

Análise Bibliométrica Acerca da Segurança de Dados no Cenário da Indústria 4.0 entre 2017 e 2021

Bruno Xavier Rodrigues

Universidade Federal do Rio de Janeiro (UFRJ)

e-mail: brunoxavier@ufrj.br

Thiago Gomes de Lima

Universidade Federal do Rio de Janeiro (UFRJ)

e-mail: thiagogomesufrj@gmail.com

Felipe Pereira Lobato Mendes

Universidade Federal do Rio de Janeiro (UFRJ)

e-mail: fepmendesoficial@gmail.com

Hugo Leal Calderon

Universidade Federal do Rio de Janeiro (UFRJ)

e-mail: hugocalderon10@gmail.com

Luiz Filipe Lopes de Azevedo

Universidade Federal do Rio de Janeiro (UFRJ)

e-mail: luiz-filipe@ufrj.br

* RECEBIDO em 21/10/2023. ACEITO em 23/02/2024.

Resumo

O avanço da tecnológico da indústria 4.0 é cada vez mais acelerado. Enquanto a gestão pode ser facilitada pelas inovações que diminuem variáveis e erros humanos e reduzem custos como o de armazenamento de informação, por outro lado, aumenta a exposição de usuários a possíveis ataques cibernéticos. O objetivo deste estudo é realizar uma análise bibliométrica da produção científica brasileira na área da segurança de dados e indústria 4.0 entre os anos de 2017 e 2021, através das plataformas Scopus e Web of Science, a fim de identificar as principais tendências e desafios. Portanto, foram mapeados e analisados 23 artigos. Os resultados mostram que alguns subtópicos se destacam em termos de atenção em pesquisas sobre segurança de dados, com ênfase a pilares da Indústria 4.0, como 'IoT', 'integração de sistemas' e 'Big Data'. No Brasil, o tema 'ataques cibernéticos' é isoladamente o mais citado entre a amostra de artigos estudados.

Palavras-chave: Indústria 4.0, segurança de dados, análise bibliométrica, Internet das Coisas, ataques cibernéticos

Abstract

The technological advancement of industry 4.0 is increasingly accelerated. While management can be facilitated by innovations that reduce variables and human errors and reduce costs such as information storage, on the other hand, it increases the exposure of users to possible cyber-attacks. The objective of this study is to carry out a bibliometric analysis of the Brazilian scientific production in the area of data security and industry 4.0 between the years 2017 and 2021, through the Scopus and Web of Science platforms, in order to identify the main trends and challenges. Therefore, 23 articles were mapped and analyzed. The results show that some subtopics stand out in terms of attention in research on data security, with emphasis on Industry 4.0 pillars, such as 'IoT', 'systems integration' and 'Big Data'. In Brazil, the theme 'cyber attacks' is alone the most cited among the sample of articles studied.

Keywords: Industry 4.0, data security, bibliometric analysis, Internet of Things, cyber-attacks.

1. Introdução.

De acordo com Bertolli (2019), 64% dos americanos nunca verificaram se foram afetados por alguma violação de dados, enquanto 56% alegaram não saber o que fazer em caso de violação de dados.

Bisso (2019) relata um caso de 2018 que envolveu o vazamento de dados de mais de 20 mil clientes do Banco Inter. E, um ano depois, mais uma falha fez com que 1,4 milhões de clientes do mesmo banco fossem expostos (PAYAO et al., 2019). Outro caso que ficou famoso mundialmente foi o vazamento de dados do Facebook, em 2019, com 540 milhões de vítimas (HERN et al., 2019).

No cenário nacional, conforme divulgado pelo Senado Federal (2014), o Brasil ocupa o posto de terceiro país do mundo em número de usuários ativos na internet, com enorme crescimento do número de organizações governamentais nacionais com serviços disponíveis na internet: de 49% em 2012, para 88% em 2014 (VIANNA E FERNANDES, 2015). Ainda segundo Vianna e Fernandes, o tema espionagem cibernética vem mais a tona em 2013, no famoso caso de espionagem de dados norte-americana em escala global, causando interferências diretas inclusive nas eleições dos Estados Unidos, através de dados coletados em redes sociais como o Facebook. Tais casos levaram o Senado Federal brasileiro a instalar uma Comissão Parlamentar de Inquérito (CPI) da espionagem em 2014.

Dada a importância deste tema, principalmente no cenário atual, muitos pesquisadores têm direcionado seus estudos para solucionar problemáticas relacionadas à segurança cibernética. Furstenau et al. (2020) em seu artigo “20 Years of Scientific Evolution of Cyber Security: a Science Mapping” enfatiza o aumento da procura pelo assunto, como pode ser observado na Figura 1. Esse fato, segundo o autor, se dá principalmente pelo avanço tecnológico e consequente incremento de inovações no dia-a-dia, criando uma maior exposição de todos os usuários.

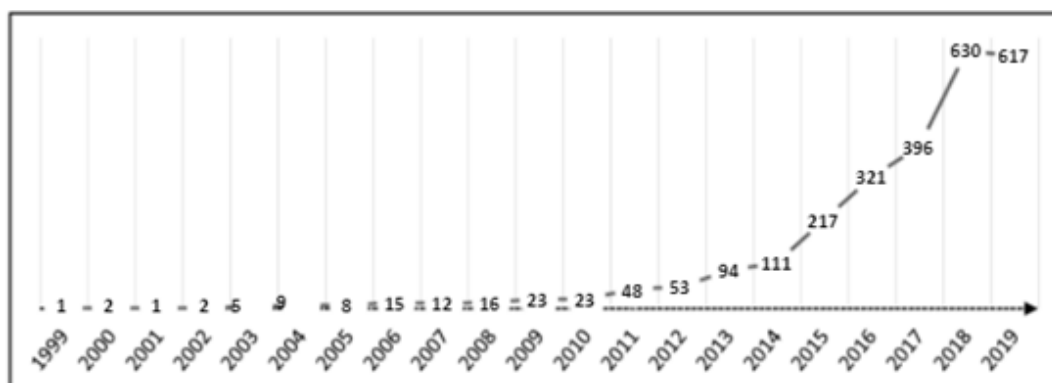


Figura 1 – Relação ao número de publicações ao longo do tempo. Fonte: Furstenau et al., 2020.

