Aspectos relevantes sobre Cibersegurança na Indústria 4.0

[1] Clóvis Roberto Regis (Universidade do Vale do Itajaí – Univali) clovisr@edu.univali.br

[2] Michele Beatriz Lopes Farias (Universidade do Vale do Itajaí – Univali) miichele.lopesf@gmail.com

[3] Moacir Marques (Universidade do Vale do Itajaí – Univali) engenheiromarques@yahoo.com.br

Resumo:
O conceito de Indústria 4.0 é recente e se baseia na construção de pilares que sustentarão a implantação deste mesmo conceito nos ambientes industriais. Entre estes pilares pode-se citar a Cibersegurança. Devido ao interesse que desperta, relacionado à segurança que deve existir para garantir o acesso autorizado aos sistemas digitais, percebe-se que existem grandes desafios a serem vencidos neste contexto. Tornar os sistemas de informação seguros, em todas as suas características, auxiliará os gestores industriais a enxergarem com mais confiança a aplicação deste novo conceito nas plantas industriais. A metodologia aplicada possui características exploratórias e descritivas. Esta mesma pesquisa procurou demonstrar, por intermédio de pesquisas em diversas literaturas, a importância dos sistemas digitais para a atual sociedade e qual o impacto que os ataques cibernéticos provocam nas organizações empresariais. Ao se compreender a dinâmica existente nesta área do conhecimento, foi possível definir algumas diretrizes que poderão nortear a aplicação dos conceitos de Cibersegurança voltados para a 4ª Revolução Industrial. Este trabalho procurou estar alinhado com as diretrizes voltadas para os aspectos preventivos relacionados aos ataques cibernéticos. Desta maneira foi possível elencar possíveis sugestões voltadas para minimizar os efeitos que tais práticas maliciosas podem provocar em organizações empresariais voltadas para a atividade econômica de produção de bens de consumo. Considerando a importância do tema em questão, devido aos altos custos que uma invasão cibernética pode acarretar para uma organização empresarial, sejam estes custos financeiros ou de propriedade intelectual, entende-se a relevância e abrangência do mesmo.
Palavras chave: Internet, Informação, Indústria, Segurança Cibernética.

Relevant Aspects of Cybersecurity in Industry 4.0

Abstract:
The Industry 4.0 concept is recent and is based on the construction of pillars that will support the implementation of this same concept in industrial environments. These pillars include cybersecurity. Due to the interest it arouses, related the security that must exist to ensure authorized access to digital systems, there are big challenges to be overcome in this context. Making information systems secure in all its features will help industrial managers to see with confidence the application of this new concept in industrial plants. The applied methodology has exploratory and descriptive characteristics. This same research sought to demonstrate, through research in various literatures, the importance of digital systems for today's society and what impact cyber-attacks have on business organizations. By understanding the existing dynamics in this area of knowledge, it was possible to define some guidelines that may guide the application of cybersecurity concepts aimed at the 4th Industrial Revolution. This paper sought to be in line with the guidelines for the preventive aspects related to cyber-attacks. Thus, it was possible to list possible suggestions aimed at minimizing the effects that such malicious practices may have on business organizations focused on the economic activity of producing consumer goods. Considering the importance of the issue at hand, due to the high costs that a cyber invasion can bring to a business organization, be it financial or intellectual property costs, its relevance and comprehensiveness are understood.
Key-words: Internet, Information, Industry, Cybersecurity.

1. Introdução

O mundo se encontra em processo de mudanças. Importantes transformações estão ocorrendo, em especial na última década. Está surgindo um novo cenário que se autodenomina de 4ª Revolução Industrial, mais conhecida como Indústria 4.0. Assim como nas outras revoluções industriais que ocorreram ao longo da história, a Indústria 4.0 também chega para gerar mudanças na forma como os produtos são manufaturados. Neste contexto entende-se que os impactos que ocorrerão com o advento deste conceito abrangerão os processos produtivos de forma relevante, pois os tornarão mais eficientes, autônomos e customizáveis. Além do impacto nos processos produtivos, o advento deste novo conceito tenderá também à reduzir os impactos ambientais que as atividades industriais geram na sua cadeia produtiva.

