FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Dener Aparecido Caldeira Paschoal

Guilherme Fontes Pereira

SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0 – FRAMEWORK NIST

Americana, SP

2019

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Dener Aparecido Caldeira Paschoal

Guilherme Fontes Pereira

SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0 – FRAMEWORK NIST

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP.

2019

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

P283s PASCHOAL, Dener Aparecido Caldeira

Segurança da Informação na indústria 4.0: framework NIST. / Dener Aparecido Caldeira Paschoal, Guilherme Fontes Pereira. – Americana, 2019.

57f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1 Inovação tecnológica 2.Segurança em sistemas de informação I. PEREIRA, Guilherme Fontes II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 332:6

Dener Aparecido Caldeira Paschoal
Guilherme Fontes Pereira

SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0 – FRAMEWORK NIST

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 06 de dezembro de 2019.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Mestre
Fatec Americana

Francisco Carlos Mancin (Membro)
Mestre
Fatec Americana

Estevão da Silva Barros (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Queremos agradecer, em primeiro lugar, a Deus, pela força e coragem durante toda esta longa caminhada.

Agradecemos a todos da nossa família, que nos apoiaram em todos os momentos da nossa vida e que estão nos acompanhando em mais essa conquista.

Nossos agradecimentos aos nossos amigos, companheiros de trabalhos e irmãos na amizade que fizeram parte da nossa formação e que vão continuar presentes em nossa vida com certeza.

A esta faculdade, seu corpo docente, direção, administração e ao nosso orientador que foram tão importantes na minha vida acadêmica e que nos acompanharam durante a graduação.

DEDICATÓRIA

Dedicamos este trabalho a Deus, que nos abençoou e deu forças sempre que precisamos, aos nossos familiares e amigos que sempre estiveram ao nosso lado e que foram pacientes conosco neste momento e aos professores desse curso, que serão sempre lembrados por todo apoio.

RESUMO

O presente trabalho tem como tema a indústria 4.0 e a segurança da informação numa empresa. Por meio da utilização de um guia com orientações para a avaliação da segurança da informação, esta pesquisa propõe a elaboração de uma ferramenta para avaliar o nível de segurança atual na organização e o nível que se deseja alcançar, a fim de identificar boas práticas e medidas de segurança a serem utilizadas, protegendo-a dos riscos que podem afetar os ativos e informações da indústria 4.0. Para tanto, este estudo parte de uma pesquisa bibliográfica para explanação dos temas abordados. Além disso, este trabalho se constitui de um estudo de caso, utilizando-se de normas como ISO 27001:2013, COBIT e o *framework* NIST para elaboração de uma planilha que será utilizada como guia para a avaliação em questão. Os resultados apontam que é necessário aprimorar a segurança da informação na indústria 4.0, que emprega a tecnologia em todos os seus processos, devendo lidar com um grande volume de coleta e análise de dados. Disso decorre a preocupação de proteger essas informações a fim de que não sejam perdidas, expostas, roubadas ou utilizadas de modo prejudicial ao negócio. Com a elaboração dessa ferramenta, fica mais fácil identificar áreas com maior vulnerabilidade, em que haja a necessidade de melhorias, bem como a identificação de áreas críticas, em que qualquer incidente de segurança possa ocasionar um grande problema para a organização. Os resultados obtidos no estudo de caso mostram que com essa ferramenta de apoio, a avaliação da segurança da informação torna-se mais fácil, proporcionando uma visão geral de todas as áreas do negócio e indicando os níveis de maturidade em que se encontram.

Palavras Chave: indústria 4.0; *framework* NIST; segurança da informação.

ABSTRACT

The present work focuses on industry 4.0 and the information security in an organization. Using of a document with guidelines for the assessment of information security, this research work aims to prepare a tool that evaluates the current level of security in the organization and the desired level to be achieved in order to identify good practices and security measures to be used, protecting it against risks that may affect assets and information in the industry 4.0. For this purpose, it was carried out a bibliographic research to explain the topics hereby covered. It is also presented a case study in which there were used standards such as ISO 27001:2013, COBIT and the NIST framework to elaborate a spreadsheet that will be used as a guide to convey the mentioned assessment. The results show that it is necessary to improve the information security in the industry 4.0, which is employs technology in all processes, dealing with a large volume of data collection and analysis. This leads to a concern towards the best way to protect this information so that they will not be to lost, exposed, stolen or used in a harmful way to the business. The development of this tool, it is easier to identify areas of greater vulnerability where improvements are needed, as well as critical areas where any security incident creates a major problem for the organization. The results of the case study show that with this support tool, security assessment becomes easier, offering an overview of all areas of the business and indicating the maturity levels in which they are found.

Keywords: industry 4.0; NIST framework; information security.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

CLP	Controles lógicos programáveis
CNI	Confederação Nacional da Indústria
COBIT	*Control Objectives for Information and Related Technologies* (Objetivo de Controle para Tecnologia da Informação e Áreas Relacionadas
CPS	*Cyber Physical Systems* (Sistemas Ciber Físicos)
DW	*Deutsche Welle*
ERP	*Enterprise Resources Planning* (Planejamento dos Recursos da Empresa)
FIESP	Federação das Indústrias do Estado de São Paulo
FIRJAN	Federação das Indústrias do Estado do Rio De Janeiro
IoS	*Internet of Services* (Internet de serviços)
IoT	*Internet of Things* (Internet das coisas)
ITGI	*Information Technology Governance Institute*
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
MRP	*Material Requirements Planning* (Planejamento das Necessidades de Materiais)
MRP II	*Manufacturing Resources Planning* (Planejamento dos Recursos de Manufatura)
NIST	*National Institute of Standards and Technologies*
PDCA	*Plan, Do, Check e Act* (Planejar, Fazer, Verificar e Agir)
TI	Tecnologia da informação
TIC	Tecnologias da informação e comunicação
ZVEI	*Zentralverband Elektrotechnik* (Associação dos Fabricantes de Eletroeletrônicos da Alemanha)

1. INTRODUÇÃO

Ao longo da história, o ser humano presenciou diversas revoluções, da mecanização, produção em massa, automatização e a mais recente, envolvendo conectividade e produção inteligente.

A indústria 4.0 é um conceito relativamente novo, criado pelos alemães em 2011, onde consiste em criarem fábricas inteligentes que reúnem inovações tecnológicas em automação, controle e tecnologia da informação para o aprimoramento de manufatura (TOTVS, 2018).

No Brasil, segundo Rolli (2019), os dados da Confederação Nacional da Indústria (CNI), apontam que o setor industrial reconhece a importância de investimentos nessa área, mas ainda é baixo o percentual de empresas que adotam ou têm a intenção de usar as tecnologias que estão relacionadas com a indústria 4.0, como por exemplo: Internet das coisas.

Por outro lado, das empresas que adotam as tecnologias presentes da indústria 4.0, uma preocupação muito importante, é a segurança da informação, de acordo com uma pesquisa da Federação das Indústrias do Estado de São Paulo (FIESP) identificou que 31% das indústrias brasileiras já sofreram ataques cibernéticos (FIESP, 2018). Segundo Almeida (2018), os riscos de um ataque cibernético não podem ser desconsiderados, pois podem resultar em parada intencional das operações, roubo de dados, sequestro e bloqueio de informações. Para o autor, “faz-se necessário assegurar a proteção das operações como um todo, implementando sistemas de segurança em um nível mais estratégico”, sendo assim, a segurança da informação tem um papel muito importante para as empresas, organizações ou indústrias.

A indústria 4.0 ou Quarta Revolução Industrial, está relacionado com a revolução digital, onde a Internet é responsável por realizar diversas mudanças no processo de manufatura das organizações, indústrias ou empresas. É o aprimoramento entre a Terceira Revolução Industrial, automação e a troca de informações, utilizando de conceitos de sistemas ciber físicos, Internet das coisas, sensores, atuadores ambos conectados pela Internet.

A relevância deste trabalho pode ser dividida em três modalidades: Acadêmica, Profissional e Pessoal.

a) Acadêmico: o estudo do tema pode apontar com a Segurança da Informação está diretamente ligado com tema, visto que é atual e ainda pouco explorado.

b) Profissional: o estudo do tema abre novas oportunidades para que os profissionais da área de Segurança da Informação atentem-se que esse tema é muito importante para as organizações e cada vez mais presente.

c) Pessoal: para os autores a escolha do tema, além da satisfação pessoal, a compreensão do assunto, pode trazer uma oportunidade de trabalho, ou de estudo aprofundado, sendo uma especialização ou pós-graduação.

Este trabalho é norteado por objetivos a serem alcançados. Esses objetivos são descritos na sequência:

a) Entender a Quarta Revolução Industrial, conhecida com Indústria 4.0, bem como a segurança da informação, importante tema nessa área.

b) Contextualizar de forma histórica as revoluções industriais da 1ª a 4ª.

c) Conceituar e compreender os termos envolvidos, vantagens e benefícios da indústria 4.0

d) Identificar boas práticas e medidas de segurança para serem utilizadas indústria 4.0.

e) Utilizar o guia de aperfeiçoamento da Segurança cibernética para infraestrutura crítica da NIST (*National Institute of Standards and Technologies*) para avaliação de segurança da informação nas indústrias 4.0.

f) Elaborar uma ferramenta para avaliação de segurança da informação nas indústrias 4.0, com foco nas funções identificar e proteger.

A transformação digital que está ocorrendo na atual revolução está promovendo diversos benefícios, contudo deve-se utilizar de diversos meios para proteger os dados a fim de impedir a ação de criminosos. Segundo Macedo (2017), o Fórum Econômico Mundial de 2017 ocorrida em Davos na Suíça, colocou a segurança cibernética, como um dos desafios enfrentados mundialmente.

Encontrar mecanismos que protegem a segurança da informação na indústria 4.0 pode representar para as organizações vantagem competitiva e uma preocupação com os dados e informações que elas manipulam, podendo assim adotar novas estratégias nos negócios.

De acordo com Sacomano *et al.* (2018), as empresas entraram em um novo patamar, onde elas experimentam e aplicam tecnologia como nunca dentro delas, possibilitando um alto nível de conectividade e compartilhamento de dados. A segurança da informação também vem se tornando cada vez mais difundida, pois as organizações estão expostas as fontes potenciais de perigos, e a informação que é um bem, tem valor, precisa ser protegida.

O presente trabalho está estruturado da seguinte forma: na introdução, que é o capítulo 1, é relatado o desenvolvimento da fundamentação teórica referente ao tema central e demais elementos fundamentais, como indústria 4.0, segurança da informação e *framework* NIST. No capítulo 2 está descrito a evolução histórica, desde a primeira revolução industrial até a atual. No capítulo 3 é explicado sobre a indústria 4.0, o seu conceito, exemplos e os elementos fundamentais. No capítulo 4 é relatado sobre a segurança da informação na indústria 4.0, as propriedades principais da segurança da informação, os motivos que aumentaram os riscos. No capítulo 5 está descrito sobre os riscos de segurança da informação. No capítulo 6 é explicado sobre o *framework* NIST, que é guia de aperfeiçoamento da segurança cibernética para infraestrutura crítica. Em seguida, no capítulo 7 é abordado o estudo de caso, que é a elaboração de uma ferramenta utilizando o *framework* NIST como guia para a avaliação de segurança da informação nas indústrias 4.0. Por fim, as considerações finais, que é o capítulo 8, onde aborda os objetivos e resultados alcançados graças ao conteúdo estudado.

2. CONTEXTUALIZAÇÃO HISTÓRICA

Para entender sobre a indústria 4.0 ou Quarta Revolução Industrial, é essencial compreender o histórico das revoluções industriais anteriores, pois estão mudando os processos industriais e fabris. Para Schwab (2016), “as revoluções têm ocorrido quando novas tecnologias e novas formas de perceber o mundo e desencadeiam uma alteração profunda nas estruturas sociais e nos sistemas econômicos”.