Para Dharminder (2020), de um lado o ambiente gerado pela Internet das Coisas (IoT) favorece principalmente a utilização de armazenamento em nuvem (cloud), minimizando o custo de computação. Por outro lado, torna essencial os gastos com fatores de defesa, como a criptografia, que tende a tornar os dados autênticos e seguros. Os estudos de Sá (2019) exploram a necessidade de sistemas de controle em rede (NCS), muito utilizados na Indústria 4.0, visando uma gestão mais eficiente. Porém, os mesmos NCS geram integração da comunicação entre físico e virtual, expondo totalmente pessoas físicas e jurídicas a terem suas informações expostas a ameaças cibernéticas.

Na visão mais legislativa de Corrêa (2016) são citadas medidas implementadas na constituição nacional, como a Lei 12.737/2012 (Lei Carolina Dieckmann), que formalizou crimes como a invasão de dispositivos informativos, por exemplo, telefones celulares. Esse autor demonstra o quão recente são leis desse tipo, que foram implementadas após escândalos nacionais causados por crimes cibernéticos, comprovando que o assunto realmente só vem ganhando força a partir da última década. Ainda assim, Corrêa conclui que o arcabouço legal do Brasil é considerado um dos mais severos e eficientes do mundo, trazendo os instrumentos necessários para punir quem comete crimes desse tipo.

Outro fato que comprova o aumento significativo da preocupação com relação ao tema é o investimento em desenvolvimento de plataformas online que permitem que o usuário verifique se suas

informações estão contidas em base de dados sobre vazamentos monitorados. Entre os exemplos cita-se Have I Been Pwned, Avast Hack Check e Firefox Monitor (CASTRO, 2019).

Portanto, o presente estudo tem como objetivo realizar uma análise bibliométrica dos artigos publicados, levando em conta que desde 2016, os top 5 incidentes anuais impactaram mais de 1 milhão de pessoas (BISSO, 2019). Para atingir este objetivo foram consultadas as bases Scopus e Web of Science delimitando a análise entre 2017 e 2021.

2. Revisão de literatura.

Nesta seção será exposta uma breve revisão da literatura acerca de indústria 4.0, segurança de dados e análise bibliométrica.

2.1. Indústria 4.0.

Na década de 60, Gordon Moore, publicou um artigo sobre o aumento do processamento de computadores. De acordo com D’Emidio (2009), a crescente duplicação do número de componentes dos microprocessadores era conhecida como Lei de Moore. Com tamanha capacidade de processamento possível o mundo estava passando por uma nova revolução industrial.

O termo indústria 4.0 é utilizado para descrever essa revolução que está tomando lugar desde o início da década de 2010 (HERMANN et al, 2016). Segundo Kagermann et al., (2013) esse termo se tornou público em 2011, na feira de Hannover na Alemanha, com intuito de aumentar a competitividade da manufatura alemã.

“Os termos “Indústria 4.0”; “smart factory”; “intelligent factory”; “factory of the future” são termos que descrevem uma visão do que será uma fábrica no futuro. Nesta visão as fábricas serão muito mais inteligentes, flexíveis, dinâmicas e ágeis. Outra definição para “Smart factory” é uma fábrica que faz produtos inteligentes, em equipamentos inteligentes, em cadeias de abastecimento inteligentes.” (H. MACKENZIE 2016 apud COELHO, 2016, p.23)

A partir de uma visão técnica, a Indústria 4.0 pode ser descrita como uma crescente digitalização e automação do ambiente de manufatura e também a criação de cadeias de valor digital (OESTERREICH & TEUTEBERG, 2016).

De acordo com Lee (2015) com o recente desenvolvimento que tem resultado numa alta disponibilidade e acessibilidade de sensores, sistema de aquisições de dados e redes de computadores, além do ambiente competitivo das indústrias de hoje tem forçado mais fábricas a migrarem para métodos de tecnologia de ponta.

A transformação ligada à indústria 4.0 abrange três pilares fundamentais (ALMADA-LOBO, 2016). O primeiro é a digitalização de produção. O segundo a automação. Por fim, o terceiro é a troca instantânea de dados. De acordo com Santos et.al., (2018) a indústria 4.0 representa uma evolução natural dos sistemas industriais anteriores, desde a mecanização do trabalho ocorrida no século XVIII à automação da produção no atual momento. A informação tem valor, de acordo com Lee (2015), há diversas ferramentas e metodologias disponíveis para converter os dados para informação, um foco intenso tem sido aplicado para desenvolver algoritmos para prognósticos e predição da funcionalidade.

Quadro 1 – Comparação da indústria da década de 2010 com a indústria 4.0.

Fonte de dados		Fábricas atuais		Indústria 4.0	
		Atributos	Tecnologias	Atributos	Tecnologias
Componente	Sensor	Precisão	Sensores inteligentes e detectores de falha	Autoconsciente	Monitoramento da degradação e tempo
				Auto-preditiva	
Máquina	Controlador	Produtividade e performance	Monitoramento condicional e diagnóstico	Autoconsciente	Tempo de atividade com monitoramento de vida
				Auto-preditiva	
				Auto Comparativa	
Sistema produtivo	Sistema em rede	Produtividade e OEE	Operações enxutas: trabalho e redução do desperdício	Auto Configurável	Produção sem preocupação
				Auto-manutenção	
				Auto-organizável	

Fonte: LEE et al. (2014).

De acordo com Oesterreich e Teuterberg (2016) apud Antunes et.al. (2019), há inúmeros obstáculos nas empresas para a integração dessas tecnologias. Os principais desafios são: custo de implementação elevado, alteração organizacionais e de processos, qualificação dos recursos humanos, segurança de dados e complexidade crescente do sistema produtivo. Na contramão dos problemas, há suas vantagens como: melhoria da qualidade do produto, das comunicações, economia de tempo e de custos, intensificação das relações clientes/consumidores e maior eficiência para desenvolver produtos e serviços personalizados.

2.2. Segurança de dados.

2.2.1 Panorama geral.

Segundo Mandarino (2009) o setor das tecnologias de informação (TICs) é muito dinâmico e exige um ritmo acelerado de inovações e ações multidisciplinares. Nesse cenário, Canongia (2009) afirma que tais avanços permitiram também um aumento significativo dos chamados ataques cibernéticos, sendo então necessário assegurar a confidencialidade e a autenticidade da informação.

Outro fato importante enfatizado por Martins (2019) é a Internet das Coisas (IoT), que cria uma ligação gigante entre vários setores, tornando os sistemas cada vez mais vulneráveis a ataques cibernéticos e consequentemente fazendo necessário o desenvolvimento de algoritmos de segurança, metodologias de análise e ferramentas de aplicações que assegurem informação de qualidade e confiável.

