ISSN: 2175-1897

Tecnologia, inovação e sustentabilidade:
50 anos de Cursos de Tecnologia no Brasil.

Segurança da informação para a Indústria 4.0: levantamento de lacunas de pesquisa

Diogo Pedriali[1] e Carlos Hideo Arima[2]

Resumo - O objetivo deste artigo foi identificar a produção científica internacional sobre a segurança da informação aplicável a indústria 4.0 nas bases de dados *IEEE*, *WoS* e Google Acadêmico, e levantar os principais artigos e as lacunas de pesquisa. Trata-se de uma pesquisa do tipo exploratória e descritiva que se utilizou de bibliometria. Foram identificados 39 trabalhos publicados nos últimos cinco anos. Os resultados sinalizam que os trabalhos publicados sobre o tema exploram o desenvolvimento de algoritmos que buscam melhorar a segurança de sistemas ciberfísicos e a principal lacuna de pesquisa sinalizam a qualificação nas normas internacionais de segurança da informação para as demandas da Indústria 4.0.

Palavras-chave: Indústria 4.0, Segurança da Informação, Estudo Bibliométrico, Lacunas de Pesquisa.

Abstract - The objective of this article was to identify the international literature about information security that is applicable to Industry 4.0 using the databases IEEE, WoS and Google Scholar, and grouping the main articles and the research gaps. This is an exploratory and descriptive research that uses bibliometrics. 39 scientific articles in the last five years have been published. The results indicate that the published works about the subject explore the development of algorithms that seek to improve the security of cyberphysical systems and the main research gap signals the qualification in the information security international standards to the demands of the Industry 4.0.

Keywords: Industry 4.0, Information Security, Bibliometric Study, Research Gaps.

[1] Centro Estadual de educação Tecnológica Paula Souza - diogo.pedriali@cpspos.sp.gov.br
[2] Centro Estadual de educação Tecnológica Paula Souza – charima@uol.com.br

1. Introdução

Este estudo apresenta o levantamento de lacunas de pesquisa utilizando como método de pesquisa a bibliometria para identificação dos principais artigos que abordam o tema da segurança da informação aplicada a Indústria 4.0.

Procurando compreender qual o estado da discussão na academia internacional por meio da identificação dos artigos mais relevantes sobre o tema deste estudo, surge a questão de pesquisa: o que se publica atualmente sobre a segurança da informação para a Indústria 4.0 e quais as oportunidades de futuros estudos que são indicados nos artigos da área de engenharia?

O objetivo desta pesquisa é mapear a produção científica sobre a segurança da informação para a Indústria 4.0 nas bases de dados, *IEEE Xplore Digital Library* (IEEE), *Web of Science* (WoS) e Google Acadêmico, considerando o período de 2015 a 2019.

Pretende-se com o agrupamento e análise dos materiais científicos obtidos por meio dos procedimentos metodológicos adotados, identificar lacunas a serem exploradas, para o desenvolvimento de uma dissertação que aborde a gestão da segurança da informação de dispositivos e aplicações industriais compatíveis com a Indústria 4.0 e também identificar os métodos de combate a incidentes de segurança da informação sugeridos pelos autores dos artigos selecionados.

A ocorrência de incidentes de segurança da informação na indústria não compõe fato inusitado, nem tampouco recente, pois diversos foram os casos no mundo que evidenciaram que a evolução da comunicação e conectividade de dispositivos e máquinas industriais, também resultou em novos alvos para ataques cibernéticos.

Um dos primeiros casos registrados, de incidente de segurança da informação industrial, aconteceu em 1982, na Rússia, quando um *trojan*, provocou a explosão de um gasoduto (RISI, 2015).

Em 2000, na Austrália, um sistema supervisório de controle e aquisição de dados (SCADA) rádio controlado de uma estação de tratamento de esgotos recebeu comandos que causaram o derramamento de mais de 800 mil litros de esgoto não tratado em parques e rios (VILLAS, 2017).

No Irã, em 2010, uma usina de enriquecimento de urânio, foi atacada pelo *malware* Stuxnet (VILLAS, 2017).

No ano de 2016, houveram também ataques relatados nos Estados Unidos da América (EUA), o primeiro causou a alteração da quantidade de produtos químicos utilizados para tratamento de água que atendia 2,5 milhões de consumidores e o segundo foi ocasionado por *hackers* iranianos que conseguiram acesso a uma pequena barragem de controle de inundação com cerca de 30 km de distância do *Central Park*, em Nova Iorque (VILLAS, 2017).

