EXACTA Engenharia de Produção eISSN 1983-9308

Artigos

https://doi.org/10.5585/exactaep.2022.21683

Check for updates

Vulnerabilidades de Segurança da Informação na Indústria 4.0: Proposição de Critérios para o uso de Análise Multicritério

Computer Security Vulnerabilities in Industry 4.0: Proposed Criteria for Using Multi-Criteria Analysis

Recebido: 22 fev. 2022
Aprovado: 31 ago. 2022
Versão do autor aceita publicada online: 31 ago. 2022
Publicado online: 13 out. 2022

Como citar esse artigo - American Psychological Association (APA):

Sotolani, R. S., Menezes, I. de A. C., Galegale, N. V., & Feitosa, M. D. (abr./jun. 2024). Vulnerabilidades de segurança da informação na indústria 4.0: proposição de critérios para o uso de análise multicritério. *Exacta, 22*(2), p. 491-522. https://doi.org/10.5585/exactaep.2022.21683

Submeta seu artigo para este periódico

Processo de Avaliação: *Double Blind Review*

Editor: Dr. Luiz Fernando Rodrigues Pinto

Dados Crossmark

EXACTA Engenharia de Produção eISSN 1983-9308

https://doi.org/10.5585/exactaep.2022.21683

Processo de Avaliação: *Double Blind Review*
Editor: Prof. Dr. Luiz Fernando Rodrigues Pinto
Recebido em: 22 fev. 2022
Aprovado em: 31 ago. 2022

Artigos

Vulnerabilidades de Segurança da Informação na Indústria 4.0: Proposição de Critérios para o uso de Análise Multicritério

Computer Security Vulnerabilities in Industry 4.0: Proposed Criteria for Using Multi-Criteria Analysis

Rodrigo Silva Sotolani, Isabella de Araújo Cionini Menezes, Napoleão Verardi Galegale[1], Marcelo Duduchi Feitosa[2]

[1] Pontifícia Universidade Católica de São Paulo – PUC/SP - São Paulo, SP – Brasil. Doutor em Controladoria e Contabilidade

[2] Doutorado em Psicologia (Psicologia Experimental). Centro Estadual de Educação Tecnológica Paula Souza - São Paulo, SP - Brasil

Nota dos autores

Autores declaram que não há conflito de interesses.

Resumo

O progresso da Indústria 4.0 tem relevância cada vez maior, considerando o aumento das vulnerabilidades de segurança da informação e da complexidade em priorizá-las na tomada de decisões. Observou-se uma lacuna de pesquisa neste tema. O objetivo deste artigo é identificar critérios na literatura científica que possam ser utilizados em um método de análise multicritério, visando a priorização de tratamento de vulnerabilidades de segurança na Indústria 4.0. Um método como o *Analytic Hierarchy Process (*AHP) é uma proposta de solução. A metodologia utilizada foi a revisão exploratória da literatura encontrada nas bases SCOPUS e *Web of Science*. O resultado identificou oito critérios e 34 subcritérios relacionados ao tratamento das vulnerabilidades de segurança na Indústria 4.0. A contribuição teórica vai ao encontro do preenchimento da lacuna em relação a este tema. A contribuição prática permite que organizações da Industria 4.0 apliquem os critérios identificados na análise multicritério para o tratamento das suas vulnerabilidades de segurança e assim alcancem melhores decisões para a entrega de produtos e serviços contribuindo para sociedade. Pesquisas futuras podem ser conduzidas por meio de entrevistas ou questionários para validação com profissionais da área dos critérios encontrados, como também a aplicação prática do método AHP.

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

Computer Security Vulnerabilities in Industry 4.0: Proposed Criteria for Using Multi-Criteria Analysis

Abstract

The progress of Industry 4.0 is increasingly relevant, considering the rise in computer security vulnerabilities and the complexity of prioritizing them in decision-making. There was a research gap on this topic. The article's objective is to identify criteria in the scientific literature that can be used in a multi-criteria analysis method to prioritize the treatment of security vulnerabilities in Industry 4.0. A method like AHP (Analytic Hierarchy Process is a proposed solution. The methodology was an

exploratory review in the SCOPUS and Web of Science databases. The result identified eight criteria and 34 sub-criteria related to the treatment of security vulnerabilities in Industry 4.0. The theoretical contribution goes towards filling the gap in relation to this topic. The practical contribution allows Industry 4.0 organizations to apply the criteria identified in the multi-criteria analysis to address their security vulnerabilities and thus reach better decisions for the delivery of products and services contributing to society. Future research can be conducted through interviews or surveys for professional validation of the criteria found, as well as the practical application of the AHP method.

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

Introdução

Os últimos anos tem mostrado um crescimento no número de artigos produzidos referentes à Indústria 4.0. Em base de dados como a SCOPUS, de 2016 até 2020, a produção de artigos sobre este tema subiu de cerca de mil para quase dezesseis mil. Uma revolução sem precedentes está sendo possível para os sistemas ciber-físicos e seus usuários por meio do rápido desenvolvimento da quarta revolução industrial, da Internet das Coisas (IoT) e da computação em nuvem, uma vez que, conforme Annual & Report (2018), o número de dispositivos interconectados é estimado a ser três vezes a população mundial, e chegará a mais de 29 bilhões em 2023.

