REVISTA DE GESTÃO E SECRETARIADO
MANAGEMENT AND ADMINISTRATIVE PROFESSIONAL REVIEW
ISSN: 2178-9010

Revista GeSec
São Paulo, SP, Brasil v. 14, n. 1, p. 1068-1082,2023

DOI: http://dx.doi.org/10.7769/gesec.v14i1.1571

O conceito da segurança da informação como estratégia organizacional no contexto da Indústria 4.0

The concept of information security as an organizational strategy in the context of Industry 4.0

Tailise Mascarenhas Martins[1]
Rafael Nunes Carneiro[2]
Ricardo Coser Mergulhão [3]

Resumo

A Indústria 4.0 traz consigo um papel importante para os Sistemas de Informação, uma vez que, todos os sistemas inteligentes são interconectados com redes com ou sem fio e passam a tomar suas próprias decisões, percebe-se que ataques cibernéticos a essas redes causarão falhas de produção irreparáveis ou danos graves. Para aumentar a segurança da informação, é necessário abordar os riscos cibernéticos e identificar estratégias de segurança. Buscando prevenir possíveis ataques a rede. O objetivo do estudo é mostrar a importância de se abordar a segurança da informação como parte da estratégia organizacional na Indústria 4.0. O método de pesquisa foi uma revisão bibliográfica utilizando como fonte de informações as publicações sobre a temática encontradas em Bases de dados eletrônicas. O estudo concluiu que é nítida a necessidade do uso da estratégia da segurança nas organizações no contexto da Indústria 4.0,

[1] Mestranda em Engenharia de Produção, Universidade Federal de São Carlos C Rodovia Washington Luís, km 235, SEP-310, São Carlos - São Paulo, CEP: 13565-905. E-mail: tailise.mascarenhas@hotmail.com
Orcid: https://orcid.org/0000-0002-8154-7715
[2] Especialista em Gestão Lean Manufacturing, SEW Eurodrive e Faculdade de Tecnologia SENAI Gaspar Ricardo Júnior, Praça Roberto Mange, R. Santa Rosália, 30, Sorocaba - SP, CEP:18090-110.
E-mail: RafaelCarneiro_27@hotmail.com Orcid: https://orcid.org/0000-0001-9685-2002
[3] Doutor em Engenharia de Produção, Universidade Federal de São Carlos (UFSCAR), Rodovia Washington Luís, km 235, SP-310, São Carlos - São Paulo, CEP: 13565-905. E-mail: mergulhao@ufscar.br
Orcid: http://orcid.org/0000-0002-3797-295X

por motivos como, maior conectividade a redes cibernéticas, maior transação de dados e informações confidenciais.

Palavras-chave: Indústria 4.0. Segurança da Informação. Estratégia.

Abstract

Industry 4.0 brings with it an important role for Information Systems, since, all intelligent systems are interconnected with wired or wireless networks and start making their own decisions, it is realized that cyber attacks on these networks will cause irreparable production failures or severe damage. To increase information security, it is necessary to address cyber risks and identify security strategies. Seeking to prevent possible attacks on the network. The purpose of the study is to show the importance of addressing information security as part of organizational strategy in Industry 4.0. The research method was a bibliographic review using as a source of information the publications on the subject found in electronic databases. The study concluded that it is clear the need for the use of security strategy in organizations in the context of Industry 4.0, for reasons such as greater connectivity to cybernetic networks, greater data transaction and confidential information.

Keywords: Industry 4.0. Information Security. Strategy.

Introdução

O mercado está passando por uma nova revolução, onde máquinas e sensores executam e monitoram de forma inteligente e autônoma todo o processo produtivo industrial, a chamada Indústria 4.0, em que os Sistemas de Informação terão um papel muito importante nesta “nova” fase industrial (RAPOSO, 2018).

Um exemplo de uso recente da Indústria 4.0, é para auxiliar no COVID-19, para a fabricação e uso da vacina, equipamentos de saúde e logística, checkup, vigilância, detecção e decisão de ações necessárias com menor envolvimento físico humano. Assim, são fornecidos uma cadeia de suprimentos inteligente de descartáveis e equipamentos médicos durante esta crise, com uma maior rapidez (JAVAID et al., 2020).