Após a apresentação de alguns incidentes que chegaram ao conhecimento da população mundial, é importante citar que as limitações do estudo aqui apresentado indicará a possibilidade da realização do aprofundamento de interpretação dos artigos selecionados como relevantes e também a oportunidade da expansão da pesquisa para que sejam adicionadas dissertações e teses publicadas sobre o assunto para o aumento da quantidade dos documentos analisados durante o estudo.

2. Referencial Teórico

A quarta revolução industrial, também chamada de Indústria 4.0, trata-se de uma abordagem estratégica para a integração de sistemas de controle avançados com tecnologia de *internet*, que permite a comunicação entre as pessoas, produtos e sistemas complexos (ANDERL, 2015).

Os fundamentos básicos da Indústria 4.0 implicam que através da conexão de máquinas, sistemas e recursos, as organizações podem criar redes inteligentes ao longo da cadeia de valor controlando os processos de produção de forma autônoma (SANTOS *et al.*, 2017).

Brettel *et al.* (2014) citam que a Indústria 4.0 comporta a comunicação entre os seres humanos, bem como com as máquinas em um sistema denominado ciberfísico (CPS) o que pode resultar o surgimento de grandes redes.

As principais tecnologias que sustentam a Indústria 4.0 são: *Internet* das Coisas (IoT), *Big Data*, Realidade móvel e aumentada, Manufatura aditiva, Computação em Nuvem e Segurança Cibernética (SANTOS *et al.*, 2017).

A grande quantidade de dados que são criados, transferidos, coletados e analisados automaticamente pelos sistemas de inteligência artificial constituem um importante ativo industrial. Tratar com a devida importância estas informações mostra-se pertinente a Indústria 4.0 pois, a perda da confidencialidade, da disponibilidade ou da integridade dos dados, pode resultar em perdas nos processos industriais (SANTOS *et al.*, 2017).

Para se ter segurança da informação deve-se garantir a confidencialidade, disponibilidade e integridade das informações, por meio da aplicação e do gerenciamento de controles que envolvem uma ampla gama de ameaças, com o objetivo de garantir a continuidade do negócio e minimizar as consequências dos incidentes de segurança (ISO/IEC 27000, 2018).

Diversos são os tipos de comunicação utilizados nos sistemas ciberfísicos da Indústria 4.0, como por exemplo *Devide to Device* (D2D) e *Machine to Machine* (M2M), que podem ser conectados por meios físicos (cabos) ou eletromagnético (*wireless*). Devido à grande diversidade de possiblidades de conexão para transmissão de dados utilizados na Indústria 4.0, também há grande variação de protocolos de comunicação, arquitetura de redes e tecnologias de rede (SANTOS; VOLANTE, 2018).

A comunicação sem fio atrai a atenção de pesquisadores e de profissionais técnicos, pois a conectividade sem fio traz grande flexibilidade para as empresas, além de conectar diferentes tipos de componentes em uma mesma rede e facilitando a efetiva comunicação entre diversos dispositivos industriais (SANTOS; VOLANTE, 2018).

Quanto ao método científico denominado bibliometria, identifica-se como uma ferramenta quantitativa que visa minimizar a subjetividade inerente à indexação e recuperação de informações, produzindo conhecimento em uma determinada área (GUEDES; BORSCHIVER, 2005) e como metodologia busca documentar os padrões de publicações dos autores, considerando as referências que citam em seus trabalhos e as em que são citados (HEBERGER; CHRISTIE; ALKIN, 2010).

Na utilização da bibliometria como método científico neste estudo, respeitou-se as principais leis da bibliometria, onde a Lei de Bradford analisa a produtividade de periódicos, a Lei de Lotka analisa a produtividade científica de autores, e a Lei de Zipf verifica a frequência de palavras.

3. Método

A metodologia utilizada neste estudo pode ser classificada, de acordo com o trabalho de Prodanov e Freitas (2013), quanto à natureza como pesquisa básica.

Quanto ao objetivo pode-se caracterizar como pesquisa exploratória e descritiva e quanto ao procedimento científico, caracteriza-se como pesquisa bibliométrica.

