a integração dos processos seguindo o conceito da indústria 4.0, os sistemas de produção passaram a ficar cada vez mais inteligentes, capazes de detectar o surgimento de necessidades produtivas, de suprimentos e de matéria-prima, o que envolve a união de tecnologias físicas e digitais e a integração das etapas do desenvolvimento de um produto ou processo.

Os sistemas produtivos caminham para a era da digitalização alavancados pela Indústria 4.0. Com ela surgiram grandes promessas para enfrentar os mais recentes desafios em sistemas de manufatura. Tudo está interconectado dentro do cenário digital com a representação virtual correspondente, permitindo que, em um nível mais alto de automação, muitos sistemas e *softwares* se comuniquem da fábrica com as últimas tendências de tecnologias de informação e comunicação, alcançando todos os elementos da cadeia de valor em um engajamento em tempo real (Alcácer & Cruz-Machado, 2019).

Os avanços tecnológicos dos sistemas produtivos criam e tratam informações valiosas que precisam ser protegidas para o sucesso industrial e segurança de todo o sistema. Em um ambiente complexo, heterogêneo e interconectado, é necessária a observação das premissas da integridade, da confidencialidade e da disponibilidade, pilares da segurança da informação.

Walker-Roberts et al. (2020) investigaram o espectro de risco de um incidente de segurança cibernética ocorrendo no mundo habilitado para física cibernética usando um banco

de dados de incidentes. O ativo mais comumente direcionado era a informação, com a maioria dos modos de ataque contando com o abuso de privilégios. A principal característica observada foram extensas violações de segurança interna, na maioria das vezes resultado de erro humano.

Com a chegada da era da Industria 4.0 e da *Internet of Things* (IoT), as vulnerabilidades de fluxo de controle desempenham um papel fundamental na detecção de invasores na IoT Industrial (IIoT), que podem concluir facilmente a sessão remota e o sequestro de fluxo de controle com base em informações confidenciais (Sha et al., 2018).

Os dispositivos da Indústria 4.0 e Sistemas Ciber-Físicos podem ser comprometidos por vários motivos. Para Walker-Roberts et al. (2020) alguns ataques, muitas vezes heurísticos, podem sequestrar dispositivos conectados e transformá-los em servidores de e-mail para spam em massa, usá-los como *botnets* para executar ataques DDoS (negação de serviço distribuída) ou simplesmente causar a interrupção dos processos de negócios.

2.3 Análise multicritério

Os desafios de segurança da Indústria 4.0 são complexos e exigem soluções assertivas. Estes problemas, no geral, envolvem muitas variáveis que devem ser analisadas para identificar a melhor solução e tomada de decisão ou até a priorização de medidas frente ao problema.

Para avaliar todos os parâmetros possíveis em uma decisão, podem ser utilizados o *Multicriteria Decision Making (MCDM)* ou o *Apoio Multicritério a decisão (AMD),* que fornecem aos tomadores de decisão ferramentas que lhes permitem avançar na solução de um problema de decisão multicritério com muitos critérios conflitantes (Zardari et al., 2015).

Segundo Leite e Freitas (2012), as principais linhas de estudo para análise multicritério são a Escola Americana e a Escola Francesa, as quais são representadas pelos métodos: *Analytic Hierarchy Process (*AHP*), Elimination and Choice Expressing Reality (*ELECTRE*) e Preference Ranking Organisation Method for Enrichment Evaluations (*PROMETHEE*).*

A Figura 1 ilustra as ramificações dos métodos de análise de decisões que é dividido entre os métodos (Zhou et al., 2006):

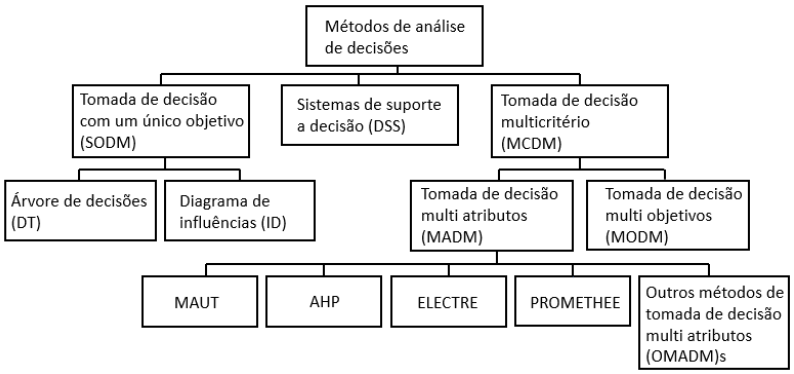

Figura 1 - Classificação dos métodos de análise de decisão
Fonte: Adaptado de Zhou; Ang; Poh (2006), Decision analysis in energy and environmental modeling: An update. Energy.

- Tomada de Decisão com um único objetivo (SODM): classe de métodos que avaliam alternativas disponíveis com resultados incertos sob uma única situação subjetiva, por exemplo árvores de decisão e diagramas de influências.
- Sistemas de Suporte à Decisão (DSS): sistemas de software interativos, flexíveis e adaptáveis que integram modelos, banco de dados e outras ferramentas de auxílio à decisão a ser usada de forma empacotadas.

- Tomada de Decisão Multicritério (MCDM): permite que decisores escolham/classifiquem alternativas avaliadas de acordo com vários critérios. As decisões são feitas com base em compensações ou compromissos entre uma série de critérios que estão em conflito entre si e são divididos em:
    - Tomada de decisão multi atributos (MADM): decisões ao avaliar e priorizar todas as alternativas caracterizadas por vários atributos conflitantes, como exemplo os métodos AHP e ELECTRE.
    - Tomada de decisão multi objetivo (MODM): são vários modelos de programação matemática que objetivam escolher o "melhor" entre todas as alternativas.

A seção seguinte aborda mais sobre o método AHP, o qual foi selecionado pelos autores deste trabalho como o possível método para realizar a avaliação das vulnerabilidades de segurança da informação na Indústria 4.0, tendo em vista a hierarquização criada por meio dos critérios identificados na literatura e sua grande aplicação no meio acadêmico e empresarial.