Na Indústria 4.0 todos os sistemas inteligentes são interconectados com redes com ou sem fio por sua própria identidade, tomando suas próprias decisões, sem interferência humana, percebe-se que ataques cibernéticos a essas redes causarão falhas de produção irreparáveis ou danos graves. Para aumentar a segurança da informação, é necessário abordar os riscos

cibernéticos e identificar estratégias de segurança. Buscando prevenir possíveis ataques a rede (AHMET, 2020).

A segurança da informação se tornou tão importante que em 2018 o Brasil criou uma legislação específica para proteção de dados e da privacidade dos seus cidadãos, a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei no 13.709/2018[1], é a legislação brasileira que regula as atividades de tratamento de dados pessoais, outros regulamentos similares à LGPD no Brasil são o Regulamento Geral sobre a Proteção de Dados (GDPR), o que enfatiza a importância de proteger e assegurar os dados e informações (BRASIL, 2018).

Em um estudo feito por Ahmad et al. (2012), sobre estratégias de segurança da informação, é visível a falta do uso de estratégias de segurança organizacional ou até mesmo, de conversas entre gerentes de segurança com a alta administração sobre questões relacionadas à estratégia, o que mostra a falta de conhecimento da alta gestão em relação a importância do tema.

Porém, com a nova revolução industrial, em que se fala muito sobre tecnologia, aumenta-se o uso de dado entre outros, a preocupação sobre o tema passa a ter uma maior atenção. A pesquisa realizada pelo Fórum World Economic (2015) expõe a segurança da informação como um impacto gerado pela Internet das coisas, um pilar da Indústria 4.0. A Confederação Nacional da Indústria - CNI (2016) cita como desafio para Indústria 4.0 no Brasil a necessidade de rever as normas existentes em relação a segurança da informação, e novas políticas, bem como estruturas comportamentais e operacionais.

Portanto com a finalidade de expor a importância da segurança da informação na estratégia das organizações no contexto da Indústria 4.0, o presente trabalho consiste em um estudo bibliográfico abordando a necessidade de priorizar a segurança da informação como parte da estratégia organizacional, com o objetivo de deixar mais clara a importância sobre o tema e aumentar os conhecimentos profissionais e acadêmicos referentes ao estudo.

Considerando-se a pertinência do tema, a questão de pesquisa é: **Por que é importante abordar a segurança da informação como parte da estratégia organizacional no contexto da Indústria 4.0?**

Dessa forma, o estudo possui como objetivo, mostrar a importância de se abordar a segurança da informação como parte da estratégia organizacional na Indústria 4.0.

Revisão bibliográfica

2.1 Segurança da informação

Para garantir que as informações comerciais forneçam suporte útil às operações de negócios de uma instituição, sem oferecer nenhum risco, várias características-chave dessas informações precisam ser preservadas. Essas características incluem confidencialidade, integridade e disponibilidade, e a preservação dessas características de dados comerciais sigilosas, asseguraram então que as informações se mantenham em seu valor. Mas, para que isto ocorra, é necessário buscar atenuar os vários riscos dessas informações, por meio da aplicação de uma faixa adequada de controles de segurança, a qual pode ser definida como, uma combinação apropriada de controles de segurança físicos, técnicos ou operacionais, por exemplo, incluindo ações como portas trancadas, senhas de login de usuários ou até mesmo políticas e procedimentos de segurança, respectivamente (BS 7799, 2005).

2.2 Estratégia de segurança da informação

O estudo feito por Ahmad et al. (2012) aponta a identificação de nove estratégias da segurança da informação após uma revisão abrangente da literatura, sendo esta:

• Prevenção - protege os ativos de informação antes de um ataque, proibindo o acesso não
autorizado;

• Dissuasão - emprega atitudes disciplinares para influenciar o comportamento humano;

• Vigilância - monitora o ambiente de segurança, desenvolvendo a consciência situacional;

• Detecção - estratégia a nível operacional destinado a identificar comportamentos de segurança específicos;

• Resposta - ações corretivas adequadas contra-ataques após identificados;

• Decepção - distrair a atenção de um atacante de ativos de informação críticos, usando chamarizes;

• Perímetro de Defesa - fronteira em torno de recursos de informação;

• Compartimentalização - reduz as oportunidades de um atacante;

• Camadas - criando uma série de desafios para o atacante.