A indústria 4.0 vem se alinhando a diversas tecnologias, como Inteligência artificial, realidade aumentada, robótica, impressão 3D, nanotecnologia, big data, Internet das coisas (IoT), manutenção preditiva, simulação e cibersegurança (FAUSTINO, 2016).

A *European Schools Science Symposim* (ESSS, 2017) entende que seja necessário desenvolver a construção de nove pilares para possibilitar a implantação do conceito de Indústria 4.0 nos diferentes segmentos industriais. Estes mesmos pilares estariam relacionados a Big Data, a Robótica, a Simulação, aos Sistemas de Integração Vertical e Horizontal, a Internet das Coisas, a Cibersegurança, a Computação em Nuvem, a Manufatura Aditiva e a Realidade Aumentada.

Sendo a Cibersegurança uma das tecnologias que servirá como pilar para a consolidação da Indústria 4.0, necessita-se entender o nível de criticidade que a mesma apresenta. A segurança das informações é fator primordial para a estratégia de um negócio. Com a evolução dos sistemas de rede, a preocupação com a Cibersegurança vem se tornando relevante. O alto nível de conectividade que a indústria exige no controle dos seus processos torna essencial que os sistemas sejam seguros. Ao se proteger as informações, minimiza-se de forma considerável as consequências danosas de possíveis ameaças e falhas que uma provável invasão possa gerar (ESSS, 2017).

Venturelli (2017) aponta como sendo desafiadores, na implantação de um sistema que seja apropriadamente seguro, os seguintes aspectos: o nível de entendimento na aplicação prática de sistemas de seguranças nas plantas industriais; a aplicação de soluções inteligentes de segurança e o monitoramento e controle de invasões.

Este trabalho tem como objetivo identificar os principais desafios que poderão ser encontrados, no quesito Cibersegurança, para se implementar o conceito de Indústria 4.0. Pretende-se assim tornar mais clara a visão sobre este cenário, identificando os aspectos relevantes e necessários neste contexto.

2. Referencial teórico

Segundo Nazário (2018) a introdução da internet na vida cotidiana de pessoas e empresas modificou profundamente a maneira de acessar e compartilhar informações. As formas de organização da sociedade estão se moldando conforme caminha a evolução da tecnologia da informação. A sociedade como um todo está se tornando dependente da internet para ter acesso aos mais variados tipos de informações.

2.1 Importância da internet

Hoje é possível disseminar de forma rápida o conhecimento com as novas tecnologias de informação que estão disponíveis. As empresas conseguem desta forma aprimorar a eficiência dos seus processos para disponibilizar produtos inovadores aos seus consumidores. Desta maneira se torna cada vez mais desafiador atender as demandas do mercado diante do cenário que se desdobra por intermédio dos benefícios da internet.

A internet possui uma capacidade ímpar para deslocar informações por toda a cadeia de produção nas atividades industriais. Pode-se comparar analogamente a importância da internet para a indústria nos dias atuais com a importância que teve o advento da eletricidade no início do século XX. Assim, a internet nada mais é do que a base tecnológica para a nova era, a "Era da Informação". É um meio de comunicação que conecta muitos usuários, atingindo uma escala global (CASTELLS, 2003).

2.2 Informação

A informação precisa estar disponível, quase que de forma instantânea, para ser acessada pelos diferentes grupos de usuários. Desta maneira percebe-se o alto nível de comprometimento que a tecnologia da informação deve ter perante as demandas da sociedade atual. Tendo em vista que a informação no cenário atual possui um grande valor, percebe-se a importância existente em manter a mesma restrita ao ambiente virtual que à administra. A integridade e a privacidade da informação tornam-se então fatores chave para o desenvolvimento da sociedade atual (NAZÁRIO, 2018).

