UNIVERSIDADE NOVE DE JULHO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

FÁBIO MARTINS DIAS

ELABORAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA TEÓRICO-PRÁTICA PARA A GESTÃO DE RISCOS DE CIBERSEGURANÇA PARA O SETOR DE SAÚDE

SÃO PAULO, 2021

UNIVERSIDADE NOVE DE JULHO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

FÁBIO MARTINS DIAS

ELABORAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA TEÓRICO-PRÁTICA PARA A GESTÃO DE RISCOS DE CIBERSEGURANÇA PARA O SETOR DE SAÚDE

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Nove de Julho -UNINOVE-, como requisito parcial para a obtenção do grau de Mestre em Engenharia de Produção.

Orientador: Prof. Dr. Wagner Cezar Lucato

SÃO PAULO, 2021

Dias, Fábio Martins.

Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saúde. / Fábio Martins Dias. 2021.

132 f.

Dissertação (Mestrado) – Universidade Nove de Julho - UNINOVE, São Paulo, 2021.

Orientador (a): Prof. Dr. Wagner Cezar Lucato.

1. Cibersegurança. 2. Sistemas cyber-físicos. 3. Gestão de riscos. 4. Indústria 4.0. 5. Gestão de saúde.
I. Lucato, Wagner Cezar. II. Título

CDU 658.5

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO

DE

Fabio Martins Dias

Título da Dissertação: Elaboração e Avaliação de uma Estrutura Teórico-Prática para a Gestão de Riscos de Cibersegurança para o Setor de Saúde.

A Comissão examinadora, composta pelos professores abaixo, considera o(a) candidato(a) Fabio Martins Dias **APROVADO**.

São Paulo, 15 de abril de 2021.

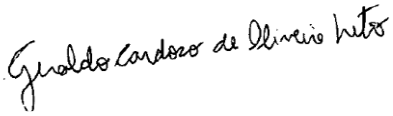
Prof(a). Dr(a).Wagner Cezar Lucato (UNINOVE / PPGEP) – Orientador

_____

Prof(a). Dr(a).Ivanir Costa (UNINOVE / PPGI) – Membro Externo

_____

Prof(a). Dr(a).Geraldo Cardoso de Oliveira Neto (UNINOVE / PPGEP) – Membro Interno



_____

“Seja a mudança que você quer ver no mundo”
(Dalai Lama)

AGRADECIMENTOS

Primeiramente agradeço a minha família por estarem presentes em todos os momentos de minha vida. Em especial a minha mãe Neide e a minha esposa Adriana, minhas duas heroínas que sempre me disponibilizaram apoio e incentivo na jornada dessa vida.

Agradeço ao meus dois orientadores durante o curso, os professores Dr. Wagner Cezar Lucato e Dr. Mauro Luiz Martens, que possibilitaram para a conclusão desta obra, sempre disponibilizando conhecimento, tempo e direção para o progresso desta dissertação.

Agradeço ao programa de Pós-Graduação em Engenharia de Produção da Universidade Nove de Julho – UNINOVE – que possibilitou a concretização dessa pesquisa. A todos os docentes do programa que diretamente/indiretamente contribuíram para a realização desse trabalho. Um especial agradecimento aos professores Dr. Geraldo Cardoso de Oliveira Neto e Dra. Rosângela Maria Vanalle que sempre compartilharam seus conhecimentos para o desenvolvimento desse trabalho.

A todos vocês minha admiração e gratidão!!!!!

RESUMO

A cibersegurança é uma tarefa hercúlea para qualquer setor. Entretanto, o setor de saúde é um dos setores mais vulneráveis encontrados na literatura científica, com dados preocupantes sobre os desafios a serem superados pela cibersegurança no setor, que é um alvo atraente e vulnerável, pois é uma fonte rica de informações valiosas. Segundo a literatura, uma solução eficiente para combater as ameaças cibernéticas é a elaboração de um plano de gerenciamento de riscos. Deste modo, está dissertação tem como objetivo, propor uma ferramenta de gestão de riscos com foco em cibersegurança no setor de saúde. Nesse sentido, desenvolve uma estrutura teórico-prática de gestão de riscos cibernéticos inspirado na ferramenta de gestão PDCA, evidenciando itens mínimos de segurança para dispositivos médicos e melhores práticas que devem ser empregadas. Para verificar a aderência da estrutura desenvolvida a situações do mundo real, utilizou-se como metodologia da pesquisa o estudo de casos múltiplos, que investigou este fenômeno internacional dentro do contexto de grandes instituições de saúde do Brasil. Como resultado, observou-se uma mesma postura encontrada em pesquisas internacionais de que, as estratégias para tratar os riscos cibernéticos concentram-se apenas na remediação, já que as instituições acreditam estarem seguras contra a cibercrimes apenas com o uso de antivírus e *firewalls*. As conclusões apontam que uma cibersegurança inadequada resulta não somente no comprometimento de informações, mas também no comprometimento de dispositivos vitais à vida, em que a paralisação traz grandes danos a sociedade, além de grande perda financeira das instituições de saúde. Conclui-se, portanto, que este trabalho contribui à teoria, na medida em que adiciona à literatura uma estrutura robusta para gerenciar os riscos cibernéticos nas instituições de saúde no Brasil, já que não há estudo semelhante é contemplado na bibliografia que trata do tema. Igualmente, gera contribuições à prática, por meio de uma melhor visão para a proteção das instituições de saúde, proporcionando uma ferramenta moderna, completa e ágil para protegê-las.

Palavras-Chave: Cibersegurança, Sistemas *cyber*-físicos, Indústria 4.0, Gestão de riscos, Gestão de saúde.

ABSTRACT

Cybersecurity is a Herculean task for any industry. However, the health sector is one of the most vulnerable sectors found in the academic literature, with worrying data on the challenges to be overcome by cybersecurity in the sector, which is an attractive and vulnerable target, as it is a rich source of valuable information. Thus, according to the literature, an efficient solution to combat cyber threats is the development of a risk management plan. Thus, this dissertation aims to propose a risk management tool with a focus on cybersecurity in the health sector. In this sense, it develops a theoretical-practical structure for cyber risk management inspired by the PDCA management tool, showing minimum safety items for medical devices and best practices that should be employed. In order to verify the adherence of the developed structure to real-world situations, the study methodology used was the study of multiple cases, which investigated this international phenomenon within the context of large health institutions in Brazil. As a result, the same stance found in international research was observed that, the strategies to deal with cyber risks focus only on remediation, since the institutions believe they are safe against cybercrimes only with the use of antivirus and firewalls. Thus, the conclusions point out that an inadequate cybersecurity results not only in the compromise of information, but also in the compromise of vital devices to life, in which the paralysis brings great damage to society, in addition to a great financial loss of health institutions. It is concluded, therefore, that this work contributes to the theory, insofar as it adds to the literature a robust structure to manage cyber risks in health institutions in Brazil, since there is no similar study contemplated in the bibliography that deals with the theme. Equally, it generates contributions to the practice, through a better vision for the protection of health institutions, providing a modern, complete and agile tool to protect them.