2.4 Analytic Hierarchy Process (AHP)

Wollmann et al. (2011) destacam que o processo AHP se inicia pela decomposição do problema em uma hierarquia de critérios ou atributos que são mais facilmente analisáveis e comparáveis de modo independente. Para Saaty (2008), essa decomposição permite tomar decisões de forma organizada da seguinte forma: a) Definir o problema e determinar o tipo de conhecimento procurado; b) Estruturar a hierarquia de decisão do topo com o objetivo da decisão, depois os objetivos de uma perspectiva ampla, passando pelos níveis intermediários até o nível mais baixo; c) Construir matrizes de comparação de pares, em que cada elemento em um nível superior é usado para comparar os elementos no nível imediatamente abaixo; d) Usar as prioridades obtidas nas comparações para ponderar as prioridades no nível imediatamente abaixo. Realizar isso para cada elemento. Em seguida, para cada elemento no nível abaixo, incluir seus valores ponderados para obter. Este processo de ponderação e adição até que as prioridades finais da alternativa no nível mais inferior sejam obtidas.

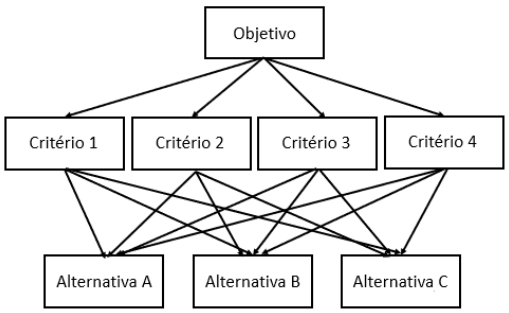

Figura 2 - Exemplo de hierarquia de critérios/objetivos genérica
Fonte: Adaptado de Saaty (2014), Toma de decisiones para líderes. RWS Publications.

Tabela 1
Característica do método AHP

Descrições	**AHP**
Entrada de dados (*input*)	
Julgamento em problemas com muitos critérios/alternativas	Alta
Processar os dados antes que estes possam ser usados	Não
Saída de dados (*output*)	
Proporciona ranking completo de alternativas	Sim
Proporciona soluções muito refinadas	Sim
Permite a avaliação de coerência dos julgamentos	Sim
Interface do tomador de decisão com o método	
Utilização de decisões em grupo	Sim
Facilidade para estruturar o problema	Alta
Possibilita o aprendizado sobre a estrutura do problema	Sim
Nível de compreensão para o decisor à forma de trabalho	Alto

Fonte: Adaptado de Guglielmetti et al. (2003), Comparação teórica entre métodos de auxílio à tomada de decisão por múltiplos critérios. ENEGEP.

3. Metodologia

A metodologia utilizada neste estudo foi uma pesquisa bibliométrica com o objetivo de se identificar os critérios apontados pelos autores de publicações relacionadas a vulnerabilidades de segurança da informação na indústria 4.0. De acordo com Prodanov e De Freitas (2013), a pesquisa pode ser classificada quanto à natureza como *pesquisa básica*. Quanto ao objetivo, como *pesquisa exploratória e descritiva*. E quanto ao procedimento científico, *pesquisa bibliométrica*.

3.1 Pesquisa bibliométrica e análise bibliográfica

O estudo bibliométrico e análise bibliográfica foram executados de acordo com as seguintes etapas: definição das bases de dados, período e palavras-chave mais adequados para atender ao objetivo da pesquisa, busca pelas publicações, refinamento dos resultados encontrados, preparação das visões gráficas e análise das publicações selecionadas.

A bibliometria foi executada com o acesso aos sites das bases de dados Scopus e *Web of Science* e as combinações das palavras-chaves "*Multicriteria Analysis*", "*Security Vulnerability*" e "*Industry 4.0*", no período compreendido entre os anos de 2011 a 2020. Os resultados obtidos na pesquisa bibliométrica estão descritos no Capítulo 4 deste artigo.

A análise bibliográfica foi executada de acordo com o protocolo PRISMA-P.

4. Análise dos resultados

Nesta seção serão apresentados os resultados da pesquisa e a sua análise através de recursos de gráficos, tabelas e figuras para ilustrar as informações das publicações encontradas.

4.1 Resultados da pesquisa bibliométrica e análise bibliográfica

A pesquisa bibliométrica retornou diferentes resultados de publicações de acordo com a combinação de palavras-chave utilizada. Os documentos retornados foram analisados quantitativa e qualitativamente com a utilização do protocolo de pesquisa PRISMA-P (*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*) com o objetivo fornecer a justificativa para a revisão sistemática e uma abordagem metodológica e analítica pré-planejada, antes do início de uma revisão. O PRISMA-P é um guia para ajudar os autores a planejarem revisões sistemáticas e meta-análises que retornem um conjunto mínimo de itens importantes a serem incluídos no protocolo de pesquisa (Moher et al., 2016).

Os dados foram analisados com o auxílio do pacote Bibliometrix, uma ferramenta de código aberto programado na linguagem R para pesquisa quantitativa e bibliometria. O pacote Bibliometrix fornece várias rotinas para importar dados bibliográficos do SCOPUS, *Web of Science*, PubMed, entre outros, realizando análises bibliométricas e construindo matrizes de dados para cocitação, acoplamento, análise de colaboração científica e análise de co-palavras.

A pesquisa bibliométrica nas bases de dados *SCOPUS* e *Web of Science (WoS)* retornou inicialmente um total de 1.128 publicações ao combinar as palavras chaves. Para a análise do material obtido, foram adotados os seguintes critérios: (a) Exclusão de materiais como teses, dissertações, monografias e livros; (b) Exclusão de publicações em idiomas diferente de português e inglês; (c) Exclusão da combinação dos grupos de palavras chaves "*multicriteria analysis*" e "*industry 4.0*", por estar fora do escopo da pesquisa;

Após a aplicação dos critérios iniciais de exclusão, restaram 236 publicações identificadas, para refinamento da busca, conforme as fases do protocolo PRISMA-P. Na fase da triagem, foram removidos 167 artigos, resultando em 69 artigos triados, conforme os filtros: (d) Exclusão de documentos duplicados; e (e) Exclusão de documentos não abertos;

Na fase de elegibilidade foram realizadas as leituras dos resumos/abstract das publicações para verificar o alinhamento da publicação com a pesquisa. Neste refinamento foram excluídas 35 publicações por falta de alinhamento com a pesquisa. As 34 publicações restantes, foram lidas na íntegra na fase da inclusão. A Figura 3 ilustra todo esse processo.