Ashibani (2017) traz a discussão em seu artigo sobre Cyber Physical Systems (CPS), isto é, sistemas em rede que contam com componentes cibernéticos e físicos em constante comunicação com nosso dia a dia. Para ele, a segurança nesta área é um problema global, de forma que CPS's robustos, seguros e eficientes são desenvolvidos diariamente, seguindo uma espécie de melhoria contínua, com estudos recorrentes. Para Ashibani, esses problemas com segurança de dados não são novos, mas os avanços na tecnologia tornam necessário o desenvolvimento de novas abordagens para proteger os dados

contra consequências indesejáveis. Conclui-se que novas ameaças continuarão a ser exploradas e os meios de se defender devem acompanhar essa evolução.

O ciberespaço (espaço cibernético) é um termo criado por Willian Gibson em sua obra “Neuromancer” (APDSI, 2005). Esse espaço é criado por redes, onde pessoas podem se comunicar, tais como salas virtuais, mensagens, etc. Pode-se concluir que informações profissionais e pessoais são trocadas infinitas vezes por dia, tornando ainda mais perigoso qualquer tipo de invasão, pois através dessas mensagens é possível tirar conclusões sobre rotina, preferências, família, trabalho, entre outras informações que podem ser perigosas em mãos erradas.

2.2.2. Segurança de dados na indústria 4.0.

Martin e Oliveira (2019) destacam os pilares para o avanço da indústria 4.0, entre eles Big Data, Internet das coisas e computação em nuvem. Os pilares têm como base informação em tempo real, com disponibilidade e desempenho, mas tudo armazenado em um cloud (nuvem).

Para Santos (2018), a quarta revolução industrial possui como pontos principais a IoT, que conecta máquinas, objetos e pessoas em tempo real, CPS para monitoramento de processos e cloud para armazenamento de dados. Para este pesquisador, com o aumento da inteligência dos dispositivos, os riscos obviamente vão aumentar, sendo de infinita importância estabelecer procedimentos que assegurem privacidade, propriedade intelectual e dados pessoais devidamente guardados.

Castro (2010) assegura que em um ambiente de nuvem é comum que os requisitos funcionais do sistema sejam priorizados com relação aos requisitos de segurança. A autora expõe o risco que as empresas acabam correndo quando as informações críticas são vazadas, podendo inclusive diminuir a garantia do cumprimento de leis. Por outro lado, pessoas físicas dentro de suas casas utilizam muitas vezes nuvens desconhecendo o processo de segurança ao qual suas informações estão sendo expostas. Além disso, esse usuário não sabe exatamente onde seus dados estão sendo armazenados e, consequentemente, não possui nenhum controle sobre essas movimentações (Kandukuri et. al., 2009).

Com ênfase na internet das coisas, dados relevantes e sensíveis em torno dos dispositivos conectados precisam abordar preocupações relacionadas à segurança e privacidade. Nessa realidade, o uso de tecnologias como o blockchain pode surgir como opção, já sendo utilizado em questões de proteção financeira. Os dados, que são coletados, armazenados e processados juntamente com todos os objetos conectados em rede dependem de blockchain para superar principalmente novas e desconhecidas ameaças (Chicarino, 2017).

2.3. Análise bibliométrica.

Neste tópico serão apresentadas definições e um breve histórico sobre a análise bibliométrica e seu uso para fins científicos.

Segundo Hérubel (1999) a análise bibliométrica pode ser definida como uma análise quantitativa de publicações relacionadas a um determinado tema, sendo que ao longo da história tem sido usada mais amplamente nas disciplinas científicas e tecnológicas.

Para Silva, Hayashi e Hayashi (2011), as primeiras premissas de medidas quantitativas na análise de produção bibliográfica remontam ao fim do século XIX, tendo evolução constante em termos de fundamentos, técnicas e aplicações dos métodos bibliométricos. Ainda segundo os mesmos autores, a definição do termo bibliometria é pleiteada por duas correntes: a dos anglo-saxônicos atribuindo a Pritchard (1969) o pioneirismo do uso do termo “bibliometria” para classificar o uso de métodos matemáticos e estatísticos para mensuração de produção bibliográfica e; a corrente dos franceses, que conferem a Paul Otlet (1934) - na obra Tratado da Documentação- a vanguarda da denominação.

Embora as técnicas de análise bibliométrica estejam postas há muito tempo, foi através do advento e evolução dos sistemas de informações que se evidenciou o uso de base de dados - com publicações indexadas facilitando as buscas- o que consequentemente, tornou muito mais comum e eficaz o uso da bibliometria (LACERDA et al, 2012). Isso porque, além de facilitar a recuperação e utilização do conhecimento científico em pesquisas, às bases de dados também fomentam indicadores

que aprimoram a visualização do potencial de impacto de periódicos em suas respectivas áreas de conhecimento (PODSAKOFF et al, 2005).

Para Borgman e Ferner (2002) há basicamente três tipos de aplicação da análise bibliométrica, a saber: descritiva, relacional e avaliativa.

Bibliometria descritiva: este tipo de análise bibliométrica se propõe a descrever as funções ou características da literatura e é utilizada para mensurar a produtividade de cientistas e cientistas da informação. A pesquisa é dividida por critérios geográficos, temporais e departamentos e disciplinas. É quantificado o número de publicações em um determinado campo de conhecimento ou a produtividade na área, buscando-se comparações de pesquisa em diferentes instituições, territórios e períodos (JACOBS, 2010).

Bibliometria avaliativa: esta abordagem foi apresentada por Narin (1976) e consiste na aplicação de bibliometria para medição da atividade científica com enfoque nos aspectos qualitativos da pesquisa. Isto é, a avaliação se baseia no controle da qualidade o que implica na análise da qualidade da pesquisa de acordo com a salvaguarda oferecida pela comunidade científica (VAN LEEUWEN, 2004).

As bases teóricas para este tipo de análise bibliométrica derivam da sociologia da ciência de Robert Merton (1973), onde se argumenta que a relevância de um trabalho acadêmico é dada pela quantidade de citações posteriores daquele trabalho.

Nesse sentido, pode-se dizer que o principal indicador de valor da pesquisa nesse tipo de análise é a contagem de citações (JACOBS, 2010).

Bibliometria relacional: este tipo de análise usa métricas híbridas de forma a captar ao mesmo tempo a produtividade e o impacto, gerando índices como número médio de citações por artigo (KOSEOGLU, 2016). Também é frequente que se analise as relações entre campos de pesquisa, o surgimento de novos temas e métodos, além dos padrões de co-citação e co-autoria (BENCKENDORFF E ZEHRER, 2013).