Keywords: Cybersecurity, Systems physical cyber, Industry 4.0, Risk management, Healthcare management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AI	Artificial intelligence
EARS	Eight aggregate response strategies
EMR	Electronic Medical Records
EUA	United States of America
FDA	Food and Drug administration
FEP	Front-end planning
FTA	Fault tree analysis
HIPAA	Health insurance portability and accountability act
IDS	Integrated Delivery Systems
IoMT	Internet of Medical Things
IoT	Internet of Things
ISO	International Organization for Standardization
KPI	Key Performance Indicator
M2M	Machine to machine
MCPS	Medical Cyber-Physical Systems
NIST	National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act
PMI	Project Management Institute
RAS	Risk analytical structure
SGSI	Information Security Management System
TI	Technical Information
TQM	Total Quality Management
VPN	Virtual Private Network

SUMÁRIO

1. INTRODUÇÃO

Cibersegurança é um conceito abrangente, que envolve entre outras coisas: melhores práticas, políticas, salvaguardas, treinamentos, diretrizes, gerenciamento de riscos, gerenciamento de crises, e tecnologias que podem ser usadas para proteger o usuário final, o ambiente cibernético e os ativos de uma organização (ALEXANDER *et al*., 2019).

Conforme Ondiege *et al.* (2017), cibersegurança é definida pela *Food and Drug administration* (FDA), como: um conjunto de práticas para impedir o acesso não autorizado, modificação, uso indevido ou negação de uso ou uso não autorizado de informações armazenadas, acessadas ou transferidas de um dispositivo médico para um destinatário não autorizado.

A análise da cibersegurança no setor de saúde é uma tarefa extremamente árdua, que requer muito empenho, recursos e foco. Sendo que o setor de saúde é um dos setores mais vulneráveis a cibercrimes (KRUSE *et al*., 2017).

Acredita-se que 90% das organizações do setor já foram vítimas de violações de cibersegurança nos últimos anos, apresentando vários fatores que contribuíram para o setor passar a ser um dos principais alvos de ataques (KRUSE *et al*., 2017). Os mesmos autores concordam que, a cibersegurança é negligenciada no setor, sendo que muitas organizações ainda estão usando sistemas operacionais, como o *Windows XP*, que não possui atualizações ou suportes desde 2014, facilitando que *hackers* ou *malwares* explorem essa vulnerabilidade.

Para os cibercriminosos, o setor de saúde é um alvo atraente e vulnerável por dois motivos: é uma fonte rica de informações valiosas e é um alvo extremante vulnerável (MARTIN *et al*., 2017).

Conforme Blanke *et al*. (2016), as informações geradas pelo setor, são ricas em conteúdo, citando como exemplo, a instituição *Ponemon*, em seu relatório anual de violação de dados de 2015, *FireEye*, e o *Experian Security Report* alertam que, as empresas do setor são vulneráveis a cibercriminosos. As informações pessoais extraídas do setor estão à venda no mercado negro em larga escala.

Portanto, uma cibersegurança inadequada pode resultar não apenas no comprometimento dos dados, mas também no comprometimento de dispositivos vitais à vida. É essencial que o setor não considere que a responsabilidade da segurança

cibernética seja apenas dos fabricantes de dispositivos médicos, mas sim de todos, inclusive do usuário final (NATSIAVAS *et al*., 2018).

Portanto, é necessário avançar em estudos para aumentar a conscientização sobre a cibersegurança, pela mudança de suas concepções, e construir uma cultura nas organizações orientadas à cibersegurança (NATSIAVAS *et al*., 2018). Sendo o setor de saúde um alvo muito atraente e vulnerável, com base em seu tamanho econômico, riqueza de informações e facilidade de pontos de acessos aos sistemas das instituições (BLANKE *et al*., 2016; MARTIN *et al*., 2017).

Anteriormente acreditava-se que o setor estava imune a ataques cibernéticos e consequentemente medidas protetivas não foram consideradas ao longo dos anos, sendo que o setor enfatizou nas últimas décadas seus esforços em cuidados médicos, sucateando seus dispositivos de proteção a ataques cibernéticos (CORONADO *et al*., 2014).

Conforme Taylana *et al.* (2014), Poursoltan *et al*. (2020) e Cagliano *et al*. (2017), proteger-se contra cibercrimes, é um desafio a qualquer organização no século XXI, embora não haja uma solução infalível para este problema, um plano de gestão de riscos adequado é uma das soluções mais adequada para combater a crescente ação de cibercriminosos.

A gestão de riscos inclui conhecer a organização, planejar o melhor uso dos recursos disponíveis, monitorar a organização ativamente, prevenir a organização contra potenciais riscos e tratar os riscos que se concretizaram (MEKHILEF; CARDINAL, 2005). Sendo que, a gestão de riscos cibernéticos é uma soma de ações, atividades, processos e condutas para evitar, prevenir e coordenar potenciais ameaças internas e externas, que as organizações estão expostas no seu funcionamento (HUTCHINS *et al*., 2015).

Deste modo, com uma boa gestão de riscos as organizações estão aptas a tomar soluções mais acertivas no combate a incertezas e ameaças que podem afetar negativamente os objetivos e metas das organizações (TAYLANA *et al*., 2014).

Neste sentido, está dissertação constatou, por meio de ampla análise da literatura, que a comunidade científica concorda que a cibersegurança no setor de saúde é negligenciada e que não há estudos relevantes referentes à cibersegurança nas instituições de saúde do Brasil. Os artigos encontrados na pesquisa bibliográfica são referentes a estudos desenvolvidos nos Estados Unidos, Europa e Ásia. Essa

ausência de estudos sobre esse tema no Brasil é a lacuna de pesquisa que suporta está presente dissertação.

1.1 PROBLEMA DE PESQUISA

Para preencher a lacuna identificada, esta pesquisa propôs desenvolver uma estrutura teórico-prática de gestão de riscos com foco em sistemas de segurança de dados no setor de saúde por meio da resposta à seguinte questão de pesquisa:

> Como uma estrutura teórico-prática para a gestão de riscos de cibersegurança pode minimizar os riscos cibernéticos em instituições de saúde do Brasil?

1.2 OBJETIVOS

Para poder responder à essa questão de pesquisa, o seguintes objetivo geral e seus quatro objetivos específicos foram estabelecidos:

1.2.1 Objetivo Geral

O presente estudo tem como objetivo geral desenvolver e avaliar uma estrutura teórico-prática para a gestão de riscos de cibersegurança para instituições de saúde do Brasil.

1.2.2 Objetivos Específicos

Como objetivos específicos:

a) Estudo da gestão de riscos e a segurança de dados no setor de saúde, com base na literatura científica que trata do tema;

b) Propor uma estrutura teórico-prática para a gestão de riscos de cibersegurança com foco em sistemas de segurança de dados para o setor de saúde, com base no levantamento realizado na literatura;

c) Avaliar essa estrutura às condições brasileiras por meio de estudos de casos a serem desenvolvidos em instituições de saúde do Brasil.;

d) Incorporar na estrutura teórico-prática inicialmente desenvolvida o aprendizado decorrente da avaliação feita no campo.

Na sequência será apresentada a justificativa para o estudo do tema proposto por esta dissertação.

1.3 JUSTIFICATIVA PARA ESTUDO DO TEMA

Em nenhum outro momento do passado houve tanta informação gerada e processada digitalmente como atualmente, decorrente de uma espiral de disseminação de informação (GUO, 2010). Com a popularização da *internet*, a humanidade passa a obter informações de uma maneira instantânea, com isso deixa rastros de todas as transações praticadas na rede, também do que se pratica fora dela (MELNIKOV; SEMENYUK 2014)

Segundo Blanke *et al*. (2016), o setor de saúde é um alvo a ciberataques devido ao seu tamanho econômico e brechas existentes nos sistemas das instituições de saúde, que não investem em cibersegurança, e como consequência, a privacidade de pacientes e segurança de dados dos sistemas aumentaram 100% desde 2010.