2.3 A importância da segurança da informação nos processos estratégicos

Alexandria, Quoniam e Riccio (2009) relatam que para o processo de segurança ser eficiente, deve ser acompanhado de perto pela alta administração. Afinal, são os mais interessados do negócio, e os quais, devem ditar as reais necessidades e prioridades da segurança. A fim de obter então, a devida atenção dos altos níveis da organização, deve-se criar um modelo de gestão que deixe clara a necessidade do acompanhamento desse processo em todos os níveis. Ahmad et al. (2012) afirmam que a segurança da informação é mais do que uma questão puramente técnica, podendo ser até mesmo uma questão estratégica e legal. Pois há uma necessidade definitiva de elevar a importância da segurança da informação e integrá-la ao programa geral de governança corporativa. Para os autores, essa integração servirá para instituir a segurança como uma das operações fundamentais de uma organização e impor responsabilidade, em termos de gerenciamento de riscos, relatórios e responsabilidade executiva ao respectivo Conselho Corporativo e CEO da empresa.

Método de pesquisa

Foi realizada uma pesquisa bibliográfica utilizando como fonte de informações as publicações sobre a temática encontradas em Bases de dados eletrônicas, sendo essas, Scopus e na Web Of Science (WOS), foram usadas as seguintes palavras-chave: “Industry 4.0”, “information security” e “strategies”.

Após as pesquisas, os artigos foram lidos e buscou-se identificar a relação entre eles, seguindo as fases propostas por Levy et al. (2006) em que, conheceu-se a literatura através de uma busca nas fontes, compreendeu-as e aplicou-as a revisão, após as leituras, analisou-se os resultados e compilou-os (síntese) através de mais algumas leituras e realizando a conexão entre as temáticas e por último os resultados foram analisados.

3.1 Planejamento

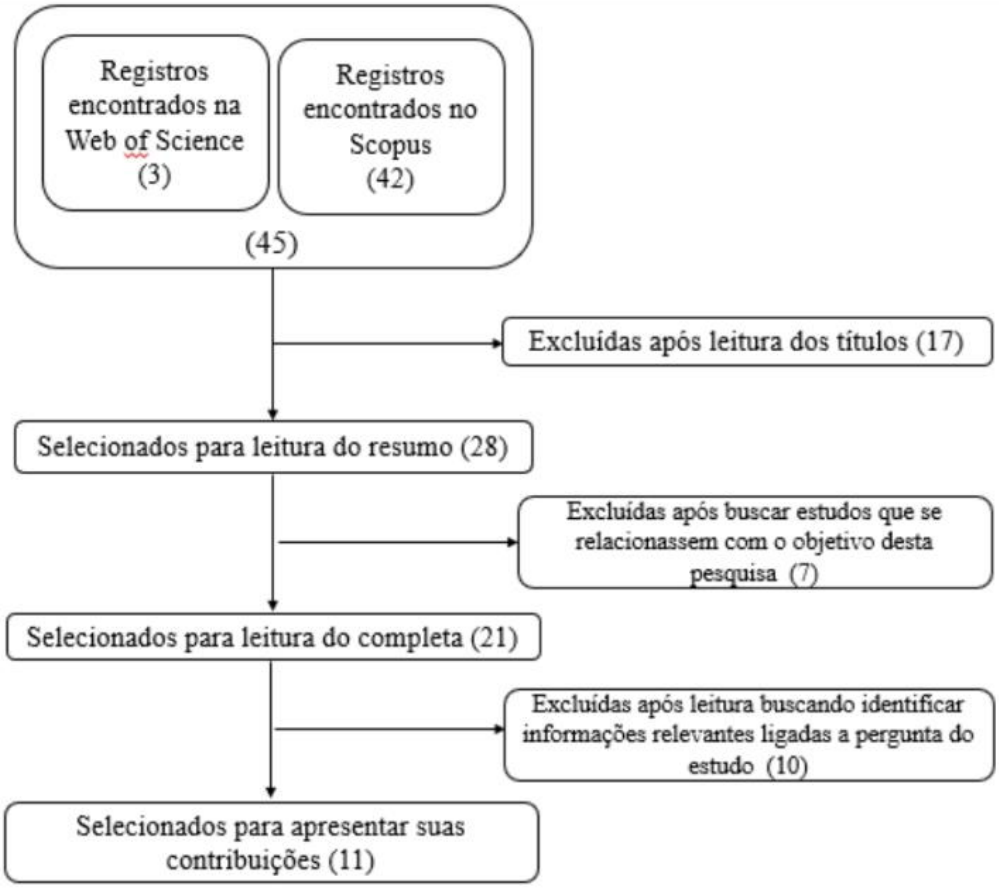
O estudo visa garantir que a implementação da segurança da informação na estratégia organizacional irá colaborar com as dificuldades da implementação da Indústria 4.0 referentes ao tema, dessa forma, iniciou-se a busca por artigos relacionando as palavras-chave através da elaboração da adaptação dos parâmetros de busca para cada base a ser pesquisada, conforme Tabela 1.