Isto porque, como afirma Jacobs (2011), se as coleções de documentos são organizadas seguindo a lógica das contagens de co-citação, é provável o surgimento de padrões que reflitam as relações científicas cognitivas. Cabe destacar ainda, segundo o mesmo autor, que o surgimento e aprimoramento dessas técnicas se deu principalmente em virtude dos avanços tecnológicos, sobretudo na informatização das bases de dados.

3. Metodologia.

As bases científicas escolhidas para realização da busca de artigos para a análise bibliométrica foram Scopus e Web of Science. A escolha se deve ao reconhecimento acadêmico e abrangência de ambas e, no caso da Web of Science, também pelo seu apelo em temas de tecnologia da informação e áreas correlatas.

Os núcleos de partida definidos foram “indústria 4.0” e “segurança de dados”, escolhidos com base no tema central deste trabalho, de forma a restringir precisamente o campo de assuntos essenciais. Os termos foram traduzidos livremente para o inglês, sendo combinados como: “industry 4.0” AND “data security”. Em seguida foram selecionados os filtros temporais restringindo os resultados para os últimos 5 anos (2017-2021).

Na base Scopus a busca resultou em 612 publicações, já na Web of Science, 294. Nesta etapa foram registrados números de publicações e suas distribuições geográfica e temporal a fim de realizar comparações preliminares entre a produção o restante do mundo e, posteriormente, foi aplicado o filtro “Brasil”, resultando em 21 documentos na base Scopus e 10 na Web of Science, sendo que 5 constavam em ambas. Além disso, após leitura dos resumos, 3 artigos foram eliminados por não se conectarem de alguma forma ao tema.

Para sintetizar as informações obtidas da leitura integral dos artigos e melhorar a visualização dos dados mais relevantes, recorreu-se frequentemente à elaboração de quadros, tabelas e rankings, combinando aspectos tanto da análise descritiva como avaliativa da bibliografia.

Com a finalidade de identificar os documentos, foram elaborados dois quadros: um para a base Scopus e outro para a Web of Science. Os seguintes itens foram dispostos em colunas: código da publicação, título da publicação, palavras-chave, autores, ano e meio de publicação.

Um segundo tipo de quadro foi elaborado com base nos pilares da indústria 4.0 de acordo com Yamada e Martins (2019), a saber: Big Data, IoT, robótica, simulação, integração de sistemas, segurança da informação, computação em nuvem, realidade aumentada e manufatura aditiva. Para compreender a abrangência destes temas nas publicações, também foi elaborado um ranking de acordo com suas respectivas frequências de ocorrência.

Para estratificar de forma mais específica a temática de segurança de dados dentro da indústria 4.0, ainda foi construído um terceiro quadro, desta vez considerando os sub tópicos visualizados mais vezes nas publicações.

Quadro 2 – Subtópicos em segurança de dados e Indústria 4.0.

1	Apresentar contra medidas para ataques cibernéticos
2	Teste de softwares/protocolo e cibersegurança
3	Ataques cibernéticos
4	Técnicas de criptografia para aumento da segurança de dados em nuvem
5	Benefícios da indústria 4.0 na cadeia produtiva
6	Inconvenientes para a aplicação da industria 4.0
7	Ataques em Sistemas de Controle em Rede (NCS)
8	Avaliação da aplicabilidade de um modelo de segurança
9	Propor direções para o desenvolvimento de conjuntos de dados confiáveis
10	Mapeamento científico na área de estudos da segurança cibernética

Fonte: Elaborado pelos autores.

Estes subtópicos também foram ranqueados usando os mesmos critérios usados para os pilares da indústria 4.0.

Por fim, com foco na análise da relevância dos trabalhos foram confeccionados rankings de publicações tendo como critério o número de citações dentro de suas respectivas bases científicas (Scopus e WoS).

4. Resultados.

A partir da análise minuciosa individual dos artigos, foi possível identificar alguns padrões e correlações da pesquisa brasileira sobre segurança de dados baseada nas informações obtidas. A etapa de identificação dos artigos teve como resultado os quadros 3 e 4.

Quadro 3 – Quadro de publicações identificadas na base Web of Science.

Base Web of Science				
Código	Título	Autores	Ano	Meio de publicação
P6	Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications	ROY, Sandip et al.	2018	IEEE Transactions on Industrial Informatics
P7	Identification of Data Injection Attacks in Networked Control Systems Using Noise Impulse Integration	DE SÁ, Alan Oliveira et al	2020	Sensors
P8	Bio-Inspired Network Security for 5G-Enabled IoT Applications	SALEEM, Kashif et al	2020	Special Section on Emerging Trends of Energy and Spectrum Harvesting Technologies
P17	Countermeasure for Identification of Controlled Data Injection Attacks in Networked Control Systems	DE SÁ, Alan Oliveira; CARMO, Luiz Fernando Rust da C. MACHADO, Raphael C. Santos	2019	2019 IEEE International Workshop on Metrology for Industry 4.0 and Internet of Things
P18	Um estudo sobre modelo de gestão dos negócios com ênfase no turismo 4.0	DE ARAÚJO, Thásia Maria Oliveira; DE FARIAS, Mayara Ferreira; FERREIRA, Lissa Valéria Fernandes.	2020	Revista Turismo Estudos e Práticas
P19	Blockchain based MFA solution: the use of hydro raindrop mfa for information security on wordpress websites	CARDOSO, João Antonio Aparecido et al	2019	Brazilian Journal of Operations Productions Management
P20	Panorama, challenges and opportunities in PROFINET protocol research	DIAS, André Luís et al.	2018	IEEE International Conference on Industry Applications
P21	Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis	KIPPER, Liane Mahlmann et al	2019	International Journal of Production Research
P22	Barriers for the digitalization of servitization	MARCON, Erico et al	2019	CIRP Conference on Industrial Product-Service Systems
P23	Security Experiences in IoT based applications for Building and Factory Automation	DE LAS MORENAS, Javier et al	2020	2020 IEEE International Conference on Industrial Technology (ICIT)

Fonte: Elaborado pelos autores.

Na Web of Science, 4 dos autores tiveram duas publicações: CARMO, MACHADO, R.C.S. e DE SÁ apareceram juntos nas publicações P7 e P17 e RODRIGUES em P6 e P8. Também é interessante notar que 40% (4) dos documentos foram publicados em eventos do IEEE, sendo que nenhum outro meio de publicação se repetiu.

Quadro 4 – Quadro de publicações identificadas na base Scopus.