Busdicker e Upendra (2017) alegam que, em 2017, foram pesquisados 500 profissionais de cibersegurança no setor de saúde, em que se constatou que, apenas 15% das organizações de saúde e 17% dos fabricantes de dispositivos médicos, tomavam medidas relevantes para evitar ataques cibernéticos. Os autores ainda alegam que, somente 22% das organizações de saúde e 41% dos fabricantes de dispositivos, têm um plano de gerenciamento de riscos em cibersegurança para lidar com o problema.

Para Kessler *et al*. (2019) de 2009 até 2018, as violações no setor já relataram mais de 2.100 violações de dados somente nos Estados Unidos. O mesmo estudo destaca que essas violações expuseram dados de mais de 176 milhões de pacientes, com um aumento exponencial ano após ano. Ainda segundo o mesmo estudo, 70% das violações de dados são causadas diretamente ou indiretamente por descuido de colaboradores das próprias instituições.

A maioria das violações está relacionada à negligência e/ou descuido dos funcionários, características que não podem ser totalmente reparadas com tecnologia ou legislação, mas sim apenas com treinamentos e políticas internas das organizações (BRODY; CHANG; SCHOENBERG 2018).

Neste sentido, o levantamento da literatura realizado para dar suporte a esta pesquisa, possibilitou a identificação de cinco constatações relevantemente citadas na Tabela 1.

Tabela 1 – Constatações observadas na literatura analisada para dar suporte a este trabalho.

Autores	Cibersegurança no setor de saúde é um tópico importante	Cibersegurança no setor de saúde é negligenciada	Não há investimentos significativos em cibersegurança no setor de saúde	As informações geradas pelo setor de saúde são ricas em conteúdo	Há falta de ações na proteção dos dados no setor de saúde
Abdelhamid *et al*. (2018)				X	
Abraham *et al*. (2019)	X	X	X	X	X
Ahmed *et al*. (2019)		X		X	
Alexander *et al*. (2019)	X	X	X	X	X
Al-Muhtadi *et al*. (2019)	X			X	X
Askar *et al*. (2019)	X	X			
Berger *et al*. (2019)	X	X	X	X	X
Bilek *et al*. (2017)	X	X			X
Bissonnette *et al*. (2017)	X	X	X		
Blanke *et al*. (2016)	X	X	X	X	X
Bojanova *et al*. (2017)			X		X
Braga *et al*. (2019)				X	
Brody *et al*. (2018)	X				
Busdicker *et al*. (2017)	X	X			X
Cleland-Huang *et al*. (2014)		X		X	
Coronado *et al*. (2014)	X	X	X	X	X
Coveney *et al*. (2016)	X				
Coventry *et al*. (2018)	X	X	X	X	
Dandage *et al*. (2018)				X	
Diggans *et al*. (2019)					X
Elizabeth *et al*. (2019)		X			X
Frontoni *et al*. (2019)			X	X	X
Ghafir *et al*. (2018)	X	X	X	X	X
Goncharov *et al*. (2019)	X				X
Gordon *et al*. (2019)	X	X	X	X	X
Grimes *et al*. (2017)		X		X	X
Habibzadeh *et al*., (2019)			X	X	
Handler *et al*. (2018)					X
Jalali *et al*. (2019)	X		X	X	
Kessler *et al*. (2019)		X			

Kharraz *et al*. (2018)	*X*	*X*	*X*	*X*	*X*
King *et al*. (2018)					*X*
Koppel *et al*. (2019)	*X*			*X*	
Kruse *et al*. (2017)	*X*	*X*	*X*	*X*	*X*
Kure *et al*. (2018)	*X*	*X*	*X*	*X*	*X*
Lebeda *et al*. (2018)			*X*	*X*	
Lechler *et al*. (2017)				*X*	*X*
Leung *et al*. (2019)		*X*	*X*		
Loi *et al*. (2019)				*X*	
Maimó *et al*. (2019)	*X*	*X*	*X*	*X*	*X*
Martin *et al*. (2017)	*X*	*X*	*X*	*X*	*X*
Natsiavas *et al*. (2018)	*X*	*X*	*X*	*X*	*X*
Ondiege *et al*. (2017)	*X*	*X*	*X*	*X*	*X*
Pesapane *et al*. (2018)	*X*		*X*	*X*	*X*
Priestman *et al*., (2019)	*X*		*X*		
Primo *et al*. (2019)	*X*	*X*			
Shneiderman *et al*. (2015)				*X*	
Stern *et al*. (2019)	*X*				*X*
Swede *et al*. (2019)	*X*	*X*			
Thaw *et al*. (2014)			*X*	*X*	
Ward *et al*. (2008)	*X*			*X*	
Wethington *et al*. (2018)				*X*	
Wiltz *et al*. (2014)			*X*	*X*	
Zhang *et al*. (2017)				*X*	
Total de Citações	***30***	***27***	***26***	***36***	***28***

Fonte: Autor.

Como pode se observar na Tabela 1 que, dos 54 artigos considerados neste trabalho, 67% atestaram que as informações geradas pelo setor de saúde são ricas em conteúdo ao mesmo tempo em que, 56% das publicações afirmaram que a cibersegurança no setor de saúde é um tópico importante. No entanto, 50% dos artigos que tratam do tema central desta pesquisa consideraram que há falta de ações na proteção dos dados no setor de saúde, setor este no qual a cibersegurança é negligenciada e no qual não há investimentos significativos para a proteção de seus dados. Ademais, se observou também que todos os artigos analisados expõem apenas dados, questões, visões e a realidade de países europeus, norte-americano e asiático, e que não são apresentadas essas informações no Brasil.

Este estudo torna-se relevante pois contribui tanto para a teoria como para a prática no setor de saúde do Brasil, na medida em que apresenta uma abordagem