O impacto no cotidiano das pessoas de uma quantidade tão grande de dispositivos conectados irá alcançar diversos domínios de aplicação, entre eles, cidades e casas inteligentes, meios de transporte, saúde, energia, entre outros. Paralelamente ao avanço da IoT, a segurança da informação teve um maior destaque, uma vez que qualquer dispositivo dessa imensa rede conectada, pode se tornar um espião a qualquer hora e em qualquer lugar. Essa ampliação da superfície de ataques, aumenta os riscos de vulnerabilidades e falhas tecnológicas nos dispositivos conectados aos Sistemas Cyber-Físicos (CPS) (Modarresi & Symons, 2020). Observa-se uma lacuna de

pesquisa sobre a utilização de métodos para a priorização de quais vulnerabilidades de segurança tratar primeiro no contexto da Indústria 4.0.

Motivados por questões financeiras, mas também por razões políticas, ideológicas, e por protestos ou espionagem, o número de *malwares* em dispositivos IoT cresceu exponencialmente desde a última década. Por exemplo, no primeiro semestre de 2018 foram detectados pelo Kaspersky IoT Lab mais de cento e vinte mil instâncias de *malwares* IoT (Phu *et al*., 2019).

Para o agravamento deste cenário, estes dispositivos têm, em sua maioria, uma longa vida útil e nem todos recebem as atualizações de *patches* (pacotes) de segurança regularmente, ou nunca o fazem, podendo resultar em consequências graves para vidas humanas, produtividade empresarial e segurança nacional devido aos possíveis ataques maliciosos. Os recursos limitados de computação, comunicação e processamento de alguns dispositivos da indústria inviabilizam a aplicação da criptografia de dados clássica e dos protocolos de comunicação seguros (Walker-Roberts *et al*., 2020).

As vulnerabilidades que são descobertas ficam mais complexas de gerenciar, tornando difícil a tarefa de avaliar a quais delas se deve priorizar (Galegale *et al*., 2017). Muitos critérios devem ser considerados em um ambiente complexo como o da Indústria 4.0, cujos dispositivos, redes, integrações, conexões e fatores humanos, necessitam avaliação em conjunto para a tomada de uma decisão, ou seja, uma análise de multicritérios. A análise multicritério é uma solução que se vislumbra para apoiar a tomada de decisão no gerenciamento das vulnerabilidades de segurança da informação na Indústria 4.0. Além disso, foi possível constatar uma lacuna de pesquisa nesta área.

Um dos modelos de análise multicritérios amplamente utilizados desde a década de 70, devido sua facilidade de aplicação é o *Analytic Hierarchy Process* (AHP), do pesquisador Thomas L. Saaty. Para Marins, Souza e Barros (2009), o AHP se destaca por auxiliar na resolução de conflitos e apoiar a tomada de decisão ao lidar com problemas com múltiplos níveis ou critérios.

A questão norteadora da pesquisa deste artigo é “Quais os critérios relevantes encontrados na literatura científica para tratamento das vulnerabilidades de segurança da informação na indústria 4.0 para uso de análise multicritério como o método AHP?”.

O objetivo da pesquisa é a identificação de critérios relevantes na literatura científica para que auxiliem na tomada de decisão por meio de análise multicritério para o tratamento das vulnerabilidades de segurança da informação na indústria 4.0. Para isso, se utilizou a metodologia de revisão exploratória da literatura, apoiando-se no protocolo de pesquisa PRISMA-P.

Referencial teórico

Este capítulo tem como finalidade apresentar o referencial teórico que foi utilizado como base para se atingir os objetivos do trabalho, sendo abordados conceitos referentes a indústria 4.0, vulnerabilidades de segurança da informação, e análise multicritério, em destaque o método AHP.

A abordagem evidencia os trabalhos que apresentam possíveis critérios e subcritérios que podem ser utilizados para o tratamento de vulnerabilidades de segurança da informação na indústria 4.0.

Indústria 4.0

Os sistemas produtivos evoluíram para a era da digital ao longo do crescimento da Indústria 4.0 com a promessa de lidar com os desafios mais atuais dos sistemas de manufatura. Conforme Alcácer e Cruz-Machado (2019), este cenário digital abrange tudo o que pode ser conectado e cria suas respectivas representações virtuais tornando possível a utilização de níveis elevados de automação e de comunicação entre sistemas, *softwares* e fábricas, com o que existe de mais recente em TI, permitindo assim alcançar em tempo real o engajamento de todos os elementos dessa cadeia de valor.

Segundo Almeida (2019), a Indústria 4.0 criou uma tendência de evolução na tecnologia e na integração entre os processos, permitindo que os sistemas produtivos se tornem mais inteligentes e detectem suas carências de produção e necessidades de abastecimento por meio do envolvimento das tecnologias físicas e digitais e da integração das fases de criação de produtos ou processos.

As significantes informações criadas, processadas e manipuladas pelos processos tecnológicos dos sistemas de produção nestes ambientes interconectados, complexos e heterogêneos demandam uma forte camada de segurança da informação observando os seus pilares: integridade, confidencialidade e disponibilidade.

Em um experimento, Walker-Roberts *et al*. (2020) usaram um banco de dados de ciberincidentes para investigar os riscos de incidentes no mundo físico e observaram como resultado que um dos ativos mais comumente atacados era a informação por meio de métodos de abuso de privilégios e que as principais caraterísticas eram as violações internas na própria organização, muitas vezes provenientes de erro humano.

As vulnerabilidades de fluxo de controle que surgiram com a chegada da era da Industria 4.0, da *Internet of Things* (IoT) e da IoT Industrial (IIoT), são importantes meios de detecção de invasão que podem facilmente culminar em um fechamento de sessão remota e sequestro de fluxo de controle baseados em informações sigilosas e confidenciais (Sha *et al*., 2018).