Base Scopus				
Código	Título	Autores	Ano	Meio de publicação
P1	Scientific mapping to identify competencies required by industry 4.0	KIPPER, Liane Mahlmann et al	2021	Technology in Society
P2	Enabling QoS-secured Enhanced Non-Public Network Slices for Health Environments	DE RESENDE, Henrique C. Carvalho et al	2020	Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good
P3	Identification of Data Injection Attacks in Networked Control Systems with Varying Setpoint Condition	DE SÁ, Alan Oliveira; MACHADO, Raphael CS	2020	2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT
P4	Proficiency Testing for Software Analysis and Cybersecurity Laboratories	MACHADO, Raphael et al	2020	2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT
P5	Proposal guidelines to implement the concepts of industry 4.0 into information technology companies	CUNHA, Tairine Pravadelli et al	2020	The TQM Journal
P6	Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications	ROY, Sandip et al.	2018	IEEE Transactions on Industrial Informatics
P7	Identification of Data Injection Attacks in Networked Control Systems Using Noise Impulse Integration	DE SÁ, Alan Oliveira et al	2020	Sensors
P9	Cybersecurity in the Power Electronics	MARTINS, Tiago; OLIVEIRA, Sérgio Vidal Garcia	2019	IEEE Latin America Transactions
P10	HTTPS Keys in the Mediterranean	PEREIRA, Diogo; ARANHA, Matheus; BORGES, Fábio	2019	2019 II Workshop on Metrology for Industry 4.0 and IoT
P11	Coverage-Based Heuristics for Selecting Assessment Items from Security Standards: A Core Set Proposal	ROSA, Ferruccio De Franco et al.	2018	2018 Workshop on Metrology for Industry 4.0 and IoT
P12	Building Reference Datasets to Support Socialbots Detection	PACHECO, Carla et al	2018	2018 Workshop on Metrology for Industry 4.0 and IoT
P13	Adoption of Industry 4.0 Technologies in Supply Chains	DALMARCO, Gustavo; BARROS, Ana Cristina	2018	Innovation and Supply Chain Management
P14	20 Years of Scientific Evolution of Cyber Security: a Science Mapping	FURSTENAU, Leonardo Bertolin et al	2020	Proceedings of the International Conference on Industrial Engineering and Operations Management
P15	PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments	DHARMINDER et al	2019	Wiley Online Library Journal
P16	Work-in-Progress: Compromising Security of Real-time Ethernet Devices by means of Selective Queue Saturation Attack	FERRARI, P. et al	2020	Electrical Engineering and Information Technology, Berne University of Applied Sciences (BFH), Berne, Switzerland
P17	Countermeasure for Identification of Controlled Data Injection Attacks in Networked Control Systems	DE SÁ, Alan Oliveira; CARMO, Luiz Fernando	2019	2019 IEEE International Workshop on Metrology for Industry 4.0 and Internet of Things

		Rust da C.; MACHADO, Raphael C. Santos		
P20	Panorama, challenges and opportunities in PROFINET protocol research	DIAS, André Luis et al.	2018	IEEE International Conference on Industry Applications
P23	Security Experiences in IoT based applications for Building and Factory Automation	DE LAS MORENAS, Javier et al	2020	2020 IEEE International Conference on Industrial Technology (ICIT)

Fonte: Elaborado pelos autores.

Na Scopus, 7 autores foram citados mais de uma vez: DE SÁ e MACHADO, R.C.S. que também têm colaborações na WoS aparecem juntos em P3, P7, P16 e P17 com CARMO colaborando com os dois anteriores em P7 e P17; KIPPER e FURSTENAU aparecem em colaboração nos documentos P1 e P14 e MACHADO, R aparece em P4 e P12.

Novamente os eventos do IEEE se destacam, contendo 30% (7) das publicações e o “*Workshop on Metrology for Industry 4.0 and IoT*” também serviu como meio de publicação para 14,28% (3) das publicações, sendo os únicos com mais de um documento publicado.

Conforme exposto na descrição da metodologia, foi realizada uma breve análise quantitativa visando comparar as publicações brasileiras e mundiais, conforme exposto na Tabela 1.

Tabela 1 – Publicações do Brasil e do mundo.

Web of Science				Scopus		
Ano	Brasil	Mundo	%Brasil/Mundo	Brasil	Mundo	%Brasil/Mundo
2017	0	23	0,00%	0	32	0,00%
2018	1	62	1,61%	4	103	3,88%
2019	5	111	4,50%	6	209	2,87%
2020	4	90	4,44%	10	241	4,15%
2021	0	8	0,00%	1	27	3,70%
Total	10	294	Média 2,11%	21	612	Média 2,92%

Fonte: Dados extraídos das bases Scopus e Web of Science em fevereiro de 2021.

Verifica-se que na base WoS o pico de produção mundial ocorre em 2019 (111) e em 2020 na Scopus (241). Nota-se também um grande crescimento em relação ao primeiro ano analisado (2017). A queda no ano de 2021 provavelmente se deve ao fato da análise ter sido realizada ao longo do mês de fevereiro.

Sobre a produção nacional, um ponto a ser destacado é o fato de não haver nenhuma publicação considerando as duas bases no ano de 2017 e apenas uma em 2021 na Scopus. Em termos relativos, o número de publicações brasileiras em relação ao mundo correspondeu a uma média anual de 2,11% e 2,92% na WoS e Scopus respectivamente.

Após a identificação dos nove pilares da indústria 4.0, foi realizada uma comparação direta com os artigos selecionados do presente trabalho, como demonstra o Quadro 5:

Quadro 5 – Publicações por pilares da Indústria 4.0.

Código da Publicação	Big Data	IoT	Robótica	Simulação	Integração de Sistemas	Segurança da Informação	Computação em Nuvem	Realidade Aumentada	Manufatura Aditiva
P1	x	x	x	x	x	x	x	x	x
P2					x	x			
P3				x	x	x			
P4		x		x	x	x			
P5	x	x	x	x	x	x	x	x	x
P6	x	x		x		x	x		
P7	x	x		x	x	x			
P8	x	x		x	x	x	x		
P9		x	x		x	x	x	x	x
P10						x			
P11		x				x			
P12						x			
P13	x	x	x	x	x	x	x		
P14	x	x			x	x	x		
P15	x	x			x	x	x		
P16		x			x	x			
P17				x	x	x			
P18	x	x	x		x	x	x	x	
P19		x			x	x			
P20	x	x		x	x	x			
P21	x	x	x	x	x	x	x	x	x
P22					x	x			
P23		x			x	x	x		

Fonte: :Elaborado pelos autores

Como esperado, a segurança de dados foi um pilar presente em todas as publicações. Porém, outros temas também tiveram um grande grau de incidência, como a integração de sistemas, IoT e computação em nuvem, que tiveram sua média de ocorrência próxima ou superior à 50%, demonstrando forte correlação com o tema de segurança de dados nas pesquisas atuais.