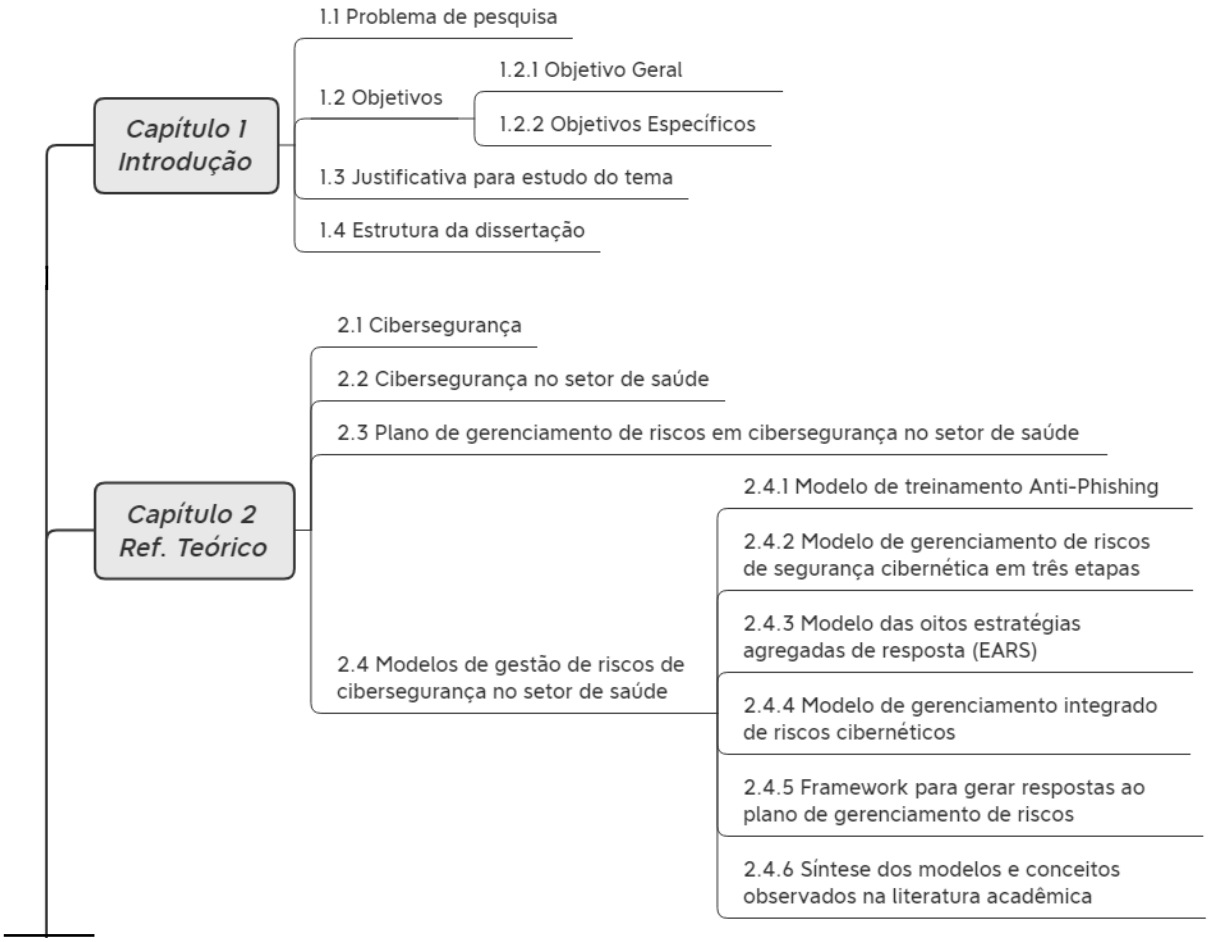
inovadora para a gestão dos riscos de cibersegurança no setor de saúde nacional, adicionando conhecimentos até então não existentes na literatura que trata do tema e fornecendo aos gestores de cibersegurança das instituições nacionais uma estrutura teórico-prática para aplicação no seu dia a dia visando aumentar o grau de segurança e proteção de seus dados e informações digitais.

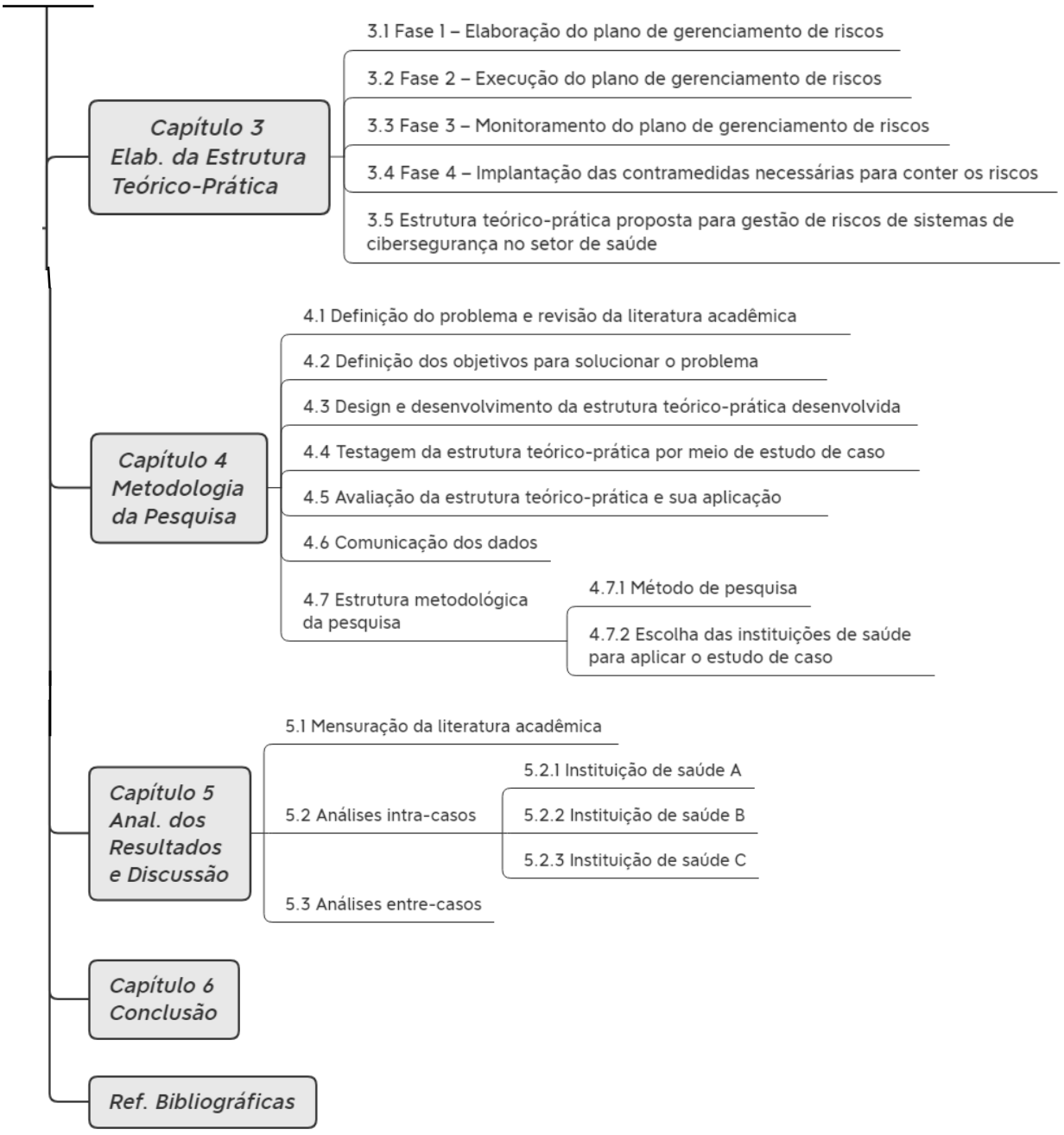
Na sequência é apresentada a estruturação desta dissertação.

1.4 ESTRUTURA DA DISSERTAÇÃO

Para atingir os objetivos propostos acima, está dissertação é estruturada em seis capítulos. A Figura 1, apresenta uma síntese gráfica da estruturação deste trabalho.

Figura 1 – Sintase da estruturação desta dissertação.





Fonte: Autor.

Na sequência será apresentada a fundamentação teórica que dá suporte a esta dissertação.

2. REFERENCIAL TEÓRICO

Neste capítulo, são apontadas as fundamentações e conceitos teóricos referentes ao tema cibersegurança e gestão de riscos com foco ao setor de saúde encontradas na literatura científica.

2.1 CIBERSEGURANÇA

A governança de cibersegurança, compreende a todos os métodos de governar, não somente por uma nação, mas também por estados regionais, mercados, desenvolvedores de *softwares* e *hardwares*, proprietários desses sistemas e equipamentos e usuários finais (KUERBIS *et al*., 2017). Com todos esses diferentes atores interagindo sobre segurança cibernética, se produz uma governança fragmentada e confusa. É improvável que uma regência ampla e eficiente surta efeito (NATSIAVAS *et al*., 2018).