As razões para que dispositivos da Indústria 4.0 e dos Sistemas Ciber-Físicos sejam atacados são diversos. Walker-Roberts *et al*. (2020) exemplificam que alguns dos ataques heurísticos partem do sequestro de dispositivos conectados para torná-los servidores de e-mail de *spam* em massa, ou usá-los como *botnets* (rede de robôs) para executar ataques DDoS (negação de serviço distribuída) ou ainda simplesmente causar a interrupção dos processos de negócios. Um exemplo de ataque de acesso remoto é o sequestro de veículos autônomos e a solicitação de um resgate para devolver o controle do veículo, máquina ou dispositivo médico. (WALKER-ROBERTS *et al*., 2020).

Vulnerabilidades de segurança da informação

À medida que a Indústria 4.0 colabora com o crescimento dos dispositivos conectados à rede, os ataques a estes também se tornam cada vez mais qualificados. Diante deste cenário, é imprescindível que sejam aplicadas as devidas precauções de segurança, para que os atacantes não se aproveitem das vulnerabilidades existentes para fazer o roubo de dados ou mau uso do *hardware* (Sommerville, 2011).

Componentes principais de infraestruturas críticas tornaram-se um grande alvo para ataques cibernéticos. O sistema de controle da rede elétrica da Ucrânia é um exemplo disto, pois devido as vulnerabilidades existentes, cerca de 230 mil pessoas foram atingidas por uma queda de energia causada por um ataque *hacker*. Sem a implementação de controles de segurança eficazes, os invasores podem causar uma série de danos, inclusive a longas distâncias (Walker-Roberts *et al.*, 2020).

Segundo Jang-Jaccard & Nepal (2014), para a execução dos ataques, o *malware* (código malicioso) é um dos meios mais utilizados para a prática do crime cibernético, podendo ocorrer por meio da exploração de vulnerabilidades existentes ou da utilização de características únicas de tecnologias emergentes.

Devido as constantes ameaças à segurança cibernética dos sistemas de controle industrial (ICS) que controlam e operam infraestrutura crítica nos EUA, a CISA e o FBI lançaram uma campanha de conscientização em julho de 2021 a fim de promover a revisão de alertas, publicações e avisos, além da aplicação das ações de mitigação (CISA, 2021).

Análise multicritério

A Indústria 4.0 compõe um segmento de maior complexidade para a segurança da informação, uma vez que envolve muitos fatores, variáveis e critérios que devem ser todos levados em conta quando da identificação da melhor solução, da tomada de decisão e até mesmo da priorização de meios para enfrentar o problema.

A título de exemplo, os seguintes critérios influenciadores de tomada de decisão podem ser citados: o retorno financeiro, a indisponibilidade de um sistema ou serviço, o número de usuários impactados, o prazo para implantação de um projeto, o custo-benefício de um recurso e o grau de eficiência de um processo.

Entre as ferramentas disponíveis para avaliar os possíveis parâmetros de uma decisão, estão o *Multicriteria Decision Making (MCDM)* ou o *Apoio Multicritério a decisão (AMD),* os quais permitem

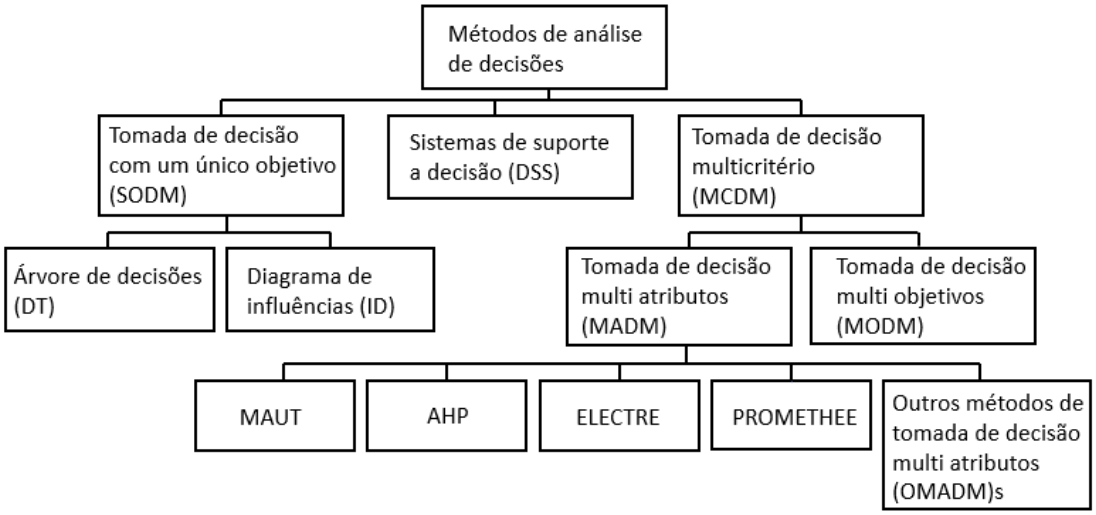
evoluir na solução de um problema de decisão multicritério com muitos critérios conflitantes (Zardari *et al*., 2015).

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

Uma árvore ilustrando as ramificações dos métodos de análise de decisões é exibida na Figura 1 (Zhou *et al*., 2006):

Figura 1

Classificação dos métodos de análise de decisão



Fonte: Adaptado de Zhou et al (2006).

De forma resumida e focando na classe de métodos de tomada de decisão multiatributos, a Figura 1, conforme Zhou *et al* (2006), pode ser descrita:

- 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 tomadores de decisão escolham ou 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 multiatributos (MADM): decisões ao avaliar e priorizar todas as alternativas caracterizadas por vários atributos conflitantes, como exemplo os métodos AHP e ELECTRE.
    - Tomada de decisão multiobjetivo (MODM): são vários modelos de programação matemática que objetivam escolher o "melhor" entre todas as alternativas.