A escolha das bases de dados IEEE, WoS e Google Acadêmico para a pesquisa se justifica pela abrangência de cobertura de áreas do conhecimento científicos. Além disso, as bases escolhidas possibilitam integração a ferramentas computacionais que auxiliam na recuperação dos metadados de interesse, o que viabiliza a execução das análises planejadas para este estudo.

À partir da bibliometria foi levantada a distribuição das publicações por ano, a identificação dos autores com maior número de publicações na temática, a identificação dos periódicos que abordam o tema, as palavras-chaves mais utilizadas pelos artigos, as palavras mais utilizadas nos títulos dos artigos, a identificação dos artigos mais relevantes sobre o tema e as lacunas de pesquisa apresentadas pelos autores dos artigos selecionados.

Como filtros aplicados nas máquinas de busca das bases de dados, utilizou-se como descritores "*Industry 4.0*" e "*information security*"; pesquisando-se somente nos títulos de artigos escritos em inglês e que foram revisados por pares.

Foi dada prioridade de leitura aos artigos publicados em periódicos da área de Engenharia.

Para ampliar a possibilidade de localização de artigos nas bases de dados escolhidas, foi utilizada a *string* (*"4.0" AND "security")* como termo de pesquisa.

A Tabela 1 apresenta o conjunto de termos utilizados para a busca inicial dos artigos nas coleções principais das bases de dados escolhidas.

Tabela 1 - Termos de busca e filtros aplicados nas bases de dados.

Base	*Strings*	Filtros aplicados	Quantidade
IEEE	*("4.0" AND "security")*	*Journal Articles;* Idioma: *English*; Período: 2015-2019.	6
WoS	*("4.0" AND "security")*	*Article*; Idioma: *English;* Período: 2015-2019.	8
Google Acadêmico	*("4.0" AND "security")*	*Article*; Idioma: *English;* Período: 2015-2019.	25

Fonte: Resultado da pesquisa.

A coleta dos dados foi realizada no período de março a junho de 2019 e foram identificados 39 trabalhos publicados nos últimos cinco anos que compõem o *corpus* deste levantamento bibliométrico.

Em seguida, exportou-se os dados dos resultados obtidos para serem tratados no programa EndNote e também para eliminar os artigos duplicados.

Foi realizada a leitura dos títulos e resumos dos artigos para validar a seleção de documentos e então iniciou-se a coleta dos dados relevantes para a

pesquisa, que estão compilados e apresentados no tópico resultados e discussão deste artigo.

Além dos dados gerados com auxílio das ferramentas disponíveis no programa EndNote, foram analisados também os aspectos qualitativos dos textos dos artigos mais relevantes, no intuito de identificar suas principais contribuições para a temática da segurança da informação para a Indústria 4.0.

4. Resultados e Discussão

Após o levantamento e tratamento dos dados bibliométricos, foram identificados 25 artigos contendo os termos "*4.0*" e "*security"* em seus títulos e que atendiam o escopo do estudo.

Estes artigos estão publicados em 20 periódicos indexados nas bases de dados utilizadas e foram escritos por 77 autores, considerando a somatória dos autores principais e co-autores. Na Tabela 2, são apresentados esses resultados.

Tabela 2 - Resultado da bibliometria.

Dados bibliométricos	Quantidade
Publicações (artigos)	25
Periódicos indexados	20
Autores	77

Fonte: Resultado da pesquisa.

A evolução anual das publicações sobre o tema deste estudo é apresentada na Figura 1. Observa-se que no período de 2015 a 2018, em média, 4,5 artigos foram publicados por ano. Vale ressaltar que referente ao ano de 2019, os dados levantados contemplam os meses de janeiro a junho e para o cálculo da média de publicações por ano estes não foram considerados.

Figura 1 - Publicações distribuídas por ano.

Fonte: Resultado da pesquisa.

O periódico internacional mais representativo sobre a temática deste estudo é o IEEE Access com 4 (17,4%) artigos publicados e possui fator de impacto h-index 56, conforme exibido na Tabela 3.

Tabela 3 - Periódicos com mais artigos publicados sobre a temática.