Base de Dados	Parâmetros de busca	Artigos
Web of Science	TS=*("Industry 4.0" AND "Information Security" AND "Strategies")*	3
Scopus	(TITLE-ABS-KEY=*("Industry 4.0" AND "Information Security" AND "Strategies")*)	42

Tabela 1 - Parâmetros de busca
Fonte: Elaborado pelo autor

A princípio restringiu-se apenas as bases de buscas com os parâmetros já apresentados, sendo encontrados 42 artigos na base Scopus e três na base Web of Science, como poucos artigos foram encontrados, foram incluídos todos os anos dos artigos disponíveis, sem limitar o tempo do estudo nem a língua, ou seja, não foram inseridos itens de inclusões e exclusões. A primeira triagem foi realizada pela leitura do título dos artigos, levando a 28 artigos. Em seguida após a leitura do resumo, buscando estudos que se relacionassem com o objetivo desta pesquisa afunilou-se para 21 artigos.

Estes 21 artigos foram submetidos a uma leitura completa, onde se procurou identificar informações relevantes sobre o tema, dessa forma, apresenta-se na sessão a seguir, 11 artigos suas principais contribuições, buscando, responder à pergunta da pesquisa em questão, esses artigos selecionados estão distribuídos em periódicos, normas, revistas e conferências. A seguir o fluxograma 1 representa o planejamento de escolha dos artigos.



Fluxograma 1 – Filtro das escolhas dos artigos
Fonte: Elaboração Própria

Análise e resultados

O artigo "*A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem*", explica sobre as estratégias de defesa que os usuários finais e corporações no espaço da Indústria 4.0 devem adotar contra ameaças cibernéticas. Como resultado, o artigo cita que não é possível evitar completamente os ataques cibernéticos no ecossistema da Indústria 4.0. Prevenindo as vulnerabilidades identificadas no estudo irão garantir que o dano é mínimo em ataques. Essas vulnerabilidades do sistema de cibersegurança identificadas e que se mostraram mais evidente no contexto da Indústria 4.0 foram determinados, e consistem em protocolos de sistemas de controle, conexões de informações desprotegidas, negligência de testes de infiltração periódicos, incapacidade de gerenciar dispositivos de rede com eficácia e pessoal não treinado e através dessas a estratégia para defesa cibernética e requisitos para essas vulnerabilidades foram determinados (SÜ, 2020).

O BS799 trata-se de uma norma criada em 1999 relatando sobre Segurança da Informação e Internet das Coisas.

Já o artigo "*Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0*", traz o conhecimento do uso de um subconjunto da Internet das coisas (IoT) para obter conectividade e descentralização na Indústria 4.0. E ainda relata que a implantação de redes industriais raramente considera segurança como uma estratégia, mas isso se torna imperativo na fabricação inteligente à medida que a conectividade aumenta. Uma vez que a combinação de infraestruturas de Operação da Tecnologia (OT) e Tecnologia da Informação (TI) na Indústria 4.0 adiciona novas ameaças de segurança, além daquelas das redes industriais tradicionais. Trazendo então as defesas em profundidade (DiD) como estratégia de segurança, para lidar com a complexidade do problema. O artigo apresenta uma análise das mais relevantes estratégias de segurança em Indústria 4.0, com foco principalmente em DiD. Com isso em mente, ele propõe uma combinação de DiD com algoritmo de criptografia leve para obter uma abordagem completa de segurança. Expondo então uma primeira etapa crítica para desenvolver meios mais adequados de realizar a estratégia de seguranda na Indústria 4.0 (Mosteito et all 2020).