A primeira revolução industrial estava focada em produtos manufaturados artesanalmente. Em 1767, foi criado por James Hargreaves, a primeira máquina de fiar, era de madeira e foi utilizada em larga escala na Inglaterra. Já o inglês Richard Arkwright, em 1769, criou o tear hidráulico, utilizando na indústria de tecidos. No mesmo ano, James Watt, iniciou o aperfeiçoamento da máquina a vapor. Edmund Catwright, em 1785, inventou o tear mecânico, que poderia ser operado por mão de obra sem especialização, foi o início da tecelagem industrial na Inglaterra, que foi chamado de Primeira Revolução Industrial. Foi na primeira revolução industrial que surgiram a classe operária, jornadas de trabalho de dezesseis horas, crianças e adolescentes trabalhavam ganhando baixos salários (SACOMANO *et al.*, 2018).

No século XIX, o aumento da produção do aço, proporcionou a fabricação de equipamentos e máquinas mais modernas, que juntamente com a energia elétrica para fins industriais impulsionou a manufatura. As estradas de ferro era um importante meio de transporte de mercadorias e pessoas. O termo “produção em massa”, “divisão e especialização do trabalho” foram adotados após as empresas se tornarem especialistas em produzir determinados produtos.

De acordo com Ferreira, Reis e Pereira (2011), Frederick Taylor (1856-1915) desenvolveu a racionalização do trabalho e aperfeiçoou a divisão do trabalho [...] marcando o início da Segunda Revolução Industrial.

A manufatura em massa, como novo processo, fez com que Henry Ford adaptasse a manufatura artesanal de produção de carros para esse novo processo. “Buscava a diminuição dos custos de produção e procurava pagar um salário aos seus funcionários, que tornasse possível a eles poder adquirir os carros que fabricavam” (SACOMANO *et al.*, 2018).

O trabalho repetitivo, forte supervisão, hierarquia similar à militar, a pressão a que os funcionários eram submetidos nas linhas de produção são características negativas dessa Segunda Revolução.

> A manufatura em massa reduziu os custos de produção e, consequentemente o preço do produto ao consumidor, propiciando que uma parcela maior da sociedade pudesse adquirir bens e serviços. Trouxe também a padronização de produtos [...] a verticalização das empresas (SACOMANO *et al.*, 2018).

Não havia ainda a preocupação com a qualidade, pois o objetivo era produzir sempre do mesmo bem e cada vez mais.

No final da Segunda Guerra Mundial, o Japão estava devastado e com recursos escassos, sendo assim, o governo japonês lançou um pacote de incentivos para toda a nação, a reduzir o desperdício, possibilitando assim, aproveitar tudo com os poucos recursos disponíveis. Foi a partir disso que a Toyota, não podendo copiar o sistema de Henry Ford, criou seu próprio sistema, denominado: Sistema Toyota de Produção, produção enxuta ou *lean manufacturing.*

> Fornecer a melhor qualidade, o menor custo e o *lead time* mais curto por meio da eliminação do desperdício [...] é mantido e melhorado por interações entre o trabalho padronizado e *kaizen*, seguidos de PDCA [...] operações [...] não teriam excesso de estoque e [...] trabalhar em parceria com seus fornecedores a fim de nivelar a produção (LEAN, [s.d.]).

Na década de 60, os controladores lógicos programáveis (CLP), facilitaram a automação industrial. Com a eletrônica evoluindo com o passar dos anos, tornou-se mais barata e pôde-se ter maior capacidade de atender a novos e maiores desafios.

A Tecnologia da Informação (TI) passou a ser usada intensamente para apoio e controle da manufatura. Alguns exemplos podem ser dados, como: o uso do *Material Requirements Planning* (MRP) – utilizado para controle da necessidade de componentes/matéria-prima, do *Manufacturing Resources Planning* (MRP II) - controle de materiais e gerenciar os recursos industriais e o *Enterprise Resources Planning* (ERP) – integra todo processo industrial à empresa.

Em síntese, a produção enxuta, automação e uso intensivo da TI, trouxeram ganhos para a indústria em geral. Sacomano *et al.* (2018), aponta esse período “convencionou-se chamar [...] de Terceira Revolução Industrial”.

Para Batista (2012), “o desenvolvimento da Internet pode ser resumido em duas importantes décadas: 1960 e 1970”. Em 1960, o Departamento de Defesa dos Estados Unidos desenvolveu um sistema de comunicação com o uso de redes de computadores, com o objetivo de manter as bases militares, em contato constante, a fim de evitar ataques nucleares. A Internet surgiu então no período da Guerra Fria.

Em 1970, esse sistema de comunicação foi expandido, disponibilizado em universidades e já em 1980, qualquer pessoa que tivesse um computador poderia utilizá-lo.

> A Internet é uma conexão de todas as redes do mundo, mas do ponto de vista do usuário, ela representa a possibilidade, quase infinita, de acesso a serviços on-line, comunicação entre pessoas ou troca de dados entre computadores [...] uma interligação de várias redes em todo o mundo utilizando os mesmos padrões de comunicação, causando uma revolução nas telecomunicações (BATISTA, 2012).

A integração remotamente entre as operações industriais com fornecedores e clientes não é nova, segundo Sacomano *et al.* (2018). No ano de 1979, o autor Joseph Harrington publicou um livro chamado: Manufatura integrada por computador, abordando o tema.

Em 1989, a Chevrolet-Pontiac-GM do Canadá, iniciou o serviço experimental de transmissão de pedidos a fornecedores pela Internet. Outros países, como Coreia do Sul e Japão tiveram ideias parecidas, porém sem sucesso. Entre os motivos do não-sucesso ou grandes avanços estão: os altos custos de implantação e manutenção do sistema, falta de capacidade dos equipamentos.

Para Sacomano *et al.* (2018), ao passar do tempo, os equipamentos eletrônicos tornaram-se cada vez mais potentes e flexíveis, novos softwares foram desenvolvidos e os preços caíram, podendo assim, realizar a integração das operações de manufatura à fornecedores, clientes e sua operação remota.

> Em 2011, o governo da Alemanha lançou um projeto durante a Feira de Hannover, denominado de Plataforma Indústria 4.0, com o objetivo de desenvolver alta tecnologia de modo a fazer com que os sistemas automatizados que controlam os equipamentos industriais pudessem se comunicar trocando [...] informações/dados entre máquinas e seres humanos, deforma a otimizar todo o processo de produção (SACOMANO *et al.*, 2018).

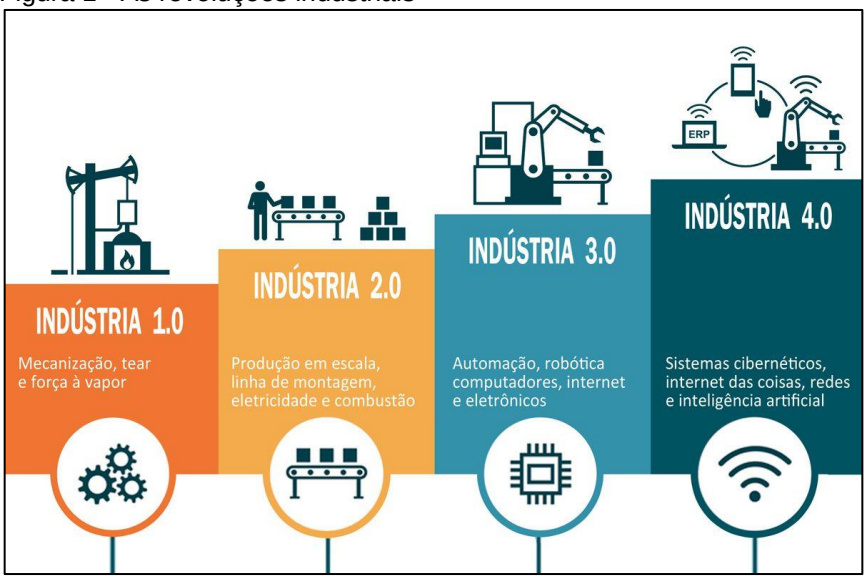
A Quarta Revolução Industrial baseia-se na revolução digital:

> É caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizagem de máquina) [...] ao permitir 'fábricas mais inteligentes' a Quarta Revolução Industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível. Isso permite a total personalização de produtos e a criação de novos modelos operacionais (SCHWAB, 2016).

Com isso, percebe-se que a Internet possibilitou o surgimento da Quarta Revolução Industrial, essa atual revolução é fundamentalmente diferente das anteriores, pois as "tecnologias emergentes e as inovações generalizadas são difundidas muito mais rápida e amplamente do que nas anteriores". (SACOMANO *et al.*, 2018).

Para melhor entendimento, a Figura 1 mostra a evolução histórica das revoluções industriais.

Figura 1 - As revoluções industriais



Fonte: Shimao (2019)

3. INDÚSTRIA 4.0

O termo “indústria 4.0” atualmente é muito discutido nas áreas acadêmicas, econômicas e sociais tanto no Brasil, como no mundo, podendo ser definido como uma série de mudanças no processo da manufatura, design, produto, operações e sistemas relacionados à produção, proporcionado assim, um aumento no valor da cadeia organizacional e em todo o ciclo de vida do produto.

O 4.0 significa a junção entre os mundos virtuais e físicos através da Internet (FIRJAN, 2016). Para *European Parliament* (2015), “tudo dentro e ao redor de uma planta operacional (fornecedores, distribuidores, unidades fabris, e até o produto) são conectados digitalmente, proporcionando uma cadeia de valor altamente integrada”.

Para Gomes (2015), do site *Deutsche Welle* do Brasil (DW), a chamada indústria 4.0, conecta máquinas, sistemas e pessoas nos processos de produção industrial, elevando a personalização dos produtos e permitindo o uso mais eficiente de recursos.

> A Indústria 4.0 reorganiza a cadeia produtiva, conectando máquinas e pessoas nas chamadas *smart factorys*. Elas são altamente adaptáveis aos processos e às necessidades de produção, além de usar os recursos de forma mais eficaz. O estoque de matérias-primas, por exemplo, pode ser facilmente controlado, dentro de uma produção totalmente integrada e conectada (GOMES, 2015).

O conceito foi apresentado pela primeira vez, em 2011, na Feira de Hannover, como parte da estratégia de alta tecnologia do governo alemão. Segundo dados, divulgados pela DW, através de membros da Associação dos Fabricantes de Eletroeletrônicos da Alemanha (*ZVEI - Zentralverband Elektrotechnik*), mais de 75% das indústrias associadas a associação citada anteriormente, já começaram a implementar algumas das premissas da indústria 4.0.

Um exemplo do uso da indústria 4.0, é o caso da Siemens, desenvolvendo um software que cria um ambiente de fábrica virtual para a montadora Volkswagen. Esse desenvolvimento de linha de produção digital fez com que se elevasse a produtividade e reduziu-se o consumo de energia (GOMES, 2015).

A indústria 4.0 assenta-se ao integrar as tecnologias da informação e comunicação (TIC), que permitem alcançar novos patamares de produtividade, flexibilidade e gerenciamento, podendo assim: gerar novas estratégias e modelos de negócio para a indústria (SACOMANO *et al.*, 2018).

> “A Quarta Revolução Industrial [...] foi possível a integração do mundo físico com o digital, conectando a produção às pessoas, permitindo a convergência de serviços e redes, [...] as redes de alta velocidade possibilitam uma transmissão de cada vez mais volumosa de dados” (STEVAN JUNIOR; LEME; SANTOS, 2018).

O conceito de sistema produtivo utilizado na indústria 4.0 não está restrito apenas as indústrias, podendo ser aplicado em outros setores produtivos, como por exemplo na agricultura (SACOMANO *et al.* 2018). Schwab (2016) diz que essa revolução: “é a única por causa da crescente harmonização e integração de muitas descobertas e disciplinas diferentes”.