Para as organizações empresariais, o desenvolvimento dos sistemas de informações aumentou a eficiência das atividades de mensuração e de monitoramento do desempenho. Desta maneira tornou-se mais eficaz a apresentação dos resultados utilizados na gestão corporativa. Com isto, as organizações passaram a depender dos sistemas de informação desde o nível estratégico até o nível operacional. Sendo assim, entende-se que os riscos com relação a violação da segurança da informação, ou dos crimes cibernéticos, passa a ser um fator à ser considerado (COSO, 2007).

2.3 Indústria 4.0

A Confederação Nacional da Indústria (CNI, 2016) descreve em seu caderno intitulado "Desafios para a indústria 4.0 no Brasil" que o conceito de Indústria 4.0 faz referência ao que se denominaria como sendo a 4ª Revolução Industrial. Esta revolução vem se caracterizando pela integração das informações advindas do monitoramento dos processos, possibilitando assim o controle autônomo dos mesmos, apoiado pelo sensoriamento dos equipamentos produtivos.

Ao se integrar as informações reais com as especificações virtuais, possibilita-se a criação de sistemas denominados como ciberfísicos. A operação funcional de tais sistemas permite então empregar o uso da inteligência artificial nas plantas industriais (CNI, 2016). Esta integração entre os sistemas está representada pela ilustração da Figura 1.

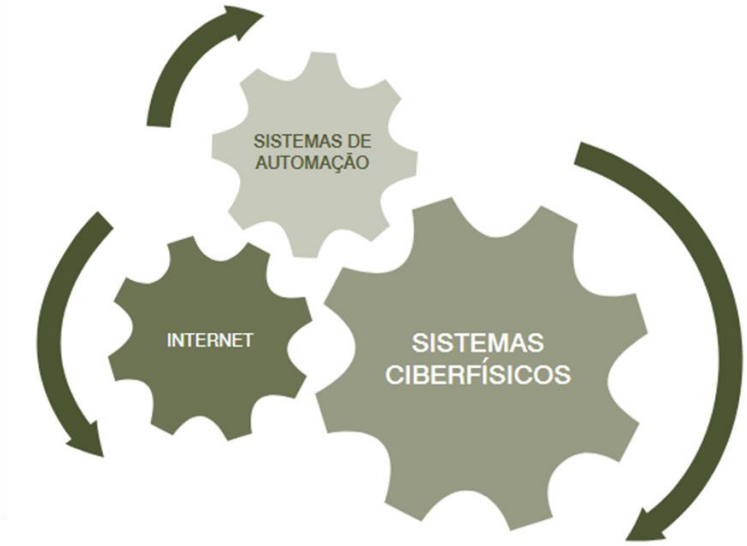

Figura 1 – Integração entre sistemas na indústria 4.0
Fonte: CNI (11p, 2016)

Já para Rüßmann (2015) a migração dos sistemas industriais tradicionais para o sistema industrial digital se dará pela interligação entre si de sensores, máquinas, produtos, hardware e softwares. Viabilizar a interconexão entre todos estes elementos elevará para outro patamar a cadeia de valor de uma planta industrial. Este autor entende que ao se proporcionar a conexão entre os elementos supracitados, será possível que o sistema consiga analisar os dados coletados, prevendo possíveis falhas. Desta maneira poderia este mesmo sistema se autoconfigurar para se adaptar a um novo cenário produtivo, evitando assim o surgimento das falhas previstas.

Os principais benefícios desta mudança de paradigma estariam relacionados à redução dos custos produtivos e ao aumento da qualidade dos produtos. A flexibilidade que se tornaria evidente para realizar as mudanças nos processos produtivos, tornando-os mais rápidos e precisos, seria fator determinante neste contexto (RÜßMANN, 2015).