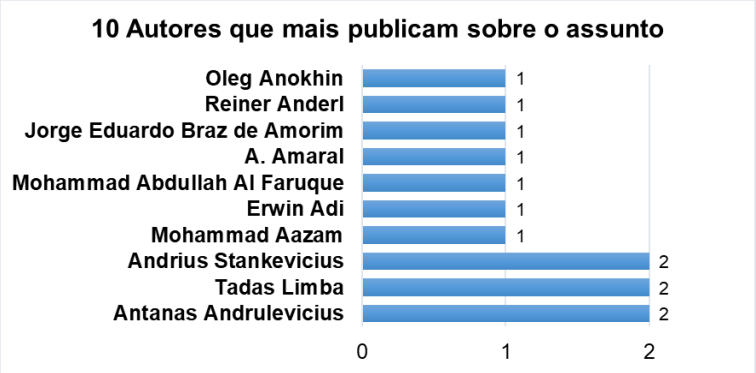
Periódicos	h-index	Quantidade de Artigos	%
IEEE Access	56	4	17,4
Informatik 2017	*	1	4,3
Asian Journal of Information and Communications	*	1	4,3
AT-Automatisierungstechnik	22	1	4,3
Computers in Industry	87	1	4,3
Global Journal of Computer Science and Technology	24	1	4,3
IEEE Transactions on Industrial Informatics	100	1	4,3
IET Information Security	26	1	4,3
Journal of Hardware and Systems Security	*	1	4,3
Processes	16	1	4,3

* Periódico ainda não avaliado.

Fonte: Resultado da pesquisa.

Após a análise dos periódicos, foram identificados os autores que possuem a maior quantidade de artigos publicados sobre a temática, nesse sentido se destacam: Antanas Andrulevicius, Tadas Limba e Andrius Stankevicius cada um deles com 2 registros de artigos publicados, conforme apresentado na Figura 2.

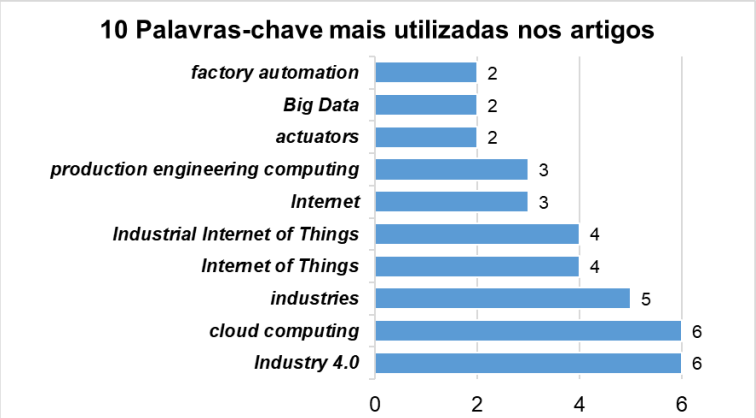
Figura 2 - Autores com maior quantidade de artigos publicados.



Fonte: Resultado da pesquisa.

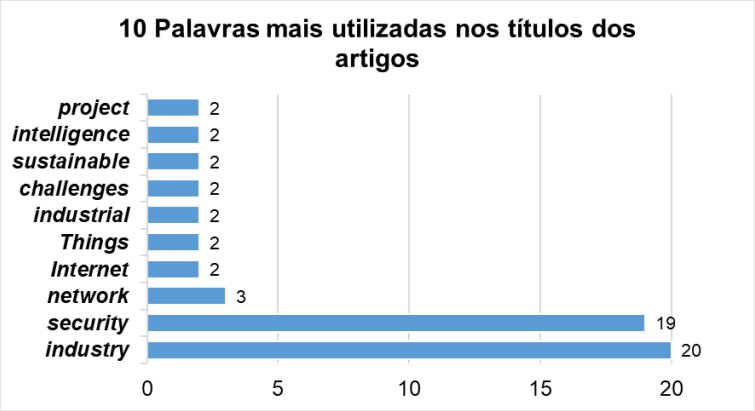
Com o objetivo de identificar os termos e as palavras-chaves que indiquem oportunidades de refinamento para futuras pesquisas, foi realizado o levantamento das palavras-chaves mais utilizadas pelos autores e das palavras que mais se repetiram nos títulos, conforme mostrado na Figura 3 e na Figura 4.

Figura 3 - Palavras-chaves mais utilizadas nos artigos encontrados.



Fonte: Resultado da pesquisa.

Figura 4 - Termos que mais aparecem nos títulos dos artigos encontrados.



Fonte: Resultado da pesquisa.

As palavras-chaves que se destacam são *Industry 4.0* e *cloud computing* com 6 ocorrências cada uma e os termos que mais se repetiram nos títulos dos artigos destacam-se *industry* com 20 ocorrências e *security* com 19 ocorrências.