Os tópicos de robótica, realidade aumentada e manufatura aditiva tiveram uma incidência bem menos significativa (cerca de 20% das publicações), indicando uma representatividade menor destes temas quando se trata de cibersegurança, como pode ser visualizado no ranking da Tabela 2.

Tabela 2 – Ranking de abordagem dos pilares da Indústria 4.0.

Posição	Pilar da indústria 4.0	Frequência
1º	Segurança da Informação	100,00%
2º	Integração de Sistemas	82,61%
3º	IoT	73,91%
4º	Big Data	47,83%
5º	Computação em Nuvem	47,83%
6º	Simulação	47,83%
7º	Robótica	26,09%
8º	Realidade Aumentada	21,74%
9º	Manufatura Aditiva	17,39%

Fonte: Elaborado pelos autores.

Dessa forma, é possível identificar um caminho que a pesquisa sobre segurança de dados vem tomando nos últimos cinco anos no Brasil, tornando assim, mais visível o grau de correlação do tema com os demais tópicos.

As informações sobre temas específicos da segurança de dados na indústria 4.0 podem ser visualizadas no Quadro 6.

Quadro 6 – Publicações por subtópicos específicos de segurança de dados em indústria 4.0.

Código	Subtópicos de segurança em indústria 4.0									
	1	2	3	4	5	6	7	8	9	10
P1					x					x
P2		x	x					x	x	
P3	x	x	x				x	x		
P4		x	x							
P5					x	x				
P6		x	x	x				x		
P7	x		x				x	x		
P8	x	x						x		
P9		x	x		x					x
P10				x						
P11										x
P12								x	x	
P13				x	x					
P14			x			x			x	x
P15				x	x			x		
P16	x	x	x				x	x	x	
P17	x		x				x	x	x	
P18					x	x				
P19	x	x	x		x				x	
P20		x	x				x			
P21			x		x	x				x
P22					x	x				
P23	x	x	x	x	x			x	x	

Fonte: :Elaborado pelos autores.

Dentre os dez temas selecionados, o tema que se repetiu com maior frequência foi o de “Ataques cibernéticos”, presente em 56,52%. Em seguida, apareceram com a mesma frequência (43,48%) os temas “Testes de software/protocolos de segurança”, “Avaliação da aplicabilidade de um modelo de segurança” e “Benefício da indústria 4.0 na cadeia produtiva”, indicando uma tendência de pesquisa e inovação em prevenção de ataques cibernéticos e proteção de sistemas. O ranking completo é apresentado na Tabela 3:

Tabela 3 – Ranking de ocorrência de temas específicos nas publicações.

Posição	Subtópico	Frequência
1º	Ataques cibernéticos	56,52%
2º	Teste de softwares/protocolo e cibersegurança	43,48%
3º	Benefício da indústria 4.0 na cadeia produtiva	43,48%
4º	Avaliação da aplicabilidade de um modelo de segurança	43,48%
5º	Apresentar contra medidas para ataques cibernéticos	30,43%
6º	Propor direções para o desenvolvimento de conjuntos de dados confiáveis	30,43%
7º	Técnica de criptografia Aumento da segurança de dados em nuvem	21,74%
8º	Inconvenientes para a aplicação da indústria 4.0	21,74%
9º	Ataques em Sistemas de Controle em Rede (NCS)	21,74%
10º	Mapeamento científico na área de estudos da segurança cibernética	21,74%

Fonte: Elaborado pelos autores.

Uma análise da relevância das publicações através do número de citações foi sintetizada por meio de rankings de citações nas tabelas 4 e 5.

Tabela 4 – Ranking de publicações por citações na Web of Science.

Posição	Publicação	Nº de citações
1º	P6	25
2º	P21	16
3º	P19	2
4º	P20	2
5º	P7	1
6º	P17	1
7º	P8	0
8º	P18	0
9º	P22	0
10º	P23	0

Fonte: Elaborado pelos autores.

Como pode ser visualizado no ranking, apenas as publicações P6 e P21 foram massivamente lembradas, o que leva a crer que são trabalhos referência. O baixo número de citações dos demais documentos podem estar relacionado à novidade dos temas no Brasil e/ou a um interesse recente de novos pesquisadores no universo de segurança de dados.

Tabela 5 – Ranking de publicações por citações na Scopus.

Posição	Publicação	Nº de citações
1º	P6	28
2º	P14	9
3º	P20	7
4º	P13	5
5º	P17	2
6º	P1	1
7º	P5	1
8º	P7	1
9º	P10	1
10º	P11	1
11º	P15	1
12º	P2	0
13º	P3	0
14º	P4	0
15º	P9	0
16º	P12	0
17º	P16	0
18º	P23	0

Fonte: Elaborado pelos autores.

Observa-se que na base Scopus, a publicação mais citada também foi a P6, já com um número de citações consideravelmente menor - entre 5 e 9 - merecem destaque os documentos P14, P20 e P13.

O artigo mais citado nas duas bases foi o P6, intitulado “*Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications*” e propõe um novo esquema para abordagem combinada de controle em pente fino para acesso de dados em multi-servidores baseados em nuvem (MCC) e um mecanismo de autenticação de usuários móveis na indústria 4.0 de healthcare. Além de seu caráter inovador que chama atenção, o esquema foi testado e respondeu satisfatoriamente em diferentes ambientes com alta heterogeneidade.

A segunda publicação mais citada (16 citações) e presente apenas na base Web of Science, intitulada “*Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis*” é uma análise bibliométrica utilizando o software SciMAT com objetivo de identificar e clusterizar as principais tendências na indústria 4.0 no período compreendido entre 2011 e 2018, consultando a base científica Scopus.

Os trabalhos P14, P20 e P13 que aparecem nesta sequência no ranking de citações da Scopus são, basicamente, análises bibliométricas e revisões bibliográficas, o que indica um crescente esforço para entender o desenvolvimento e adoção de tecnologias características da indústria 4.0.

O P14, “*20 Years of Scientific Evolution of Cyber Security: a Science Mapping*”, traz uma análise bibliométrica mapeando o crescimento das obras sobre cibersegurança entre os anos 1999 e 2019. No P20, “*Panorama, challenges and opportunities in PROFINET protocol research*”, a bibliometria é debruçada sobre um conjunto de 92 obras com finalidade de avaliar o uso do protocolo

PROFINET. Já em P13, “*Adoption of Industry 4.0 Technologies in Supply Chains*”, é feita uma revisão bibliográfica a fim de avaliar as vantagens da adoção de tecnologias da indústria 4.0 em cadeias de suprimentos, neste caso, o tema da segurança de dados é apenas tangenciado.