2.4 Cibersegurança

A forte relação existente entre a taxa de crescimento econômico da nação brasileira com a taxa de crescimento de usuários dos serviços de internet é relevante. De todas as conexões de internet existentes, apenas uma pequena fração deste universo está preparada para se defender de forma eficaz das ameaças cibernéticas. Um simples clique em um link enviado por uma fonte desconhecida poderia desencadear uma sequência de violações de sistemas com consequências nefastas para os usuários (OPPERMANN, 2014). Vale ainda lembrar que o universo de usuários que podem ser atingidos por estas práticas maliciosas é abrangente, pois tal prática pode alcançar as grandes corporações e também os usuários domésticos.

Na indústria 4.0 os sistemas de hardware e software são responsáveis pela implementação dos processos, agindo de forma automática, com inteligência própria para assim atingir a eficiência total. Uma consequência desta revolução que surge é o fato de que a indústria se torna altamente dependente dos sistemas de informação. Diante disto surgem novos riscos relacionados a este modelo de gestão industrial. Neste sentido um dos maiores desafios está relacionado com questão voltada para os procedimentos de Cibersegurança.

A violação dos dados responsáveis pela automação dos sistemas industriais torna-se uma

das maiores preocupações neste contexto. Custos envoltos em uma possível violação são elevados e difíceis de mensurar. Isto faz com que as organizações dediquem atenção a esta problemática para que estejam preparadas e consigam mitigar os riscos em casos de possíveis violações dos seus sistemas de informação e controle. Assim sendo, a garantia da proteção dos sistemas é um assunto que ganha cada vez mais relevância neste cenário (GOES, 2019).

Gois (2018) ressalta que as invasões maliciosas de sistemas de informações provocam desordens e grandes perdas para diversas instituições públicas e privadas, demandando assim debates sobre os procedimentos e as tecnologias necessárias para minimizar os efeitos desta prática danosa.

De acordo com Machado (2019), a Cibersegurança é um conceito que se estabelece para denominar as boas práticas tecnológicas que devem ser adotadas na preservação da segurança das informações, de redes e de sistemas de hardware e software. Este mesmo autor destaca que entre os eventuais prejuízos que uma invasão maliciosa pode acarretar estariam à espionagem industrial, o roubo de dados de acessos bancários e a manipulação indevida de dados das corporações.

O que torna uma invasão cibernética tão perigosa são as características que a mesma apresenta. O ataque pode ocorrer quase que de forma instantânea, atingindo vários alvos ao mesmo tempo e não encontrado barreiras geográficas para sua atuação.

Para tornar as informações de uma organização protegidas com relação ao acesso não autorizado, evitando-se modificações inapropriadas, deve-se abordar três diferentes temas. Estes mesmos temas estariam relacionados a confidencialidade, a integridade e a disponibilidade (COBIT 5, 2012).

Nazário (2018) também destaca estes três temas, descrevendo-os como:

- Confidencialidade: desvio de informações e acompanhamento das atividades;
- Integridade: modificação das informações;
- Disponibilidade: impedimento de acesso ao sistema pelos usuários.

Conforme a CNI (2016), existem vários desafios à serem abordados na implantação deste novo conceito para os sistemas de manufatura no Brasil. Um destes desafios seria a criação de padrões de Cibersegurança, com legislação própria que responsabilize os autores do ato malicioso, para que assim se possa reduzir a quantidade de ataques cibernéticos. Desta maneira se minimizariam os efeitos que tais contravenções acarretariam as corporações industriais, caso fossem atingidas por estes atos.

3. Metodologia

No desenvolvimento deste artigo foi realizada uma pesquisa com características exploratórias. Segundo Prodanov e Freitas (2013), as pesquisas exploratórias objetivam proporcionar um leque maior de informações sobre o assunto a ser investigado para assim defini-lo e delineá-lo. Nos cenários que normalmente envolvem levantamentos bibliográficos ou quando envolvem aspectos relacionados à análise de exemplos e entrevistas com pessoas, este modelo de pesquisa se faz apropriado.

A pesquisa também tem caráter descritivo, pois se entende que os fatos abordados são apenas descritos, ordenados e registrados, sem haver alguma interferência do narrador (PRODANOV; FREITAS, 2013).

