Research, Society and Development, v. 9, n. 2, e38921949, 2020
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v9i2.1949

Segurança da informação na Logística 4.0: um estudo bibliométrico

Information security in Logistics 4.0: a bibliometric study

Seguridad de la información en Logística 4.0: un estudio bibliométrico

Recebido: 29/10/2019 | Revisado: 29/10/2019 | Aceito: 07/11/2019 | Publicado: 08/11/2019

Diogo Pedriali
ORCID: https://orcid.org/0000-0002-4579-2393
Centro Estadual de Educação Tecnológica Paula Souza, Brasil
E-mail: diogo.pedriali@cpspos.sp.gov.br
Carlos Hideo Arima
ORCID: https://orcid.org/0000-0001-7922-0943
Centro Estadual de Educação Tecnológica Paula Souza, Brasil
E-mail: charima@uol.com.br
Fabrício José Piacente
ORCID: https://orcid.org/0000-0001-8306-4541
Centro Estadual de Educação Tecnológica Paula Souza, Brasil
E-mail: fabricio.piacente@fatec.sp.gov.br

Resumo

O objetivo deste artigo foi identificar o nível de importância da segurança da informação que a Logística 4.0 tem demandado por meio da análise da literatura científica internacional. Foram consultadas as bases de dados Google Acadêmico e CORE, e o período pesquisado foi de 2014 a 2019. Este estudo trata-se de uma pesquisa do tipo exploratória e descritiva que se utilizou de bibliometria e de computação cognitiva. Foram selecionadas 33 publicações que abordam a segurança da informação, a logística interna industrial e a Logística 4.0. Percebe-se que há oportunidade de desenvolvimento de ferramentas que auxiliem a segurança das informações compartilhadas com a cadeia de suprimentos.

Palavras-chave: Segurança da Informação; Logística 4.0; Bibliometria.

Abstract

The objective of this paper was to identify the level of information security importance that Logistics 4.0 has demanded analyzing the international scientific literature. The Google Scholar and CORE databases were consulted, and the search period was from 2014 to 2019.

This study is an exploratory and descriptive research that used bibliometrics and cognitive computing. Thirty-three publications were selected and addressing information security, internal industrial logistics and Logistics 4.0. There is opportunity to develop tools that help to preserve the security of information shared with the supply chain.

Keywords: Information security; Logistics 4.0; Bibliometrics

Resumen

El objetivo de este trabajo fue identificar el nivel de importancia de la seguridad de la información que Logistics 4.0 ha exigido a través del análisis de la literatura científica internacional. Se consultaron las bases de datos Google Academic y CORE, y el período de investigación fue de 2014 a 2019. Este estudio es una investigación exploratoria y descriptiva que utilizó bibliometría y computación cognitiva. Se seleccionaron 33 publicaciones sobre seguridad de la información, logística industrial interna y Logística 4.0. Se observa que existe la oportunidad de desarrollar herramientas que ayuden a la seguridad de la información compartida con la cadena de suministro.

Palabras clave: Seguridad de la Información; Logística 4.0; Bibliometría

1. Introdução

O setor logístico desempenha papel fundamental nos sistemas econômicos e na rotina cotidiana. Dadas necessidades de aumentar a eficiência, a lucratividade e a redução dos custos de produção e mão-de-obra em todos os setores empresarias, a redução dos custos de logística mostrou-se uma tarefa importante para os gerentes.

Nesse sentido um conjunto de investimentos em inovações de processos e gestão são aplicados cotidianamente nas diversas esferas das organizações na busca de melhoria. Galhardi & Zaccarelli. (2005) identificou que o problema do desenvolvimento de inovações tecnológicas é complexo, e que não existe necessariamente uma relação linear entre o nível de financiamento disponível e o número de inovações que realmente funcionam a nível empresarial. Assim, a busca por alternativas tecnológicas na área de informática tem ganhado destaque no setor de logística.

A adoção das Tecnologias de Informação e Comunicação (TIC) por diversas empresas têm apresentado como resultados o aumento da eficiência operacional, a diminuição dos erros de entrada de dados, a diminuição dos custos e o aumento do nível de atendimento ao cliente (Muhammad et al., 2014).

Nota-se que devido ao aumento da competitividade entre as empresas, a evolução do departamento de logística' se mostra como medida estratégica diferenciada. Deve-se buscar diminuir a utilização de computadores básicos e impressão de documentos, e aumentar o uso de tecnologia de automação logística, tais como, sistemas computacionais avançados, servidores de dados e robôs de movimentação de materiais por todo o espaço de trabalho sem a necessidade de entrada ou supervisão humana (Wood et al., 2014).

No futuro, as fábricas confiarão totalmente em software compatível com tempo real que pode ser interligado espontaneamente (Sauer, 2014).

É um grande desafio o desenvolvimento de infraestruturas seguras para o compartilhamento de dados com as diferentes partes interessadas do negócio, e que garanta a privacidade e a segurança dos dados (El Kadiri et al., 2016).

Galegale et al. (2017) analisaram os controles citados nas políticas de segurança da informação das organizações visando identificar a existência de dispositivos recorrentes para subsidiar a tomada de decisão pelo gestor da informação, acerca dessa política. Destacaram a importância dos controles criptográficos que protegem a confidencialidade, a autenticidade ou a integridade das informações transitadas dentro e fora das organizações.

No trabalho de Wood et al.(2014), as tecnologias logísticas são categorizadas em cinco elementos, sendo sistemas de informações logísticas, sistemas de gerenciamento de transporte, Sistemas de Informação Geográfica (SIG), Sistemas Avançados de Planejamento (SAP) para controle de inventário e sistemas de gerenciamento de eventos da cadeia de suprimento (SCEM). Os sistemas de Planejamento de Recursos Empresariais (ERP) substituem ou incorporam essas estas formas de tecnologia logística.

Nota-se que ainda há a necessidade de abordar os problemas ligados a definição de infraestruturas e padrões apropriados, a garantia da segurança dos dados e o treinamento de funcionários para seguir o caminho da Indústria 4.0 (Hofmann & Rusch, 2017).

A frequência e o impacto financeiro dos ataques cibernéticos nas empresas dobraram nos últimos cinco anos e devem triplicar nos próximos cinco anos. A violação da segurança cibernética representa um desafio dinâmico para as empresas e ameaça suas operações e sua vantagem competitiva (Sarder & Haschak, 2019).

O objetivo geral deste artigo é identificar, através de um estudo bibliométrico em bases de artigos científico, como as pesquisas tem abordado o nível de importância da segurança da informação que a Logística 4.0 demanda.

Neste artigo especial atenção é dada a segurança cibernética e na identificação de quais técnicas de segurança têm sido aplicadas na logística interna das indústrias.