Segundo Hermann, Pentek e Otto (2015), dizem existir quatro componentes-chave para a formação da indústria 4.0, já para Sacomano *et al.* (2018), diz que esses elementos são considerados “elementos base ou fundamentais”, onde a Indústria 4.0 se apoiam e sem os quais não poderia existir, representando assim a base tecnológica fundamental dessa nova revolução.

a) Sistemas ciber físicos, ou *cyber physical systems*, é uma forma de implantar sistemas de informação e automação que torna possível a troca de informação, execução de comandos e acompanhamento de um processo produtivo de maneira distante e em tempo real. (SACOMANO *et al.* 2018). “Em outras palavras, são sistemas que permitem a fusão dos mundos físico e virtual, através de computadores embarcados e redes que controlam os processos físicos gerando respostas instantâneas” (FIRJAN, 2016). São exemplos de CPS: uma unidade de controle, que comanda os sensores e atuadores, tecnologias de identificação, banco de dados, análises de dados.
b) Internet das coisas (IoT) é uma rede de objetos físicos, sistemas, plataformas e aplicativos com tecnologia embarcada para realizar ações como: comunicar, sentir ou interagir com ambientes internos e externos (FIRJAN, 2016), na IoT emissor e/ou receptor são coisas, objetos que utilizam a Internet como um canal de comunicação. Em outra definição,

pode ser dita como a relação entre as coisas e as pessoas que é possível por plataformas e tecnologias conectadas (SCHWAB, 2016). São exemplos de objetos de IoT: geladeiras inteligentes, *smart products*. A IoT cria oportunidades para novos tipos de serviços, e até aplicações de mercado em massa (SACOMANO *et al.* 2018).

c) Internet de serviços (IoS) é definido como a criação de novos serviços que são disponibilizados por meio da Internet ou internamente à empresa (SACOMANO *et al.* 2018). Para os mesmos autores, a IoS pode ser exemplificada da seguinte forma: ao invés de comprar uma máquina, uma indústria poderá comprar somente o serviço que ela oferece, ou seja, os serviços de manutenção poderão ser solicitados diretamente pelo próprio equipamento que os necessita.
d) Fábricas inteligentes (*smart factories)* para alguns autores, como: Hermann, Pentek e Otto (2015) incluem as fábricas inteligentes como componentes-chaves ou elementos base ou fundamentais. As fábricas inteligentes, os consumidores, dispositivos e sistemas formam uma produção dinâmica, organizados de forma inteligente, baseando-se em informações disponíveis na rede (STEVAN JUNIOR; LEME; SANTOS, 2018). A comunicação será própria entre os produtos, máquinas e linhas de montagem, serão monitorados, independe do local e será em tempo real (FIRJAN, 2016).

4. SEGURANÇA DA INFORMAÇÃO NA INDÚSTRIA 4.0

As empresas entraram em um novo patamar, onde as mesmas experimentam e aplicam tecnologia como nunca dentro delas; possibilitando um alto nível de conectividade e compartilhamento de dados. A tecnologia é móvel, a informação está mais acessível para executivos, funcionários, clientes e fornecedores, sendo o processo interativo, instantâneo de qualquer lugar e possibilitando assim a geração de resultados para as tomadas de decisões.

A informação chega a qualquer parte do mundo de acordo com a disponibilidade e confidencialidade, em questão de poucos segundos através da Internet (SACOMANO *et al.* 2018).

Para Fontes (2006), a segurança da informação tem se tornado cada vez mais conhecida, pois as organizações possuem suas informações processadas e armazenadas no ambiente computacional e são dependentes desse ambiente para realizarem seus negócios, tendo o acesso à informação disponível a todos os colaboradores da organização.

As fontes de potenciais perigos para a segurança da informação podem estar relacionadas a diversos fatores. Para Sêmola (2014), podendo ser: crescimento exponencial na digitalização das informações, aumento dos elementos de conectividade dentro da companhia, desenvolvimento de relações eletrônicas entre as empresas e compartilhamento de informações.

A facilidade de aquisição devido ao baixo custo dos equipamentos de informática, como por exemplo, computadores e todos os dispositivos que têm acesso à Internet, a popularização de dispositivos pessoais (smartphones, proporcionando uma alta capacidade de interconectividade dentro do ambiente de trabalho e fora dele também) e a disponibilidade de acesso à Internet, agravam-se questões relacionadas à segurança da informação, tais como: as regras ineficientes para identificação de usuários na Internet, proliferação de técnicas de ataque de invasão, desconhecimento dos usuários, amplitude e uma certa confusão nos mecanismos legais para responsabilizar malfeitores de crimes digitais e tipificação do estereótipo do hacker, apontado como um gênio e herói que obteve êxito em uma invasão.

A informação é um bem, tem valor para a empresa e deve ser protegida. A informação deve ser cuidada por meio de políticas e regras, da mesma maneira que os recursos financeiros e materiais são tratados dentro de uma empresa, a informação é um ativo de valor, um recurso crítico para o negócio e a execução da missão (FONTES, 2006).

Toda informação envolve três propriedades principais: confidencialidade, integridade e disponibilidade, conforme pode ser visto na Figura 2 associados aos aspectos de autenticidade e legalidade que completam estas influências.

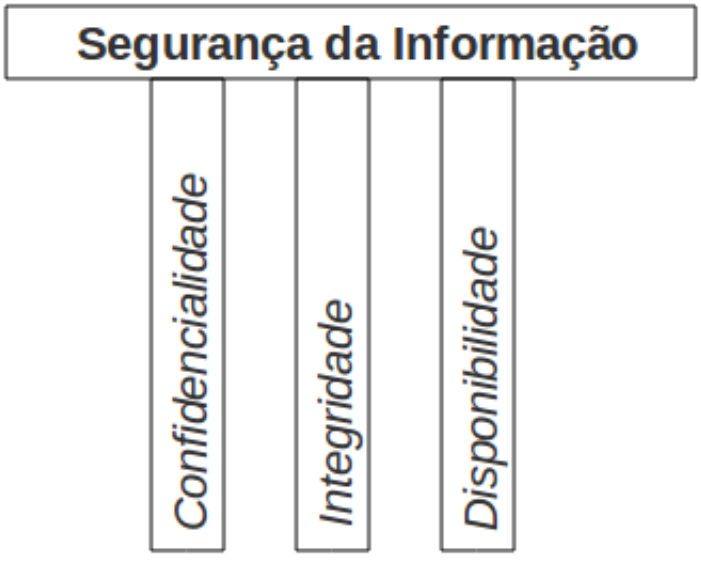
Para Fontes (2006), a proteção da informação significa garantir a disponibilidade, integridade, confidencialidade, legalidade, auditabilidade e não-repúdio.

Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.

Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.

Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; necessita de uma autorização prévia. A Figura 2 mostra a tríade da segurança da informação.

Figura 2 - Tríade da Segurança da Informação

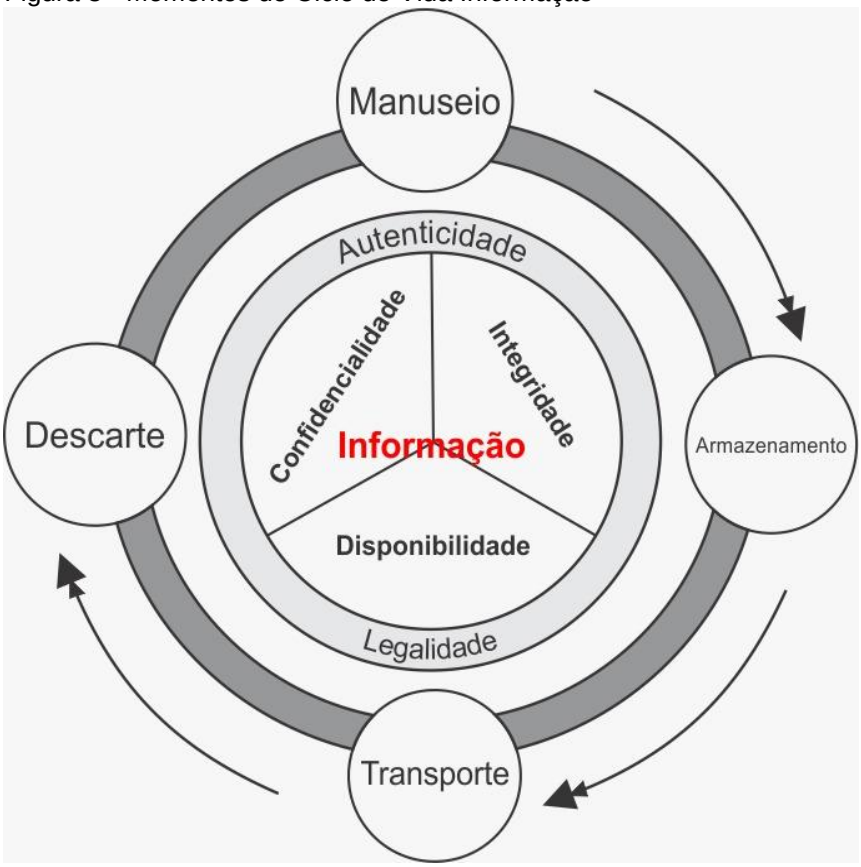


Fonte: Lucas (2010)

O ciclo de vida da informação é completo quando veem com atenção os momentos em que os dados sofrem com a ocorrência dos riscos. Por isso, deve-se observar que a manipulação da informação, acontece ao executar processos que contribuem para a operação das empresas, essa manipulação acontece de três maneiras: nos ativos tecnológicos, nos ativos físicos e nos seres humanos (SACOMANO *et al.* 2018).

Existem quatro momentos do ciclo de vida da informação que requer muita atenção, pois correspondem as situações onde a informação é exposta a ameaças colocando em risco a integridade. São os quatro momentos: manuseio, armazenamento, transporte e descarte da informação, conforme Figura *3*.

Figura 3 - Momentos do Ciclo de Vida Informação



Fonte: Sêmola (2014)

Para Sacomano *et al.* (2018), manuseio corresponde pelo momento em que a informação é criada ou manipulada, seja para acessar uma pasta com documentos,

digitar senhas para autenticar em um sistema, digitar informações geradas em uma aplicação, por exemplo.

O armazenamento, é caracterizado ao momento onde a informação é armazenada, pode ser em um banco de dados dentro da empresa, em nuvem, anotações em papel, pasta compartilhada na rede.

O transporte corresponde ao momento que a informação é transportada, seja por e-mail, telefone, upload de arquivo para a Internet.

E por último, o descarte, onde a informação não é mais útil, e que pode ser depositado em uma lixeira, descarte de mídia, ou simplesmente apagando o arquivo. É um momento crítico extremamente importante no sentido da segurança da informação.

5. RISCOS DE SEGURANÇA DA INFORMAÇÃO

A transformação digital que ocorre na atual revolução promove inúmeros benefícios. No entanto, deve exigir diversos meios de proteger os dados a fim de impedir a ação de criminosos, ou pessoas mal-intencionadas, pois cada vez mais, as mídias reproduzem notícias sobre ataques de hackers, roubo de dados e arquivos, vazamento de informações confidenciais, entre outros.

Nessa atual revolução, faz-se o uso intenso das tecnologias digitais sobretudo aquelas que são apoiadas pela Internet*,* vem cada dia mais se fundindo aos processos da produção industrial e transformando os conceitos da indústria convencional (CNI 2016; *EUROPEAN PARLIAMENT* 2015)

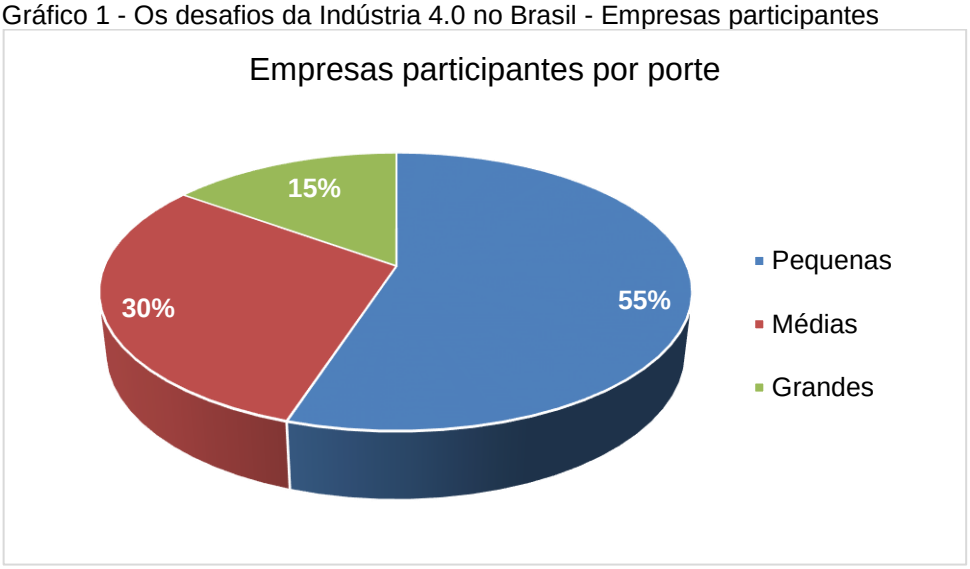
Segundo a Ernest Young (2017), o Fórum Econômico Mundial de 2017, classifica uma falha de grande escala na segurança cibernética como um dos riscos mais sérios que o mundo enfrenta hoje, de acordo com o documento "*The Global Risks Report 2017 – 12th Edition*" (FWE, 2017).