A seção seguinte aborda o método AHP, o qual pode ser classificado como um método de tomada de decisão de multiatributos e que foi selecionado pelos autores deste trabalho como um possível método elegível para a realização de uma avaliação das vulnerabilidades de segurança da informação na Indústria 4.0. O método AHP, que é um exemplo de sucesso no meio científico e empresarial, permitiria a criação de hierarquias desses critérios que foram identificados na literatura.

Analytic Hierarchy Process (AHP)

A decomposição do problema em uma hierarquia de critérios ou atributos que são mais facilmente analisáveis e comparáveis de modo independente é como o processo AHP se inicia, de acordo com Wollmann *et al*. (2011). A partir dessa forma organizada de decompor o problema, a tomada de decisão é realizada da seguinte maneira:

a) Definir o problema e o tipo de conhecimento a ser encontrado;

b) Estruturar a hierarquia com o objetivo da decisão no topo, seguido dos objetivos mais amplos, passando pelos níveis intermediários até o nível mais baixo;

c) Criar matrizes de comparação de pares, comparando os elementos entre si;

d) Ponderar as prioridades no nível imediatamente abaixo a partir das prioridades obtidas nas comparações do nível superior, para cada um dos elementos;

e) Incluir os valores ponderados para cada elemento no nível abaixo até que as prioridades finais da alternativa no nível mais inferior sejam obtidas.

Algumas das principais características do método AHP podem ser descritas, conforme Guglielmetti *et al*. (2003), quanto à entrada de dados (*input*) contém alto grau de julgamento em problemas com muitos critérios/alternativas e não exige processar os dados antes que estes possam ser usados; quanto à saída de dados (*output*), proporciona ranking completo de alternativas e soluções muito refinadas, como também permite a avaliação de coerência dos julgamentos. E finalmente, quanto à interface do tomador de decisão, permite a utilização de decisões em grupo e possibilita o aprendizado sobre a estrutura do problema, como também dispõe de alto grau de facilidade para estruturar o problema e de nível de compreensão para o tomador de decisão à sua forma de trabalho.

Metodologia

Para este estudo, a metodologia adotada foi uma revisão exploratória da literatura, com o objetivo de se verificar quais são os critérios, referentes a vulnerabilidades de segurança da informação na indústria 4.0 são citados pelos autores nas publicações retornadas. Essa pesquisa pode ser enquadrada como uma pesquisa básica quanto à sua natureza, exploratória e descritiva quanto a seu objetivo, sendo seu procedimento científico, uma pesquisa bibliométrica (PRODANOV & DE FREITAS, 2013).

Para a pesquisa bibliométrica e análise bibliográfica, foram realizadas as seguintes atividades: identificação das bases de dados, definição do período e palavras-chave a serem pesquisadas. Com o retorno da pesquisa das publicações encontradas, foi realizado um refinamento destas e posterior análise das publicações que foram selecionadas de acordo com os critérios estabelecidos.

A pesquisa foi conduzida por meio do protocolo PRISMA-P (*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*). A sua utilização possibilitou uma abordagem metodológica e analítica pré-planejada, antes de se iniciar a revisão. Moher *et al* (2016), definem o protocolo PRISMA-P como sendo um guia que auxilia os autores no planejamento de revisões sistemáticas e meta-análises em que um conjunto mínimo de itens devem ser considerados para a realização da pesquisa.

Procedimentos de coleta e tratamento de dados

As bases de dados selecionadas para a coleta foram a SCOPUS e a *Web of Science*, utilizando-se a combinações das seguintes palavras-chaves "*Multicriteria Analysis*", "*Security Vulnerability*" e "*Industry 4.0*", no período entre os anos de 2011 e 2020.

A partir de 1.128 publicações que somaram a combinação das palavras-chave entre si, os seguintes critérios excludentes foram utilizados para a análise das publicações:

i. Publicações que não fossem em português ou inglês;

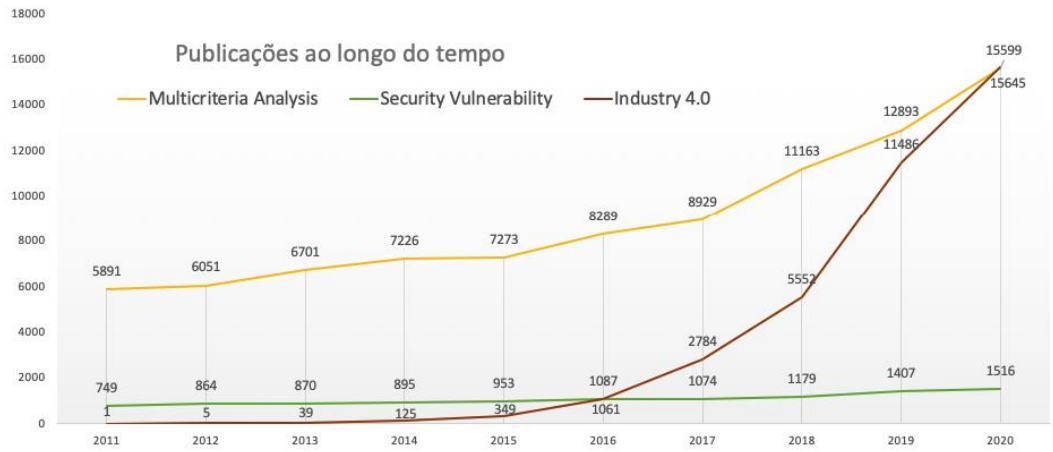
ii. Materiais como monografias, livros, dissertações e teses;

iii. Publicações que foram retornadas pela combinação das palavras-chave "*Multicriteria Analysis*" e "*Industry 4.0*", por não ser escopo para este estudo.