A coleta e análise de dados neste estudo se limitou às bases de dados CORE (core.ac.uk) e Google Acadêmico e somente os documentos científicos que tratam dos sistemas de informação da logística interna da produção industrial foram utilizados.

O artigo contêm, além da introdução, na sequência, o referencial teórico que apresenta os conceitos fundamentais do trabalho; o método utilizado para o desenvolvimento do estudo, que está contido na terceira seção; na quarta seção são apresentados os resultados e as discussões pertinentes a síntese dos documentos coletados; as considerações finais, bem como a identificação de limitações e oportunidades de estudos futuros são apresentadas na quinta seção deste trabalho.

2. Referencial Teórico

Gestores utilizam a informação para tomada de decisão fazendo com que as organizações alcancem seus objetivos e melhorem seu desempenho no mercado. Assim, a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação (TI) nos processos organizacionais e deve ter proteção adequada. A segurança da informação e seus problemas são tratados em diversas dimensões e por diversas iniciativas, tanto na literatura como dentro das organizações dos mais variados seguimentos.

Assim, segundo Galegale (2017), as falhas na segurança da informação comprometem a informação e podem representar tanto prejuízos financeiros como danos à imagem das organizações.

Define-se segurança da informação como sendo as ações de proteção da informação, de modo a preservar as suas propriedades de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio. Evitando que as vulnerabilidades dos ativos a ela relacionados sejam exploradas por ameaças e possam ocasionar perdas para os negócios de uma organização, não estando restrita a sistemas de computação, nem à informação em formato eletrônico (Gordon & Loeb, 2002; ABNT, 2006).

2.1 A Indústria 4.0

A plataforma da Indústria 4.0 foi oficialmente apresentada durante a feira Hannover Messe Industrie, na Alemanha, em 2011, desde então as empresas identificam e reconhecem o potencial dos aplicativos I 4.0, bem como suas aplicações e benefícios resultantes (Wang et al., 2017).

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).

Como objetivo latente, proposta pela plataforma de tecnologias da Indústria 4.0, busca-se a consolidação da manufatura digital, também denominada fábrica "inteligente", e que utilizará redes inteligentes, mobilidade, flexibilidade das operações industriais e sua interoperabilidade, integração de clientes e modelos de negócios inovadores (Pereira et al., 2017).

Assim como na primeira, segunda e terceira revolução industrial, na quarta revolução industrial os regulamentos e normas legais foram parcialmente ignorados e desta forma a cibersegurança não foi considerada em seu potencial máximo. A explicação para esta observação é porque as tecnologias, conceitos e protocolos utilizados nas operações da indústria ainda não foram conectados totalmente entre si (Kondiloglu et al., 2017).

Observa-se que os sistemas e dispositivos industriais atualmente usados na Indústria 4.0 não foram projetados para o modo de operação interconectada em que estão sendo implantados. Esses sistemas geralmente não fornecem todos os recursos de segurança de informações necessários (Wang et al., 2017).

Novas soluções tecnológicas sempre carregam vulnerabilidades de segurança, que na maioria das vezes revelam riscos inesperados. Com a crescente dependência da tecnologia para obtenção de vantagem competitiva, os problemas de segurança têm sido um dos requisitos mais críticos e desafiadores para a realização de negócios bem-sucedidos (Pereira et al., 2017).

A Indústria 4.0 ainda desempenhará um papel significativo na transformação de empresas tradicionais em "fábricas inteligentes", com a ajuda da Internet das Coisas (IoT) e de Sistemas Ciberfísicos (Eerboz, 2017).

A fábrica inteligente por natureza é interconectada com muitos outros sistemas, o que por consequência observa-se aumento da complexidade do sistema total e com a complexidade surge também o aumento significativo das vulnerabilidades de segurança anteriormente não esperadas (Pereira et al., 2017). Com o aumento da conectividade e o uso de protocolos de comunicação padrão que acompanham o setor 4.0, a necessidade de proteger sistemas industriais e linhas de fabricação críticas contra ameaças de segurança cibernética aumenta dramaticamente (Stefaniuk, 2016).

Sarder & Haschak (2019) definem o termo cibersegurança como a capacidade de impedir, de defender e de recuperar-se de interrupções causadas por ataques cibernéticos de

adversários. A cibersegurança deve compor um dos principais focos dos governos e das empresas.

A existência e a implantação da plataforma tecnológica identificada como Indústria 4.0 adicionam a possiblidade de automatização de departamentos e setores fabris inteiros. Por haver o direcionamento de tecnologias mais adequadas para cada departamento surgem também denominações derivativas com a Logística 4.0.

2.2 Logística 4.0 na cadeia de suprimentos

Nowak (2015) divide o gerenciamento logístico, em cinco áreas básicas de tomada de decisão que qualquer empresa da cadeia de suprimentos precisa abordar diariamente sendo estas a produção, o estoque interno, armazenagem de produtos finalizados, transporte e sistema de informação.

Com base nestas cinco áreas de tomada de decisão, torna-se possível a designação dos tipos de logística que serão utilizados neste estudo. Estas serão denominadas de logística de suprimentos, de logística interna, de logística de distribuição e de logística reversa.

Na Logística 4.0, busca-se a automação dos processos ligados à área de logística. Uma sugestão de configuração integradora da logística interna produtiva é apresentada no trabalho de Zhang et al.(2018), o autor apresenta um framework de Sistema Inteligente de Produção e Logística (SPLS). Este framework considera a utilização de tecnologias da Indústria 4.0, tais como sistemas ciberfísicos (CPS), Internet das Coisas Industriais (IIoT) e Sistemas de Informação .

Como sugestão de método de Segurança da Informação (SI) e da privacidade de dados no SPLS, Zhang et al.(2018) apontou que a detecção de intrusão deve ser usada como barreira protetora inicial, enquanto que os métodos de criptografia e as técnicas de segurança da camada física devem ser utilizadas para o aumento do sigilo das comunicações sem fio.

É possível observar que a lógica por trás da gestão estratégica de SI e da gestão logística estratégica são muito próximas e complementares; onde a logística estratégica consiste em imaginar e desenvolver ações estratégicas que seriam impossíveis sem fortes competências logísticas e um conjunto de dados (informações) confiáveis (Muhammad et al., 2014).

Os Sistemas de Informação e Comunicação (SIC) dão suporte individual ou concomitantemente ao Sistema de Gestão de Transporte (TMS), ao Sistema de Gestão de Armazenagem (WMS), ao Sistema de Gerenciamento de Demanda (DMS). Também se

figuram como elemento importante para a segurança da competitividade das empresas (Muhammad et al., 2014).

O trabalho de Muhammad et al. (2014) conclui que a comunicação e a tecnologia da informação são elementos cruciais para o setor de logística e que as empresas interessadas em fornecer, desde produtos e serviços de infraestrutura até serviços ligados ao capital humano, devem lidar com as necessidades recentes e o rápido desenvolvimento destes elementos.