De acordo com Wentzel (2017), o estudo é divulgado anualmente pelo Fórum Econômico Mundial. No ano de 2017, os cinco grandes riscos globais mencionados foram:

1. Eventos climáticos extremos – como o aquecimento global;
2. Imigração em larga escala – motivado por catástrofes naturais, conflitos violentos, ondas migratórias;
3. Grandes desastres naturais – simulação de impacto destrutivo de uma enchente na China, por exemplo;
4. Terrorismo e vigilância – ataques terroristas, restrições às liberdades de expressão;
5. Fraudes eletrônicas e roubo de dados – segurança cibernética.

Uma pesquisa realizada pela Federação das Indústrias do Estado de São Paulo (FIESP, 2018) identificou os desafios da Indústria 4.0 no Brasil. Participaram da pesquisa 227 empresas, 55% pequenas, 30% médias e 15% grandes, como mostrado no Gráfico 1.

Gráfico 1 - Os desafios da Indústria 4.0 no Brasil - Empresas participantes

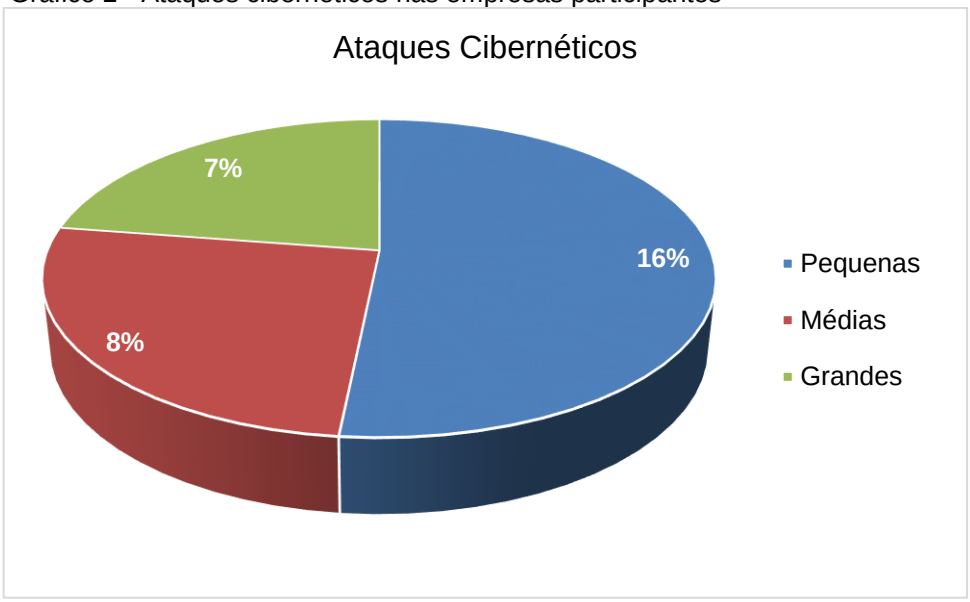


Fonte: Adaptado de FIESP (2018).

Um dos temas que fizeram parte da pesquisa foi: cibersegurança, “uma vez que indústrias cada vez mais conectadas elevam o risco de segurança da informação e de paradas não programadas”. Conforme os Gráficos 2, 3, 4 e 5 a pesquisa mostrou que:

a) 31% já sofreram ataques cibernéticos (16% pequenas, 8% médias e 7% grandes);

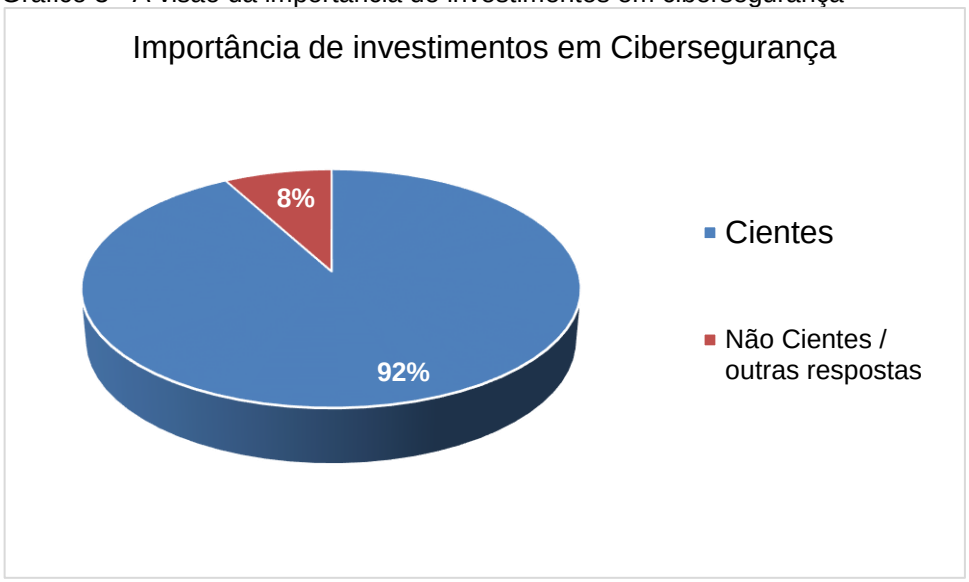
Gráfico 2 - Ataques cibernéticos nas empresas participantes



Fonte: Adaptado de FIESP (2018).

b) 92% estão cientes da importância de investir em cibersegurança;

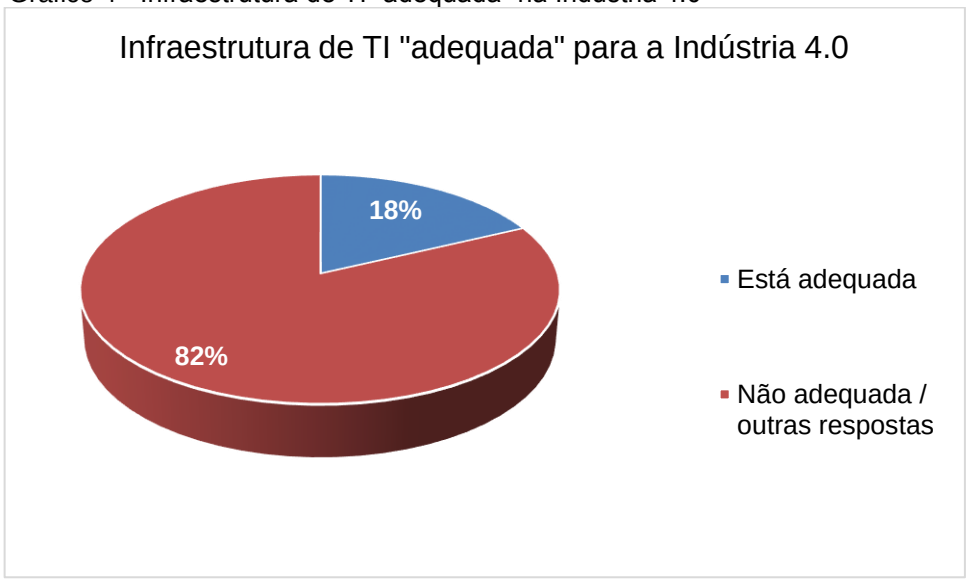
Gráfico 3 - A visão da importância de investimentos em cibersegurança



Fonte: Adaptado de FIESP (2018).

c) 18% disseram que a infraestrutura de tecnologia da informação “está adequada” para suportar as tecnologias da Indústria 4.0;

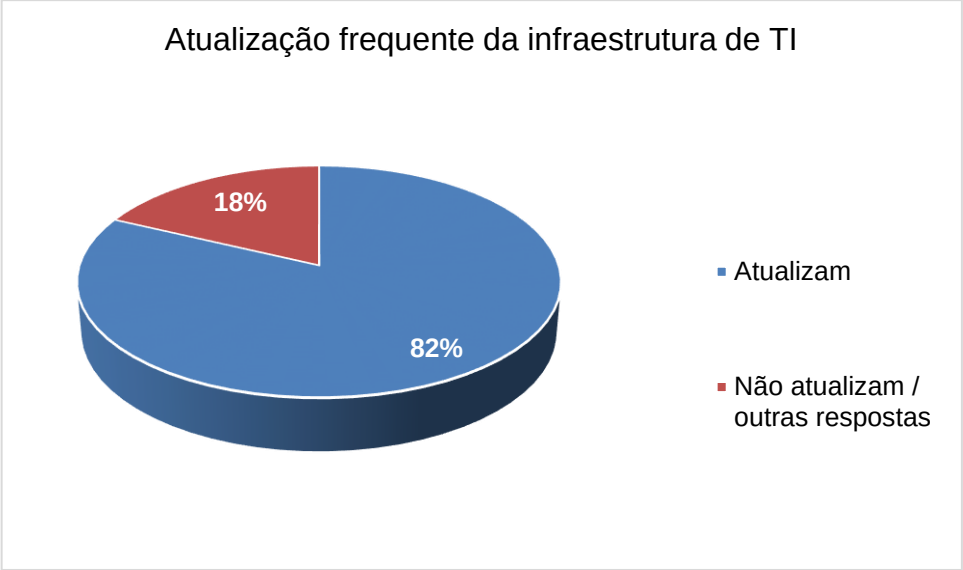
Gráfico 4 - Infraestrutura de TI “adequada” na Indústria 4.0



Fonte: Adaptado de FIESP (2018).

d) 82% atualizam com frequência, softwares, hardwares, equipamentos, ferramentas e sistemas operacionais.

Gráfico 5 - Atualização frequente de infraestrutura de TI



Fonte: Adaptado de FIESP (2018).

Segundo a FIESP (2018), também é importante incentivar investimentos na infraestrutura de TI, uma vez que apenas 18% das empresas consideram que estão adequadas para as tecnologias dessa atual revolução, “isso é preocupante para as grandes empresas, pois são os maiores alvos de ataques cibernéticos”.

6. *FRAMEWORK* NIST

De acordo com *U.S. Chamber of Commerce* (2018), o instituto norte americano NIST (*National Institute of Standards and Technologies*) elaborou um *framework* chamado “Guia de aperfeiçoamento da segurança cibernética para infraestrutura crítica”. Esse guia estabelece orientações para facilitar e apoiar o desenvolvimento de diretrizes sobre risco de segurança cibernética e usa indicadores para orientar atividades e considerar os riscos de segurança como parte do gerenciamento de riscos da organização. A *U.S. Chamber of Commerce* (2018) alega ainda que:

Para gerenciar os riscos de segurança, é necessário um entendimento dos indicadores de negócio da organização, além dos riscos, as prioridades e sistemas são específicas para organização. Este guia ajuda a lidar com a segurança nas dimensões físicas, cibernéticas e referentes a pessoas. Na organização seu foco pode ser usado na área de tecnologia da informação (TI), sistemas de controle industrial (ICS), sistemas ciber-físicos (CPS) ou em dispositivos como a Internet das Coisas (IoT), visando reduzir e gerenciando os riscos de segurança em cada uma dessas áreas ou na estrutura como um todo.

Cada organização pode usar o guia na melhor forma que atende, para aplicá-lo na gestão dos riscos de sua infraestrutura, aproveitando a parte que mais necessita. Uma organização pode utilizar das funções da estrutura básica para analisar os riscos mais críticos, outra organização pode optar pelos níveis de implementação para o gerenciamento de riscos previstos, para auxiliar com as necessidades dos operadores de infraestruturas críticas em um ambiente com possíveis vulnerabilidades, riscos e ameaças.