5. Conclusões.

O estudo demonstrou o quanto a atividade de pesquisa relacionada a segurança de dados no cenário da indústria 4.0 está aumentando a cada ano no mundo. Os trabalhos de autores com nacionalidade brasileira ainda representam um baixo percentual comparados ao restante do mundo. Porém é visível uma evolução a partir de 2017, com ressalva do ano 2021, ainda em progresso. Mesmo assim, a média inferior a 3% em relação ao resto do mundo mostra uma participação não muito significativa.

Em ambas as plataformas de pesquisa, WoS e Scopus, é possível identificar os nomes de DE SÁ, MACHADO, KIPPER e FURSTENAU como destaques que se repetem, demonstrando engajamento específico sobre o tema da Indústria 4.0 relacionado a segurança de dados. O ranking de citações mostrou que diversos artigos têm ao menos algum grau de conexão com segurança de dados na indústria 4.0, ainda que não seja o tema central. Além disso, é possível concluir que alguns subtópicos se destacam em termos de atenção em pesquisas sobre segurança de dados, com ênfase a pilares da Indústria 4.0, como ‘IoT’, ‘integração de sistemas’ e ‘Big Data’.

Quando se fala de temas mais específicos, que possibilitam destrinchar ainda mais o caminho de tendência de estudos atuais no Brasil sobre o tema, ‘ataques cibernéticos’ é o tema mais citado entre a amostra de artigos estudados. Em segundo lugar é possível identificar empatados três temas: ‘Teste de softwares/protocolo e cibersegurança’, ‘Benefício da indústria 4.0 na cadeia produtiva’ e ‘Avaliação da aplicabilidade de um modelo de segurança’. A maioria dos artigos refere-se a ataques cibernéticos e estudos sobre aplicação e viabilidade de soluções em softwares e protocolos. Também se mostra importante definir os benefícios da indústria 4.0, para que o foco não seja apenas nos problemas dessa nova realidade. Ou seja, os temas específicos com maior relevância se comunicam diretamente.

Finalmente, esse estudo oferece insights e perspectivas futuras sobre o tema, baseadas no enredo presente da pesquisa nacional sobre segurança de dados. É necessário que novos estudos sejam desenvolvidos, uma vez que a indústria 4.0 exerce influência crescente no cotidiano da população brasileira. Portanto, um eixo importante para o desenvolvimento da indústria 4.0, está relacionado ao engajamento dos pesquisadores e das organizações no universo da segurança de dados, afim de contribuir com a solução das problemáticas presentes, minimizar os danos que a fragilidade na segurança de dados tem gerado para sociedade como um todo e ampliar o quantitativo de pesquisas brasileiras em relação a produção global acerca do tema.

Referências.

ALMADA-LOBO, Francisco. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES). **Journal of innovation management**, v. 3, n. 4, p. 16-21, 2015.

ARAÚJO, Carlos AA. Bibliometria: evolução histórica e questões atuais. **Em questão**, v. 12, n. 1, p. 11-32, 2006.

BENCKENDORFF, Pierre. Themes and trends in Australian and New Zealand tourism research: A social network analysis of citations in two leading journals (1994–2007). **Journal of Hospitality and Tourism Management**, v. 16, n. 1, p. 1-15, 2009.

BERTOLLI, Emília. Conheça as principais estatísticas em segurança digital para 2020. **Blog Varonis**. 17 de dez. de 2019. Segurança de Dados. Disponível em: <<https://blog.varonis.com.br/conheca-as-principais-estatisticas-em-seguranca-digital-para-2020>>. Acesso em: 16 de fev. de 2021.

BORGMAN, Christine L.; FURNER, Jonathan. Scholarly communication and bibliometrics. **Annual review of information science and technology**, v. 36, n. 1, p. 2-72, 2002.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 15 de fev. de 2021.

CARDOSO, João Antonio Aparecido et al. Blockchain Based MFA Solution: the use of hydro raindrop MFA for information security on WordPress websites. **Brazilian journal of operations and production management**, 2019.

COELHO, Pedro Miguel Nogueira. **Rumo à indústria 4.0**. 2016. Tese de Doutorado. 00500:: Universidade de Coimbra.

CUNHA, Tairine Pravadelli et al. Proposal guidelines to implement the concepts of industry 4.0 into information technology companies. **The TQM Journal**, 2020.

DALMARCO, Gustavo; BARROS, Ana Cristina. Adoption of Industry 4.0 technologies in supply chains. In: **Innovation and Supply Chain Management**. Springer, Cham, 2018. p. 303-319.

DE ARAÚJO, Thásia Maria Oliveira; DE FARIAS, Mayara Ferreira; FERREIRA, Lissa Valéria Fernandes. Um estudo sobre modelo de gestão dos negócios com ênfase no turismo 4.0. **Revista Turismo: Estudos e Práticas**, v. 9, n. 2, 2020.

DE LAS MORENAS, Javier et al. Security Experiences in IoT based applications for Building and Factory Automation. In: **2020 IEEE International Conference on Industrial Technology (ICIT)**. IEEE, 2020. p. 322-327.

DE RESENDE, Henrique C. Carvalho et al. Enabling QoS-secured Enhanced Non-Public Network Slices for Health Environments. In: **Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good**. 2020. p. 18-23.

DE SÁ, Alan Oliveira et al. Identification of data injection attacks in networked control systems using noise impulse integration. **Sensors**, v. 20, n. 3, p. 792, 2020.

DE SÁ, Alan Oliveira; CARMO, Luiz Fernando Rust da C.; MACHADO, Raphael C. Santos. Countermeasure for identification of controlled data injection attacks in networked control systems. In: **2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)**. IEEE, 2019. p. 455-459.

DE SÁ, Alan Oliveira; MACHADO, Raphael CS. Identification of Data Injection Attacks in Networked Control Systems with Varying Setpoint Condition. In: **2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT**. IEEE, 2020. p. 447-451.

D'EMIDIO, Marcelo. Avaliação da lei de Moore e Proposta de um Modelo de Previsão Alternativo Baseado em Técnicas de Extrapolação de Tendências. **Future Studies Research Journal: Trends and Strategies**, v. 1, n. 2, 2010.

DHARMINDER, Dharminder et al. PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments. **Software: Practice and Experience**, 2020.

DIAS, Andre Luis et al. Panorama, challenges and opportunities in PROFINET protocol research. In: **2018 13th IEEE International Conference on Industry Applications (INDUSCON)**. IEEE, 2018. p. 186-193.