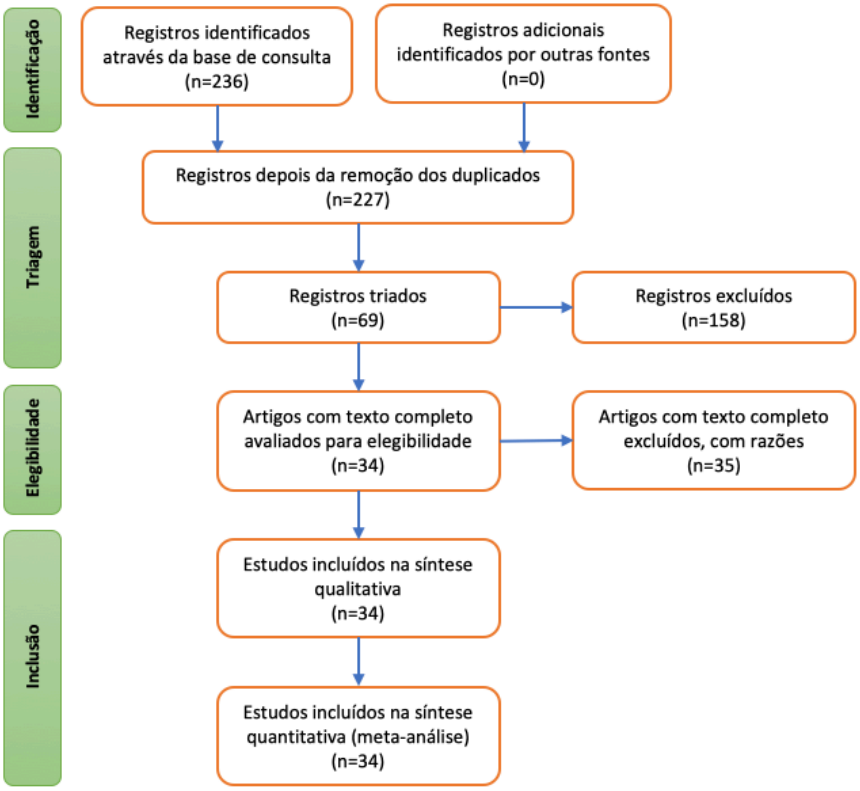

Figura 3 - Detalhamento das fases do protocolo PRISMA-P
Fonte: os autores (2021).

A Tabela 2 ilustra os resultados iniciais obtidos nas bases SCOPUS e *Web of Science* entre 2011 e 2020. É observado que os termos "*multicriteria analysis*", "*industry 4.0*" e "*security vulnerability*", quando consultados individualmente, apresentam uma quantidade significativa de artigos publicados. Estes termos representam na tabela, respectivamente, os grupos A, B e C, para a base do SCOPUS e como D, E e F, para a *WoS*.

Avançando com a combinação dos termos entre si, verificou-se uma quantidade reduzida de artigos produzidos. Considerando os resultados da base de dados SCOPUS, ao combinar A e B ("*multicriteria analysis*" AND "*industry 4.0*") foram obtidos 830 artigos. Combinando B e C ("*industry 4.0*" AND "*security vulnerability*") 102 artigos foram obtidos. Os termos A e C ("*multicriteria analysis*" AND "*security vulnerability*") trouxeram 100 artigos. E finalmente, combinando os três termos juntos, A e B e C ("*multicriteria analysis*" AND "*industry 4.0*" AND "*security vulnerability*") resultou apenas em três artigos.

As mesmas combinações aplicadas aos resultados da base de dados da *Web of Science*, resultaram em: termos D e E ("*multicriteria analysis*" AND "*industry 4.0*") trouxeram 62 documentos. Os termos E e F ("*industry 4.0*" AND "*security vulnerability*"), 19 documentos. Os termos D e F combinados ("*multicriteria analysis*" AND "*security vulnerability*") trouxeram 12 artigos. E a combinação dos três termos juntos, D e E e F ("*multicriteria analysis*" AND "*industry 4.0*" AND "*security vulnerability*") não resultou nenhum artigo.

Tabela 2
Pesquisa bibliométrica realizada na base da SCOPUS

Base de pesquisa	Grupo	Termos consultados	Docs.
SCOPUS	A	*ALL ("multicriteria analysis" OR "AHP" OR "analytic hierarchic process") ***	90.015
	B	*(ALL ("industry 4.0" OR "fourth industrial revolution") ***	37.047
	C	*(ALL ("computer security" AND "vulnerability*") ***	10.594
	A e B	*((ALL ("industry 4.0" OR "fourth industrial revolution"))) AND (ALL ("multicriteria analysis" OR "AHP" OR "analytic hierarchic process") ***	830
	B e C	*((ALL ("industry 4.0" OR "fourth industrial revolution"))) AND ((ALL ("computer security" AND "vulnerability*")) **	102
	A e C	*((ALL ("computer security" AND "vulnerability*"))) AND (ALL ("multicriteria analysis" OR "AHP" OR "analytic hierarchic process")) ***	100
	A e B e C	*((ALL ("industry 4.0" OR "fourth industrial revolution"))) AND ((ALL ("computer security" AND "vulnerability*"))) AND (ALL ("multicriteria analysis" OR "AHP" OR "analytic hierarchic process")) ***	3
Web of Science	D	*ALL= ("multicriteria analyses" OR "AHP" OR "analytic hierachy process") ***	18.585
	E	*ALL= ("industry 4.0" OR "fourth industrial revolution") ****	11.446
	F	*ALL=(("computer" OR "cyber") AND "security" AND "vulnerability") ****	2.709
	D e E	*ALL= (("multicriteria analyses" OR "AHP" OR "analytic hierarchy process") AND ("industry 4.0" OR "fourth industrial revolution")) ****	62
	D e F	*ALL= (("multicriteria analyses" OR "AHP" OR "analytic hierarchy process") AND (("computer" OR "cyber") AND "security" AND "vulnerability")) ****	12
	E e F	*ALL= ("industry 4.0" OR "fourth industrial revolution") AND (("computer" OR "cyber") AND "security" AND "vulnerability")) ****	19
	D e E e F	*ALL= (("multicriteria analyses" OR "AHP" OR "analytic hierarchy process") AND ("industry 4.0" OR "fourth industrial revolution") AND (("computer" OR "cyber") AND "security" AND "vulnerability")) ****	0

Fonte: os autores (2021). ***AND PUBYEAR > 2010 AND PUBYEAR < 2021. *** Índices=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI Tempo estipulado=2011-2020.*