O artigo "*Cyber security based machine learning algorithms applied to industry 4.0 application case: Development of network intrusion detection system using hybrid method*", apresenta uma estratégia de segurança cibernética, desenvolvida diante dos riscos que pesam sobre as empresas, e ainda mais sobre seus dados confidenciais e motivados pela maior a necessidade de criar uma estratégia de segurança cibernética para Indústria 4.0. Essa necessidade surgiu em meio a uma variedade de atacantes com objetivos e habilidades diferentes nos sistemas industriais, sistemas esses, que já há muito tempo são na realidade vulneráveis a ataques, mas, com a introdução da Indústria 4.0 passou a visualizar essa carência de estudo de forma mais ampla (TAMY et all 2020).

O artigo "*Paradigm shift and challenges in IoT security*", expõe o paradigma que a Indústria 4.0 traz de permitir que os objetos exibam a capacidade de se comunicarem uns com os outros, bem como com um sistema central e, portanto, com seres humanos, a qual é uma premissa da Internet das coisas (IoT) e um esforço que certamente traz novas melhorias e eficiência em nossas vidas. Nas últimas décadas tem-se testemunhado ataques cibernéticos fortes e ativos e criado ameaças de proteção a segurança das redes. O artigo também relata que em formação de dados na abordagem Tecnologia a indústria aprendeu muito com essas ameaças e as documentou para encontrar soluções corretas e apropriadas. Em contraste, o ambiente de Tecnologia Operacional em torno de formação de dados a tecnologia foi mantido em suspenso em muitas organizações. Assim, dificilmente se encontra a história e a documentação de sistemas de ciberataques construídos em torno de tecnologia operacional.

Sendo assim, o artigo fornece uma perspectiva histórica da Tecnologia Operacional de segurança, sendo que, ao longo de um período das últimas décadas o assunto evoluiu, e mostra quais são alguns dos desafios reais que a indústria está enfrentando. A fase final do artigo concentra-se em algumas das medidas e etapas práticas reais que foram tomadas para criar um ambiente industrial mais seguro e protegido, incluindo as melhores práticas na criação de sinergia entre as redes de tecnologia e segurança da informação e os ambientes industriais (A., 2020).

O artigo "*Information Security and Adoptable Solutions in the Implementation of Industry 4.0 Strategy for the Fourth-generation Industrial Revolution*", analisa a segurança da informação na implementação da estratégia no contexto da Indústria 4.0, propondo medidas específicas para garantir a segurança da informação da Indústria 4.0, a partir das perspectivas da estratégia de segurança do sistema de controle industrial, medidas de segurança, consciência de segurança, proteção de segurança de dados, responsabilidade pela segurança de dados e tecnologia de criptografia. Além disso, o sistema de controle distribuído e a construção da plataforma de comunicação de segurança de rede de TI são aplicados para resolver o problema de segurança da informação da Indústria 4.0. As soluções adotáveis fornecerão uma referência importante para manter a segurança da informação da Indústria 4.0 (CHENG, 2020).

O artigo "*A view point on management practices for cybersecurity in industry 4.0 Environment*" aponta que no contexto da indústria 4,0 as empresas são bombardeadas com grande volume e variedade de dados com grande velocidade. Os dados se tornaram ativos estratégicos significativos para empresas, o que torna crucial a proteção desses dados e acesso seguro. A confiança está se tornando um fator muito sério nas negociações comerciais. É um pensamento antigo que a segurança cibernética gerencia apenas riscos cibernéticos, pois gerencia também a confiança. As empresas estão expostas a riscos cibernéticos além de seu controle direto e isso resultou de complexas cadeias de valor digital. Existe a possibilidade de danos graves devido a ataques cibernéticos em termos de operações comerciais contínuas, danos à reputação e roubo de dados confidenciais. Este artigo chama a atenção para o importante papel das práticas de gestão da cibersegurança e identifica os desafios mais relevantes da gestão da cibersegurança no contexto de Indústria 4,0. Afinal a cibersegurança precisa, detectar, prevenir e analisar e solucionar todos os cibers incidentes (ZIA, 2020).