Oláh et al.(2018) acreditam que os investimentos em Tecnologia da Informação (TI) permanecerão importantes no futuro. Acrescentou que a introdução e o aproveitamento das melhores tecnologias podem gerar vantagens competitivas e maiores recompensas financeiras para os provedores de serviços de logística.

De acordo com Muhammad et al.(2014), a TI na logística é usada para compartilhamento de carga entre diferentes fábricas e para alavancar volume. Os dispositivos conectados com a internet reúnem informações sobre matérias-primas, processo e disponibilidade; sistemas de gerenciamento de demanda (DMS), ajudam a planejar os níveis de estoque de acordo com as demandas dos clientes. Além disso, fazem a identificação da localização das remessas em fabricação de modo a possibilitar que os clientes tenham conhecimento preciso sobre o tempo estimado de chegada dos produtos.

Muhammad et al. (2014), alguns dos métodos de comunicação padrão e de gestão de informações na logística: o computador com acesso à internet, intranet ou extranet; sistema de comunicação sem fio ou radiofrequência (incluindo telefones celulares); sistema de informação financeira (contábil); código de barras e digitalização; intercâmbio eletrônico de dados; roteamento de veículos; TMS; WMS; ERP; Computador de mão ou de bordo; Sistema de Posicionamento Global (GPS); veículo guiado automaticamente (AVG) e sistema automatizado de armazenamento e recuperação.

Durante a execução da pesquisa percebeu-se o uso do termo *cloud logistics*, ou logística em nuvem, pelos autores dos artigos consultados. A logística em nuvem inclui os serviços centrados em informações (por exemplo, desembaraço aduaneiro, identificação ou rastreamento de materiais). Sendo assim, também demandará atenção quanto aos atendimentos dos requisitos de segurança da informação (Glockner et al., 2017).

Os problemas de comunicação do setor logístico, identificados no trabalho de Muhammad et al. (2014), que podem afetar ou colaborar para a ineficácia da logística são a falta de recursos de TIC, o aumento do custo operacional, o aumento da demanda e da oferta, aumento da concorrência, falta de recursos humanos competentes, instabilidade política, mudanças rápidas nas tecnologias e burocracia demasiada.

Muitas empresas gerenciam fornecedores externos nos quais o compartilhamento e o acesso à informação estão envolvidos. Isso pode gerar vulnerabilidades, especialmente se os processos forem automatizados. Para tanto, a empresa deve adotar medidas como mapear o fluxo de dados na cadeia de suprimentos, planejar uma avaliação abrangente dos riscos, alinhar-se aos padrões emergentes e estabelecer expectativas claras em todos os contratos da cadeia de suprimentos para buscar a adequada segurança de seus dados (Sarder & Haschac, 2019).

Conforme Sarder & Haschak (2019), os cibercriminosos podem explorar vulnerabilidades e assumir o controle de dispositivos individuais, parte de um sistema ou de todo o sistema e criar danos substanciais, incluindo interrupções no serviço, perda de dados, danos ao equipamento, danos a infraestrutura ou ferimentos a pessoas.

Como citado no trabalho de Schuhmacher & Hummerl (2016), a academia tem observado a oportunidade do desenvolvimento de um método genérico para um controle autônomo e descentralizado de sistemas intralogísticos híbridos variáveis.

Nota-se que com a Logística 4.0, o problema da segurança da informação é um elemento particularmente importante, onde fornecedores individuais de mercadorias (matérias-primas, produtos semi acabados, atacadistas, varejistas) cooperam com empresas, competindo em várias cadeias de suprimentos. Sob essas condições, também os prestadores de serviços de logística colaboram com os clientes, competindo entre si. Levando em consideração a possibilidade de oportunismo em tais condições, deve-se direcionar esforços para a redução do risco de gerenciamento incorreto das informações (Malkus & Awak, 2015).

O tipo e o nível das medidas de segurança da informação devem variar de acordo com a situação da ameaça, o valor dos ativos considerados e os requisitos de proteção do processo. Na Indústria 4.0 a segurança da informação pode ser afetada por fatores de *hardware*, *software* e humanos, de modo que seus pontos fracos a tornam complexa (Kondiloglu et al., 2017).

Preocupados com a tratativa de vulnerabilidades, os autores Shin et al.(2015) identificam as principais fraquezas de segurança da informação em um processo logístico internacional. Nesse estudo, os autores utilizaram os modais rodoviário, marítimo e aéreo, com auxílio de etiquetas de identificação eletrônica e sistema de reconhecimento de dados RFID. As principais fraquezas foram perda da proteção de dados, falha na preservação da privacidade, falsificação de senhas, vírus e cavalo de tróia nos dispositivos informatizados, administração inadequada, espionagem, ataques do tipo *man-in-the-middle*, rastreamento não

autorizado, problemas de segurança de dados e de rede, ataque de negação de serviço (DoS), *sniffing*.

Os usuários da tecnologia são o principal elemento em vazamentos de dados e violações de segurança; portanto, os padrões e procedimentos de segurança da informação não funcionarão sem a consideração desse fator-chave (Nowak, 2015).

As ameaças à segurança da informação aplicadas à Indústria 4.0 estão ligadas: a espionagem industrial; ciber espionagem; vazamento de informações confidenciais e de propriedade intelectual; ataque DoS; vazamento de informações confidenciais pela cadeia de fornecimento e pelos sistemas de extensão. Destaca-se ao fato de que o fornecedor é vulnerável a um ataque do tipo phishing e suas credenciais de privilégio são furtadas, resultando em exposição de dados em massa; novos dispositivos apresentam vulnerabilidades, mesmo os desenvolvidos para a Segurança Inteligente (Yutanto, 2018) e para a Fábrica Inteligente (Pereira et al., 2017).

Os autores Zhang et al.(2018), citam que a integração do CPS e da IIoT no SPLS aumenta as ameaças de segurança ao domínio cibernético e ao domínio físico, por meio de ataques de espionagem e ataques arbitrários ao processo físico.

Alguns dos impactos dos ataques cibernéticos nas empresas são: alteração das configurações de instalação podendo causar danos físicos ao equipamento; alteração das configurações de produção podendo levar a produtos defeituosos que resultarão em perda de lucro; mau funcionamento do equipamento podendo levar à liberação de poluentes nocivos na planta industrial e arredores; roubo de dados confidenciais, como segredos de fabricação e informações do cliente (Sarder & Haschak, 2019)

3. Métodologia

Neste estudo os métodos escolhidos para a coleta de informações foram a revisão bibliográfica automática, denominada conforme Vroegindeweij & Carvalho (2019) de sistema de computação cognitiva; e a pesquisa bibliográfica na base de dados Google Acadêmico.