Contudo, a função das nações a respeito de cibersegurança deve ser enquadrada como uma questão de segurança nacional, devido sua importância e relevância (KUERBIS *et al*., 2017). Neste sentido, várias empresas do setor privado também buscam soluções para esse problema contemporâneo. A título de exemplo, a gigante de tecnologia *Microsoft,* propôs recentemente uma espécie de convenção digital de Genebra, contra os cibercrimes, na qual comprometeu-se a ajudar as organizações a combater as vulnerabilidades, ameaças e evolução de armas cibernéticas (KUERBIS *et al*., 2017).

Já Martin *et al*. (2017), apontam três pilares no âmago do problema: uma **governança fragmentada**, em que há falta de clareza sobre responsabilidades por proteger sistemas e dados, uma **cultura do setor** de focar-se somente no atendimento aos clientes e a **falta de investimentos** significativos para proteger os sistemas.

Ainda segundo os mesmos autores, o setor de cibersegurança vem ao longo dos últimos anos tendo crescimentos constantes com bens e serviços de US$ 65 bilhões em 2012, passando para US$ 120 bilhões em 2017 e com projeções de US$ 202 bilhões até 2021. Este crescimento do mercado de cibersegurança vem sendo impulsionado por atividades especificas como a análise especializada de ameaças em

segurança de *softwares*, a segurança de dispositivos móveis e a segurança da *Internet of Things* (IoT).

Conforme Berger e Schneck (2019), a cibersegurança reflete os riscos experimentados à medida que a *internet* cresce e se diversifica. Já que a *internet* inicialmente foi desenvolvida sem uma preocupação na proteção, armazenados ou trânsito dos dados, sendo a cibersegurança uma preocupação posterior.

O crescente desenvolvimento de sistemas *cyber-físicos*, foi igualmente acompanhada pela crescente proliferação de crimes cibernéticos. Sendo que, a carência em medidas de segurança digitais adequadas, resulta na relutância de muitos usuários em usufruir toda a comodidade que as inovações tecnológicas oferecem, devido a desconfiança com relação à segurança oferecidas em todos os segmentos de mercados (NATSIAVAS *et al*., 2018).

Consequentemente, as estratégias atuais para lidar com os riscos cibernéticos concentram-se principalmente na remediação após o fato (LECHLER *et al*., 2017).

Conforme Mostfa *et al*. (2016), todos os setores econômicos devem se blindar contra diversos tipos de ameaças tais como: ***malware****,* (*software* desenvolvido com o objetivo de danificar dispositivos, roubar dados ou prejudicar as pessoas, podendo ser vírus, cavalos de Tróia, *spywares* ou *ransomware).* ***Phishing*** (técnica para enganar os usuários para conseguir informações confidenciais, geralmente uma página da *internet* ou *e-mail* se passando por uma instituição verdadeira). **Engenharia social** (habilidade de conseguir informações confidenciais por meio da persuasão dos usuários que possuam as informações). ***DOS*** (faz com que os recursos dos sistemas, geralmente o processamento dos dados e/ou tráfico da rede fiquem sobrecarregados). ***Botnet*** (é geralmente feita a invasão de vários sistemas por meio de “robôs” que controlam esses sistemas escravos, muitas vezes sem os usuários se saibam que estão infectados) e o ***ransomware*** (bloqueia o acesso ao sistema fazendo a vítima ter que pagar um valor para poder acessar novamente o sistema).

Por fim, é observado também a existência de uma pequena hegemonia de países quanto ao assunto cibersegurança, conforme Kuerbis *et al*. (2017), 70% das empresas de segurança cibernética são compostas por apenas três países, sendo que os Estados Unidos sozinho representem 60%, seguidos por Reino Unido com 7% e Canadá com 3%. Os 30% restantes das companhias são representados por dezenas de outros países. Ainda segundo os mesmos autores, países como China, Brasil e Rússia juntas representam somente pouco mais de 2,5% deste mercado.

Posteriormente, o próximo tópico, irá enquadrar a cibersegurança sob o prisma do setor de saúde.

2.2 CIBERSEGURANÇA NO SETOR DE SAÚDE

A cibersegurança é um tema importante e que vêm frequentemente sendo reportado diversos casos nos principais noticiários mundiais. Entretanto, como pode ser observado por este estudo, o setor de saúde é um dos setores que menos está preparado para encarar este desafio contemporâneo.

Conforme Alexander *et al*. (2019) a cibersegurança é uma tarefa extremamente árdua em qualquer setor na atual era da informação, o setor de saúde é um dos alvos mais vulneráveis a ataques cibernéticos devido a sua infraestrutura ser obsoleta e não projetada especificamente para as necessidades do setor. Ainda segundo os mesmos autores, muitos dispositivos médicos modernos como: monitores de pressão arterial e frequência cardíaca, glicosímetros, marca-passos, bombas de insulina etc., contêm sistemas computacionais embarcados que estão cada vez mais interconectados, mas sem uma preocupação em proteger estes componentes contra ameaças cibernéticas.

Igualmente a outros setores, o setor de saúde está constantemente incorporando inovações tecnológicas para satisfazer as necessidades atuais aos cuidados de saúde dentro e fora do ambiente hospitalar (WETHINGTON *et al*., 2018). Novos paradigmas como por exemplo a *Internet* das Coisas Médicas (IoMT) – que por padronização é utilizado neste trabalho com a nomenclatura apenas de *internet* das coisas (IoT) - e os Sistemas Ciber-Físicos Médicos (MCPS), oferecem novas soluções de monitorar, diagnosticar e tratar pacientes através de interconexões médicas, por meio de dispositivos com sistemas computacionais integrados (MAIMÓ *et al*., 2019).

Neste sentido, a projeção atual de especialistas é que, em poucos anos, esses MCPS tragam soluções para prevenir epidemias, auxiliar no tratamento de doenças crônicas, evitar mortes, além de trazer o cruzamento de dados para a análise dos denominados *big data* (BILEK *et al*., 2017). Atualmente, a equipe médica já tem instantaneamente todas as informações médicas dos pacientes, acessando os MCPS em qualquer lugar com acesso à *internet*, possibilitando receber alertas de adversidades do estado clínico imediatamente com o monitoramento fisiológico em tempo real (MAIMÓ *et al*., 2019).

As bases de dados dos pacientes foram substituídas por Registros Médicos Eletrônicos (EMR), em que são armazenadas todas as informações pessoais e clínicas dos pacientes. Com isso, se expande ainda mais a superfície para ataques e cria-se grandes desafios para a segurança digital dessas instituições (GORDON *et al*., 2019). Neste sentido, segundo Maimó *et al*. (2019) o MCPS, que também engloba o EMR, refere-se a sistemas médicos interconectados, que são críticos para a segurança dos pacientes, que analisam os sinais vitais coletados através de dispositivos eletrônicos, inferindo o estado de saúde do paciente para os profissionais de saúdes iniciarem tratamentos adequados (MAIMÓ *et al*., 2019).

Também há vários benefícios pela utilização desses dispositivos, como: rápida transmissão de informações clínicas dos pacientes para os médicos e o gerenciamento da terapia em tempo real, entretanto toda está conectividade, pode colocar os pacientes em risco de vulnerabilidades de segurança cibernética (ALEXANDER *et al*., 2019).

Neste sentido, a IoT é um dos principais pilares dessa nova realidade nos centros médicos, que já está afetando a humanidade positivamente, sendo imperativo que esses sistemas possuam altos níveis de segurança cibernética e confiabilidade. Sendo um dos principais desafios do setor a falta de padrões de segurança cibernética, a dificuldade de identificação dos dispositivos afetados e dos dados comprometidos (ROMANIUK 2018).