Os artigos selecionados como mais relevantes para este estudo estão relacionados no Quadro 1.

Quadro 1 - Artigos selecionados de acordo com a temática do estudo.

ID	Título do Artigo	Periódico
1	*Concept and use case driven approach for mapping it security requirements on system assets and processes in Industrie 4.0*	*Procedia CIRP*
2	*Information security breaches and precautions on Industry 4.0*	*Technology Audit and Production Reserves*
3	*Network and information security challenges within Industry 4.0 paradigm*	*Procedia Manufacturing*
4	*Interoperability and security challenges of Industry 4.0*	*Informatik 2017*
5	*A new threat intelligence scheme for safeguarding Industry 4.0 systems*	*IEEE Access*

(continuação)

6	*Effect of cooperation on manufacturing IT project development and test bed for successful Industry 4.0 project: safety management for security*	*Processes*
7	*Integration of cyber security frameworks, models and approaches for building design principles for the Internet-of-Things in Industry 4.0*	*IET Information Security*
8	*A review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories*	*IEEE Access*
9	*An efficient web authentication mechanism preventing man-in-the-middle attacks in Industry 4.0 supply chain*	*IEEE Access*
10	*An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components*	*Computers in Industry*

Fonte: Resultado da pesquisa.

Também foi realizada a síntese de informações coletadas por meio da análise do título, do resumo, dos resultados e das considerações finais de cada artigo e o resultado é apresentado no Quadro 2.

Quadro 2 - Síntese dos artigos selecionados.

ID	Síntese dos artigos
1	Aborda um modelo arquitetural de referência da Indústria 4.0 (RAMI 4.0) por meio do desenvolvimento de um algoritmo que busca promover a segurança da informação de sistemas industriais 4.0. (WANG; ANOKHIN; ANDERL, 2017)
2	Apresenta estudo das vulnerabilidades comuns a segurança da informação em sistemas computacionais da Indústria 4.0 e propõe plano de segurança. (KONDILOGLU *et al.*, 2017)
3	São destacadas reflexões sobre a segurança da informação e discute-se as boas práticas para promover a integridade, privacidade e disponibilidade de informação para a Indústria 4.0. (PEREIRA; BARRETO; AMARAL, 2017)
4	Apresenta visão geral de padrões, como IEC 62443, série ISO 27000, Arquitetura Unificada de Conectividade Aberta IEC 62541 (OPC UA) e Redes Sensíveis ao Tempo (TSN) (IEEE 1722-2016), para promover a interoperabilidade e a segurança dos dispositivos para a Indústria 4.0. (WATSON *et al.*, 2017)
5	Propõe um mecanismo de Markov de mistura oculta beta (MHMM) para projetar inteligência de ameaças que monitora e reconhece ataques cibernéticos de sistemas da Indústria 4.0. (MOUSTAFA *et al.*, 2018)
6	Compara projetos de integração de sistemas (SI) normais com projetos de desenvolvimento e operações (DevOps), para propor um método de desenvolvimento viável para a fabricação de projetos de TI para a Indústria 4.0. (PARK; JUN-HO, 2018)
7	Propõe nova arquitetura para a integração de *frameworks* para segurança da informação na Indústria 4.0 e discute modelo holístico de avaliação de impacto econômico para o risco cibernético da *internet* das coisas. (RADANLIEV *et al*., 2018)
8	Apresenta estudo das aplicações industriais mais relevantes baseadas em *blockchain* para cada tecnologia da Indústria 4.0, com foco na segurança cibernética. (FERNÁNDEZ-CARAMÉS; FRAGA-LAMAS, 2019)
9	Propõe um mecanismo de autenticação baseado em segurança da camada de transporte (TLS) para aplicativos da Web que usam o protocolo TLS para proteger a comunicação HTTP contra ciber ataques na Indústria 4.0. (ESFAHANI *et al.*, 2019)
10	Demonstra a importância de focar no ser humano ao iniciar o projeto de sistemas da Indústria 4.0 para constituir adequadamente um sistema humano ciberfísico (CPHS). (SHARPE *et al*., 2019)

Fonte: Resultado da pesquisa.