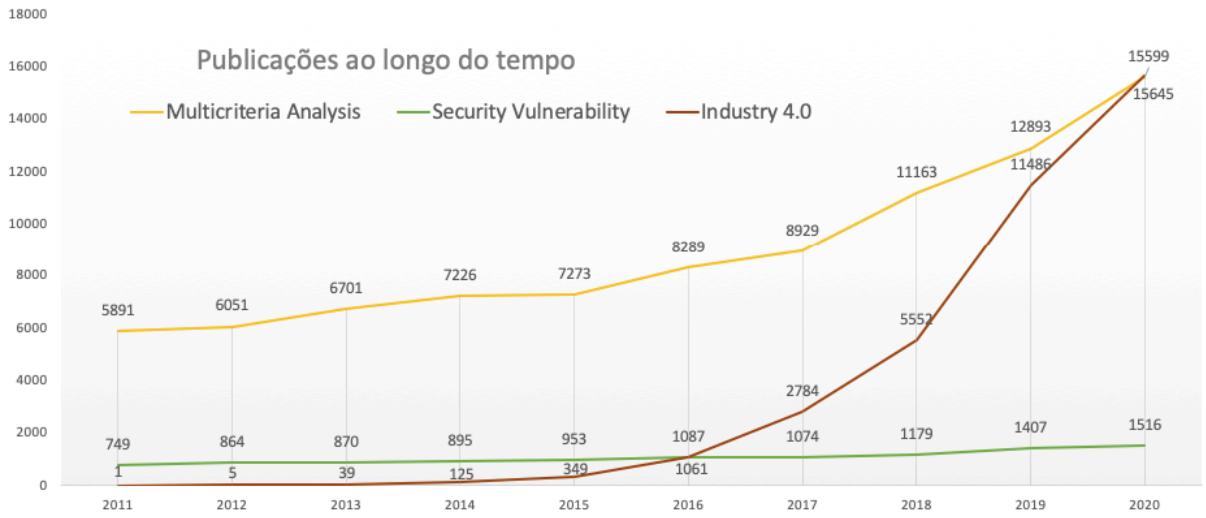

Figura 4 - Publicações sobre *Multicriteria Analysis, Security Vulnerability* e *Industry 4.0* ao longo do tempo, pela base SCOPUS
Fonte: os autores (2021).

Ao longo do tempo, os três temas da pesquisa apresentam crescimento constante, conforme ilustrado pela Figura 4, destacando-se o tema "*industry 4.0*" que apresentou crescimento com tendência exponencial a partir do ano 2015. Entretanto, o termo "*Security Vulnerability*" apresentou pequena variação de crescimento ano após ano.

Aos resultados encontrados foram aplicados os seguintes filtros: somente documentos com acesso livre; somente artigos; e somente idiomas inglês e português. A Tabela 3 apresenta estes resultados e destaca somente os escolhidos, os quais serão analisados para a fase de elegibilidade do PRISMA-P. Desse modo, foram considerados apenas 69 documentos.

Dos 69 resultados, se destacam os dois artigos resultado da intersecção dos grupos "*multicriteria analysis*", "*security vulnerability*" e "*industry 4.0*", os quais são (S. Pandey et al., 2020) e (Sha et al., 2018). Este resultado tão enxuto demonstra a possiblidade de se explorar melhor a utilização de ferramentas de análise multicritério para o tratamento de vulnerabilidades de segurança da informação na indústria 4.0.

Tabela 3
Resultado após a aplicação dos filtros: somente documentos com acesso livre; somente artigos; e somente idiomas inglês e português

Base de pesquisa	Grupo	Resumo dos termos consultados	Docs.
SCOPUS	B e C	*"industry 4.0" AND "computer security vulnerability"*	34
	A e C	*"multicriteria analysis" AND "computer security vulnerability"*	23
	A e B e C	*"multicriteria analysis" AND "industry 4.0" AND "computer security vulnerability"*	2
Web of Science	E e F	*"industry 4.0" AND "computer security vulnerability"*	10
Total			**69**

Fonte: os autores (2021).

A última fase do protocolo PRISMA-P que é a da inclusão, considerou apenas 34 artigos. Os artigos foram analisados integralmente para a produção dos resultados. Esta análise foi dividida em duas partes: uma para o grupo de "*industry 4.0*" e "*computer security vulnerability*" e outra para "*multicriteria analysis*" e "*computer security vulnerability*". A próxima seção tratará da análise do resultado da combinação dos grupos "*industry 4.0*" e "*computer security vulnerability*".

4.2 Resultados dos grupos "*industry 4.0*" e "*computer security vulnerability*"

Os resultados encontrados ao combinar os grupos "*industry 4.0*" e "*computer security vulnerability*" resultaram 34 artigos. Estes documentos se originam de 26 fontes científicas diferentes e 28 deles são artigos enquanto seis são artigos de conferência. A média de citações por documento é de 10,21 citações e a média de anos da publicação é de 1,74 anos, variando de 2016 a 2020. Este resultado demonstra quão emergente está o tema, apesar dos filtros iniciais considerarem o período de 2011 a 2020. Os autores mais relevantes são Butun, I, Fernández-Caramés, TM, Fraga-Lamas, P e Maple, C.

Com a ferramenta Biblioshine da biblioteca Bibliometrix foi possível produzir o mapa temático desses 34 artigos ilustrado a seguir na Figura 5. Ao aplicar um algoritmo de clusterização na rede de palavras chaves, é possível destacar diferentes temas de um dado domínio. Cada cluster/tema pode ser representado em um ponto particular conhecido como mapa temático ou estratégico. A centralidade pode ser lida como a importância do tema para o campo de pesquisa inteiro enquanto a densidade como uma medida do desenvolvimento do tema. No caso da Figura 5, é possível ver que os temas encontrados estão, na sua maioria, no quadrante "*motor theme*". Os nomes das bolhas representam o seu *cluster*, enquanto o seu

tamanho é proporcional ao número de ocorrências das palavras. As posições das bolhas são definidas de acordo com o cluster de Callon de densidade e centralidade.

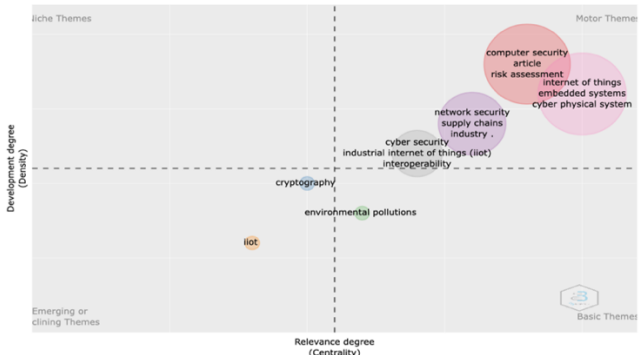

Figura 5 - Mapa temático dos grupos "*industry 4.0*" e "*computer security vulnerability*"
Fonte: os autores (2021).