Em relação ao artigo "*A general view of industry 4.0 revolution from cybersecurity perspective*", este relata sobre a ampla rede e o compartilhamento de dados de alto nível que por meio da Indústria 4.0 vai aumentar rapidamente a demanda da cibesegurança devido às

suas vulnerabilidades e novas ameaças emergentes. Portanto, as grandes corporações precisam de um sistema de gestão de risco e estratégia de segurança adaptado às suas necessidades e com compromisso de melhorar a proteção para que suas operações e resultados não sejam adversamente afetados. A fim de proteger produtos, dados e propriedade intelectual contra pessoas não autorizadas, as empresas devem absolutamente tomar medidas de segurança dos dados para cumprir os requisitos da Indústria 4.0. Este artigo visa abordar quais tipos de problemas as empresas devem lidar contra-ataques cibernéticos e ilustrar como governos tomam precauções e referem esta questão em seus documentos de política na era de Indústria 4.0. A digitalização da produção pavimentou o caminho para uma existência cada vez maior de conceitos como Big Data, Computação em Nuvem, Impressão 3-D, Realidade Aumentada e Internet das Coisas em produção. Com o surgimento desses conceitos, a necessidade da cibersegurança também está se tornando crucial. Este artigo destaca muitas questões da pesquisa de literatura e análise de risco abrangente, comparando a história moderna das TIC (Em Tecnologia da Informação e Comunicação) e futuras fábricas inteligentes (EFE, 2020).

O artigo "*Secure production within the iiot - hardware-based security solutions protect data and systems*" é bem voltado a parte de tecnologia da informação, mas foca no estabelecimento da proteção dos dados originados da TI nas infraestruturas recém conectadas com foco na confiabilidade, baseado em hardware de segurança, pelo contexto da quarta revolução industrial se conectar a sistemas de produção com comunicação moderna e tecnologia da informação. No entanto, digitalização industrial e conectividade com base em diferentes estratégias da Indústria 4.0 também tem suas desvantagens: oferece aos hackers e criminosos cibernéticos novos pontos de entrada e alvos (M., 2017)

O artigo "*Reconciling digital transformation and knowledge protection: A research agenda*", traz o contexto da transformação digital não apenas em ambientes de escritório, mas também em ambientes de trabalho físico, como manufatura ou construção. Novas formas de combinar inovações digitais e físicas são intensificadas. O compartilhamento do conhecimento torna-se cada vez mais importante, mas sua natureza intraorganizacional e a indefinição das fronteiras organizacionais criam desafios para a proteção do conhecimento. A pesquisa existente sobre proteção do conhecimento concentra-se principalmente em organizações individuais ou em relações diádicas. Arranjos complexos de compartilhamento e especialmente o compartilhamento em redes receberam pouca atenção até agora. Mas agrega no estudo por meio do contexto em que aborda o início da preocupação com segurança da informação (ILVONEN et all 2018).

E por último o artigo "*Secure concept for online trading of technology data in global manufacturing Market*" que demonstra um novo modelo de negócio para comércio online, automação e fabricação mecânica na indústria, visto que ainda hoje existem desafios em relação a expansão do comércio digital na questão da segurança de informações para operação das máquinas com o uso de dados, mesmo com diversos modelos de negócios empregados em comércio de bens, e-books, músicas, ainda há poucos modelos para a indústria que possibilite o uso de dados nas máquinas. Com base nos modelos existentes nas empresas, o artigo apresenta um conceito, baseado em um fluxo de trabalho, além de vários modelos de licenças necessárias para o controle de uso de dados, que possibilite que os dados necessários para operação das máquinas nos processos de fabricação sejam comercializados (SHAABANY et all 2017), um artigo mais antigo que traz os desafios enfrentados na época em relação a segurança da informação.

Conforme as leituras dos artigos encontrados, percebeu-se a escassez do uso da segurança da informação na estratégia organizacional para Indústria 4.0 em si. Mas ficou claro a necessidade do uso da estratégia da segurança nas organizações no contexto da Indústria 4.0 em diversos modelos de negócios, por motivos muito próximos ou iguais, em que através da maior conectividade a redes cibernéticas, maior transação de dados e informações confidenciais entre outros, passou-se a receber mais ataques as redes e aumentou gradativamente a preocupação e visualização na abordagem da estratégia de segurança no contexto da Indústria 4.0, o que responde assim, a pergunta questão da problemática do estudo, sobre o porquê da importância em abordar a segurança da informação como parte da estratégia organizacional no contexto da Indústria 4.0, que é por questões até mesmo de competitividade em relação a confiança do cliente e o principal a proteção a ataques cibernéticos e segurança das informações que aumentaram com o novo contexto industrial, sendo na tabela 2 explicito a semelhança entre as necessidades em criar a segurança da informação e a forma como desenvolver a estratégia.