As publicações relacionadas aos temas da pesquisa apresentaram crescimento ao longo do tempo, sendo possível destacar "*Industry 4.0*" e "*Multicriteria Analysis*" que tiveram expressivo aumento principalmente a partir do ano de 2015. **Figura 2**O termo "*Security Vulnerability*", apesar de apresentar uma variação menor no gráfico em comparação aos outros, de 2011 a 2020, teve o crescimento dobrado, mostrando crescimento constante. A Figura 2 mostra a quantidade de publicações por ano na base SCOPUS.

Figura 2

Publicações sobre Multicriteria Analysis, Security Vulnerability e Industry 4.0 ao longo do tempo, pela base SCOPUS



Fonte: resultado da pesquisa.

Tabela 1

Pesquisa bibliométrica realizada nas bases SCOPUS e Web of Science

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 hierarchy 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: Resultado da pesquisa. **AND PUBYEAR > 2010 AND PUBYEAR < 2021. *** Índices=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI Tempo estipulado=2011-2020.

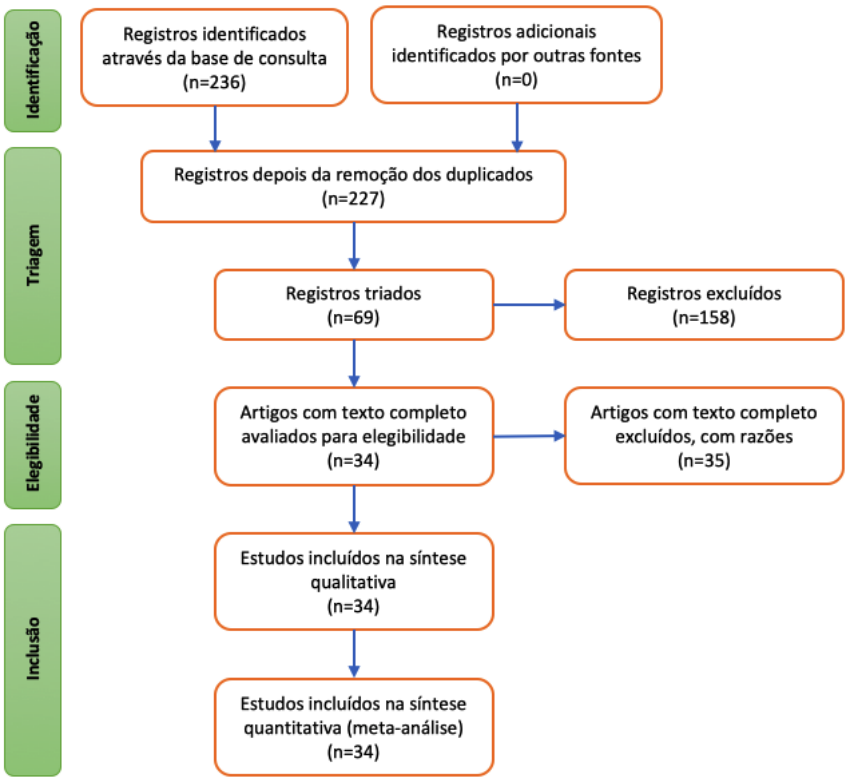
A Tabela 1 detalha os termos e resultados utilizados. Os termos "*Security Vulnerability*", "*Industry 4.0*" e "*Multicriteria Analysis*", retornam uma quantidade significativa de publicações quando consultados individualmente. Estes termos são representados por grupos na Tabela 1, sendo os grupos A, B e C pertencente à base SCOPUS e os grupos D, E F à *Web of Science*.

Com relação a base de dados SCOPUS, ao se relacionar os grupos A e B ("*multicriteria analysis*" AND "*industry 4.0*"), foram obtidas 830 publicações. A relação de B e C ("*industry 4.0*" AND "*security vulnerability*"), retornou 102 artigos. Já A e C ("*multicriteria analysis*" AND "*security vulnerability*"), 100 artigos. Logo, ao se realizar a combinação entre A e B e C ("*multicriteria analysis" AND "industry 4.0" AND "security vulnerability*") foram obtidos apenas três artigos.

Para base de dados da *Web of Science* foram combinados os grupos: D e E ("*multicriteria analysis" AND "industry 4.0*"), como resultado foram obtidos 62 artigos. Os grupos E e F ("*industry 4.0" AND "security vulnerability*") trouxeram 19 publicações. Os grupos D e F ("*multicriteria analysis*" AND "*security vulnerability*") 12 artigos. Já a combinação entre os grupos D e E e F não obteve nenhum artigo.

Figura 3

Aplicação do protocolo PRISMA-P



Fonte: resultado da pesquisa

A Figura 3 detalha a aplicação do protocolo PRISMA-P. Com a remoção dos materiais que atendiam algum dos critérios de exclusão , o protocolo começa com 236 publicações na fase de Identificação. Avançando para a fase de Triagem, foi realizado um refinamento deste material, sendo desconsiderados para a pesquisa 167 artigos, resultando em 69 artigos triados segundo os filtros: (a) remoção de documentos não abertos e (b) remoção de documentos duplicados.