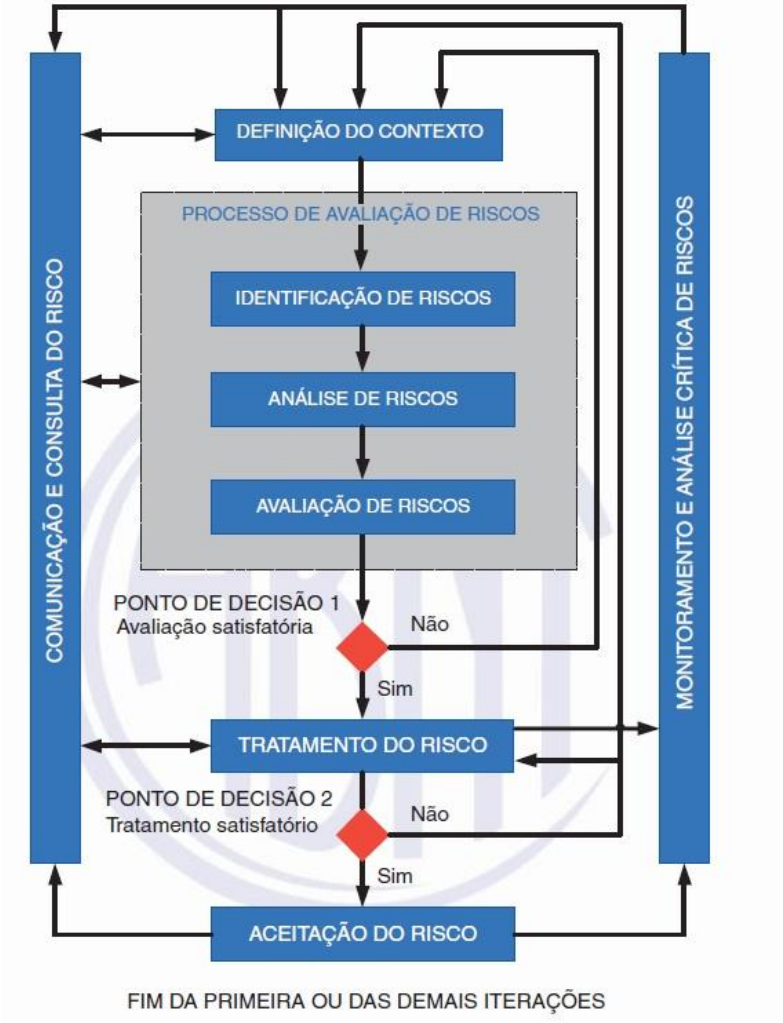
A segurança cibernética da infraestrutura, para manter a privacidade das informações, é essencial para a boa imagem da organização, aumentando a credibilidade perante os clientes, colaboradores e usuários, tanto por empresas privadas quanto por órgãos públicos. Por isso a utilização de guias, normas e boas práticas de segurança estão sendo cada vez mais necessárias.

Porém esse guia não é a solução para todos os problemas de riscos de segurança cibernéticas, em cada organização ele poderá assessorar de forma diferentes para cada necessidade e auxiliar gerenciar e reduzir as ameaças. Ele

complementa o processo de gerenciamento de segurança, potencializando as medidas necessárias já utilizadas, alinhando-se com os negócios da organização.

Para gerenciar os riscos as organizações devem avaliar os possíveis eventos e quais impactos terão na organização. Esse processo é contínuo de análise, avaliação e resposta ao risco. Depois desse processo é necessário qual decisão será tomada, a de prevenir, transferir, mitigar ou aceitar o risco, conforme Figura 4.

Figura 4 - Processo de gestão de riscos de segurança da informação



Fonte: ABNT NBR ISO 31000:2009 (2009).

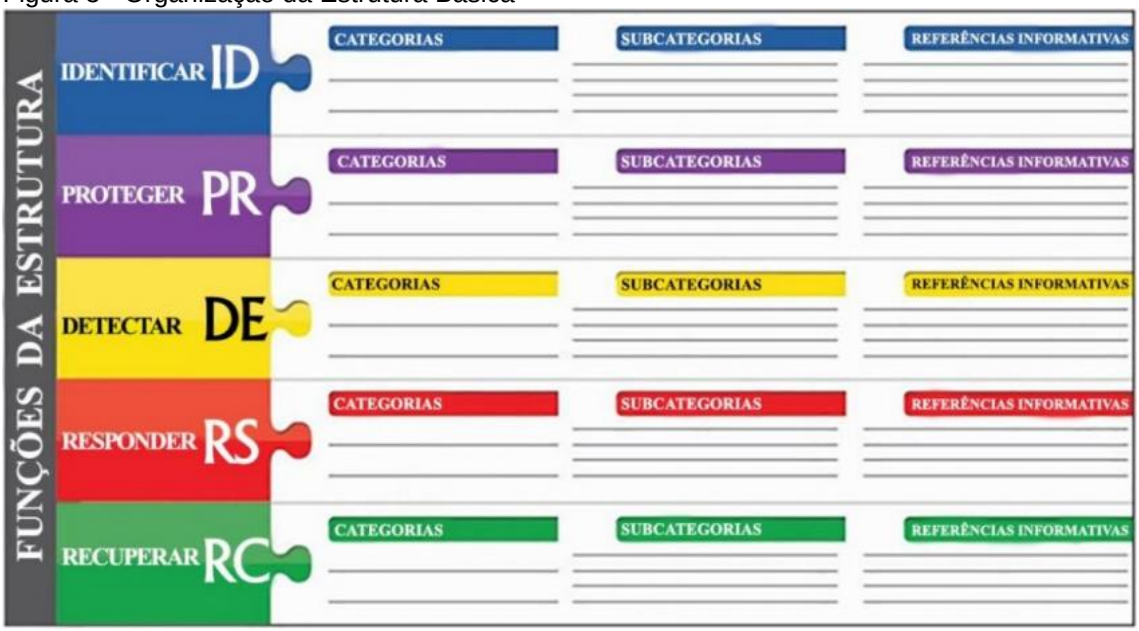
Com base nesses padrões, diretrizes e práticas, o Guia oferece uma taxonomia e mecanismos comuns para que as organizações:

1) Descrevam sua situação atual no que tange à segurança cibernética;
2) Descrevam seus objetivos no que tange à segurança cibernética;
3) Identifiquem e priorizem oportunidades de aperfeiçoamento dentro do contexto de um processo contínuo e reproduzível;
4) Avaliem seus progressos frente aos objetivos;
5) Comuniquem-se com *stakeholders* internos e externos sobre os riscos apresentados na atual segurança cibernética (*U.S. CHAMBER OF COMMERCE*, 2018).

De acordo com *U.S. Chamber of Commerce* (2018), O guia está dividido em três partes: a Estrutura Básica, os Níveis de Implementação e as Avaliações da Estrutura.

A Estrutura Básica apresenta padrões, diretrizes e práticas de segurança, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica, também permite a comunicação das atividades e dos resultados em toda organização. A estrutura básica consiste em cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar. Para cada função são divididas em categorias e subcategorias, passando referências para cada subcategoria de alguns guias, normas ou boas práticas como, ISO 27001:2013 ou COBIT 5. A Figura 5, mostra a organização da estrutura básica do *framework*:

Figura 5 - Organização da Estrutura Básica



Fonte: *U.S. Chamber of Commerce* (2018)

As funções organizam as atividades em um nível mais alto, ajudam ao gerenciamento de risco organizando informações, tratando ameaças e melhorando de acordo com atividades já realizadas anteriormente. As cinco funções são:

- Identificar: a função essencial para o gerenciamento de riscos, para compreender a organização como um todo, analisando sistema pessoas, ativos dados e recursos. Com uma identificação eficaz consegue-se priorizar os recursos em área mais críticas ou com maiores demandas.

- Proteger: Implementar proteções necessárias nas áreas identificadas na função anterior. Proteger sistemas e informações, áreas físicas e treinar e conscientizar os usuários e colaboradores que utilizam dos sistemas de informações, explicando a importância das proteções utilizadas e os possíveis impactos que podem ser causados por erros ou imprudências.
- Detectar: Desenvolver atividades para detecção de eventos de segurança. Alguns exemplos são processo de detecção de anomalias e monitoramento contínuo.
- Responder: Atividades estipuladas para executar caso algum incidente de segurança ocorra, contendo o impacto ou minimizando os efeitos. Alguns exemplos dessa função são planejamento de resposta e notificações de incidentes.
- Recuperar: Implementar atividades para restaurar recursos ou serviços que foram prejudicados por algum incidente de segurança. Oferece apoio para reestabelecer as funções normais depois de um evento de segurança com o mínimo de impacto possível.

Os Níveis de Implementação da Estrutura, classifica em níveis como a organização lida com os riscos de segurança e os processos para gerência. Esses níveis são divididos em 1, parcial; 2, risco informado; 3, reproduzível e 4, adaptável. Esses níveis classificam as práticas de gerenciamento de risco e para a classificação devem ser analisados alguns fatores como requisitos legais, objetivos de negócios, entre outros. O nível deve ser selecionado para atender às metas e reduzir os riscos em ativos e recursos críticos para níveis aceitáveis das organizações.

As definições de níveis são as seguintes:

1. Parcial – no processo de gerenciamento de risco as práticas de gerenciamento de risco não são formalizadas, o risco é gerenciado de forma reativa e não há prioridade das atividades de segurança de acordo com os objetivos de risco ou pelos requisitos de negócio da organização. No programa integrado de gerenciamento de risco, existe uma consciência limitada do risco, o gerenciamento de risco é feito de forma irregular e pode não haver processos de informações de segurança que permitam que sejam compartilhados internamente. Na

participação externa, a organização não envia e nem recebe informações de outras entidades e não tem consciência dos riscos dos produtos e serviços que utiliza.

2. Risco informado – as práticas de gerenciamento de risco são aprovadas pela administração, a prioridade das atividades é permeada pelos objetivos de riscos ou requisitos de negócios. No programa integrado de gerenciamento de risco há uma conscientização do risco de segurança, informações são compartilhadas na organização e a avaliação do risco cibernético de ativos organizacional ocorre. Na participação externa a organização colabora e recebe algumas informações de outras entidades, está ciente dos riscos da cadeia de suprimentos.
3. Reproduzível – no processo de gerenciamento de risco, as práticas de gerenciamento de risco são formalmente aprovadas e expressas como política na organização, as práticas são atualizadas regularmente de acordo com o cenário atual. No programa integrado de gerenciamento de risco, políticas, processos e procedimentos de conhecimento de risco são implementados e revisados em toda organização, os funcionários possuem conhecimento e habilidades para realizar suas funções com responsabilidade perante os riscos. A organização monitora o risco de segurança dos ativos e os executivos de segurança se comunicam com outras áreas sobre os riscos. Na participação externa compartilha informações com outras entidades, está ciente dos riscos dos produtos e serviços e age formalmente sobre esses riscos, com acordos por escritos, implantação e monitoramento de políticas.
4. Adaptável – no processo de gerenciamento de risco, a organização adapta suas práticas de segurança com base em atividades anteriores e atuais com base em um processo de aperfeiçoamento contínuo e responde de maneira eficaz às ameaças. No programa integrado de gerenciamento de risco, a organização utiliza políticas, processos e procedimentos para abordar possíveis ameaças de segurança, os executivos monitoram os riscos, o gerenciamento de riscos de segurança evolui a partir da conscientização e a organização pode responder de forma eficiente às mudanças sobre como o risco é

abordado e comunicado. Na participação externa contribui com a comunidades sobre os riscos, compartilha quase em tempo real sobre essas informações da cadeia de suprimentos e utiliza mecanismos formais e informais de comunicação para divulgar informações de segurança sobre produtos e serviços.

A Tabela 1 detalha as definições de níveis de implementação da estrutura.