O escopo desta pesquisa foi restringido aos estudos técnicos acerca dos elementos de segurança da informação abordados pelos sistemas de comunicação aplicados à área de logística interna de empresas.

Foi escolhido o método de informática cognitiva, por se tratar de um método que proporciona a possibilidade de coleta automatizada de documentos científicos publicados em bases de dados. Para esse estudo, a base escolhida foi a CORE, uma vez que se adequa melhor ao tema proposto, além de permitir a identificação automática dos principais trechos internos

dos documentos científicos que atendem as perguntas de interesse da pesquisa. Para tanto utilizou-se a plataforma *online* IBM Watson Discovery.

Escolheu-se realizar a pesquisa bibliográfica utilizando diretamente a máquina de pesquisa disponibilizado no site Google Acadêmico, para garantir a contemplação da pesquisa de todos os termos escolhidos por meio do método de pesquisa comum, diferentemente da pesquisa e identificação por meio de inteligência artificial.

O estudo de Fernandes et al. (2019) teve como objetivo principal realizar uma revisão bibliométrica sobre o emprego de óleos ácidos para diversos setores industriais. A base de dados utilizada foi a *Web of Science*® (WoS). A partir dos resultados de pesquisa, os autores construíram um banco de artigos, observando-se publicações sobre caracterização de diferentes óleos ácidos e seus empregos. Os autores concluíram que a relevância na pesquisa sobre petróleos ácidos, e a frequente tentativa científica de propor novos métodos para sua utilização, indicam que ainda há campo de pesquisa a ser explorado.

Firmes & Celeste (2018), realizou uma revisão bibliométrica na base Web of Science sobre os métodos não-intrusivo de monitoramento de cargas, a fim de mostrar o estado da arte dessa temática, e os principais avanços e entraves para o desenvolvimento dessa tecnologia. Como resultado, os autores observaram observa-se a relevância dos estudos nessa área, que está em pleno crescimento em países como Canadá, Estados Unidos e Índia.

Venturin & Silva (2019) realizaram uma revisão bibliométrica sobre autilização da modelagem e simulação no processo de secagem do arroz com casca, trazendo um panorama geral dos avanços alcançados, aspectos a serem desenvolvidos e oportunidades. A pesquisa foi realizada na base de dados *Web of Science*, seguida de uma análise qualitativa dos artigos mais relevantes. Os resultados demonstraram a evolução da área e um grande potencial a ser explorado, principalmente na aplicação destes modelos no controle, automatização dos sistemas e no suporte à tomada de decisão em processos reais e em grande escala.

A coleta automática de dados e a bibliometria, ocorreram no período de agosto e setembro de 2019. Os termos de pesquisa utilizados foram: *logical security; logistics information security; internal logistics communication; logistics data security; production process logistics; logistics 4.0;* e *logistics software*.

A restrição de pesquisa e aplicação de filtros de seleção de documentos se deram por meio das delimitações: somente ocorrência dos termos escolhidos no título dos documentos; artigos em inglês; publicados entre 2014 e 2019; somente arquivos em PDF; e de acesso livre.

Mesmo utilizando-se métodos de coletada de dados diferentes, a pesquisa possui natureza exploratória, e adotou-se abordagem documental e restrita a documentos científicos - artigos de acesso livre provenientes de periódicos e eventos científicos, dissertações e teses.

Para identificação da literatura principal e também para fundamentação e delineamento do referencial teórico do estudo, realizou-se bibliometria, que conforme as Leis de Lotka, Bradford e Zipf, buscou-se identificar a produtividade dos autores, a relevância dos periódicos selecionados, a distribuição da frequência de publicações sobre a temática nos últimos cinco anos e a frequência das palavras-chave.

A produtividade dos autores foi identificada por meio do levantamento do Scopus h-index de cada autor. A identificação da relevância dos periódicos foi realiza por meio da consulta direta, por meio do auxílio da utilização da máquina de pesquisa do site *scimagojr.com*. A distribuição da frequência das publicações selecionadas, bem como a frequência das palavras-chave, foi levantada por meio do programa EndNote.

Para esse estudo, a opção por uma pesquisa básica, de natureza exploratória e descritiva, teve como objetivo identificar as lacunas de segurança da informação para a logística interna. E apontar quais os programas computacionais auxiliares do sistema de informação e comunicação interna com foco a logística, utilizados pelas empresas.

A coleta automática de dados, utilizada neste estudo, foi realizada por meio do *software* R. Para isso foi criado um *script* de pesquisa automática, utilizando um cadastro prévio na base de dados CORE e na plataforma de inteligência artificial IBM Watson Discovery.

O *script* utilizado disponibiliza a possiblidade de pesquisar os termos definidos pelo usuário, somente nos títulos dos documentos disponíveis na base de dados, no idioma inglês e no período de publicação de interesse. Possibilita a obtenção organizada e padronizada dos meta dados de interesse do pesquisador e também a criação automática de planilha eletrônica com os metadados resultantes da pesquisa automática. Também há a automatização, após a geração da planilha de meta dados, da obtenção dos documentos científicos encontrado e em formato PDF, por meio do *download* para pasta definida pelo pesquisador.

Após o agrupamento dos documentos coletados automaticamente, foram utilizados os *softwares* Mendeley (para geração de arquivo de metadados BIBTEX) e EndNote, este último para refinamento de filtro e extração dos dados bibliométricos.

Finalizado o processo de refinamento de seleção de documentos, os arquivos foram enviados a plataforma de inteligência artificial IBM Watson Discovery, plataforma esta que trabalha em nuvem. Nesta plataforma, por meio de informática cognitiva, automaticamente

foi gerada análise de sentimento dos artigos selecionados e as palavras mais utilizadas para conceitualização teórica pelos autores dos documentos científicos.

No ambiente de pesquisa, consultas (*queries)* foram elaboradas para buscar a identificação automática dos trechos dos documentos de indicar o interesse do estudo. Vale ressaltar que nesta identificação não se considerou apenas o retorno dado automaticamente pela máquina de inteligência artificial. Esse recurso permite a identificação rápida dos trechos mais relevantes de cada um dos documentos, de acordo com os termos escolhidos. Desta forma, identificaram-se quais os documentos são relevantes e que assim deveriam ser detalhadamente analisados pelos pesquisadores.

Além da utilização do método de informática cognitiva, deste trabalho constituído pelo uso dos *softwares* R; Mendeley; EndNote e IBM Watson Discovery, foi também utilizado o Excel, para filtrar os meta dados obtidos e identificar os artigos relevantes para este estudo.

Após a análise dos dados, realizou-se primeiramente a verificação da consistência do estudo, para buscar identificar o nível de atendimento dos objetivos inicialmente definidos e também a consolidação da síntese dos resultados evidenciados.