Artigo	Motivações para criar uma estratégia de segurança da informação	Ferramentas utilizadas para estabelecer estratégia da segurança	Ano da publicaçã
(SÜ, 2020)	Risco de ataque cibernético continuará a aumentar na Indústria 4.0 que tem como combustível o uso de dados e onde quer que esses dados digitais estejam disponíveis, ataques cibernéticos são uma ameaça.	Combate as vulnerabilidades que o sistema cibernetico apresenta, fazendo uso da cibersegurança preventiva.	2020
BS 7799	Norma criada em 1999 relatando sobre Segurança da Informação e Internet das Coisas.	Foco em características-chave e ações para proteção dessas	2020
Mosteito et all 2020	Á medida que a conectividade aumenta, novas ameaças de segurança, além daquelas das redes industriais tradicionais surgem, criando a necessidade de buscar novas estratégias de segurança	Propõe uma combinação de Defesa em Profundidade (DiD) com algoritmo de criptografia leve para obter uma abordagem completa de segurança.	2020
TAMY et all 2020	Desenvolvida diante dos riscos que pesam sobre as empresas, e ainda mais sobre seus dados confidenciais e motivados pela maior necessidade de criar uma estratégia de segurança cibernética para Indústria 4.0	Estratégia de segurança cibernetica	2020
A., 2020	Através do testemunho de ataques cibernéticos fortes e ativos e criado ameaças de proteção a segurança das redes	Criação de sinergia entre as redes de tecnologia, a segurança da informação e os ambientes industriais.	2020
CHENG, 2020	Garantir a segurança da informação da Indústria 4.0.	Através das perspectivas da estratégia de segurança do sistema de controle industrial, medidas de segurança, consciência de segurança, proteção de segurança de dados, responsabilidade pela segurança de dados e tecnologia de criptografia	2020
ZIA, 2020	Preocupação com os possíveis danos graves gerados devido a ataques cibernéticos em termos de operações comerciais contínuas, danos à reputação e roubo de dados confidenciais	Melhores práticas de cibersegurança adequadas para facilitar as empresas a acompanhar o ritmo da Indústria 4.0	2020
EFE, 2020	Diante da necessidades das grandes corporações por um sistema de gestão de risco e estratégia de segurança adaptado às suas necessidades de segurança e com compromisso de melhorar a proteção para que suas operações e resultados não sejam adversamente afetados.	Aborda quais tipos de problemas as empresas devem lidar contra-ataques cibernéticos e ilustrar como governos tomam precauções e referem esta questão em seus documentos de política na era de Indústria 4,0.	2020
M., 2017	Criar confiabilidade, devido a possibilidade dos hackers e criminosos cibernéticos terem acessos aos dados da empresa.	Hardware de segurança	2017
ILVONEN et all 2018	Desafio para a proteção do conhecimento criado pelo compartilhamento maior do conhecimento de forma intraorganizacional.	Pesquisa sobre proteção do conhecimento.	2018
SHAABANY et all 2017	Demonstra um novo modelo de negócio para comércio online, automação e fabricação mecânica na indústria.	Traz os desafios enfrentados na época em relação a segurança da informação.	2017

Tabela 2 - Resumo dos artigos encontrados
Fonte: Elaboração própria

Conclusão

A chegada da Indústria 4.0 aumenta o fluxo de informação gradativamente, surgindo então, uma necessidade maior de segurança da informação, uma vez, que se trata de um ativo valioso para a organização realizar suas operações, e como qualquer outro ativo importante precisa ser protegido. Além de contribuir também com uma relação mais confiável com seus clientes, fornecedores e outros parceiros de negócios, corroborando então, até mesmo com a competitividade da empresa.

Percebe-se, portanto, a importância em considerar uma abordagem como a governança de segurança da informação nas organizações e obter uma administração executiva, incluindo gestores e o CEOs ativamente envolvidos nesses esforços. Expondo os motivos de inserir a estratégia de segurança da informação em sua estratégia global.

O estudo visa garantir que a implementação da segurança da informação na estratégia organizacional irá colaborar com as dificuldades da implementação da Indústria 4.0 referentes ao tema.

Sendo assim, no âmbito teórico, espera-se ajudar a diminuir a lacuna de conhecimento relacionada à falta de pesquisas relacionadas a estratégia da segurança da informação, podendo esclarecer a importância dos fatores críticos de sucesso desse processo.

Já no âmbito prático, espera-se poder ajudar as instituições a visualizar os motivos para implementar a segurança da informação na estratégia organizacional, além de colaborar com a dificuldade em relação a segurança da informação no processo de execução da Indústria 4.0.