Tabela 1 - Definições de Nível do *Framework* NIST

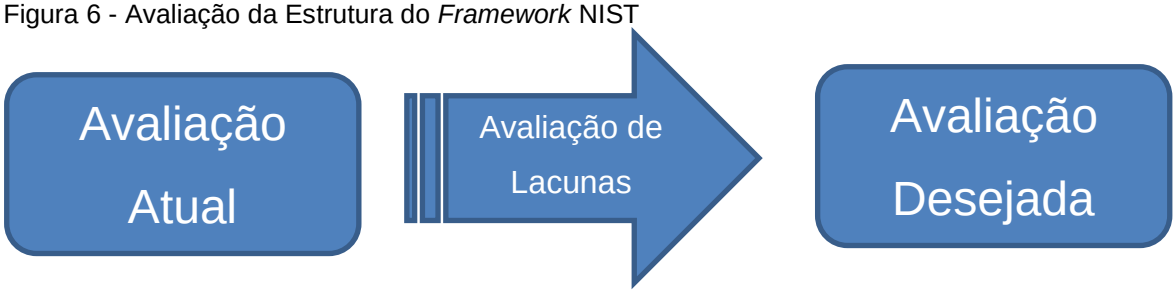
Definições de Nível		
1	Parcial	As práticas não são formalizadas. Consciência limitada do risco.
2	Risco Informado	As práticas são aprovadas pela administração. Conscientização do risco, informações são compartilhadas, avaliações de risco cibernético de ativo organizacional ocorrem.
3	Reproduzível	As práticas são formalmente aprovadas e expressas como política; são atualizadas regularmente.
4	Adaptável	A organização adapta as práticas de segurança com base em atividades anteriores e atuais com base em um processo de melhoria contínua. Utiliza-se de políticas, processos e procedimentos. Monitoram-se riscos e ameaças.

Fonte: Elaborado pelos autores.

De acordo com *U.S. Chamber of Commerce* (2018), Avaliação da Estrutura são os resultados de uma análise comparativa entre uma avaliação atual com uma avaliação desejada com base nas necessidades da organização de acordo com as categorias e subcategorias da estrutura básica. Essa avaliação permite que a organização estabeleça um roteiro para reduzir os riscos de acordo as prioridades e os requisitos legais. A avaliação atual ajuda a dar prioridades, determinando quais são mais importantes. Na avaliação desejada será estipulada resultados necessários para atingir metas de gerenciamento de riscos de segurança cibernética. A comparação de avaliações pode mostrar lacunas que precisam ser melhoradas para

atender os objetivos da organização. Isso pode priorizar recursos necessários para atingir a meta, conforme Figura 6.

Figura 6 - Avaliação da Estrutura do *Framework* NIST



Fonte: Elaborado pelos autores.

Esse presente trabalho, aborda, conforme discorrido anteriormente, as duas primeiras funções: Identificar (ID) e Proteger (PR) presente dentro do *framework* NIST.

Dentre as categorias, existem as subcategorias e para cada subcategoria, há referências informativas, como por exemplo: CIS CSC, COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013, NIST SP 800-53.

Para esse trabalho, utiliza como referência informativa, a ISO 27001:2013 (ABNT, 2013) e quando uma subcategoria não houver essa referência, adotará o COBIT 5. A Figura 8, detalha as funções identificar e proteger:

Tabela 2 - Funções Identificar e Proteger

Identificador Exclusivo de Função	Função	Identificador Exclusivo de Categoria	Categoria
ID	Identificar	ID.AM	Gerenciamento dos Ativos
		ID.BE	Contexto Empresarial
		ID.GV	Governança
		ID.RA	Avaliação de Risco
		ID.RM	Estratégia de Gerenciamento de Riscos
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimento
PR	Proteger	PR.AC	Gerenciamento de identidade e controle de acesso
		PR.AT	Conscientização e Treinamento
		PR.DS	Segurança de Dados
		PR.IP	Processos e Procedimentos de Proteção da Informação
		PR.MA	Manutenção
		PR.PT	Tecnologia Protetora

Fonte: *U.S. Chamber of Commerce* (2018)

6.1 Função Identificar (ID)

Gerenciamento de Ativos (ID.AM): Segundo o *framework* NIST essa categoria tem como função: identificar dados, pessoal, dispositivos, sistemas e instalações, que estão relacionados com o negócio e estão gerenciados de acordo com a importância e a risco da organização.

Dentro da categoria de Gerenciamento de Ativos (ID.AM) apresentam seis subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID.AM-1 – Dispositivos físicos e sistemas dentro da organização são inventariados.
- ID.AM-2 – Plataformas de software e aplicações dentro da organização são inventariados.
- ID.AM-3 – Comunicação organizacional e fluxos de dados são mapeados.
- ID.AM-4 – Sistemas de informação externos são catalogados.
- ID-AM-5 – Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios.
- ID-AM-6 – Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos.

Contexto Empresarial (ID.BE): tem como objetivo verificar se a missão, objetivos, *stakeholders* são compreendidos e priorizados pela organização. E se essas informações são utilizadas para informar funções, responsabilidades e de gerenciamento de riscos da segurança cibernética.

Dentro da categoria de Contexto Empresarial (ID.BE) apresentam cinco subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID-BE-1 – O papel da organização na cadeia de suprimentos é identificado e comunicado.
- ID-BE-2 – O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado.

- ID-BE-3 – Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas.
- ID.BE-4 – Dependências e funções críticas para a entrega de serviços críticos são estabelecidas.
- ID.BE-5 – Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos as condições operacionais (por exemplo, sob coerção/ ataque, durante a recuperação, operações normais).

Governança (ID.GV): está relacionado ao gerenciamento e monitoramento dos requisitos, como por exemplo, as regulamentações, leis, riscos, ambientais, operacionais. Esses requisitos devem ser compreendidos e informado ao gerenciamento do risco de segurança cibernética.

Dentro da categoria de Governança (ID.GV) apresentam quatro subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID.GV-1 – A política organizacional de segurança cibernética é estabelecida e comunicada.
- ID.GV-2 – As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos.
- ID.GV-3 – Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados.
- ID.GV-4 – Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética.

Avaliação de risco (ID.RA): está relacionada diretamente ao risco de segurança cibernética para as operações, é um processo de entendimento para a organização. Nessa categoria, aborda-se as vulnerabilidades dos ativos, informações sobre ameaças que ocorrem, identifica-se as ameaças internas e externas, os impactos, determinar o grau, quais as respostas e priorizações de risco.

Dentro da categoria de Governança (ID.GV) apresentam seis subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID.RA-1 – As vulnerabilidades dos ativos são identificadas e documentadas.

- ID.RA-2 – Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações.
- ID.RA-3 – Ameaças internas e externas são identificadas e documentadas.
- ID.RA-4 – Potenciais impactos no negócio e probabilidades são identificados na organização.
- ID.RA-5 – Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos.
- ID.RA-6 – As respostas ao risco são identificadas e priorizadas.

Estratégia de Gerenciamento de Riscos (ID.RM): após realizar as avaliações de risco, a categoria (ID.RM) faz o estabelecimento da priorização, restrição, tolerância e suposições do risco da organização e isso é utilizado para o apoio de decisões sobre os riscos operacionais.

Dentro da categoria de Governança (ID.RM) apresentam três subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID.RM-1 – Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos *stakeholders* organizacionais.
- ID.RM-2 – Tolerância ao risco organizacional é determinada e claramente expressa.
- ID.RM-3 – A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor.

Gerenciamento de Riscos da Cadeia de Suprimento (ID.SC): segundo Bezerra (2017), a cadeia de suprimentos envolve todo o processo logístico de um determinado produto ou serviço, desde o processo de fabricação até a entrega ao consumidor final; conecta e alinha as áreas de produção, armazenamento, transporte, reduzindo os custos. Com isso, o *framework*, a organização tem que identificar, avaliar e gerenciar os riscos encontrados na cadeia de suprimentos.

Dentro da categoria de Governança (ID.SC) apresentam cinco subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- ID.SC-1 – Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.

- ID.SC-2 – Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos.
- ID.SC-3 – Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos.
- ID.SC-4 – Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais.
- ID.SC-5 – O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados.

6.2 Função Proteger (PR)

Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC): abordam tópicos referentes ao acesso físico, acesso remoto, permissões de acesso e autorizações, proteção/integração de rede, identificação e autenticação de usuários, dispositivos, por exemplo.

Dentro da categoria de Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC) apresentam sete subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR.AC-1 – Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.
- PR.AC-2 – O acesso físico aos ativos é gerenciado e protegido.
- PR.AC-3 – O acesso remoto é gerenciado.
- PR.AC-4 – Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas.

- PR.AC-5 – A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).
- PR.AC-6 – As identidades são revisadas, vinculadas a credenciais e confirmadas em interações.
- PR.AC-7 – Usuários, dispositivos e outros recursos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).

Conscientização e Treinamento (PR.AT): essa categoria permite verificar se os funcionários, parceiros da organização estão treinados, conscientizados, sabem sobre suas obrigações e responsabilidades de questões relacionadas à segurança cibernética, diante de procedimentos e acordos estabelecidos.

Dentro da categoria de Conscientização e Treinamento (PR.AT) apresentam cinco subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR.AT-1 – Todos os utilizadores são informados a respeito e treinados.
- PR.AT-2 – Os usuários privilegiados compreendem suas funções e responsabilidades.
- PR.AT-3 – *Stakeholders* terceirizados (por exemplo, fornecedores, clientes, parceiros) entendem suas funções e responsabilidades.
- PR.AT-4 – Executivos seniores compreendem suas funções e responsabilidades.
- PR.AT-5 – Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades.

Segurança de Dados (PR.DS): nesta categoria, o *framework* traz uma abordagem envolvendo as informações e o registros, ou seja, dados, como estão sendo gerenciados, baseados na estratégia de risco e na tríade de segurança da informação.

Dentro da categoria de Segurança de Dados (PR.DS) apresentam oito subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR.DS-1 – Os dados em repouso são protegidos.
- PR.DS-2 – Os dados em trânsito são protegidos.
- PR.DS-3 – Ativos são formalmente gerenciados durante a remoção, transferências e disposição.

- PR.DS-4 – A capacidade adequada para garantir a disponibilidade é mantida.
- PR.DS-5 – As proteções contra vazamentos de dados são implementadas.
- PR.DS-6 – Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações.
- PR.DS-7 – O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção.
- PR.DS-8 – Mecanismos de verificação de integridade são usados para verificar a integridade do hardware.

Processos e Procedimentos de Proteção da Informação (PR.IP): tem como objetivo verificar se as políticas de segurança, processos e procedimentos são utilizados para proteger sistemas e ativos da informação.

Dentro da categoria de Processo e Procedimentos de Proteção da Informação (PR.IP) apresentam doze subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR.IP-1 – Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).
- PR.IP-2 – Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado.
- PR.IP-3 – Processos de controle de mudança de configuração estão em funcionamento.
- PR.IP-4 – Os Backups de informações são realizados, conservados e testados.
- PR.IP-5 – As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos.
- PR.IP-6 – Os dados são destruídos de acordo com a política.
- PR.IP-7 – Os processos de proteção são aperfeiçoados.
- PR.IP-8 – A eficácia das tecnologias de proteção é compartilhada.

- PR.IP-9 – Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados.
- PR.IP-10 – Planos de recuperação e resposta são testados.
- PR.IP-11 – A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal).
- PR.IP-12 – Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.

Manutenção (PR.MA) – permite identificar se a manutenção e os reparos de ativos organizacionais são realizados bem como de acordo com a política e procedimentos.

Dentro da categoria de Manutenção (PR.MA) apresentam duas subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR. MA-1 – Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas.
- PR.MA-2 – A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado.
- A última categoria dentro da função Proteger (PR) é chamada de Tecnologia Protetora (PR.PT), onde são abordados itens relacionados a auditorias, gerenciamento de mídias removíveis, segurança de redes de comunicação e controle, por exemplo.

Dentro da categoria de Tecnologia Protetora (PR.PT) apresentam cinco subcategorias. De acordo com o *U.S. Chamber of Commerce* (2018), são:

- PR.PT-1: Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política.
- PR.PT-2: As mídias removíveis são protegidas e seu uso é restrito de acordo com a política.
- PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais.
- PR.PT-4: Redes de comunicação e controle são protegidas.

- PR.PT-5: Alguns mecanismos (por exemplo, *fail-safe, load balancing, hot swap*) são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas.

7. ESTUDO DE CASO

Para o estudo de caso os autores elaboraram uma ferramenta baseada no *framework* NIST com a finalidade de avaliar a situação atual de uma organização com relação a segurança da informação e posteriormente indicar os itens necessários a serem melhorados.