Acresce também a telessaúde que se refere a um conceito amplo, englobando várias atividades distintas como: serviços remotos, diagnósticos, pesquisas e educação, também possuí dentro do seu leque de possibilidades o telediagnóstico, que possibilita diagnosticar doenças a distância com “paciente e médico em locais distintos” (COVENTRY *et al*., 2018). Estas novas ferramentas, reúnem benefícios à pacientes, profissionais e gestores do setor de saúde. Pacientes utilizam cada vez mais seus próprios dispositivos móveis que permitem integração com os sistemas médicos, obtendo um gerenciamento colaborativo de doenças e a coordenação de cuidados (HANDLER 2018).

Do mesmo modo, como já salientado, é constatado que os dispositivos conectados as redes como IoT e MCPS, são vulneráveis a violações da segurança cibernética. Em 2015, a título de exemplo, a indústria automobilística teve que implementar um *recall* de 1,4 milhões de veículos da empresa *Fiat Chrysler* nos Estados Unidos, devido a problemas de cibersegurança, em que foi possível controlar

remotamente o veículo *Jeep Cherokee* (ALEXANDER *et al*., 2019). Ainda conforme os mesmos autores, o setor de saúde, devido à natureza crítica dos dispositivos médicos e sua capacidade de impactar a saúde do paciente, o potencial de dano em uma violação da segurança cibernética é catastrófico.

Outro exemplo encontrado na literatura científica mostra dispositivos cardíacos implantáveis distribuídos pela *St. Jude Medical* em 2018 também foram detectados problemas de cibersegurança com possíveis acessos não autorizados por *hackers*. A *Food and Drug Administration* (FDA) emitiu um comunicado de segurança sobre possíveis vulnerabilidades encontrados em marcapassos, cardioversores-desfibriladores implantáveis, dispositivos de ressincronização cardíaca e monitores implantáveis entre outros (ALEXANDER *et al*., 2019).

Estudos nos Estados Unidos sobre a resiliência do setor de saúde contra cibercriminosos em 22 grandes cidades do país, observaram que não há um modelo padrão de segurança cibernética adequado que proteja essas instituições (AL-MUHTADI *et al*., 2019).

Já no Reino Unido, 50 hospitais foram afetados diretamente por ataques de *ransomware*, em que a única maneira de recuperar o acesso ao computador e aos dados infectados é pagando o resgate ou limpar o sistema e recuperar um possível *backup* (MARTIN *et al*., 2017).

Neste sentido, na atual era da informação, os ataques cibernéticos podem comprometer milhares de pacientes simultaneamente. Porém, antes do surgimento dos EMR, essas violações eram limitadas aos funcionários dos hospitais. Porém, atualmente esses dados podem ser acessados remotamente, aumentando o potencial de violações (COVENTRY *et al*., 2018).

Igualmente, com todos esses avanços, a cibersegurança é um componente que se torna cada vez mais importante na infraestrutura das organizações de saúde. Ataques recentes sofridos por essas instituições impactaram negativamente suas operações, resultando em perda de informações, cancelamentos de consultas e procedimentos clínicos, alto custo monetário além de um custo incalculável que é a imagem negativa das instituições (GORDON *et al*., 2019).

Os ataques cibernéticos têm como objetivos acessar, alterar ou destruir informações confidenciais, tendo como principal motivação o ganho financeiro. Porém, os reflexos dos ataques trazem diversos problemas tanto às instituições como para a população que necessita dos cuidados médicos, tanto a curto como a longo prazo.

Deve-se contabilizar em um ataque todos os reflexos causados por ele. Sendo que praticamente muitos dos problemas são incalculáveis devido a criticidade do setor e os danos causados à população (AHMED *et al*., 2019).

Além disso, pequenas informações médicas comprometidas, podem causar danos catastróficos, como exemplo a alteração de grupos sanguíneos ou resultados de testes e exames que podem prejudicar milhares de usuários. A título de exemplo, somente em 2014, mais de 300 dispositivos médicos foram identificados como em potencial risco de ataques cibernéticos nos Estados Unidos (MARTIN *et al*., 2017).

Com salientado atualmente a principal razão de ataque é o ganho financeiro. Contudo, não se deve descartar motivações políticas cujo objetivo é tirar vidas, em uma forma de guerra cibernética que são projetadas por especialistas como uma evolução da motivação dos ataques para os próximos anos (COVENTRY *et al*., 2018).

É constatado que esse tipo de malfeitoria, já extorquiu bilhões de dólares nos últimos anos do setor de saúde, principalmente com a venda dessas informações na *dark web*. As informações extraídas, também possibilitam o acesso a medicamentos de uso controlados, extorsões, a abertura de contas bancárias, empréstimos ou passaportes. Esses dados também possuem valor político. Por exemplo, informações médicas de esportistas, celebridades e políticos sempre foram alvo de violações (COVENTRY *et al*., 2018).

Entretanto, como pode ser observado no setor de cartão de crédito que é excelente na detecção de fraudes e na inativação de cartões roubados, praticamente não se empenham a levar a justiça os criminosos reais por trás das infrações. Ao que tudo indica, o custo de levá-los à justiça supera os benefícios adquiridos. Contudo esses infratores quase sempre apresentem riscos contínuos à segurança (HUANG 2014, BOJANOVA *et al*., 2017).

Contudo, apenas recentemente a cibersegurança tornou-se um tópico importante dentro do setor de saúde, como decorrência de todo o potencial de comprometer os dispositivos médicos. Felizmente ainda não há relatos em estudos nos Estados Unidos de lesões ou mortes de pacientes relacionadas a incidentes na cibersegurança (CORONADO *et al*., 2014).

Além disso, conforme a literatura científica, os especialistas em cibersegurança são caros e escassos. Por isso, as organizações de saúde geralmente não podem arcar com as taxas de mercado por seus serviços e acabam dispondo de equipes sem o devido preparo para os desafios atuais (MARTIN *et al*., 2017).

Conforme apresentado, o setor obtém um crescimento de ataques cibernéticos exponencialmente a cada novo ano. Como exemplo, no ano de 2015 o setor de saúde teve 112 milhões de registros comprometidos, mostrando de maneira evidente a dimensão desse problema. Como já salientado, estudos demostram que as informações médicas são de 20 a 50 vezes mais valiosas para os cibercriminosos do que informações furtadas no setor financeiro. A venda de dados médicos são uma fonte de renda altamente valorizada no comercio ilegal, sendo que, um conjunto completo de credenciais médicas, é vendido por mais de US$ 1.000 nos Estados Unidos (COVENTRY *et al*., 2018).

Conforme a visão de Abraham *et al*. (2019), no setor de saúde, apenas 40% dos executivos de alto nível têm um entendimento profundo dos protocolos de segurança cibernética. Isso sugere que a alta gerência não está assumindo uma liderança ou responsabilidade de garantir uma governança forte de segurança cibernética. Também é demostrado um baixo grau de comprometimento de recursos de 0% a 3% do orçamento total de TI, dedicados ao gerenciamento da cibersegurança.

Entretanto, os investimentos geralmente são feitos sem a criação de um plano de gerenciamento adequado, fazendo com que, além de insuficientes, os recursos quando empregados são mal utilizados. Ao contrário, outros setores da economia chegam a gastar em média de 4% a 10% de seus orçamentos no gerenciamento da cibersegurança (ABRAHAM *et al*., 2019).

Portanto, prevenir riscos deliberados ou acidentais geralmente envolve o uso de sistemas de segurança cibernética e de informações que incluem soluções comportamentais e tecnológicas (BERGER *et al*., 2019).