Primeiramente o artigo apresentou uma pesquisa bibliográfica sobre a indústria 4.0 e alguns tópicos importante relacionados a tecnologia da informação. Objetivou-se assim compreender o contexto existente sobre como as empresas estão se alinhando com as tecnologias atuais, orientadas para esta nova revolução industrial.

Posteriormente foi abordado o tema sobre a questão da Cibersegurança. Desta maneira foi possível compreender melhor sobre a influência que este tema possui neste novo modelo de concepção de manufatura.

Ao se estabelecer estes dois pontos, procurou-se apresentar informações que fossem relevantes no sentido de se minimizar o impacto que os ataques cibernéticos podem gerar nos sistemas digitais de manufatura. Desta maneira foi possível contribuir com o tema em questão.

4. Desafios da Cibersegurança

Diante do referencial levantado, enxerga-se como a evolução da tecnologia da informação é importante não somente para o desenvolvimento da Indústria, mas também para toda a humanidade. Com isto, garantir a segurança das informações que estão disponíveis em todos os lugares é o grande desafio deste início de século. A Cibersegurança não se torna apenas necessária, mas apresenta-se como um ponto central à ser discutido para auxiliar no desenvolvimento sustentável da humanidade.

As empresas, ao utilizarem a tecnologia, precisam ter a garantia de que terão a proteção necessária das suas informações para que a operação ocorra da maneira desejada. Como foi constatado por Nazário (2018) e também pela COBIT 5 (2012) a tecnologia, para que possa atender os requisitos de segurança das empresas, precisa incluir em seu pacote de serviços as condições de confidencialidade, integridade e disponibilidade das informações.

Segundo Cruz Júnior (2013), garantir a proteção das informações estratégicas, abrangendo a infraestrutura de hardware e os programas de software, é ponto relevante a ser considerado na alocação de recursos que visem a atualização tecnológica dos sistemas. Entende o autor que determinadas atualizações podem também servir de porta de entrada para as temidas invasões de sistemas.

Já para Lima (2016), a defesa cibernética poderia ser conceituada como sendo um conjunto de ações orientadas para somente proteger os ambientes virtuais de possíveis ataques cibernéticos. As principais ações propostas estariam relacionadas a utilização de ferramentas tecnológicas, na aplicação de metodologias para realizar a gestão de riscos e na alocação de recursos e treinamentos constantes para manter atualizadas os conceitos e as proteções dos sistemas de informações.

4.1. Aspectos estratégicos

De acordo com Oppermann (2014), a Organização para a Cooperação e Desenvolvimento Econômico – OCDE seria um exemplo de entidade internacional que procura coordenar estratégias voltadas para implementar políticas de segurança cibernética nos seus países membros. Tais políticas procuram incluir nesta discussão os diferentes atores que são influenciados pelas invasões maliciosas que ocorrem neste contexto. O mesmo autor destaca a existência de cinco atores principais que participam do desenvolvimento destas estratégias, sendo os quais: o setor público, o setor privado, o terceiro setor, as instituições de ensino superior e a sociedade como um todo.

Em relação a participação do setor privado neste processo, CNI (2016) ressalta que as organizações empresariais necessitam implementar procedimentos de Cibersegurança. Esta mesma demanda também seria aplicada junto ao poder público, pois o mesmo necessitaria criar legislações específicas para atender as premissas que são inerentes a proteção das informações corporativas.

Conforme Cruz Júnior (2013) a defesa cibernética poderia ser explorada além das ações com foco nas situações de proteção das informações estratégicas. Poderia-se também explorar as ameaças envolvidas e promover atividades ofensivas que objetivassem prejudicar o sistema invasor.

4.2. Aspectos preventivos

Uma condição relevante relacionada a Cibersegurança diz respeito ao nível de conhecimento que se deve ter sobre as vulnerabilidades existentes em um sistema digital de controle e gestão de informações. A probabilidade de ocorrer uma invasão maliciosa é tanto maior quanto menor for o conhecimento sobre as brechas existentes no sistema e não menos importante, sobre os impactos que uma provável invasão possa ocasionar à uma organização empresarial (GOES, 2019).