4. Resultados e Discussão

Após o levantamento dos dados bibliométricos nas coleções das bases de dados CORE e Google Acadêmico foram selecionados 33 artigos contendo os termos da pesquisa. O resultado da aplicação de filtros e indicação automática de relevâncias dos documentos é apresentado na Tabela 1, onde são identificadas as quantidades de documentos selecionados sob o foco de cada um dos termos de pesquisa.

Tabela 1: Resultado da pesquisa realizada

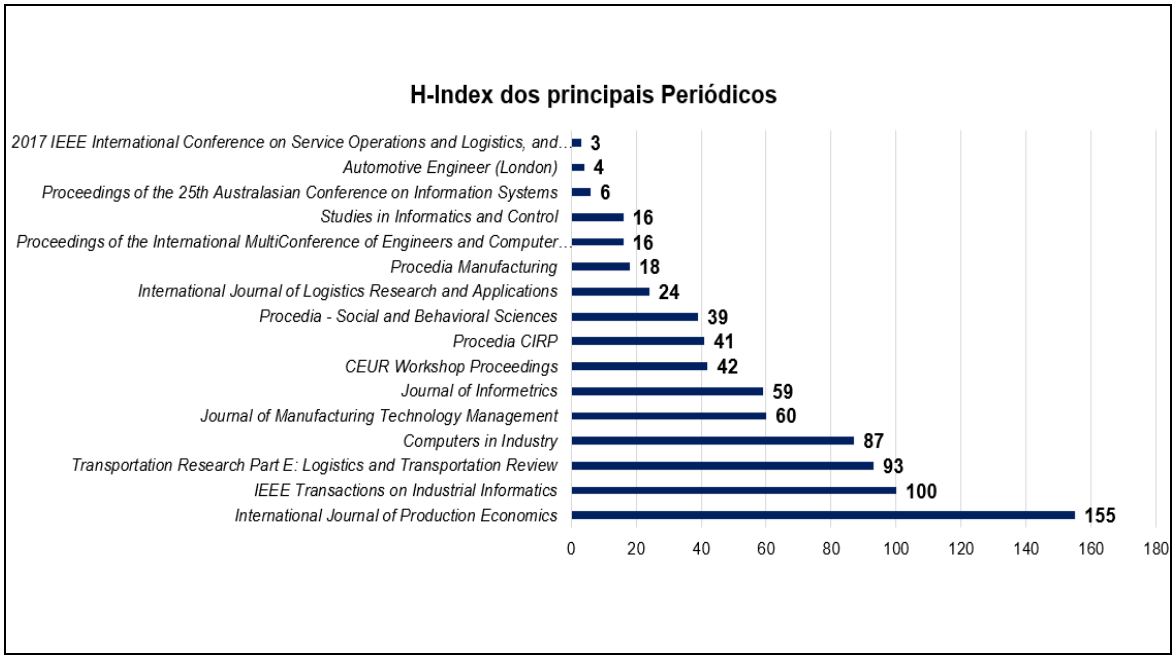
Ternos de busca	**Base de Dados**		**Seleção**
	CORE.AC.UK	**Google Acadêmico**	
logical security	5112	998	0
logistics information security	2772	8	6
internal logistics communication	3525	2	0
logistics data security	4724	5	13
production process logistics	3900	46	0
logistics 4.0	246	104	5
logistics software	5990	499	9
Total	*26.269*	*1.662*	*33*

Fonte: Elaborado pelos autores.

Os artigos utilizados estão publicados em 27 periódicos indexados nas bases de dados escolhidas. Conforme é possível observar na Figura 1. O periódico de maior relevância é o *International Journal of Production Economics* com *h-index* 155, definido pelo *Scimago Journal & Country Rank* (SJR), seguido pelos periódicos *IEEE Transactions on Industrial Informatics*, com *h-index* SJR 100 e *Transportation Research Part E: Logistics and Transportation Review*, com *h-index* SJR 93.

Os artigos selecionados foram escritos por 110 autores, considerando a somatória dos autores principais e co-autores. Conforme é possível observar na Figura 2, os autores mais relevantes foram: Angappa Gunasekaran, o autor com o maior índice de produtividade *h-index* Scopus 64, seguido pelos autores Mike Thelwall, com um *h-index* Scopus 58 e Huei Lee, com *h-index* Scopus 40.

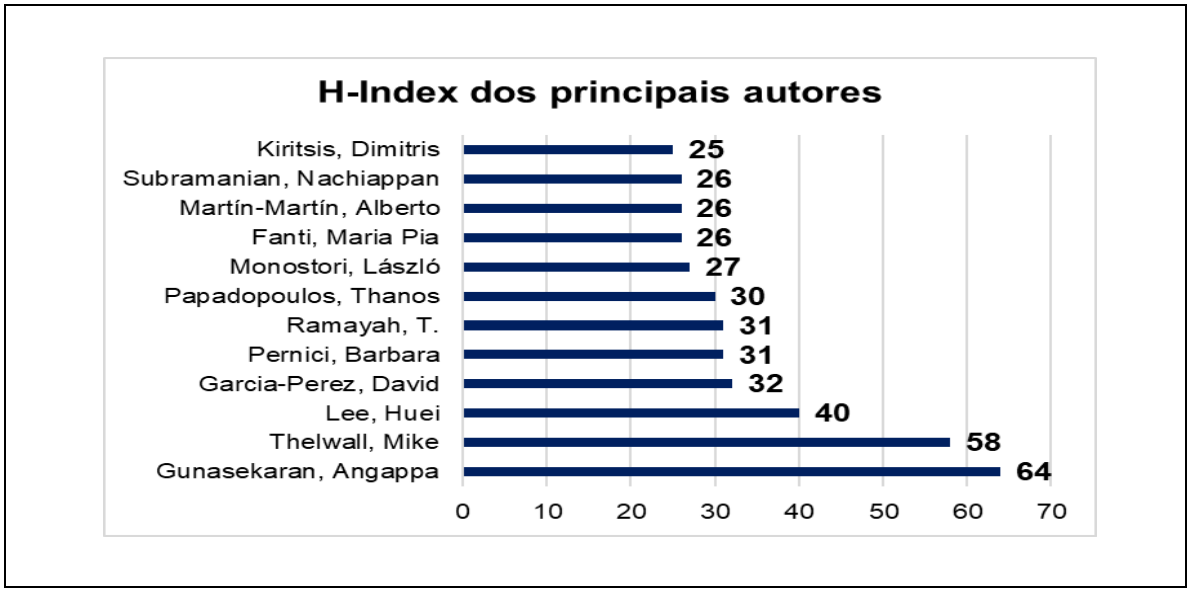
Figura 1: Índice de relevância dos principais periódicos dos artigos selecionados



Fonte: Elaborado pelos autores a partir dos dados obtidos das buscas.