Como limitações do estudo pode-se apresentar a falta da atualização de normas tecnológicas, além da falta de estudos recentes sobre segurança da informação, podendo diminuir a eficácia dos resultados encontrados.

Como sugestão para trabalhos futuros, considera-se a aplicação prática da estratégia de segurança em uma organização por meio de um estudo de caso ou uma pesquisa-ação com o intuito de analisar o quanto a segurança da informação pode auxiliar na implementação dos conceitos da Indústria 4.0. Também pode-se recomendar uma investigação com coleta de dados quantitativos (*Survey*) com empresas brasileiras para mensurar a efetividade do uso das diretrizes da estratégia de segurança no mercado nacional.

Referências

A., C. Paradigm shift and challenges in IoT security**. Journal of Physics: Conference Series**, v. 1432, n. 1, 2020.

AHMAD, A.; MAYNARD, S. B.; PARK, S. Information security strategies: Towards an organizational multi-strategy perspective. **Journal of Intelligent Manufacturing**, 2012.

ALEXANDRIA, J. C. S. DE; QUONIAM, L. M.; RICCIO, E. L. **Gestão da Segurança da Informação – Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica**. [s.l: s.n.].

BS 7799. BS 7799: code of practice for information security management as a base for certification. 1999.

CHENG X.A, B, Z. P. . Information Security and Adoptable Solutions in the Implementation of Industry 4.0 Strategy for the Fourth-generation Industrial Revolution. **Journal of Physics: Conference Series**, v. 1682, n. 1, 2020.

CNI, C. N. DA I. Desafios para indústria 4.0 no Brasil. **Confederação Nacional da Indústria**, n. INDUSTRIA 4.0, p. 34, 2016.

EFE A.A, I. A. . A general view of industry 4.0 revolution from cybersecurity perspective. **International Journal of Intelligent Systems and Applications in Engineering**, v. 8, n. 1, p. 11–20, 2020.

ILVONEN I.A,THALMANN S.B,MANHART M.C, S. C. . Reconciling digital transformation and knowledge protection: A research agenda. **Knowledge Management Research and Practice**, v. 16, n. 2, p. 235–244, 2018.

JAVAID, M. et al. Diabetes & Metabolic Syndrome : Clinical Research & Reviews Industry 4 . 0 technologies and their applications in fi ghting COVID-19 pandemic. **Diabetes & Metabolic Syndrome: Clinical Research & Reviews**, v. 14, n. 4, p. 419–422, 2020.

LEVY, YAIR; ELLIS, T. J. A systems approach to conduct an effective literature review in support of information systems research. **Informing Science: International Journal of an Emerging Transdiscipline**, v. 9, n. 1, p. 181–212, 2006.

M., P. Secure production within the iiot - hardware-based security solutions protect data and systems. **ZWF Zeitschrift fuer Wirtschaftlichen Fabrikbetrieb**, v. 112, n. 4, p. 257–260, 2017.

MOSTEIRO-SANCHEZ A.A, BARCELO M.A, ASTORGA J.B, U. A. . Securing IIoT using Defence-in-Depth:Towards an End-to-End secure Industry 4.0. **Journal of Manufacturing Systems**, v. 57, p. 367–378, 2020.

RAPOSO, D. R.; REIS, A. J. DA R. **Indústria 4.0: Realidade, Mudanças e Oportunidades.** [s.l.] Universidade Federal de Ouro Preto, 2018.

SHAABANY G.,FRISCH S., A. R. Secure concept for online trading of technology data in global manufacturing market. **IFIP Advances in Information and Communication Technology**, v. 517, p. 690–700, 2017.

SÜ, A. A. A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4 . 0 Ecosystem. n. February, p. 1–12, 2020.

TAMY S.A,BELHADAOUI H.A,RABBAH N.B, R. M. . Cyber security based machine learning algorithms applied to industry 4.0 application case: Development of network intrusion detection system using hybrid method. **Journal of Theoretical and Applied Information Technology**, v. 98, n. 12, p. 2078–2091, 2020.

ZIA N.U., O. V. K. **A viewpoint on management practices for cybersecurity in industry 4.0 Environment**. European Conference on Information Warfare and Security, ECCWS. **Anais**...2020

Submetido em: 16.12.2022
Aceito em: 19.01.2023