De acordo com Rüßmann (2015), para se atuar na prevenção de ataques cibernéticos no meio industrial, torna-se necessário manter as comunicações protegidas por intermédio da adoção de rígidos protocolos de acesso. O autor entende que a manutenção de uma gestão sofisticada, de identificação para acesso dos sistemas de hardware e para a permissão dos usuários, se torna cada vez mais preponderante.

Goes (2019) procura destacar algumas condições que são relevantes no tocante às ações preventivas que uma organização deve adotar para proteger os seus sistemas digitais.

4.2.1. Segurança periférica

Em relação à segurança periférica, o autor entende que para se criar uma primeira linha de defesa, deve-se definir um perímetro de segurança por intermédio de recursos de firewall, de sistemas de detecção de intrusão (IDS) e de sistemas de prevenção de intrusão (IPS).

4.2.2. Proteção de rede

Na abordagem referente a proteção de rede, Goes (2019) observa que existem variados meios para serem utilizados na proteção da mesma. Configurar terminais para que sejam acessados somente por pessoal autorizado, utilizando soluções de *Neetwork Acess Control* (NAC) seria uma das alternativas. Já a segmentação da rede conferindo uma lógica que possa diferenciar grupos de hardwares e que possa gerenciar a transferência de informações entre os mesmos hardwares dificultaria a ocorrência de acessos indevidos.

Ainda neste quesito, Goes (2019) descreve que a implantação de diferentes domínios de segurança também dificultaria o acesso indevido ao sistema. Já a utilização de hardwares que permitam somente a comunicação unilateral tornaria o sistema imune ao retorno de informações pela via utilizada na invasão maliciosa. O autor entende ainda que para proteger as redes de forma complementar, devem-se tomar medidas preventivas de forma sequencial e diferenciada. Desta maneira tornaria-se a defesa do sistema mais profunda, aumentando-se assim a possibilidade do agente invasor ser detectado.

4.2.3. Segurança dos dados

As soluções de criptografia permitem garantir a autenticação dos usuários que possuem permissão de acesso aos sistemas. Além da criptografia, o uso de mecanismos que permitam utilizar várias chaves de acesso também se faz apropriado para promover as garantias necessárias na utilização dos certificados digitais. Tais medidas corroboram para manter as informações intactas e confidenciais (GOES, 2019).

4.2.4. Atualizações de sistemas

Não menos importante neste contexto está o fato relacionado a boa prática de avaliação constante sobre a necessidade de atualização dos equipamentos de hardware e dos sistemas de software. Havendo negligência neste contexto, possibilita-se a abertura de oportunidades para agentes invasores promoverem ataques cibernéticos, pois os mesmos procuram estar em constante evolução, em estratégia e conhecimento tecnológico.

4.3. Gestão de riscos

Para Goes (2019) ao se elencar, analisar e documentar todas as possíveis variáveis que podem ocorrer e que são relativas à segurança dos sistemas digitais, torna-se possível trabalhar na criação de cenários hipotéticos referentes aos ataques cibernéticos. Ainda, ao se determinar estes cenários é possível definir ações de contenção visando implementar procedimentos de respostas, para assim minimizar potenciais danos que possam ocorrer no momento da identificação da invasão que esteja em curso.

Manter a gestão de riscos atualizada permanentemente, utilizando metodologias próprias para este fim (ciclo de observação, orientação, decisão e ação) e definindo métricas específicas para monitorar esta mesma gestão, são condições de segurança recomendáveis (GOES, 2019).

Este mesmo autor procura ressaltar que existe uma necessidade premente de se viabilizar planos de testes de penetração na rede para se avaliar o potencial de resistência do sistema de segurança e também, para se encontrar os pontos fracos deste mesmo sistema. Desta maneira se objetivaria avaliar o nível de segurança e a *performance* da rede.