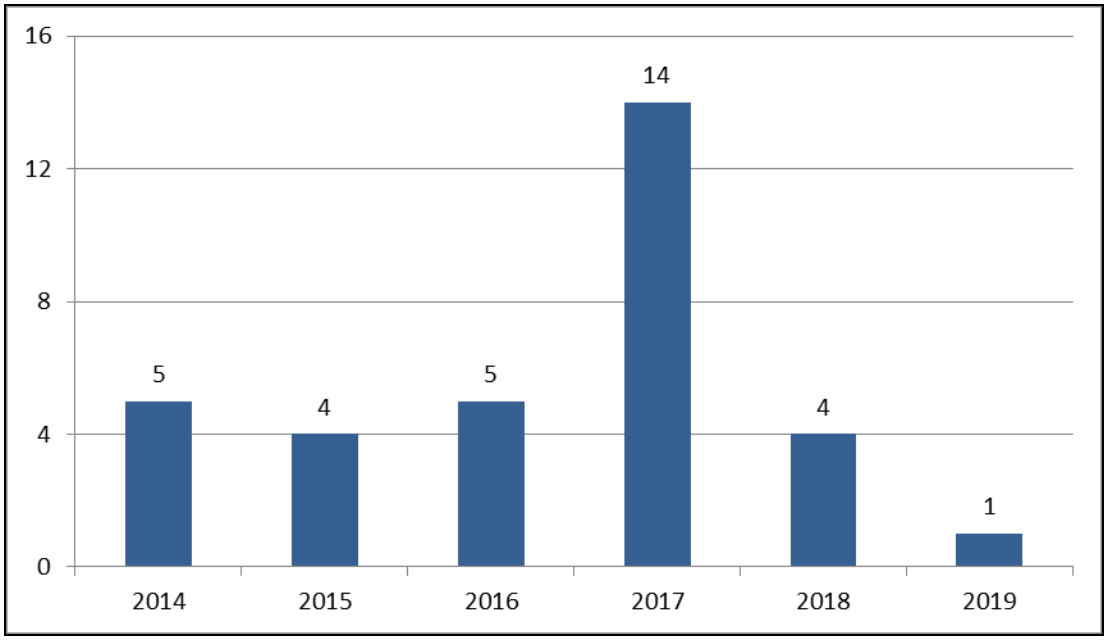
A distribuição anual das publicações selecionadas sobre o tema é apresentada na Figura 3. Observa-se que a maior quantidade de artigos selecionados sobre a temática se deu no ano de 2017 e a menor quantidade de artigos publicados é do ano de 2019. Ressalta-se que os dados referentes ao ano de 2019 foram levantados entre os meses de agosto e setembro deste ano e que por estar ainda em percurso, a quantidade de publicações de 2019 não encontra-se finalizada.

Figura 2: Índice de produtividade dos principais autores



Fonte: Elaborado pelos autores a partir dos dados obtidos das buscas.

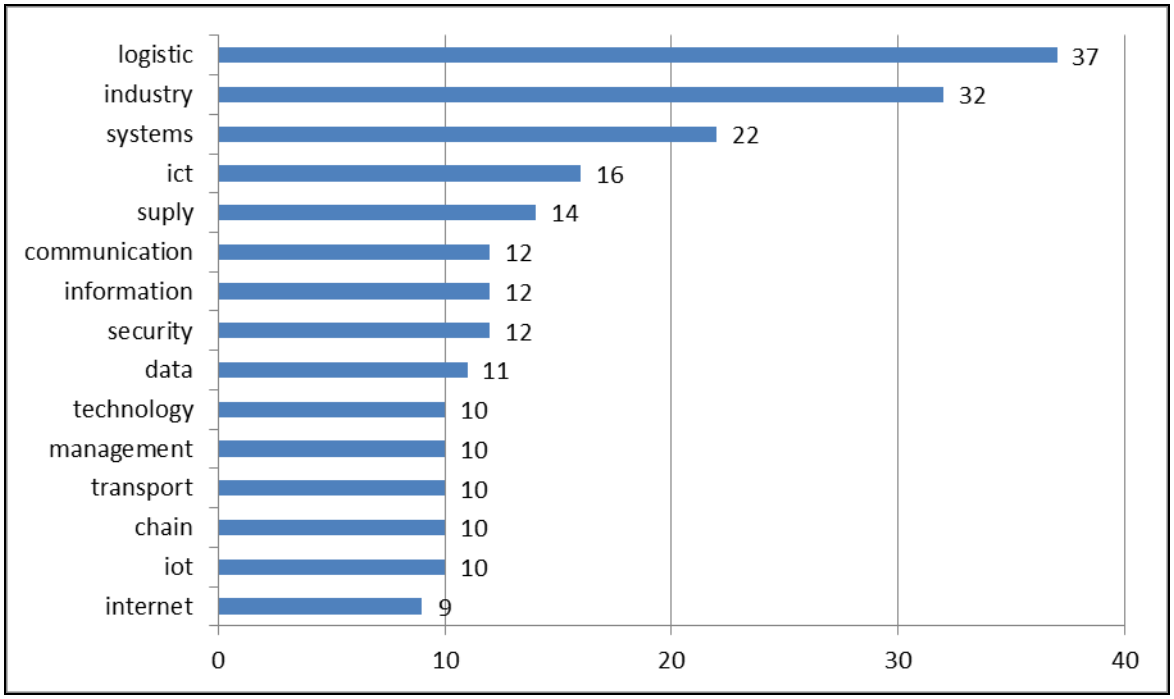
Figura 3: Distribuição dos artigos selecionados por ano de publicação



Fonte: Elaborado pelos autores a partir dos dados obtidos das buscas.

As palavras mais utilizadas nos artigos selecionados, pelos autores, são apresentadas na Figura 4. As palavras que surgem com maior frequência nos títulos e nos resumos dos documentos selecionados são *logistics*, com 37 ocorrências, *industry*, com 32 ocorrências e *systems* com 22 ocorrências. A abreviação ICT referencia os termos *information and communications technologies* e IOT referencia *internet of things.*

Figura 4: Frequência dos principais termos encontrado nos artigos selecionados



Fonte: Elaborado pelos autores a partir dos dados obtidos das buscas.

É possível verificar que as palavras que ocorrem com maior frequência estão direcionadas a temática da pesquisa. Este fato adiciona ao contexto um elemento qualitativo quanto aos documentos selecionados o que reforça a escolha dos mesmos para a construção deste artigo.

Para validação da seleção automática de artigos foi realizada leitura do resumo de cada um dos artigos para comprovar a correlação com a temática deste trabalho. Após consolidar a seleção de documentos, realizou-se a construção lógica e conceitual deste artigo.