Esta ferramenta aborda somente os dois itens necessários para atingir o objetivo do trabalho que são: identificar e proteger.

A ferramenta foi desenvolvida com o auxílio do software aplicativo Microsoft Office Excel. Na ferramenta existe a guia avaliação, onde será realizado a avaliação atual da empresa em relação à segurança da informação.

A guia avaliação possui as seguintes informações: função, categoria, identificador, subcategorias, nível atual, avaliação desejada, referência e objetivo.

Os objetivos de cada subcategoria apresentada, são baseados nas referências normativas que a ferramenta estabelece, nesse caso, a ISO/IEC 27001:2013 ou na ausência dessa norma, utiliza-se o COBIT 5.

Para realizar o diagnóstico da maturidade de cada subcategoria, foi utilizado o modelo de maturidade do *framework* COBIT 4.1, que apresenta níveis de maturidade de 0 a 5.

> O CobiT é um modelo e uma ferramenta de suporte que permite aos gerentes suprir as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. O CobiT habilita o desenvolvimento de políticas claras e boas práticas para controles de TI em toda a empresa (ITGI, 2007).

Quando se utiliza os modelos de maturidade do COBIT 4.1, a gerência pode identificar, onde a empresa está hoje, onde o mercado está, onde quer chegar e o caminho a ser realizado entre o “como está” e “como será”. A Tabela 3, mostra o modelo de maturidade do COBIT 4.1.

Tabela 3 - Modelo de Maturidade do COBIT 4.1

Modelo de Maturidade do COBIT 4.1	
0	Inexistente
1	Inicial / *Ad Hoc*
2	Repetível, porém intuitivo
3	Processo Definido
4	Gerenciado e Mensurável
5	Otimizado

Fonte: Elaborado pelos autores.

- Maturidade Nível 0 – Inexistente. A empresa não reconheceu que existe uma questão a ser trabalhada. Segundo ITGI (2007), “completa falta de um processo reconhecido”.
- Maturidade Nível 1 – Inicial / *Ad Hoc.* A empresa já sabe que existem problemas ou questões que precisam ser trabalhadas. Contudo, não existe um processo padronizado. Eles também podem ser denominados *Ad Hoc,* pois as questões são trabalhadas de forma individual ou caso-a-caso, o gerenciamento é desorganizado.
- Maturidade Nível 2 – Repetível, porém intuitivo. Para ITGI (2007), “os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa”. Não há treinamento formal, ou uma comunicação sobre os procedimentos padronizados, a responsabilidade é tratada de maneira individual. Existe alto grau e dependência dos conhecimentos dos indivíduos envolvidos e erros ocorrem frequentemente.
- Maturidade Nível 3 – Processo Definido. Os procedimentos são padronizados, documentados e comunicados por treinamentos. Os processos são obrigados a serem seguidos. É formalizado, porém não são sofisticados, os procedimentos e práticas.
- Maturidade Nível 4 – Gerenciado e Mensurável. A gerência realiza o monitoramento e mede a adesão dos procedimentos através de treinamentos e ações são tomadas onde os processos estão acontecendo de forma adequada. Os processos são sempre aprimorados e fornecem boas práticas.

A automação e as ferramentas são utilizadas de maneira limitada ou fragmentada.

- Maturidade Nível 5 – Otimizado. Os processos estão em um nível de boas práticas, levando em consideração os resultados de melhoria contínua e modelos de maturidade de outras empresas. Segundo ITGI (2007), “TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se”.

Em avaliação desejada, deverá ser preenchido, o nível em que a empresa pretende chegar, utilizando também como referência o modelo de maturidade do COBIT 4.1.

O item objetivo está abordando de forma sintetizada, o que diz as referências normativas da subcategoria, para que a empresa compreenda o que a subcategoria quer avaliar e assim apontar o nível atual de forma correta.

Além das normas já citadas, outra norma que poderá ser consultada para melhores orientações é a ISO/IEC 27002:2013.

Outro item existente na ferramenta é chamado de gráficos, onde para cada categoria existe um gráfico que apresenta todas as subcategorias correspondentes, o nível atual e avaliação desejada. Quanto mais longe do centro, melhor o nível de maturidade da subcategoria. O gráfico utilizado é o gráfico de radar.

O gráfico de radar realiza a comparação de valores agregados de várias séries de dados, ele é de fácil visualização comparativa e é parecido com uma teia de aranha com linhas, seus indicadores mostram que quanto maior o valor, mais distante do centro ele ficará.

E por último a guia r*oadmap*, onde através das avaliações das subcategorias e das comparações entre avaliação atual e avaliação desejada, devem-se definir quais ações serão tomadas para alcançar a avalição desejada, baseando-se no tempo de um a quatro semestres e quais ações serão tomadas no primeiro, segundo e terceiro ano para melhorar a maturidade dos processos, procedimentos e práticas.

> Na prática, um *roadmap* é uma espécie de linha do tempo visual [...] uma espécie de mapa, uma poderosa ferramenta visual e descritiva que apontará como será o produto ou projeto a cada período de sua evolução (ENDEAVOR, 2017).

7.1 Análise de Dados

Utilizando essa ferramenta como avaliação, o presente trabalho analisou duas subcategorias e seus respectivos gráficos para demonstrar as necessidades da empresa para atingir os objetivos de segurança da informação.

Na categoria identificar foi escolhido a subcategoria gerenciamento de ativos, que permite identificar e gerenciar dispositivos, instalações e sistemas, possibilitando assim que a organização atinja os objetivos de negócios e estabeleça toda a estrutura base para atingir a segurança da informação, conforme Tabela 4 e 5.

Tabela 4 - Gerenciamento de Ativos

Categoria	Identificador	Subcategorias	Nível Atual	Avaliação Desejada
Gerenciamento de Ativos	ID.AM-1	Dispositivos físicos e sistemas dentro da organização são inventariados	0	3
	ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	1	3
	ID.AM-3	Comunicação organizacional e fluxos de dados são mapeados	2	3
	ID.AM-4	Sistemas de informação externos são catalogados	1	3
	ID.AM-5	Recursos são priorizados com base em suas classificações, criticidade e valor para os negócios	1	3
	ID.AM-6	Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros são estabelecidos	1	3

Fonte: Elaborado pelos autores

Tabela 5 - Gerenciamento de Ativos - Continuação

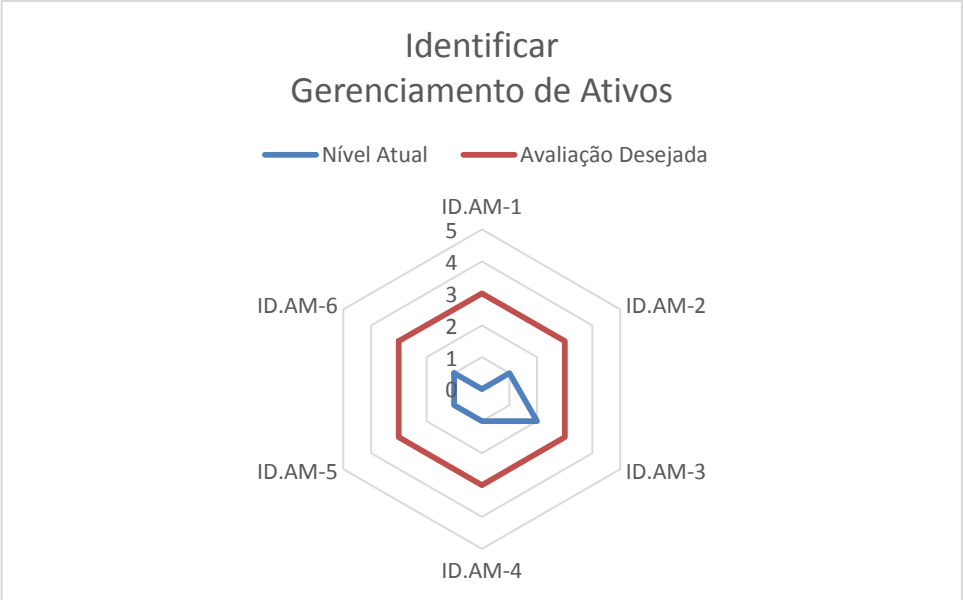
Identificador	Referência	Objetivo
ID.AM-1	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2	Os ativos que envolvem a informação e seu processamento devem ser identificados. Um inventário de ativos deve ser estruturado e mantido, além de possuir um proprietário.
ID.AM-2	ISO/IEC 27001:2013 A.8.1.1,	Os procedimentos que controlam a instalação de software em sistemas operacionais devem ser implantados.

Identificador	Referência	Objetivo
	A.8.1.2, A.12.5.1	
ID.AM-3	ISO/IEC 27001:2013 A.13.2.1, A.13.2.2	A organização deve estabelecer políticas, procedimentos e controles de transferência de informações por meio do uso de todos os tipos de recursos de comunicação e acordos para transferência segura de informações relacionadas ao negócio da organização e partes externas.
ID.AM-4	ISO/IEC 27001:2013 A.11.2.6	São tomadas medidas de segurança para ativos que operam fora do local, do ponto de vista que existem diferentes riscos de se trabalhar externamente da organização.
ID.AM-5	ISO/IEC 27001:2013 A.8.2.1	A informação é classificada pelo seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação, divulgação não-autorizada.
ID.AM-6	ISO/IEC 27001:2013 A.6.1.1	As responsabilidades pela segurança da informação devem ser definidas e atribuídas.

Fonte: Elaborado pelos autores.

O gráfico de radar do gerenciamento de ativos, aponta que esse item requer ações imediatas, pois o processo está em fase inicial, não existindo um processo padronizado e o gerenciamento é desorganizado, conforme mostra o Gráfico 6.

Gráfico 6 - Gráfico de radar de Gerenciamento de Ativos



Fonte: Elaborado pelos autores.

Na categoria proteger foi escolhido a subcategoria conscientização e treinamento, que tem como objetivo verificar se os funcionários e parceiros da organização estão cientes das obrigações, responsabilidades, políticas, procedimentos e acordos em relação à segurança da informação, conforme Tabela 6 e 7.

Tabela 6 - Conscientização e Treinamento

Categoria	Identificador	Subcategorias	Nível atual	Avaliação Desejada
Conscientização e Treinamento	PR.AT-1	Todos os utilizadores são informados a respeito e treinados	3	3
	PR.AT-2	Os usuários privilegiados compreendem suas funções e responsabilidades	2	3
	PR.AT-3	*Stakeholders* terceirizados entendem suas funções e responsabilidades	2	3
	PR.AT-4	Executivos seniores compreendem suas funções e responsabilidades	1	3
	PR.AT-5	Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades	1	3

Fonte: Elaborado pelos autores.

Tabela 7 - Conscientização e Treinamento - Continuação

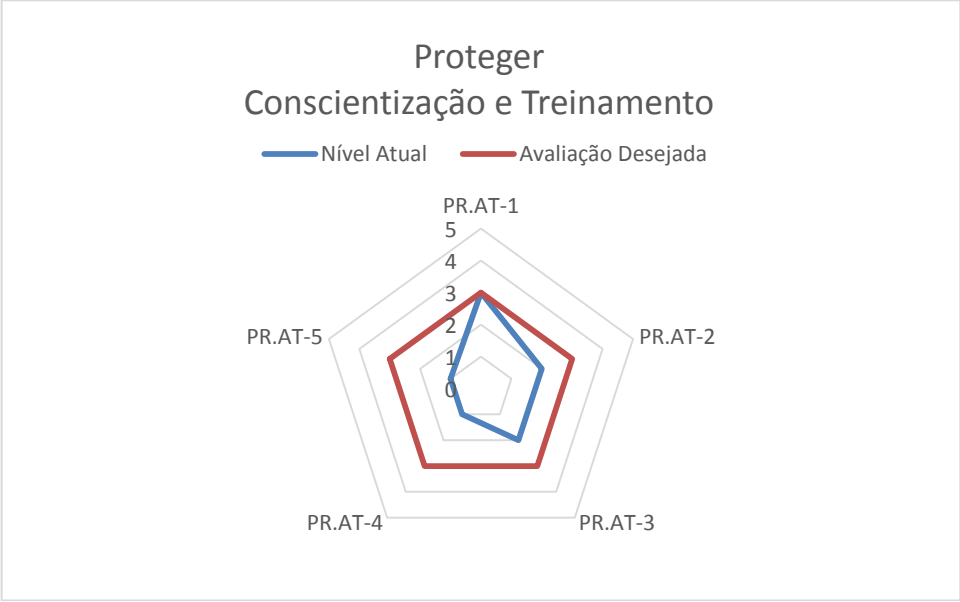
Identificador	Referência	Objetivo
PR.AT-1	ISO/IEC 27001:2013 A.7.2.2, A.12.2.1	Os funcionários e partes externas da organização devem receber treinamentos, educação e conscientização em SI de forma adequada, as atualizações das políticas e procedimentos devem acontecer de forma regular. Devem ser implementados controles de detecção, prevenção e recuperação para proteção contra *malwares* e programa de conscientização para o usuário.
PR.AT-2	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2	As responsabilidades pela segurança da informação devem ser definidas e atribuídas. Os funcionários e partes externas da organização devem receber treinamentos, educação e conscientização em SI de forma adequada, as atualizações das políticas e procedimentos devem acontecer de forma regular.