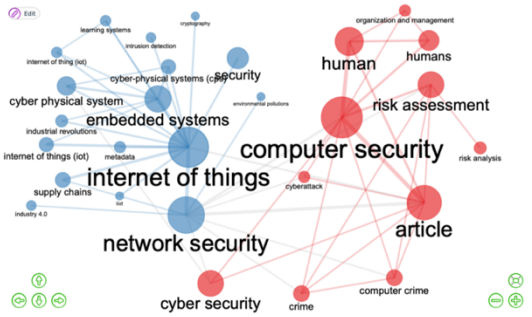

Figura 6 - Rede de co-ocorrência dos grupos "*industry 4.0*" e "*computer security vulnerability*"
Fonte: os autores (2021).

Na Figura 6 observa-se a estrutura conceitual de rede de co-ocorrência das palavras chaves dos artigos selecionados. Os itens centrais e maiores representam os de maior importância e ser relacionam entre si. As bolhas maiores têm maior número de citações enquanto os links entre elas também apresentam diferenças de espessura indicando maior ligação entre os temas. As cores representam os clusters que cada palavra pertence.

Entre as palavras chaves mais relevantes encontradas nos textos dos 34 documentos, as duas mais relevantes são "*internet of things*" e "*computer security*" e se encontram dentro dos resultados das palavras chaves "*industry 4.0*" "*security vulnerability*", respectivamente.

4.3 Resultados dos grupos "*multicriteria analysis*" e "*computer security vulnerability*"

A combinação dos grupos "*multicriteria analysis*" e "*computer security vulnerability*" resultaram em 23 artigos, sendo cada um deles de uma fonte diferente. A média de citações por documento é de 19,62 e a média de anos da publicação é de 3,29, variando de 2012 a 2020. Este resultado demonstra quão emergente está o tema. Os autores mais relevantes são Agrawal, A, Khan, RA, Kumar, R e Alenezi, M.

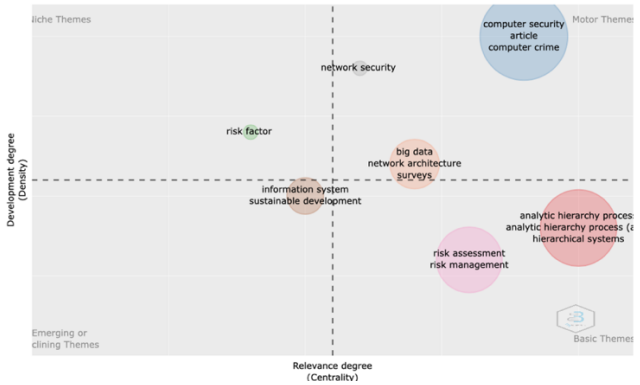

Figura 7 - Mapa temático para os grupos "*multicriteria analysis*" e "*computer security vulnerability*"
Fonte: os autores (2021).

Figura 8 - Rede de co-ocorrência para os grupos "*multicriteria analysis*" e "*computer security vulnerability*"
Fonte: os autores (2021).

O mapa temático desses 23 artigos pode ser observado na Figura 7, trazido pelo *Bibliometrix*. É possível ver que os temas encontrados estão, na sua maioria, distribuídos nos quadrantes "*motor theme*" e "*basic themes*", como "*computer security*"/"*big data*" e "*analytic hierarchy process"/* "*risk assessment*", respectivamente.

A rede de co-ocorrência deste grupo é ilustrada pela Figura 8. Entre as palavras mais relevantes estão: "*risk assessment*", "*analytic hierarchy process*", "*computer security*" e "*risk management*". Observam-se três clusters na rede de co-ocorrência, relacionando entre si apenas "*risk assessment*" e "*computer security*". Estes resultados serão condizentes com os resultados dos 34 artigos para a elaboração da lista de possíveis critérios para tratamento de vulnerabilidades de segurança da informação na Indústria 4.0.

4.4 Possíveis critérios e subcritérios encontrados para análise multicritério no tratamento de vulnerabilidades de segurança da informação na indústria 4.0

Após a leitura dos 34 artigos finais, foi possível correlacionar os achados demonstrados na bibliometria através da utilização do *Bibliometrix* e demonstrado nas seções anteriores. Desse modo, foi produzida uma lista de possíveis critérios e subcritérios que poderiam ser considerados para análise multicritério no tratamento de vulnerabilidades de segurança da informação na Indústria 4.0.

O resultado desse trabalho pode ser observado na Tabela 4, que contém as colunas Critérios, Subcritérios e Trabalhos relacionados, esta última contém as referências nos trabalhos que utilizaram os termos escolhidos nos critérios e subcritérios.

Tabela 4
Critérios e subcritérios encontrados na literatura pesquisada

Critérios	Subcritérios	Trabalhos relacionados
Segurança computa-cional	Confiden-cialidade	(Agrawal et al., 2020; Ankele et al., 2019; Butun et al., n.d., 2020; Dimitriadis et al., 2020; Kim et al., 2020; Lara et al., 2020; Liang et al., 2019; Luo et al., 2015; Murch et al., 2018; Ratasich et al., 2019; Samaila et al., 2020; Sun & Liu, 2012; Willing et al., 2020)
	Integridade	(Agrawal et al., 2019; Ankele et al., 2019; Bolbot et al., 2020; Butun et al., n.d., 2020; Dimitriadis et al., 2020; Kim et al., 2020; Lara et al., 2020; Liang et al., 2019; Luo et al., 2015; Mohamed et al., 2020; Moraitis et al., 2020; Ratasich et al., 2019; Sun & Liu, 2012; Willing et al., 2020)
	Disponi-bilidade	(Agrawal et al., 2019, 2020; Al-Mhiqani et al., 2018; Bolbot et al., 2020; Butun et al., n.d., 2020; Dimitriadis et al., 2020; Liang et al., 2019; Luo et al., 2015; Mohamed et al., 2020; Ratasich et al., 2019; Sun & Liu, 2012; Willing et al., 2020)
	Autenticação	(Ankele et al., 2019; Bolbot et al., 2020; Butun et al., n.d.; Fernández-Caramés & Fraga-Lamas, 2020a; He et al., 2016; Lara et al., 2020; Samaila et al., 2020)
	Fatores humanos	(Ani et al., 2019; Bolbot et al., 2020; Fekete & Rhyner, 2020; Kim et al., 2020; Liang et al., 2019; Mohamed et al., 2020; Samaila et al., 2020; Walker-Roberts et al., 2020)
	Cyber ataque	(Al-Mhiqani et al., 2018; Ani et al., 2019; Ankele et al., 2019; Anuar et al., 2013; Bolbot et al., 2020; Butun et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020a, 2020b; Kim et al., 2020; Lara et al., 2020; Luo et al., 2015; Mohamed et al., 2020; Moraitis et al., 2020; Mourtzis et al., 2019; Prislan et al., 2020; Ratasich et al., 2019; Samaila et al., 2020; Sun & Liu, 2012; Walker-Roberts et al., 2020; Willing et al., 2020)
	Avaliação de vulnerabilidade	(Al-Mhiqani et al., 2018; Ani et al., 2019; Bolbot et al., 2020; Butun et al., n.d., 2020; Fekete & Rhyner, 2020; Fernández-Caramés & Fraga-Lamas, 2020a; Kim et al., 2020; Liang et al., 2019; Luo et al., 2015; Mourtzis et al., 2019; Murch et al., 2018; Ratasich et al., 2019; Russo et al., 2019; Samaila et al., 2020; Yan et al., 2020)