Na fase de Elegibilidade, os resumos das publicações foram lidos visando avaliar o seu alinhamento com o estudo, sendo removidas 35 publicações por não estarem alinhadas com a pesquisa. Sendo as 34 publicações restantes, lidas na íntegra na etapa de Inclusão.

Na última fase do PRISMA-P é realizada a inclusão, na qual foram considerados apenas 34 artigos que foram lidos na íntegra para a apresentação dos resultados. A análise foi realizada em duas partes, sendo uma para o grupo "*industry 4.0*" e "*security vulnerability*" e outra para "*multicriteria analysis*" e "*security vulnerability*".

Análise dos resultados

Esta seção apresenta os resultados obtidos pela pesquisa. Os recursos gráficos, figuras e tabelas apresentados a seguir, visam ilustrar os dados retornados e as informações analisadas nas publicações. A análise dos dados foi realizada por meio do pacote Biblioshine da biblioteca Bibliometrix, uma ferramenta de código aberto desenvolvida na linguagem R, que visa auxiliar pesquisas quantitativas e bibliometria. Esta ferramenta oferece facilidades na importação dos dados bibliográficos das bases PubMed, SCOPUS, *Web of Science* e outras, permite a construção de matrizes de dados para cocitação, acoplamento, análise de colaboração científica e análise de palavras para a análise bibliométrica. As próximas seções mostram os resultados por grupos.

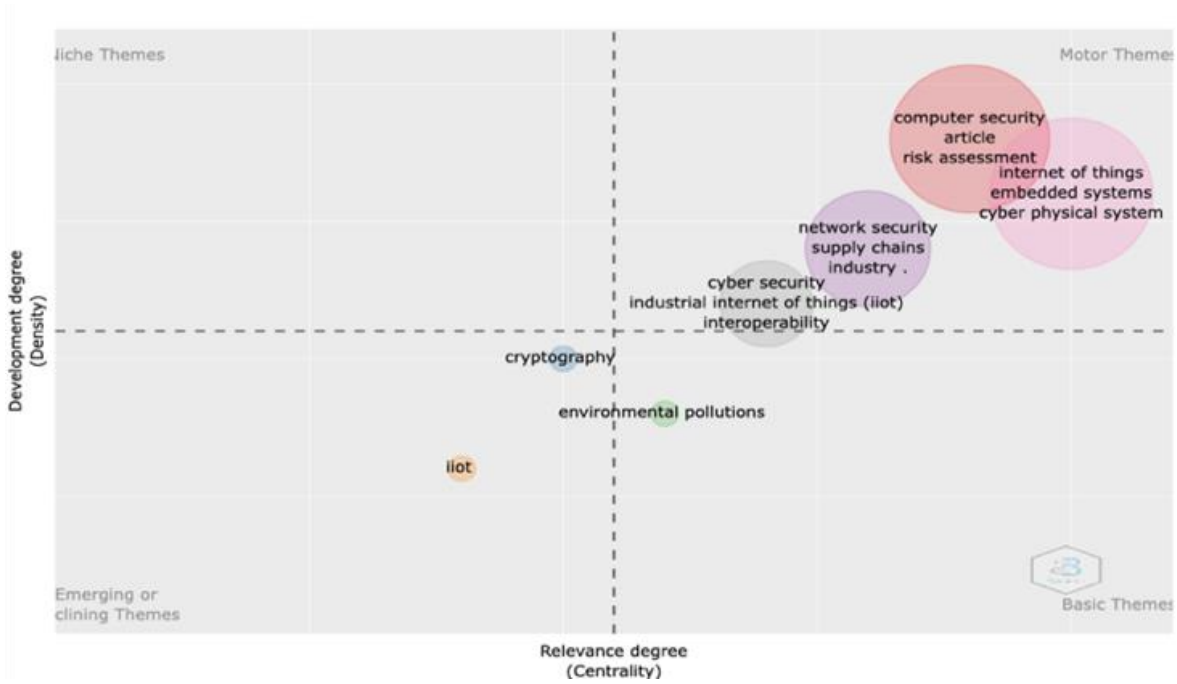
Resultados dos grupos "Industry 4.0" e "Security Vulnerability"

Os artigos obtidos pela combinação de "Industry 4.0" e "Security Vulnerability", são advindos de 26 fontes científicas diferentes. Os artigos têm uma média de 10,21 citações, com uma média de publicações de 1,74 anos, com variações de 2016 a 2020.

Com o uso do Biblioshine, o mapa temático dos 34 artigos analisados é apresentado na Figura 4.

Figura 4

Mapa temático dos grupos "Industry 4.0" e "Security Vulnerability"



Fonte: resultado da pesquisa

Por meio de um algoritmo de clusterização nas palavras-chave, foi possível evidenciar diferentes temas de um único domínio. Cada um dos temas/clusters é representado por um ponto particular, sendo conhecido por ponto estratégico/temático. A centralidade pode ser entendida como a relevância do tema para o campo de pesquisa como um todo. Na Figura 4, é possível visualizar que os temas, em sua maioria, encontram-se no quadrante "*motor theme*". O tamanho das bolhas refere-se à quantidade de ocorrências das palavras, o nome representa o *cluster* e as posições das bolhas estão de acordo com o *cluster* de Callon de densidade e centralidade.**Figura 4** Erro! Fonte de referência não encontrada.**Resultados dos grupos "Multicriteria Analysis" e "Security Vulnerability"**

A relação entre estes grupos retornou um total de 23 publicações, todos de fontes diferentes. Estes artigos tiveram em média de 19,62 citações, sendo a média de anos de publicação

de 3,29, com variações entre os anos de 2012 e 2020. Estes dados mostram o quão emergente está este tema.