FERRARI, P. et al. Work-in-Progress: Compromising Security of Real-time Ethernet Devices by means of Selective Queue Saturation Attack. In: **2020 16th IEEE International Conference on Factory Communication Systems (WFCS)**. IEEE, 2020. p. 1-4.

FURSTENAU, Leonardo Bertolin et al. 20 years of scientific evolution of cyber security: A science mapping. In: **Proc. Int. Conf. Ind. Eng. Oper. Manage.(IEOM)**. 2020. p. 314-325.

GARCÉS, Lina; OQUENDO, Flavio; NAKAGAWA, Elisa Yumi. Software mediators as first-class entities of systems-of-systems software architectures. **Journal of the Brazilian Computer Society**, v. 25, n. 1, p. 1-23, 2019.

GEHLEN, Marco Aurélio; DE MELLO LOURENCAO, Paulo Tadeu; TRABASSO, Luís Gonzaga. Educating Engineers for the Development of Product Service Systems (PSS). **31st Congress of the International Council of the Aeronautical Sciences**. International Council of the Aeronautical Sciences (ICAS), 2018.

GODIN, Benoît. The culture of numbers: the origins and development of statistics on science. **RECIIS**, v. 2, n. 1, p. 7-18, 2008.

HERMANN, Mario; PENTEK, Tobias; OTTO, Boris. Design principles for industrie 4.0 scenarios. In: **2016 49th Hawaii international conference on system sciences (HICSS)**. IEEE, 2016. p. 3928-3937.

HÉRUBEL, Jean-Pierre VM. Historical Bibliometrics: Its Purpose and Significance to the History of Disciplines. **Libraries & Culture**, v. 34, n. 4, 1999.

JACOBS, Daisy. Demystification of bibliometrics, scientometrics, informetrics and webometrics. In: **11th DIS Annual Conference**. 2010. p. 1-19.

KAGERMANN, Henning et al. Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group. **Forschungsunion: Berlin, Germany**, 2013.

KIPPER, Liane Mahlmann et al. Scientific mapping to identify competencies required by industry 4.0. **Technology in Society**, v. 64, p. 101454, 2021.

KIPPER, Liane Mahlmann et al. Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis. **International Journal of Production Research**, v. 58, n. 6, p. 1605-1627, 2020.

KOSEOGLU, Mehmet Ali et al. Bibliometric studies in tourism. **Annals of Tourism Research**, v. 61, p. 180-198, 2016.

LACERDA, Rogério Tadeu de Oliveira; ENSSLIN, Leonardo; ENSSLIN, Sandra Rolim. Uma análise bibliométrica da literatura sobre estratégia e avaliação de desempenho. **Gestão & Produção**, v. 19, n. 1, p. 59-78, 2012.

LEE, Jay; BAGHERI, Behrad; KAO, Hung-An. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. **Manufacturing letters**, v. 3, p. 18-23, 2015.

MACHADO, Raphael et al. Proficiency Testing for Software Analysis and Cybersecurity Laboratories. In: **2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT**. IEEE, 2020. p. 441-446.

MARCON, Erico et al. Barriers for the digitalization of servitization. **Procedia CIRP**, v. 83, p. 254-259, 2019.

MARTINS, Tiago; OLIVEIRA, Sérgio Vidal Garcia. Cybersecurity in the Power Electronics. **IEEE Latin America Transactions**, v. 17, n. 08, p. 1300-1308, 2019.

MERTON, Robert K. **The sociology of science: Theoretical and empirical investigations**. University of Chicago press, 1973.

NARIN, Francis et al. **Evaluative bibliometrics: The use of publication and citation analysis in the evaluation of scientific activity**. Cherry Hill, NJ: Computer Horizons, 1976.

NIGAM, Vivek; TALCOTT, Carolyn. Automated Construction of Security Integrity Wrappers for Industry 4.0 Applications. In: **International Workshop on Rewriting Logic and its Applications**. Springer, Cham, 2020. p. 197-215.

OESTERREICH, Thuy Duong; TEUTEBERG, Frank. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. **Computers in industry**, v. 83, p. 121-139, 2016.

PACHECO, Carla et al. Building reference datasets to support socialbots detection. In: **2018 Workshop on Metrology for Industry 4.0 and IoT**. IEEE, 2018. p. 198-202.

PEREIRA, Diogo; ARANHA, Matheus; BORGES, Fábio. HTTPS keys in the mediterranean. In: **2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4. 0&IoT)**. IEEE, 2019. p. 449-454.

PODSAKOFF, Philip M. et al. The influence of management journals in the 1980s and 1990s. **Strategic Management Journal**, v. 26, n. 5, p. 473-488, 2005.

PRITCHARD, Alan et al. Statistical bibliography or bibliometrics. **Journal of documentation**, v. 25, n. 4, p. 348-349, 1969.

ROSA, Ferruccio De Franco et al. Coverage-based heuristics for selecting assessment items from security standards: a core set proposal. In: **2018 Workshop on Metrology for Industry 4.0 and IoT**. IEEE, 2018. p. 192-197.

ROY, Sandip et al. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. **IEEE Transactions on Industrial Informatics**, v. 15, n. 1, p. 457-468, 2018.

SALEEM, Kashif et al. Bio-Inspired Network Security for 5G-Enabled IoT Applications. **IEEE Access**, v. 8, p. 229152-229160, 2020.

SANTOS, Beatrice Paiva et al. Indústria 4.0: desafios e oportunidades. **Revista Produção e Desenvolvimento**, v. 4, n. 1, p. 111-124, 2018.

SENADO FEDERAL. Espionagem cibernética : rede vulnerável.**Em Discussão!:os principais debates do Senado Federal**. Brasília: Secretaria de Comunicação Social. v. 5, n. 21,p.1-66, 2014.

SILVA, Márcia Regina; HAYASHI, Carlos Roberto Massao; HAYASHI, Maria Cristina Piumbato Innocentini. Bibliometric and scientometric analyses: challenges for specialists working in the field. **InCID: Revista de Ciência da Informação e Documentação; v. 2 n. 1 (2011); 110-129**, v. 24, n. 2, p. 129-110, 2018.

VAN LEEUWEN, Thed. Descriptive versus evaluative bibliometrics. In: **Handbook of quantitative science and technology research**. Springer, Dordrecht, 2004. p. 373-388.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science: research trends**, v. 9, n. 1, 2015.

YAMADA, Viviane Yukari; MARTINS, Luís Marcelo. Indústria 4.0: um comparativo da indústria brasileira perante o mundo. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, v. 34, n. esp., p. 95-109, 2019.