Critérios	Subcritérios	Trabalhos relacionados
Criptografia		(Ankele et al., 2019; Lara et al., 2020; Samaila et al., 2020)
Impacto nos ativos	Criticidade	(Anuar et al., 2013; Luo et al., 2015)
	Capacidade de manutenção	(Agrawal et al., 2020; Ani et al., 2019; Anuar et al., 2013; Luo et al., 2015; Prislan et al., 2020; Sun & Liu, 2012)
	Capacidade de substituição	(Ani et al., 2019; Anuar et al., 2013)
	Confiabilidade	(Agrawal et al., 2020; Anuar et al., 2013; Luo et al., 2015)
	Dano colateral	(Luo et al., 2015)
	Controle e remediação	(Ani et al., 2019; Anuar et al., 2013; Luo et al., 2015; Prislan et al., 2020; Walker-Roberts et al., 2020)
Probabi-lidade de ameaça e vulnera-bilidade	Severidade	(Agrawal et al., 2020; Anuar et al., 2013; Mendonça Silva et al., 2016; A. K. Pandey & Alsolami, n.d.)
	Explorabilidade	(Anuar et al., 2013; Luo et al., 2015; A. K. Pandey & Alsolami, n.d.; Sun & Liu, 2012)
	Sensibilidade	(Anuar et al., 2013; Luo et al., 2015; Yan et al., 2020)
	Similaridade e distribuição de alvo	(Agrawal et al., 2020; Anuar et al., 2013; Luo et al., 2015; Sun & Liu, 2012)
	Frequência	(Anuar et al., 2013)
Riscos	Avaliação de risco	(Ani et al., 2019; Anuar et al., 2013; Bolbot et al., 2020; Dimitriadis et al., 2020; Kim et al., 2020; Mendonça Silva et al., 2016; Mohamed et al., 2020; Moraitis et al., 2020; Mourtzis et al., 2019; S. Pandey et al., 2020; Russo et al., 2019; Willing et al., 2020; Yan et al., 2020)
	Probabilid. de evento/ ameaça	(Anuar et al., 2013; A. K. Pandey & Alsolami, n.d.; Sun & Liu, 2012; Walker-Roberts et al., 2020)
	Gestão de risco	(Anuar et al., 2013; Bolbot et al., 2020; Dimitriadis et al., 2020; Fekete & Rhyner, 2020; Kim et al., 2020; Mohamed et al., 2020; Prislan et al., 2020; Russo et al., 2019)
	Impacto do evento/ameaça	(Anuar et al., 2013)
Segurança de rede	Cadeias de suprimento	(Fekete & Rhyner, 2020; He et al., 2016; Moraitis et al., 2020; Murch et al., 2018)
	Sistemas de segurança	(Ankele et al., 2019; Butun et al., 2020; Lara et al., 2020; Luo et al., 2015; Mohamed et al., 2020; A. K. Pandey & Alsolami, n.d.; Russo et al., 2019; Samaila et al., 2020)
	Interopera-bilidade	(Agrawal et al., 2019; Butun et al., 2020; Dimitriadis et al., 2020; Modarresi & Symons, 2020; Ratasich et al., 2019; Willing et al., 2020)
	Ameaças de segurança	(Al-Mhiqani et al., 2018; Ankele et al., 2019; Bolbot et al., 2020; Butun et al., 2020; Dimitriadis et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020b; He et al., 2016; Kim et al., 2020; Lara et al., 2020; Liang et al., 2019; A. K. Pandey & Alsolami, n.d.; Ratasich et al., 2019; Russo et al., 2019; Walker-Roberts et al., 2020; Yan et al., 2020)
Internet das Coisas (iot)	Sistemas embarcados	(Fernández-Caramés & Fraga-Lamas, 2020a; He et al., 2016; Kim et al., 2020; Lara et al., 2020; Liang et al., 2019; Mohamed et al., 2020; Ratasich et al., 2019)
	Sistemas cyber-físicos (cps)	(Al-Mhiqani et al., 2018; Ankele et al., 2019; Bolbot et al., 2020; Butun et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020b; He et al., 2016; Liang et al., 2019; Mohamed et al., 2020; Moraitis et al., 2020; Mourtzis et al., 2019; Ratasich et al., 2019)
	Internet das coisas industrial	(Ani et al., 2019; Ankele et al., 2019; Butun et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020b; He et al., 2016; Mendonça Silva et al., 2016; Mourtzis et al., 2019; Samaila et al., 2020)
	Big data e data mining	(Ankele et al., 2019; Fernández-Caramés & Fraga-Lamas, 2020b; He et al., 2016; Liang et al., 2019; Mendonça Silva et al., 2016; Murch et al., 2018)

Critérios	Subcritérios	Trabalhos relacionados
	Aquisição de dados e privacidade	(Butun et al., n.d., 2020; He et al., 2016; Lara et al., 2020; Liang et al., 2019; Mohamed et al., 2020; Mourtzis et al., 2019; Murch et al., 2018; Samaila et al., 2020; Yan et al., 2020)
	Comunicação	(Ankele et al., 2019; Bolbot et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020b; He et al., 2016; Modarresi & Symons, 2020; Mohamed et al., 2020; Mourtzis et al., 2019; Ratasich et al., 2019)
Sistemas de informação	Sistemas de aprendizagem	(Agrawal et al., 2019; Ankele et al., 2019; Fernández-Caramés & Fraga-Lamas, 2020a, 2020b; Liang et al., 2019; Mohamed et al., 2020)
	Organização e gestão	(Ani et al., 2019; Dimitriadis et al., 2020; Fernández-Caramés & Fraga-Lamas, 2020a, 2020b; He et al., 2016; Mendonça Silva et al., 2016; Mohamed et al., 2020; Prislan et al., 2020; Russo et al., 2019; Willing et al., 2020)

Fonte: os autores (2021).