Figura 5

Rede de co-ocorrência para os grupos "Multicriteria Analysis" e "Security Vulnerability"

Fonte: os autores (2021)

Figura 5A Figura 5 apresenta a estrutura conceitual de rede de co-ocorrência de palavras-chave apontadas nas publicações que foram selecionadas. As diferentes cores, indicam o cluster em que a palavra está inserida, os itens maiores e que são apresentados no centro possuem mais relevância e são relacionados. Além disso, as bolhas maiores têm um número mais elevado de citações e a diferença de espessura de seus links mostram a ligação entre os temas.

Entre as palavras mais relevantes identificadas estão: "*risk assessment*", "*analytic hierarchy process*", "*computer security*" e "*risk management*". Observam-se três *clusters* na rede de co-ocorrência, entretanto se relacionam entre si apenas os *clusters* "*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.

Discussão dos resultados

Após a leitura das 34 publicações selecionadas, foram identificados na literatura e listados quais os possíveis critérios e subcritérios que poderiam ser utilizados para uma análise multicritério no tratamento de vulnerabilidades de segurança da informação na Indústria 4.0. O Quadro 1 apresenta essa listagem dos critérios e subcritérios, juntamente com as referências aos trabalhos em que estes termos foram coletados.

Quadro 1

Critérios e subcritérios encontrados na literatura pesquisada

Critérios	*Subcritérios*	*Trabalhos relacionados*
Segurança computacional	*Confidencialidade*	*(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)*
	Disponibilidade	*(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)*
Criptografia		*(Ankele et al., 2019; Lara et al., 2020; Samaila et al., 2020)*

Critérios	Subcritérios	Trabalhos relacionados
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)
Probabilidade de ameaça e vulnerabilidade	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-	(Agrawal et al., 2019; Butun et al., 2020; Dimitriadis et al., 2020;

Critérios	Subcritérios	Trabalhos relacionados
	bilidade	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)
	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: resultado da pesquisa

A Figura 6, ilustra de maneira gráfica todo o conteúdo do Quadro 1, ou seja, os critérios e subcritérios que foram abordados pela literatura, agrupando os achados em uma estrutura hierárquica de critérios.

Figura 6

Proposta de critérios e subcritérios de vulnerabilidades de segurança da informação na indústria 4.0 encontrados na literatura

*Figura 6***Erro! Fonte de referência não encontrada.**

Fonte: resultado da pesquisa

Observam-se nos resultados, como descrito por Zhou *et al* (2006), as características de avaliação e priorização de alternativas representadas por vários atributos conflitantes, típica de um método de tomada de decisão multiatributos (MADM) como o AHP.

A proposta de critérios e subcritérios apresentada, responde à questão da pesquisa ao identificar os critérios relevantes encontrados na literatura científica para tratamento das vulnerabilidades de segurança da informação na indústria 4.0 para uso de análise multicritério, constatando-se a utilização na prática dos achados teóricos.

Os achados se alinham ao agrupamento realizado no referencial teórico, sendo identificáveis os critérios relacionados à Indústria 4.0 e às vulnerabilidades de segurança da informação.

De acordo com Wollmann *et al*. (2011), a forma organizada em decompor o problema cobriu: (1) a sua definição e o tipo de conhecimento a ser encontrado; e (2) a estrutura hierárquica com o objetivo da decisão no topo, seguida dos objetivos mais amplos, dos níveis intermediários;

Galegale *et al*. (2017) descreveram que as vulnerabilidades descobertas ficam mais complexas de gerenciar, tornando difícil a tarefa de avaliar a quais delas se deve priorizar . Com isso, o objetivo da pesquisa é alcançado pois, com os critérios identificados, os gestores podem tomar decisão com o auxílio da análise multicritério.

Pode-se dizer que os critérios e subcritérios estão agrupados com o viés da engenharia de produção e sistemas produtivos, reforçando a importância identificada por Alcácer e Cruz-Machado (2019) e Almeida (2019), uma vez que os resultados encontrados, como “Internet das Coisas”, “Cadeias de suprimentos”, “Interoperabilidade”, “Sistemas embarcados”, “Sistemas cyber-físicos”, remetem a essa área do conhecimento.

Critérios como “Confidencialidade”, “Integridade”, “Disponibilidade” e “Autenticação” representam termos que ratificam a validade da pesquisa, pois são tidos como os pilares da segurança da informação, conforme visto em Walker-Roberts *et al*. (2020). Esses itens de “Segurança computacional”, bem como os itens do grupo “Segurança de rede” já são tradicionalmente considerados nas análises de tratamento de vulnerabilidades dentro da área de tecnologia da informação.

A pesquisa de Jang-Jaccard & Nepal (2014) vai ao encontro dos subcritérios "*Cyber* ataques" e "Avaliação de vulnerabilidades", do critério "Segurança computacional", ao mencionar a execução de *malware* para a prática do crime cibernético por exploração de vulnerabilidades

Com o critério "Segurança de rede", se pode resgatar os exemplos de Walker-Roberts *et al*. (2020) como os ataques heurísticos, o sequestro de dispositivos, o *spam* em massa, os *botnets* e os ataques DDoS.

O grupo de critérios de "Riscos" apresenta a sua importância para ser considerado em uma análise multicritérios. Da mesma maneira, os grupos "Impacto nos ativos" e "Probabilidade de ameaça e vulnerabilidade" andam lado a lado com a análise de riscos em uma eventual tomada de decisão relacionada à segurança.