Quanto aos principais *softwares* da área de logística citados nos artigos, identificou-se, por meio do trabalho de Harris et al. (2015), a citação dos *softwares:* SURFF; WELCOM; EUROPE-TRIS; IWV; F-MAN; MarNIS; COREM; INTERPORT; EUROSCOPE; SURFF; IP; CHINOS; SAIL; MIT; MULTITRACK; TRACAR; ParcelCall; D2D; M-TRADE; EURIDICE; INTEGRITY; SMART-CM; CASSANDRA; DOLPHINS; THEMIS; ALSO; DANUBE; GIFTS; E-FRAME; FREIGHTWISE; KOMODA; e-FREIGHT; e iCargo.

Também são citadas como plataformas de informação para a área logística, o EPCIS (SHIN et al., 2015; SANTOS et al., 2016); o iFloW (SANTOS et al., 2016); ADVANCE (ILIE-ZUDOR et al., 2014); AEOLIX e CO-GISTICS (FANTI et al., 2017).

Quanto aos métodos de segurança da informação, Sauer (2014), cita que na fábrica do futuro, os mecanismos de segurança, incluindo autenticação e autorização (gerenciamento de direitos) devem ser integrados à arquitetura dos sistemas ciberfísicos. Mecanismos de segurança padronizados, com criptografia e assinatura de dados, bem como autenticação de dados e componentes de controle, devem ser usados para garantir que apenas componentes autorizados possam participar do sistema de produção. Portanto, a segurança aspirada para mecanismos confiáveis do tipo *plug-and-work* só pode ser alcançada com base em componentes protegidos e claramente identificáveis.

Cada empresa deve definir e implementar soluções personalizadas, garantindo que a segurança das informações seja alcançada nas áreas mais sensíveis, como relacionamento com clientes e fornecedores (Nowak, 2015).

Os controles de acesso tradicionais citados no trabalho de Shin *et al.* (2015) são o Controle de Acesso Obrigatório (MAC), o Controle de Acesso Discricionário (DAC) e o Controle de Acesso Baseado em Função (RBAC).

Reconhecimento de segurança, controle de acesso por meio de mecanismos de autenticação, processos criptográficos e análise comportamental são os mecanismos de segurança que podem ajudar a impedir a invasão da cadeia de suprimentos (Pereira et al., 2017).

O controle de acesso auxilia o gerenciamento e controle de segurança relacionado à integridade, disponibilidade e confidencialidade de informações (ISO/IEC 27000, 2018).

As empresas devem investir na implantação de tecnologias de segurança, tais como sistemas de inteligência de segurança, governança avançada de identidade e acesso, automação, orquestração e aprendizado de máquina, uso extensivo de análises cibernéticas e análises de comportamento do usuário, implantação extensiva de tecnologias de criptografia, gerenciamento automatizado de políticas (Sarder & Haschak, 2019).

Erboz (2017) cita que é importante construir sistemas nacionais de defesa e treinar funcionários contra ataques cibernéticos.

As tecnologias de segurança serão necessárias para proteger os dispositivos e plataformas da IoT contra ataques de informações e violações físicas (Haddud et al., 2017).

Nenhum dos métodos de proteção, seja física ou lógica, fornece 100% de proteção, mas o treinamento dos funcionários deve ser uma prioridade (Kondiloglu et al., 2017).

5. Considerações finais

Os atuais trabalhos acadêmicos demonstram grande interesse em auxiliar empresas de todos os setores, inclusive as que possuem como principal foco a logística, a manter ou aumentar a competitividade, a lucratividade, por meio do uso de tecnologias de comunicação e informação. As atuais tecnologias de comunicação, bem como os sistemas de informação estão proporcionando integrações com todas as partes interessadas na cadeia produtiva, tal como é sugerida pela plataforma Indústria 4.0.

Por meio do uso, cada vez mais intenso dos dispositivos inteligentes de comunicação, além dos já comuns na logística, tais como, computadores, tablets, coletores ópticos e smartphones, uma nova gama de tecnologias tem sido inserida, por meio da Logística 4.0.

Na Logística 4.0, por meio da integração de SI, que dão suporte a sistemas ciberfísicos e estes por sua vez utilizam-se de dispositivos industriais conectados à *internet*, faz com que sejam evidenciados benefícios e desafios a serem superados.

Como benefício principal observa-se a possibilidade de por meio da automação de todos os processos, reduzir falhas e desperdícios e, portanto, aumento da lucratividade das operações.

Os autores analisados para esse estudo bibliográfico apontam que a integração aumenta a complexidade e controle do sistema, o que resulta em aumento da vulnerabilidade quanto as informações confidenciais e estratégicas das empresas. Quanto mais se amplia a extensão de aplicação das tecnologias inteligentes no fluxo de informações produtivas, mais lacunas potenciais de segurança da informação serão evidenciadas.

Tratar a segurança da informação como elemento prioritário e estratégico é salutar para as empresas que buscam sustentabilidade em seus sistemas de gestão.

Deve-se também considerar que os usuários das tecnologias podem colaborar com os vazamentos de dados e violações de segurança, desta forma, as empresas necessitam avaliar os riscos envolvidos caso seus ativos lógicos sejam perdidos. Também há de se planejar e implantar protocolos preventivos e até mesmo utilizar tecnologias de monitoramento e análise de comportamento dos usuários de seu sistema de informação.

Percebe-se também por meio deste estudo que mesmo havendo diversos *softwares* dedicados a área logística há ainda a oportunidade de desenvolvimento de programas computacionais que adotem protocolos e métodos para a garantia da segurança da informação logística. Especialmente as informações que são compartilhadas com fornecedores de insumos e serviços que possuem ligação com diversas empresas, inclusive com empresas concorrentes.

Quanto ao método escolhido de coleta e identificação automática de artigos, o sistema de computação cognitiva, mostra-se como método viável para o direcionamento inicial de uma pesquisa científica. Ele permite a identificação rápida e automática de trechos importantes dos documentos científicos escolhidos pelo pesquisador. Porém, o sistema ainda demanda melhoria quanto ao refinamento e aumento da precisão na identificação de termos em contexto. A utilização da computação cognitiva atualmente não exclui a necessidade de análise humana, bem como não irá substituir tão logo a arte de interpretação, sintetização e escrita de produtos científicos.

Identificam-se como oportunidades de futuros trabalhos a realização de estudos empíricos e longitudinais que utilizem métodos estruturados de triangulação de dados, para validação dos fatores de segurança da informação que são importantes para a Logística 4.0; e assim como indicado por Hofmann e Rüsch (2017), ainda há oportunidade de se investigar os efeitos da Indústria 4.0 nas estruturas organizacionais, operacionais e jurídicas das empresas do setor logístico.