Ao realizar a construção da síntese dos artigos selecionados neste estudo, identifica-se como lacunas de pesquisa sobre segurança da informação para a Indústria 4.0, o desenvolvimento de estudos de caso sobre políticas e estratégias de segurança desenvolvidas nas organizações dentro do paradigma da Indústria 4.0, para determinar o nível de conscientização existente dentro das organizações, bem como para explicar as dificuldades e apontar os benefícios gerais de implementação.

A segunda lacuna observada sinaliza a oportunidade da aplicação de testes para qualificar as recomendações dos padrões internacionais de segurança da informação tais como: IEC 62443, IEC 62541, ISO 27000 e IEEE1722-2016, para avaliar se são suficientes e eficientes com base nos requisitos da internet industrial das coisas (IIoT) e da Indústria 4.0.

E a terceira lacuna indica a possibilidade do desenvolvimento de *framework* que integre modelos eficazes de avaliação de impacto econômico e de risco cibernético, com viés à Indústria 4.0.

5. Considerações finais

Identificar como é constituído o processo e como deve ser aplicada a bibliometria auxilia os pesquisadores na identificação e coleta de informações que subsidiem a adequada produção de conhecimento científico.

Ao final da aplicação do método de bibliometria neste estudo, foi possível estabelecer o referencial teórico atual sobre a segurança da informação aplicável a Indústria 4.0, identificar as principais lacunas de pesquisa sobre a temática, e, portanto, os objetivos específicos deste trabalho foram atingidos.

Como um dos critérios de seleção aplicados durante o levantamento bibliométrico foi de somente buscar identificar artigos científicos, há a possiblidade de extensão desta pesquisa ao buscar a seleção dos demais materiais científicos, tais como dissertações e teses.

As lacunas identificadas por meio da coleta de dados e sintetização das sugestões de trabalhos futuros registradas pelos autores dos artigos selecionados proporciona a identificação do sentido que os futuros estudos sobre a segurança da informação para a Indústria 4.0 pode seguir.

Entre os três pilares que sustentam a segurança da informação: confidencialidade, disponibilidade e integridade, este último (integridade) é o pilar que para a Indústria 4.0 se apresenta como o principal em termos de importância de estudo como vista a segurança da informação, pois as atuais tecnologias de criptografia e as boas práticas de disponibilização de acesso sustentam satisfatoriamente os dois primeiros pilares (confidencialidade e disponibilidade).

Os dados e as informações consolidam-se como ativos de uma empresa, principalmente para as empresas que produzem conhecimento, produtos e serviços inovadores. Para estas empresas a perda da integridade dos dados podem resultar em perdas financeiras irreparáveis.

Por fim, o uso das bases de dados IEEE, WoS e Google Acadêmico pode ser apresentada nestas considerações finais como um limitante e como indicativo de possibilidade de ampliação deste estudo.

Referências

ANDERL, Reiner. Industrie 4.0: fundamentals, scenarios for application and strategies for implementation. *Diálogo Brasil-Alemanha de Ciência, Pesquisa e Inovação*, São Paulo, v. 4, 2015. Disponível em: <https://dwih.com.br/sites/default/files/imce_default/reiner_anderl.pdf>. Acesso em: 2 jun. 2019.

BRETTEL, Malte; FRIEDERICHSEN, Niklas; KELLER, Michael; ROSENBERG, Marius. How virtualization, decentralization and network building change the manufacturing landscape: an Industry 4.0 perspective. *International Journal of Information and Communication Engineering*, v. 8, n. 1, p. 37-44, 2014. Disponível em: <https://waset.org/publications/9997144/how-virtualization-decentralization-and-network-building-change-the-manufacturing-landscape-an-industry-4.0-perspective>. Acesso em: 2 jun. 2019.

ESFAHANI, Alireza; MANTAS, Georgios; RIBEIRO, Jose; BASTOS, Joaquim; MUMTAZ, Shahid; VIOLAS, Manuel A.; DUARTE, A. Manuel de Oliveira; RODRIGUEZ, Jonathan. An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. *IEEE Access*, v. 7, p. 1-9, 2019.

FERNÁNDEZ-CARAMÉS, Tiago M.; FRAGA-LAMAS, Paula. A review on the application of blockchain for the next generation of cybersecure Industry 4.0 smart factories. *IEEE ACCESS*, p. 45201-45218, 2019. Disponível em: <http://arxiv.org/abs/1902.09604>. Acesso em: 2 jun. 2019.