Os itens desses três grupos tiveram destaque nas ações da CISA e FBI para a revisão de alertas, publicações, avisos e aplicação de ações de mitigação relacionadas à infraestrutura crítica nos EUA (CISA, 2021).

O grupo de critérios "Internet das Coisas" representa o item com maior acoplamento aos conceitos da Indústria 4.0, como no exemplo das vulnerabilidades de fluxo de controle de Sha *et al*. (2018). Subcritérios importantes são trazidos para serem considerados na análise multicritério de vulnerabilidades de sistemas produtivos modernos, como os sistemas cyber-físicos.

Por fim, "Criptografia" e "Sistemas de informação" são os critérios com menos identificação de subcritérios, o que pode indicar necessidade de maior investigação na literatura ou através de levantamento prático com profissionais da área de segurança da informação da Indústria 4.0.

Conforme Guglielmetti *et al*. (2003), os critérios identificados podem são usados por meio de alto grau de julgamento sem exigir o processamento dos dados antes que estes possam ser usados. Além disso, proporcionam saída de dados na forma de um *ranking* completo de alternativas e soluções muito refinadas.

Ainda segundo Guglielmetti *et al*. (2003), o tomador de decisão pode utilizar decisões em grupo, criar aprendizado sobre a estrutura do problema, e estruturar o problema e o nível de compreensão para sua forma de trabalho de forma mais fácil.

Considerações finais

O objetivo deste trabalho foi de identificar os possíveis critérios e subcritérios que podem ser utilizados em uma análise multicritério para o tratamento de vulnerabilidades de segurança da informação na Indústria 4.0. A pesquisa exploratória da literatura permitiu verificar as publicações existentes que abordam sobre este tema.

Com a análise da bibliometria foi possível observar que o interesse em pesquisas nesta temática acompanha o crescimento acelerado da Indústria 4.0 e, da mesma maneira, os crimes e incidentes cibernéticos se tornam cada vez mais aperfeiçoados, significativos e exigentes de constante aprimoramento nos mecanismos de segurança da informação.

O progresso que a Indústria 4.0 e a *Internet of Things* alcançaram, consequentemente, aumentaram as vulnerabilidades de segurança da informação em seus diversos dispositivos, interfaces, redes, organizações e pessoas. Dessa forma, torna-se mais complexo saber quais vulnerabilidades priorizar e quais decisões devem ser tomadas, considerando os múltiplos fatores envolvidos. Um método de análise multicritério como o *Analytic Hierarchy Process* (AHP), é uma proposta de solução para este cenário.

Utilizando as bases científicas do SCOPUS e *Web of Science*, delimitando o período de busca entre os anos de 2011 e 2020, e relacionando as principais palavras-chaves "*industry 4.0*", "*security vulnerability*" e "*multicriteria analysis*", a pesquisa de análise bibliométrica identificou nos resultados os critérios e subcritérios relacionados a vulnerabilidades de segurança da informação na Indústria 4.0.

O resultado da pesquisa na literatura científica 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 facilidade de utilização, auxiliando a fazer escolhas importantes para trazer mais resultados e melhorar a performance da relacionadas à gestão da segurança.

A pesquisa contribuiu para a teoria ao auxiliar o preenchimento da lacuna em relação a este tema. Também contribui para a prática ao ter identificado e reunido critérios e subcritérios, viabilizando que organizações da Industria 4.0 apliquem a análise multicritério para o tratamento das vulnerabilidades de segurança da informação de forma simplificada e eficaz promovida por um método com o AHP. A contribuição para a sociedade pode ser obtida pelo auxílio que gestores podem ter na tomada de decisão para priorizar qual vulnerabilidade ter o devido tratamento, o que refletirá em uma melhor gestão da segurança da informação e consequentemente, no reforço aos pilares da integridade, disponibilidade e confidencialidade.

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 fatores. A identificação dos critérios e subcritérios abordados na literatura têm um papel importante, principalmente por auxiliar na aplicação da análise multicritério em cenários complexos de vulnerabilidades de segurança da informação. Evitar que crimes cibernéticos ocorram na Indústria 4.0 e proporcionar um ambiente seguro é essencial em uma sociedade cada vez mais conectada.

Como trabalhos futuros, considerando que a pesquisa tem o escopo limitado na análise da literatura recente existente, os resultados encontrados permitem conduzir novas pesquisas para a validação, acréscimo ou remoção dos critérios e subcritérios identificados, por meio de outros métodos científicos como entrevistas e *survey*, bem como, uma demonstração da aplicação prática do método AHP com os critérios e subcritérios que foram 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). http://dx.doi.org/10.14569/IJACSA.2018.090169

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., & Osterberg, P. (2019). Security Implications of Fog Computing on the Internet of Things. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-6). IEEE. https://doi.org/10.1109/ICCE.2019.8661909

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. Encontro Nacional de Engenharia de Produção, 23. Disponível em: http://www.din.uem.br/sbpo/sbpo2003/pdf/arq0131.pdf

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 for Evolutionary Computing & Other Computational Intelligence. IEEE Computational Intelligence Society. https://doi.org/10.1109/CEC.2016.7743900

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. Disponível em http://www.abepro.org.br/biblioteca/enegep2012_TN_STP_162_944_20906.pdf

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. Disponível em http://www.din.uem.br/sbpo/sbpo2009/artigos/55993.pdf

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, Iss.7). https://dx.doi.org/10.14569/IJACSA.2020.0110725

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. http://dx.doi.org/10.1504/IJSSCI.2008.017590

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. http://dx.doi.org/10.2991/emeit.2012.517

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/10.15675/gepros

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://dx.doi.org/10.1007/978-3-319-12586-2

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