Para ilustrar os critérios e subcritérios de maneira gráfica foi elaborada, com a ferramenta Miro, a Figura 9 contendo todo o conteúdo da Tabela 4.

Figura 9 – Proposta de critérios e subcritérios de vulnerabilidades de segurança da informação na indústria 4.0 encontrados na literatura
Fonte: os autores (2021).

5. Considerações finais

Este trabalho teve como objetivo verificar na literatura quais os possíveis critérios a serem considerados em um método de análise multicritério para a tomada de decisão no tratamento de vulnerabilidades de segurança da informação na indústria 4.0. Com a realização da pesquisa bibliométrica foi possível identificar a quantidade de publicações existentes que abordam os temas de vulnerabilidades de segurança da informação das tecnologias empregadas na indústria 4.0.

A bibliometria permitiu identificar que o tema vem ganhando bastante destaque, pois a indústria 4.0 cresce em um ritmo acelerado, e de mesma forma, os crimes cibernéticos tornam-se cada vez mais aperfeiçoados, o que reforça a necessidade de constante aprimoramento nos mecanismos de segurança da informação nas tecnologias empregadas na indústria 4.0.

O progresso da Indústria 4.0 e *Internet of Things* também faz aumentar as vulnerabilidades de segurança da informação, tornando mais complexo priorizá-las e tomar decisões. Um método de análise multicritério como o *Analytic Hierarchy Process (*AHP) é uma proposta de solução.

A pesquisa bibliométrica utilizou as bases SCOPUS e Web of Science, entre 2011 e 2020, relacionando as palavras-chaves "*industry 4.0*", "*security vulnerability*" e "*multicriteria analysis*", identificou nos resultados os critérios e subcritérios relacionados a vulnerabilidades de segurança da informação na indústria 4.0.

O resultado da pesquisa identificou oito critérios e trinta e quatro subcritérios relacionados ao tratamento das vulnerabilidades de segurança da informação da indústria 4.0 que poderiam ser avaliados para aplicação de um método de análise multicritério, como o AHP, devido a hierarquização dos critérios e a sua popularidade tanto no meio acadêmico quanto no empresarial, auxiliando a gestão da segurança. Desta forma, foi possível concluir que um método multicritério pode ter um papel importante, pois auxilia na tomada de decisão desse ambiente de complexidade e múltiplos critérios.

Os critérios e subcritérios encontrados na literatura podem ter papel importante em auxiliar a tomada de decisão em um ambiente de complexidade e múltiplos critérios das vulnerabilidades de segurança da informação, contribuindo na proteção contra crimes cibernéticos da Indústria 4.0.

Como trabalhos futuros, os resultados encontrados permitem conduzir novas pesquisas para a validação, acréscimo ou remoção dos critérios e subcritérios identificados na literatura através de survey e também a demonstração da aplicação prática do método AHP com os critérios e subcritérios identificados neste artigo.

Referências

Agrawal, A., Alenezi, M., Kumar, R., & Khan, R. A. (2020). A unified fuzzy-based symmetrical multi-criteria decision-making method for evaluating sustainable-security of web applications. *Symmetry*, *12*(3). https://doi.org/10.3390/sym12030448

Agrawal, A., Zarour, M., Alenezi, M., Kumar, R., & Khan, R. A. (2019). Security durability assessment through fuzzy analytic hierarchy process. *PeerJ Computer Science*, *2019*(9). https://doi.org/10.7717/peerj-cs.215

Alcácer, V., & Cruz-Machado, V. (2019). Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems. In *Engineering Science and Technology, an International Journal* (Vol. 22, Issue 3, pp. 899–919). Elsevier B.V. https://doi.org/10.1016/j.jestch.2019.01.006

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Zaheera, Z., Abidin, N., Salih, A., & Abdulkareem, H. (2018). Cyber-Security Incidents: A Review Cases in Cyber-Physical

Systems. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 9, Issue 1). www.ijacsa.thesai.org

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Ankele, R., Marksteiner, S., Nahrgang, K., & Vallant, H. (2019, August 26). Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3339252.3341482

Annual, C., & Report, I. (2018). *White paper Cisco public*.

Anuar, N. B., Papadaki, M., Furnell, S., & Clarke, N. (2013). Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). *Security and Communication Networks*, *6*(9), 1087–1116. https://doi.org/10.1002/sec.673

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, *131*. https://doi.org/10.1016/j.ssci.2020.104908

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys and Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Butun, I., Sari, A., & Patrik¨osterberg, P. P. (n.d.). *Security Implications of Fog Computing on the Internet of Things*.

CISA. (2021, July 20). *Significant Historical Cyber-Intrusion Campaigns Targeting ICS*. CISA.

de Almeida, P. S. (2019). *Indústria 4.0: Princípios básicos, aplicabilidade e implantação*. Saraiva Educação.

Dimitriadis, A., Flores, J. L., Kulvatunyou, B., Ivezic, N., & Mavridis, I. (2020). Ares: Automated risk estimation in smart sensor environments. *Sensors (Switzerland)*, *20*(16), 1–19. https://doi.org/10.3390/s20164617

Fekete, A., & Rhyner, J. (2020). Sustainable digital transformation of disaster risk—integrating new types of digital social vulnerability and interdependencies with critical infrastructure. *Sustainability (Switzerland)*, *12*(22), 1–18. https://doi.org/10.3390/su12229324

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020a). Teaching and learning IoT cybersecurity and vulnerability assessment with shodan through practical use cases. *Sensors (Switzerland)*, *20*(11). https://doi.org/10.3390/s20113048

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020b). Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era. *Applied Sciences (Switzerland)*, *10*(16). https://doi.org/10.3390/app10165607

Galegale, N. V., Fontes, E. L. G., & Galegale, B. P. (2017). Uma contribuição para a segurança da informação: Um estudo de casos múltiplos com organizações brasileiras. *Perspectivas Em Ciencia Da Informacao*, *22*(3), 75–97. https://doi.org/10.1590/1981-5344/2866

Guglielmetti, F. R., Augusto, F., Marins, S., Antonio, V., & Salomon, P. (2003). Comparação Teórica entre Métodos de Auxílio à Tomada de Decisão por Múltiplos Critérios. *XXXV SBPO*.