Conforme Maimó, *et al*. (2019), os mecanismos de proteção cibernéticas existentes, tais como: antivírus, sistemas de detecção de intrusões (IDS), *firewalls*, *webfilters*, VPN’s etc. não são suficientes para defender os sistemas organizacionais de ataques cibernéticos, devido ao fato que, atualmente, os sistemas transformam dados em informação, estes em conhecimento e consequentemente em metadados.

Em suma, se os problemas de segurança cibernética não forem resolvidos em tempo hábil, o impacto será catastrófico e causará o surgimento de problemas sociotécnicos (AL-MUHTADI *et al*., 2019).

Conclui-se, a existência de diversos estudos referentes a segurança cibernética no setor de saúde em países na América no Norte, Europa e Ásia, como os de Alexander *et al*. (2019); Ondiege *et al*. (2017); Kruse *et al*. (2017); Martin *et al*. (2017);

Blanke *et al*. (2016); Natsiavas *et al*. (2018); Al-Muhtadi *et al*. (2019) e Kuerbis *et al*. (2017). Entretanto, é observado uma lacuna na literatura científica de pesquisas nacionais sobre este tema, que este trabalho procurará preencher.

Neste sentido, como uma resposta para combater os problemas de cibersegurança encontrados acima, o próximo tópico reúne estudos que demonstram como solução um plano de gerenciamento para riscos cibernéticos para o setor de saúde.

2.3 PLANO DE GERENCIAMENTO DE RISCOS EM CIBERSEGURANÇA NO SETOR DE SAÚDE

Proteger o acesso indevido a dispositivos médicos e a seus dados confidenciais, é um desafio a qualquer organização de saúde no século XXI. Embora seja impossível garantir uma segurança infalível ou zero incidente, as organizações têm que visar mitigar os riscos de ameaças cibernéticas (PESAPANE *et al*., 2018).

As organizações devem possuir uma estrutura de segurança baseada em risco cibernéticos, para identificá-los, classificá-los, preveni-los e remediá-los. Ressalte-se que os riscos não são apenas para a segurança da informação, mas também para as atividades do negócio (PRIMO *et al*., 2018).

Neste sentido, o gerenciamento de riscos em cibersegurança no setor de saúde, exige em tomar decisões diariamente, já que os incidentes estão se tornando cada vez mais comuns e é perceptível a dificuldade das organizações em enfrentar tais eventualidades (WORLD ECONOMIC FORUM 2017).

Os artigos obtidos na revisão bibliográfica realizada focam seus esforços apenas na detecção de ataques (KURE *et al*., 2018). Entretanto, uma abordagem geral dos artigos de avaliação de riscos de segurança cibernética conclui que é importante ter um método abrangente de gerenciamento de riscos que cubra todas as etapas desse processo, desde a identificação do risco até uma possível resposta a esse risco (ABRAHAM *et al*., 2019).

Para gerenciar uma organização, se faz necessário ter uma boa gestão de riscos. Gerir uma organização sem uma política estabelecida de gestão de riscos é algo irresponsável e que o mercado atual não perdoa. Isso devido ao fato que riscos são inerentes a qualquer negócio (MASSEY & LARSEN 2006).

Segundo a literatura científica, uma solução para combater as ameaças dos crimes cibernéticos é a elaboração de um plano de gerenciamento de riscos cibernéticos. Criar um plano nesse sentido, é o processo de documentar as ações necessárias para definir os riscos, eliminar ou reduzir as suas incertezas, aperfeiçoar os processos existentes no combate, integrar a organização para fazer frente às ameaças e integrar os planos auxiliares de gerenciamento de riscos (BUSDICKER *et al*., 2017).

Com um bom gerenciamento de riscos, as organizações podem se preparar e dar respostas eficientes aos riscos expostos, estando aptas a reduzir ou até mesmo eliminar os existentes. Aptas a melhorar a performance e efetividade, irão melhorar o relacionamento com as partes interessadas e irão clarificar para elas os riscos em potencial e quais ações tomar caso eles ocorram. Com um bom gerenciamento de riscos as organizações irão estar sempre em busca de uma melhoria contínua. O processo consiste em atividades interligadas entre si, e todas as atividades incluem etapas para dar suporte a tarefas específicas relacionadas ao gerenciamento de riscos (ABRAHAM *et al*., 2019).

Neste sentido, é sugerido que um maior número de atores da organização participe do processo de elaboração do plano de gerenciamento de riscos, pois diferentes atores podem ter interpretações diferentes sobre o mesmo risco, o que irá propiciar uma maior gama de soluções mais profundas e assertivas. Contudo, esse processo não é uma atividade isolada que deva ser implantada apenas uma única vez, mas sim um ciclo ininterrupto que deve ser praticado durante todo o ciclo de vida da organização (MAROSIN *et al*., 2014).

Ainda se observa que a desordem não é uma abordagem que combine com o gerenciamento de riscos em segurança cibernética. Entretanto, muitas organizações caem nessa armadilha por motivos como: falta de prioridades, falta de comprometimento da gerência, complexidade organizacional, numerosos e incompatíveis sistemas, orçamento inadequado etc. Conforme evidências, as organizações de saúde dos Estados Unidos e provavelmente de todo o mundo, carecem de uma estratégia deliberada, organizada e abrangente de ciber-resiliência (ABRAHAM *et al*., 2019).

Segundo Ondiege *et al*. (2017) o método de gerenciamento de risco moderno inclui os requisitos regulatórios existentes convertendo-os em objetivos de controle

para a organização. As estruturas e padrões incluídos neste gerenciamento de riscos são:

- NIST, que é o instituto nacional de padrões e tecnologia dos Estados Unidos;
- ISO 31000 (2018), que são padrões e normas sobre gestão de riscos;
- ISO 27001 (2013), que são padrões e normas sobre segurança da informação;
- HIPAA, é uma lei de portabilidade e responsabilidade do setor de saúde dos Estados Unidos, que implementa salvaguardas para proteger informações confidenciais dos usuários;
- PMBOK, que é um conjunto de melhores práticas e conhecimentos em gerenciamento de projetos.

Ainda se observa na literatura científica que, com a estrutura de gerenciamento de riscos orientada a objetivos, esses padrões fornecem diretrizes para as atividades de gerenciamento de riscos (ONDIEGE *et al*., 2017).

Gerenciar os riscos de segurança cibernética deve ser encarado como um ato de equilíbrio entre segurança e resiliência. Nenhuma organização pode ser completamente segura, mas pode desenvolver a capacidade de minimizar as ameaças e se recuperar rapidamente de um ataque (ABRAHAM *et al*., 2019).

Conforme Kure *et al*. (2018) e Abraham *et al*. (2019), é importante possuir uma visão geral de várias questões importantes de ameaças reais de segurança cibernética e avaliação de riscos. Os planos de gerenciamento de riscos devem fazer uma associação de diferentes cenários de ataque e violação. Uma organização de saúde deve na avaliação de riscos cibernéticos analisar consequências negativas como: o pagamento de *ransomware*; envio de pacientes/clientes para locais alternativos para serviços de assistência; dano à reputação da instituição; sanções do governo; custos de recuperação de dados, substituição de equipamentos e implementação de medidas de segurança adicionais (ABRAHAM *et al*., 2019).

A literatura mostra que o plano deve servir como um guia, sendo a principal referência para gestores e colaboradores. Ele deve descrever como os riscos à segurança da organização devem ser monitorados, controlados e executados. Deve-se avaliar os riscos na organização da mesma forma como os riscos financeiros, clínicos ou operacionais (MARTIN *et al*., 2017).