4.4. Recursos e treinamentos

Para tornar a Cibersegurança efetiva, as empresas necessitam revisar os métodos utilizados. As mesmas precisam alinhar em direção a este objetivo todos os aspectos organizacionais ligados aos procedimentos e as políticas e priorizações das atividades de segurança cibernética. Os profissionais envolvidos devem estar capacitados para intervir no momento certo e assim evitar que as violações de sistema aconteçam.

Conforme Goes (2019), a documentação interna referente aos procedimentos de segurança cibernética deve salvaguardar o cumprimento dos objetivos estratégicos de uma organização, seja ela de direito público ou de direito privado.

Algumas medidas à serem tomadas estariam relacionadas ao compartilhamento de informações e das experiências que ocorrem neste contexto. O compartilhamento dos resultados de análises de riscos com todos os atores envolvidos se faz pertinente, para que os mesmos estejam cientes dos possíveis problemas ou então das soluções encontradas. Definir padrões de segurança também é um ponto importante a ser debatido objetivando incorporar esta análise na cultura organizacional das empresas. Tornar padrão o uso de normas de utilização de e-mails, acessos de servidores, utilização de programas e softwares entre outras ações preventivas seria apropriado (ANTONIAZZI, 2017).

Muito além da capacitação patrocinada pelas organizações empresariais, como conclui Canongia e Mandarino Junior (2009), a formação de recursos humanos especializados em segurança cibernética deveria ser considerada em todos os níveis da formação educacional. Poderia iniciar já no ensino básico e se estender até a pós-graduação. Por outro lado, pouco vale a capacitação técnica sem que exista a conscientização sobre a importância da segurança da informação. A exploração destes dois aspectos precisaria caminhar em conjunto para assim se alcançar uma cultura orientada para esta abordagem em específico.

5. Conclusões finais

Para qualquer organização empresarial, manter as suas informações e o seu parque fabril sob segurança absoluta e constante é uma condição primária a ser orientada para se viabilizar a implantação da 4ª Revolução Industrial.

A Cibersegurança é um tema ainda novo, que necessita ser entendido e explorado com maior profundidade, tanto pelas organizações empresariais de direito privado como pelas organizações de direito público. Sendo uma problemática que começa a se tornar evidente, seja pela sua relevância e abrangência ou pelos aspectos legais que representa, torna-se apropriado investir recursos para tornar a segurança dos sistemas digitais efetiva nos resultados que necessita apresentar.

O presente trabalho procurou apresentar de forma objetiva e sucinta os principais tópicos existentes sobre a importância de se manter protegidos os sistemas digitais, observando-se pelo contexto da aplicação em sistemas de manufaturas voltados para o conceito de Indústria 4.0.

Torna-se relevante entender os aspectos estratégicos e preventivos voltados para este contexto, pois caso seja negligenciada a questão referente a segurança dos sistemas digitais, possivelmente haverá um impacto negativo nas taxas de crescimento da aplicação do conceito de Indústria 4.0 pelas organizações empresariais.

6. Referências

ANTONIAZZI, Felipe. **Gestão de riscos cibernéticos**. 2017. Disponível em: <https://www.arcon.com.br/blog/gestao-de-riscos-ciberneticos>. Acesso em: 14 set. 2019.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, p.21-46, dez. 2009. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 15 set. 2019.

CASTELLS, Manuel. **A galáxia da internet:** Reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=nCKFFmWOnNYC&oi=fnd&pg=PA5&dq=evolu%C3%A7%C3%A3o+da+internet&ots=_DEUQEy6ZR&sig=YjE7xO5A3HPX8OAYem7M9FTkH_I#v=onepage&q&f=false>. Acesso em: 15 ago. 2019.

CNI. **Desafios para indústria 4.0 no Brasil.** Confederação Nacional da Indústria. Conselho Temático Permanente de Política Industrial e Desenvolvimento Tecnológico – COPIN. Brasília: CNI, 2016. 34 p. Disponível em: <https://bucket-gw-cni-static-cms-si.s3.amazonaws.com/media/filer_public/d6/cb/d6cbfbba-4d7e-43a0-9784-86365061a366/desafios_para_industria_40_no_brasil.pdf>. Acesso em: 14 ago. 2019.