GUEDES, Vânia L. S.; BORSCHIVER, Suzana. Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *VI CINFORM - UFBA*, Salvador, p. 1–18, 2005. Disponível em: <http://www.cinform-anteriores.ufba.br/vi_anais/docs/VaniaLSGuedes.pdf>. Acesso em: 2 jun. 2019.

HEBERGER, Anne E.; CHRISTIE, Christina A.; ALKIN, Marvin C. A bibliometric analysis of the academic influences of and on evaluation theorists' published works. *American Journal of Evaluation*, v. 31, n. 1, p. 24-44, 2010. Disponível em: <http://journals.sagepub.com/doi/10.1177/1098214009354120>. Acesso em: 2 jun. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000: Information technology - overview and vocabulary. 2018. 38 p. Disponível em: <http://k504.khai.edu/attachments/article/819/ISO_27000_2014.pdf>. Acesso em: 27 jun. 2019.

KONDILOGLU, Adil; BAYER, Harun; CELIK, Enes; ATALAY, Muhammet. Information security breaches and precautions on Industry 4.0. *Technology Audit and Production Reserves*, v. 6, n. 4, p. 58-63, 2017.

MOUSTAFA, Nour; ADI, Erwin; TURNBULL, Benjamin; HU, Jiankun. A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access*, v. 6, p. 32910–32924, 2018.

PARK, Sangil; JUN-HO, Huh. Effect of cooperation on manufacturing IT project development and test bed for successful Industry 4.0 project: safety management for security. *Processes*, v. 6, n. 7, 2018. Disponível em: <http://search.proquest.com/docview/2125025496/>. Acesso em: 2 jun. 2019.

PEREIRA, T.; BARRETO, L.; AMARAL, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, v. 13, p. 1253–1260, 2017. Disponível em: <https://doi.org/10.1016/j.promfg.2017.09.047>. Acesso em: 2 jun. 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. *Metodologia do trabalho cientifico:* métodos e técnicas de pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book Metodologia do Trabalho Cientifico.pdf%0Ahttps://www.cambridge.org/core/product/identifier/CBO9781107415324A009/type/book_part>. Acesso em: 14 maio 2019.

RADANLIEV, Petar; DE ROURE, Dave; NURSE, Jason R.C.; NICOLESCU, Razvan; HUTH, Michael; CANNADY, Stacy; MONTALVO, Rafael Mantilla. Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. *IET Information Security*, p. 1-6, 2018.

RISI. *CIA trojan causes siberian gas pipeline explosion.* 2015. Disponível em: <https://www.risidata.com/Database/event_date/asc>. Acesso em: 2 jun. 2019.

SANTOS, Diego Rafael Guedes dos; VOLANTE, Carlos Rodrigo. A importância da tecnologia sem fio na Indústria 4.0. *Interface Tecnológica*, p. 245–254, 2018.

SANTOS, Maribel Yasmina; OLIVEIRA, Jorge; ANDRADE, Carina; LIMA, Francisca Vale; COSTA, Eduarda; COSTA, Carlos; MARTINHO, Bruno; GALVÃO, João. A Big Data system supporting Bosch Braga Industry 4.0 strategy. *International Journal of Information Management*, p. 1–11, 2017. Disponível em: <http://dx.doi.org/10.1016/j.ijinfomgt.2017.07.012>. Acesso em: 2 jun. 2019.

SHARPE, Richard; VAN LOPIK, Katherine; NEAL, Aaron; GOODALL, Paul; CONWAY, Paul P.; WEST, Andrew A. An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components. *Computers in Industry*, v. 108, p. 37-44, 2019. Disponível em: <https://doi.org/10.1016/j.compind.2019.02.007>. Acesso em: 2 jun. 2019.

VILLAS, Marcos. *Segurança 4.0*. 2017. Disponível em: <https://canaltech.com.br/seguranca/in-seguranca-40-102354/>. Acesso em: 2 jun. 2019.

WANG, Yübo; ANOKHIN, Oleg; ANDERL, Reiner. Concept and use case driven approach for mapping it security requirements on system assets and processes in industrie 4.0. *Procedia CIRP*, v. 63, p. 207-212, 2017. Disponível em: <http://dx.doi.org/10.1016/j.procir.2017.03.142>. Acesso em: 2 jun. 2019.

WATSON, Venesa; TELLABI, Asmaa; SASSMANNSHAUSEN, Jochen; LOU, Xinxin. Interoperability and security challenges of industry 4.0. *Informatik 2017*, p. 973-985, 2017.