Identificador	Referência	Objetivo
PR.AT-3	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2	As responsabilidades pela segurança da informação devem ser definidas e atribuídas. A direção deve exigir aos funcionários e partes externas que pratiquem a SI de acordo com as políticas e procedimentos da organização. Os funcionários e partes externas da organização devem receber treinamentos, educação e conscientização em SI de forma adequada, as atualizações das políticas e procedimentos devem acontecer de forma regular.
PR.AT-4	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2	As responsabilidades pela segurança da informação devem ser definidas e atribuídas. Os funcionários e partes externas da organização devem receber treinamentos, educação e conscientização em SI de forma adequada, as atualizações das políticas e procedimentos devem acontecer de forma regular.
PR.AT-5	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2	

Fonte: Elaborado pelos autores.

O gráfico de radar da subcategoria Conscientização e Treinamento está mais próximo da avalição desejada pela empresa, com isso, as ações tendem a ser realizadas com mais facilidade, possibilitando assim alcançar seus objetivos mais rapidamente, conforme mostra o Gráfico 7.

Gráfico 7 - Gráfico de radar de Conscientização e Treinamento



Fonte: Elaborado pelos autores.

Após a avaliação, notou-se que a empresa tem diversos aspectos a serem melhorados, visto que quando mais perto do centro, maior será o nível de adequações a serem realizados. Para isso, a empresa deverá procurar adequar seus processos, procedimentos e políticas de acordo com a funções que o próprio *framework* NIST, ISO/IEC 27001:2013 e COBIT propõem e que estejam condizentes com a avaliação desejada.

É importante salientar que o *roadmap* ajudará também a empresa a organizar de forma visual, as atividades a serem desenvolvidas ao longo de quatro semestres, atuando como um cronograma, conforme Tabela 8 e 9.

Tabela 8 - *Roadmap* de Gerenciamento de Ativos

Gerenciamento de Ativos	Semestre 1	Semestre 2	Semestre 3	Semestre 4
Dispositivos físicos e sistemas dentro da organização são inventariados				
Plataformas de software e aplicações dentro da organização são inventariados				
Comunicação organizacional e fluxos de dados são mapeados				
Sistemas de informação externos são catalogados				
Recursos são priorizados com base em suas classificações, criticidade e valor para os negócios				
Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros são estabelecidos				

Fonte: Elaborado pelos autores.

Tabela 9 - *Roadmap* de Conscientização e Treinamento

Conscientização e Treinamento	Semestre 1	Semestre 2	Semestre 3	Semestre 4
Todos os utilizadores são informados a respeito e treinados				
Os usuários privilegiados compreendem suas funções e responsabilidades				
Stakeholders terceirizados entendem suas funções e responsabilidades				
Executivos seniores compreendem suas funções e responsabilidades				
Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades				

Fonte: Elaborado pelos autores.

8. CONSIDERAÇÕES FINAIS

Este trabalho possibilitou entender o nível de segurança adequado para uma indústria 4.0, quais áreas e processos iniciais essenciais para que seja necessário adequar para ter um ambiente seguro, a diferença entre as revoluções industriais, passando pela mecanização, linhas de montagem, uso dos computadores, Internet e até o uso da inteligência artificial, IoT e sistemas cibernéticos como forma de aprimorar os métodos de funcionamento das organizações.

A partir da apresentação e análise dos dados, observa-se que as tecnologias possibilitaram as organizações mudarem os seus processos, como por exemplo, o uso da IoT. Com todos os processos conectados e automatizados, graças a Indústria 4.0, aumentou-se os riscos de incidentes de segurança da informação e existe a necessidade da melhora da segurança dos ativos. Porém a segurança precisa ser especializada para essas novas tecnologias.

Outra questão importante diz respeito as fontes bibliográficas utilizadas como referência para criação da ferramenta de avaliação da segurança da informação de uma organização, foi utilizado o guia de aperfeiçoamento da segurança cibernética para infraestrutura crítica do NIST e paralelamente também foi pesquisado em outras normas e guia de boas práticas como ISO/IEC 27001:2013 e COBIT. Apesar de existir inúmeras fontes bibliográficas para o assunto, muitos se repetem, então foram analisados itens de todas as fontes citadas acima, sempre utilizando os mais atuais.

Para que o trabalho não se limitasse a teoria e dada à importância do assunto no desenvolvimento de formas de agilizar a análise em segurança, foi elaborado a ferramenta para auxiliar o processo de avaliação de segurança da informação. Apesar de o guia do NIST possuir cinco funções, nesta ferramenta foram utilizadas duas funções, identificar e proteger.

Em relação a trabalhos futuros, esse trabalho fornece opções para continuidade do desenvolvimento da ferramenta, aumentando para as cinco funções do guia do NIST e aplicando em mais de uma organização, para se fazer uma análise comparativa para melhorias e revisões posteriores. Também podendo ser

compactado, com revisão de alguns itens, deixando somente os necessários para alguma organização específica.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Eduardo**. O papel da segurança da indústria 4.0.** Disponível em: <https://cio.com.br/o-papel-da-seguranca-na-industria-40/>. Acesso em: 10 nov. 2019.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:** Técnicas de segurança. Sistemas de gestão de segurança da Informação. Requisitos. Rio de Janeiro, 2013.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:** Gestão de Riscos - Princípios e diretrizes. Rio de Janeiro. 2009.

BATISTA, Emerson de Oliveira. **Sistemas de informação:** o uso consciente da tecnologia para o gerenciamento. 2a edição. São Paulo. Saraiva. 2012.

BEZERRA, Filipe. **Cadeia de Suprimentos**: do conceito à gestão. Disponível em: <https://www.portal-administracao.com/2017/05/cadeia-de-suprimentos-conceito-gestao.html> Acesso em 10 nov. 2019.

CNI - CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Desafios para indústria 4.0 no Brasil**. Brasília: CNI, 2016.

ENDEAVOR. **Roadmap:** a bússola para desenvolver seu produto ou projeto. Disponível em: <https://endeavor.org.br/estrategia-e-gestao/roadmap/>. Acesso em 24 nov. 2019.

ERNEST YOUNG. **20ª pesquisa global sobre segurança da informação 2017-2018**. Retomada da segurança cibernética: como se preparar para enfrentar os ataques cibernéticos. Disponível em: <https://www.ey.com/Publication/ vwLUAssets/EY-GISS-2017/%24File/GISS-2017-Port.pdf>. Acesso em 10 nov. 2019.

EUROPEAN PARLIAMENT. **Industry 4.0 digitalisation for productivity and growth**. Disponível em: <http://www.europarl.europa.eu/RegData/etudes/BRIE /2015/568337/EPRS_BRI(2015)568337_EN.pdf>. Acesso em: 10 nov. 2019.

FIESP - FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO. **FIESP identifica desafios da indústria 4.0 no Brasil e apresenta propostas.** Disponível em: <http://www.fiesp.com.br/sicab/noticias/fiesp-identifica-desafios-da-industria-4-0-no-brasil-e-apresenta-propostas/>. Acesso 10 nov. 2019.

FIRJAN - FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DO RIO DE JANEIRO. **Programa de inovação:** indústria 4.0. Rio de Janeiro: FIRJAN, 2016. Disponível em <https://www.firjan.com.br/lumis/portal/file/fileDownload.jsp?fileId=2C908A8A555B47FF01557D8802C639A4>. Acesso em 10 nov. 2019.

FERREIRA, A. A.; REIS, A. C. F.; PEREIRA, M.I. **Gestão empresarial:** de Taylor aos nossos dias: evolução e tendências da moderna administração de empresas**.** São Paulo. Cengage Learning, 2011.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva. 2006.

GOMES, Karina. **Indústria 4.0 projeta as fábricas inteligentes do futuro**. 2015. Disponível em: <https://www.dw.com/pt-br/ind%C3%BAstria-40-projeta-as-f%C3%A1bricas-inteligentes-do-futuro/a-18250199> Acesso em: 10 nov. 2019.

HERMANN, M; PENTEK, T; OTTO, B. **Design principles for industrie 4.0 scenarios:** a literature review**.** Disponível em: <http://www.snom.mb.tu-dortmund.de/cms/de/forschung/Arbeitsberichte/Design-Principles-for-Industrie-4_0-Scenarios.pdf>. Acesso em: 10 nov. 2019.

ITGI - Information Technology Governance Information. **COBIT 4.1**. Rolling Meadows, USA, 2007.

ISACA. **COBIT 5** - Enabling Processes. Rolling Meadows, USA, 2012

LEAN. **Sistema Toyota de produção** (Toyota Production System - TPS). Disponível em: <https://www.lean.org.br/conceitos/117/sistema-toyota-de-producao-(toyota-production-system---tps).aspx> Acesso em: 10 nov. 2019.

LUCAS, Thiago José. **Princípios da Segurança da Informação**. Disponível em <https://thiagolucas.wordpress.com/2010/11/18/principios-da-seguranca-da-informacao/> Acesso em 10 nov. 2019.

MACEDO, Fausto. **Ataques cibernéticos:** maior risco no mundo corporativo atual. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/ataques-ciberneticos-maior-risco-no-mundo-corporativo-atual/>. Acesso em 10 nov. 2019.

ROLLI, Claudia. **Indústria 4.0 pode gerar economia de R$ 73 bilhões ao ano**. 2019. Disponível em: <https://www1.folha.uol.com.br/seminariosfolha/2019/02 /industria-40-pode-gerar-economia-de-r-73-bilhoes-ao-ano.shtml>. Acesso em 19 jun. 2019.

SACOMANO, J. B. et al. **Indústria 4.0 -** conceitos e fundamentos**.** São Paulo: Blucher. 2018.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro. 2016.

SÊMOLA. Marcos. **Gestão da Segurança da Informação** - uma visão executiva. 2a edição. Rio de Janeiro: Elsevier, 2014.

SHIMAO, Victor. **Versatilidade da engenharia:** expansão de mercado. Disponível em <https://betaeq.com.br/index.php/2019/06/13/versatilidade-da-engenharia-expansao-de-mercado-2/>. Acesso em 10 nov.

STEVAN JUNIOR, S. L.; LEME, M. O; SANTOS M. M**. Indústria 4.0 -** Fundamentos, perspectivas e aplicações. São Paulo. Érica. 2018.

TOTVS. **Entenda o que é a Industria 4.0 e quais são seus impactos**. Disponível em < https://www.totvs.com/blog/entenda-o-que-e-a-industria-4.0-e-quais-sao-seus-impactos/>. Acesso em 24 nov. 2019.

U.S. CHAMBER OF COMMERCE. **Guia de aperfeiçoamento da Segurança cibernética para infraestrutura crítica**. Tradução com permissão do NIST. 2018. Disponível em <https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf>. Acesso em 24 out. 2019.

WENTZEL, Marina. **De desastres naturais a terrorismo:** os 5 grandes riscos globais em 2017, segundo Fórum Econômico Mundial. Disponível em: <https://www.terra.com.br/economia/de-desastres-naturais-a-terrorismo-os-5-grandes-riscos-globais-em-2017-segundo-o-forum-economico-mundial,78c744fb111d52987d71bddaa764cc13rtgh9ah4.html>. Acesso em 10 nov. 2019.