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016). The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities forEvolutionary Computing & Other ComputationalIntelligence. *IEEE Computational Intelligence Society*.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01145-7

Lara, E., Aguilar, L., Sanchez, M. A., & García, J. A. (2020). Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial internet of things. *Sensors (Switzerland)*, *20*(2). https://doi.org/10.3390/s20020501

Leite, I. M. S., & Freitas, F. F. T. (2012). Análise Comparativa dos Métodos de Apoio Multicritério a Decisão: AHP, ELECTRE e PROMETHEE. *XXXII Encontro Nacional de Engenharia de Produção - ENEGEP*.

Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access*, *7*, 158126–158147. https://doi.org/10.1109/ACCESS.2019.2948912

Luo, S., Dong, M., Ota, K., Wu, J., & Li, J. (2015). A security assessment mechanism for software-defined networking-based mobile networks. *Sensors (Switzerland)*, *15*(12), 31843–31858. https://doi.org/10.3390/s151229887

Marins, C. S., Souza, D. de O., & Barros, M. da S. (2009). O Uso do Método de Análise Hierárquica (AHP) na Tomada de Decisões Gerenciais – Um Estudo de Caso. *XLI SBPO*.

Mendonça Silva, M., Poleto, T., Silva, L. C. E., Henriques De Gusmao, A. P., & Cabral Seixas Costa, A. P. (2016). A grey theory based approach to big data risk management using FMEA. *Mathematical Problems in Engineering*, *2016*. https://doi.org/10.1155/2016/9175418

Modarresi, A., & Symons, J. (2020). Technological Heterogeneity and Path Diversity in Smart Home Resilience: A Simulation Approach. *Procedia Computer Science*, *170*, 177–186. https://doi.org/10.1016/j.procs.2020.03.023

Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2020). Cyber–physical systems forensics: Today and tomorrow. *Journal of Sensor and Actuator Networks*, *9*(3). https://doi.org/10.3390/JSAN9030037

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L. A., Estarli, M., Barrera, E. S. A., Martínez-Rodríguez, R., Baladia, E., Agüero, S. D., Camacho, S., Buhring, K., Herrero-López, A., Gil-González, D. M., Altman, D. G., Booth, A., … Whitlock, E. (2016). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Revista Espanola de Nutricion Humana y Dietetica*, *20*(2), 148–160. https://doi.org/10.1186/2046-4053-4-1

Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., & Makropoulos, C. (2020). Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. *Journal of Environmental Engineering*, *146*(9), 04020108. https://doi.org/10.1061/(asce)ee.1943-7870.0001765

Mourtzis, D., Angelopoulos, K., & Zogopoulos, V. (2019). Mapping vulnerabilities in the industrial internet of things landscape. *Procedia CIRP*, *84*, 265–270. https://doi.org/10.1016/j.procir.2019.04.201

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology*, *6*(APR). https://doi.org/10.3389/fbioe.2018.00039

Pandey, A. K., & Alsolami, F. (n.d.). Malware Analysis in Web Application Security: An Investigation and Suggestion. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 11, Issue 7). www.ijacsa.thesai.org

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042

Phu, T. N., Dang, K. H., Quoc, D. N., Dai, N. T., & Binh, N. N. (2019). A Novel Framework to Classify Malware in MIPS Architecture-Based IoT Devices. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/4073940

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, *15*(9 September). https://doi.org/10.1371/journal.pone.0238739

PRODANOV, C. C., & de FREITAS, E. Cesar. (2013). *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico* (2ª). Editora Feevale.

Ratasich, D., Khalid, F., Geissler, F., Grosu, R., Shafique, M., & Bartocci, E. (2019). A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems. *IEEE Access*, *7*, 13260–13283. https://doi.org/10.1109/ACCESS.2019.2891969

Russo, P., Caponi, A., Leuti, M., & Bianchi, G. (2019). A web platform for integrated vulnerability assessment and cyber risk management. *Information (Switzerland)*, *10*(7). https://doi.org/10.3390/info10070242

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *Int. J. Services Sciences*, *1*(1), 83–98.

SAATY, T. L. (2014). *Toma de decisiones para líderes*. RWS Publications.

Samaila, M. G., Sequeiros, J. B. F., Simoes, T., Freire, M. M., & Inacio, P. R. M. (2020). IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space. *IEEE Access*, *8*, 16462–16494. https://doi.org/10.1109/ACCESS.2020.2965925

Sha, L., Xiao, F., Chen, W., & Sun, J. (2018). IIoT-SIDefender: Detecting and defense against the sensitive information leakage in industry IoT. *World Wide Web*, *21*(1), 59–88. https://doi.org/10.1007/s11280-017-0459-8

Sommerville, I. (2011). *Engenharia de software* (Vol. 19). Pearson Education.

Sun, Z., & Liu, M. (2012). Application of Fuzzy AHP Method in the Effect Evaluation of Network Attack. *2nd International Conference on Electronic & Mechanical Engineering and Information Technology*.

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, *76*(4), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9

Willing, M., Dresen, C., Haverkamp, U., & Schinzel, S. (2020). Analyzing medical device connectivity and its effect on cyber security in german hospitals. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01259-y

Wollmann, D., Steiner, M. T. A., Vieira, G. E., & Steiner, P. A. (2011). Utilização da técnica AHP para análise da concorrência entre operadoras de planos de saúde. *GEPROS Gestão Da Produção, Operações e Sistemas*, *6*(4), 111–124. https://doi.org/https://doi.org/10.15675/gepros.v0i4.901

Yan, X., Fan, Y., Lee, H. H., & Qiu, R. (2020). Research on personal information risk assessment model in smart cities. *Tehnicki Vjesnik*, *27*(5), 1403–1409. https://doi.org/10.17559/TV-20190104101416

Zardari, N. H., Ahmed, K., Shirazi, S. M., & Yusop, Z. bin. (2015). *Weighting Methods and their Effects on Multi-Criteria Decision Making Model Outcomes in Water Resources Management*. SPRINGER BRIEFS IN WATER SCIENCE AND TECHNOLOGY . http://www.springer.com/series/11214

Zhou, P., Ang, B. W., & Poh, K. L. (2006). Decision analysis in energy and environmental modeling:An update. *Energy*, *31*(14), 2604–2622. https://doi.org/10.1016/j.energy.2005.10.023