COBIT 5. **A Business Framework for the Governance and Management of Enterprise IT**. Rolling Meadows, Il: ISACA, 2012. Disponível em: <https://static1.squarespace.com/static/56b3cadb59827ecd82b02b43/t/56d8c0d84d088e673055c308/1457045725120/COBIT-5_res_eng_1012.pdf>. Acesso em: 15 ago. 2019.

COSO. **Gerenciamento de Riscos Corporativos - Estrutura Integrada**. Jersey City: Aicpa, 2007. Disponível em: <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>. Acesso em: 09 set. 2019.

CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Instituto de Pesquisas Aplicadas – Ipea. Brasília. 2013. Disponível em: <http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=19183>. Acesso em: 17 ago. 2019.

ESSS. **Os pilares da Indústria 4.0**. 2017. Disponível em: < https://www.esss.co/blog/os-pilares-da-industria-4-0/>. Acesso em 08 ago. 2019.

FAUSTINO, Bruno. **Seis princípios básicos da Indústria 4.0 para os CIOs.** 2016. Disponível em: <https://cio.com.br/seis-principios-basicos-da-industria-4-0-para-os-cios/>. Acesso em: 08 ago. 2019.

GOES, Nuno. Cibersegurança na Indústria Nacional: Dossier Sobre Cibersegurança Industrial. **Robótica**, Porto, v. 1, n. 114, p.56-62, 15 jan. 2019. Trimestral. Disponível em: <http://www.robotica.pt/PDF/ROB114/dossier_.pdf>. Acesso em: 19 set. 2019.

GOIS, Alexsandro Barreto. Segurança Cibernética. **O Comunicante**, [S.l.], v. 8, n. 3, p. 40-47, out. 2018. ISSN 2594-3952. Disponível em: <http://ebrevistas.eb.mil.br/index.php/OC/article/view/1796>. Acesso em: 22 ago. 2019.

LIMA, Davi Marques; LIMA, Álvaro Vieira. **A importância da segurança cibernética em sistemas de controle industrial.** Congresso Virtual Brasileiro – CONVIBRA. 2016. Disponível em: <http://www.convibra.com.br/artigosp.asp?opc=2&ev=22&lang=pt&busca=A+IMPORT%C2NCIA+DA+SEGURAN%C7A+CIBERN%C9TICA+EM+SISTEMAS+DE+CONTROLE+INDUSTRIAL&B2=Buscar>. Acesso em: 17 ago. 2019.

MACHADO, Walmor. **Cibersegurança: o que é e qual a relação com a Indústria 4.0.** 2019. Disponível em: <https://www.voitto.com.br/blog/artigo/ciberseguranca>. Acesso em: 13 ago. 2019.

NAZÁRIO, Bárbara Ferreira. **Cybersecurity, Cyberspace e Relações Internacionais**. 2018. Monografia (Graduação em Relações Internacionais) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2018. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/12986>. Acesso em: 18 ago. 2019.

OPPERMANN, Daniel. Governança da Internet e Segurança Cibernética no Brasil. **Monções: Revista de Relações Internacionais da UFGD**, Dourados, v. 2, n. 4, p. 259-283, mar. 2014. ISSN 2316-8323. Disponível em: <http://ojs.ufgd.edu.br/index.php/moncoes/article/view/3097>. Acesso em: 20 ago. 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico.** 2. ed. Novo Hamburgo: Universidade Feevale, 2013.

RÜßMANN, Michael *et al*. **Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries**. Boston Consulting Group. 2015. Disponível em: < https://www.bcg.com/pt-br/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries.aspx> Acesso em: 19 set. 2019.

VENTURELLI, Márcio. **A segurança de dados na Indústria 4.0**. 2017. Disponível em: <https://www.automacaoindustrial.info/seguranca-de-dados-na-industria-4-0/>. Acesso em: 08 ago. 2019.