Referências

Associação Brasileira de Normas Técnicas (2006). *NBR ISO/IEC 27001: 2006 Tecnologia da informação - Técnicas de segurança - Sistema de Gestão de segurança da informação - Requisitos*. Rio de Janeiro.

El Kadiri, S.S.; Bernard G.B.; Thoben, K.; Hribernik, K.; Emmanouilidis C; Ciemenski, C.V. & Kiritsis, D. (2016). Current trends on ICT technologies for enterprise information systems. *Computers in Industry*, 79: 14–33.

Erboz, G. (2017). How to define Industry 4.0: the main pillars of Industry 4.0. Szent Istvan University, *Gödöllő,* p. 1-9.

Fanti, M. P.; Iacobellis, G.; Pierro, B. D.; Ukovich, W.; Mangini, A. M. (2018). A Connectivity Platform for Intermodal Transportation and Logistics Systems. *Systems Man and Cybernetics (SMC) 2018 IEEE International Conference*, pp. 2491-2496, 2018.

Firmes, V.P. & Celeste, W.C. (2018). Uma revisão bibliométrica sobre a identificação de cargas similares em Smart Grid. *Research, Society and Development*, 7(12): 01-13.

Fernandes, H. A.; Freitas, R. R.; Ribeiro, D. C; Vicente; Santos, M. F. P., M. A. (2019). Acidez total em petróleos: uma análise Bibliométrica. *Research, Society and Development***.** 8(1).

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 Ciência da Informação*, v.22, n.3, p.75-97, jul./set.

Galhardi, A. C. & Zaccarelli, S. B. (2005). Inovação e Imitação tecnológica como estratégia compateitiva. *Revista Brasileira de Gestão e Negócios – FECAP*. Ano 7, nº 17, abril, p. 23-29.

Glöckner, M.; Ludwig, A.; Franczyk, B. (2017). Go with the flow: design of cloud logistics service blueprints. *In: Proceedings of the 50th Hawaii International Conference on System Sciences.*

Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, v. 5, n, 4, p. 438-457.

Haddud, A.; Desouza, A.; Khare, A.; Lee, H. (2017). Examining potential benefits and challenges associated with the Internet of Things integration in supply chains. *Journal of Manufacturing Technology Management*, v. 28, n. 8, p. 1055–1085.

Harris, I; Wang, Y; Wang, H. (2015). ICT in multimodal transport and technological trends: Unleashing potential for the future. *International Journal of Production Economics*, v. 159, p. 88–103.

Hofmann, E. & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, v. 89, p. 23–34.

Ilie-zudora, E.; Keménya, Z.; Ekártb, A.; Buckinghamb, C. D.; Monostori, L. (2014). A solution for information management in logistics operations of modern manufacturing chains. *Procedia CIRP*, v. 25, p. 337–344, 2014.

International Organization for Standardization (2018). *ISO/IEC 27000:2018 Information technology - overview and vocabulary*. p. 38.

Kondiloglu, A.; Bayer H.; Celik E.; Atalay M. (2017). Information security breaches and precautions on Industry 4.0. *Technology Audit and Production Reserves*, v. 6, n. 4, p. 58–63, 2017.

Małkus, T.; Awak, S. (2015). Information security in logistics cooperation. *Acta logistica*, v. 2, n. 1, p. 9–14.

Muhammad, M. Hasan, H.; Fiah, F. M.; Nor, A. M. (2014). Effective communication systems for Malaysian logistics industry. *Procedia - Social and Behavioral Sciences*, v. 130, p. 204–215.

Nowak, J. G. (2015). Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains. *Logistyka*, p. 639–654.

Oláh, J.; Karmazin, G.; Pető, K.; Popp, J.(2018). Information technology developments of logistics service providers in Hungary. *International Journal of Logistics Research and Applications*, v. 21, n. 3, p. 332–344.

Pereira, T.; Barreto, L.; Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, v. 13, p. 1253–1260.

Santos, D. R. G. & Volante, C. R. (2018). A importância da tecnologia sem fio na Indústria 4.0. *Interface Tecnológica*, p. 245–254.

Santos, M. Y.; Oliveira, J.; Andrade, C.; Lima, F. V.; Costa, E.; Costa, C.; Martinho, B.; Galvão, J. (2017). A Big Data system supporting Bosch Braga Industry 4.0 strategy. *International Journal of Information Management*, p. 1–11.

Sarder, M.D. & Haschak, M. (2019). Cyber security and its implication on material handling

and logistics. *College-Industry Council on Material Handling Education*, p. 1–18.

Sauer, O. (2014). Information technology for the factory of the future: state of the art and need for action. *Procedia CIRP*, v. 25, p. 293–296.

Schuhmacher, J. & Hummel, V. (2016). Decentralized control of logistic processes in cyber-physical production systems at the example of ESB Logistics Learning Factory. *Procedia CIRP*, v. 54, p. 19–24.

Shin, M. S.; Ju, Y. W.; Kang, H. K.; Jeong, S. P. (2015). Applying RBAC security control model to manufacturing and logistics service platform. *Studies in Informatics and Control*, v. 24, n. 3, p. 339–350.

Stefaniuk, T. (2016). New dimensions of information and knowledge security in reality of Industry 4.0. *Cracow University of Economics*, p. 1–9.

Venturin, A. C. Z. & Silva, L. C. (2019). Modelagem e simulação da secagem de arroz com casca: uma análise bibliométrica. *Research, Society and Development*. V. 8, n.1, p. 1-22.

Vroegindeweij, R. & Carvalho, A. (2019). Do healthcare workers need cognitive computing technologies? A qualitative study involving IBM Watson and dutch professionals. *Journal of the Midwest Association for Information Systems (JMWAIS)*, v. 2019, n. 1, p. 51–68.

Wang, Y. Y.; Fakhry R.; Rohr, S.; Anderl, R. (2017). Combined secure process and data model for IT-Security in Industrie 4.0. In**:** *Proceedings of the International Multiconference of Engineers and Computer Scientists 2017*, Hong Kong. Anais... Hong Kong.

Wood, L. C.; Wood A.; Reiners T.; Duong N. K.; Wang, X. (2014). An exploration of the New Zealand use of technology to facilitate logistics. *Proceedings of the 25th Australasian Conference on Information Systems*, ACIS 2014.

Yutanto, H. (2018). Security intelligence for industry 4.0: design and implementation. *Theoretical & Applied Science*, v. 65, n. 09, p. 228–243.

Zhang, Y.; Guo, Z.; Lv, G.; Liu, Y. (2018). A Framework for Smart Production-Logistics Systems based on CPS and Industrial IoT. *IEEE Transactions on Industrial Informatics*, v. 14, n. 9, p. 4019–4032.

Porcentagem de contribuição de cada autor no manuscrito

Diogo Pedriali – 60%

Carlos Hideo Arima – 20%

Fabrício José Piacente – 20%