Neste sentido, o plano de gerenciamento de riscos, deve incluir a descrição de ataques, a identificação das vulnerabilidades, a prescrição de controles específicos para a vulnerabilidade e a implementação de plano de controle (BLANKE *et al*., 2016).

À medida que as ameaças à segurança vêm crescendo exponencialmente nos últimos anos, as organizações precisam de um sistema abrangente de gerenciamento de riscos à segurança cibernética para identificar ameaças exclusivas ou tendências. Uma solução é uma abordagem em camadas para avaliar os riscos com base na segurança para prevenir, mitigar e tolerar ataques aos dispositivos médicos e infraestruturas cibernéticas (KURE *et al*., 2018).

Ainda segundo a visão dos mesmos autores, o gerenciamento de riscos é um processo (uma caminhada) estruturada em pequenas etapas. Essa estratégia ajuda a identificar qual risco precisa ser controlado, seguindo diferentes estratégias de controle. O gerenciamento de riscos como processo tem várias etapas tais como identificar, avaliar, analisar, verificar, classificar e monitorar os riscos desde a sua origem até a sua eliminação.

Desta forma, o plano de gerenciamento de riscos é um documento oficial da organização, sendo a principal referência para o combate a cibercrimes. Ele descreve como a organização irá agir contra as ameaças atuais dos cibercriminosos. Esse plano contém diversos elementos conforme apresentados na Quadro 1.

Quadro 1 - Elementos do plano de gerenciamento de riscos

Elemento	Definição
Ator	O ator, pode ser representado por: um indivíduo, um usuário, um funcionário, consumidores, clientes, um sistema, uma organização um processo, por partes interessadas etc. O qual realiza atividades específicas para gerar ações de gerenciamento de riscos de segurança cibernética ou gerar ações de outro ator.
Escopo	O objetivo que se deseja alcançar, o alvo, o que a organização terá como finalidade. É a definição do que precisa ser feito, deve incluir todo o trabalho que deve ser realizado para alcançar os objetivos propostos.
Metas	As metas são objetivos que se pretende alcançar, é extremamente importante uma definição clara das metas por todas as partes interessadas. As metas compreendem tarefas específicas, que devem ser cumpridas em um determinado período estabelecido, como uma etapa necessária para alcançar os objetivos programados.

Ativos	Os ativos podem ser bens, valores, créditos, direitos e assemelhados podendo serem tangíveis ou intangíveis. Deve-se identificar os principais ativos da organização, e a agregação de valor a cada ativo-chave no processo de gerenciamento de riscos. Os ativos principais podem ser pessoas, serviços, instalações, processos dentre outros.
Controles	Os controles, consistem em planos, métodos e procedimentos utilizados pelas organizações para atender suas metas e objetivos e proteger seus ativos. E minimizando os riscos de segurança. Os controles são mecanismos usado para fornecerem segurança as organizações e são caracterizados pela combinação de controles técnicos e controles não técnicos que são usados para impedir que ameaças explorem vulnerabilidades conhecidas.
Cenário de ataque cibernético	É um evento que induz a um impacto negativo nos ativos da organização. Os componentes que determinam um ataque cibernético incluem tipos de ameaças, habilidade, capacidade e localização do ator, ativos, eventos e horário. As organizações devem pensar antecipadamente em todos os possíveis cenários para desenvolver respostas a estes possíveis cenários
Vulnerabilidade	É a fraqueza de um sistema da organização, que pode ser explorado por uma ameaça para obter acesso não autorizado a um determinado ativo. A vulnerabilidade é a confluência de três elementos, suscetibilidade do sistema, acesso do atacante à falha e a capacidade do atacante de explorar a falha. Podendo existir três propriedades, impacto, tipo e pontuação de peso.
Políticas	As políticas são os princípios de ação adotados ou propostos dentro de uma organização. Elas podem ser classificas como: Políticas internas, Políticas externas, Políticas obrigatórias, Políticas implícitas e Políticas definidas.

Fonte: Adaptado de Coronado e Wong (2014,), Kure *et al*. (2018) e Abraham, *et al*. (2019).

Já conforme a ISO 31000 (2018), uma boa gestão de risco propicia muitos benefícios às organizações. Entre eles podemos destacar dez benefícios: Melhorar a governança; Aumentar a probabilidade de atingir os objetivos; Melhorar os controles; Aumentar a resiliência da organização; Melhorar a aprendizagem organizacional; Minimizar perdas; Melhorar a eficácia e a eficiência operacional; Estabelecer uma base confiável para a tomada de decisão e o planejamento; Melhorar a identificação de oportunidades e ameaças; Melhorar a confiança das partes interessadas.

O trabalho de Kure *et al*. (2018) alertam que, as interdependências entre os sistemas e seus componentes podem ser classificadas em quatro categorias: interdependência física, cibernética, lógica e geográfica.

Para elaborar um plano de gerenciamento de riscos em cibersegurança se faz necessário primeiro entender e definir o que são riscos. Segundo o PMI (2017) riscos

são incertezas, são acontecimentos, condições ou circunstâncias futuras que poderão provocar um impacto negativo, podendo ou não dar prejuízo ou danos. Quanto mais se souber de antemão sobre os riscos e seus impactos, mais preparado se estará para lidar com eles caso ocorram.

Kure *et al*. (2018), o risco é a combinação entre a probabilidade de ocorrência de um determinado evento e os impactos negativos resultantes caso ele ocorra. O risco é inevitável em uma organização, no entanto, é papel de todos os atores garantir que eles sejam mitigados para atingir os objetivos organizacionais. Ainda conforme os mesmos autores, o risco é originário da incerteza, porém, ele não é exatamente imprevisível. Segundo Coronado *et al*. (2014), é possível determinar sua quantificação, qualificação, impacto, probabilidade etc., e consequentemente preparar-se para a caso ele se concretize, mitigá-lo, transferi-lo ou simplesmente eliminá-lo, mediante um plano de gerenciamento de risco.

O risco pode ser considerado como um perigo latente. Já as ameaças são situações ou ações não controladas que podem ser associadas a pessoas mal-intencionadas ou a fatores fora de controle como a intempéries, falhas físicas etc. Elas podem obter controle, danificar ou destruir um ativo dentro das organizações. As ameaças podem se referir, mas não se limitam, a aspectos técnicos, aspectos funcionais, aspectos legais, aspectos pessoais ou a aspectos políticos (NATSIAVAS *et al*. 2018).

Para entender e definir os riscos, deve-se incluir análises de fatores ambientais das empresas. Estes incluem, mas não se limitam, a cultura e a estrutura organizacional, padrões governamentais ou do setor, infraestrutura, as condições do mercado, produtos/serviços/resultados disponíveis no mercado, fornecedores e reputação ou desempenho anterior, termos e condições atuais das organizações (CORONADO *et al*., 2014).

Neste sentido, com a análise dos fatores ambientais da empresa, deve-se compreender a visão, missão, valores, crenças e expectativas compartilhadas da organização. Além da disponibilidade e distribuição geográfica das instalações, recursos, infraestruturas e materiais que são utilizados (PMI 2017).

Outra análise importante, é a análise dos ativos de processos organizacionais, em que se deve procurar entender os planos, processos, políticas, procedimentos e todas as bases de conhecimento das organizações ou por ela usados. Nesta fase

deve se entender como a organização pensa como ela funciona como um todo, pois cada organização é única e tem sua própria personalidade (PMI 2017).

Já para Abraham *et al*. (2019), é importante se conhecer a tolerância de riscos das organizações. A tolerância de riscos da organização é o nível em que as partes interessadas das organizações se sentem confortáveis para encarar um risco porque os benefícios a serem alcançados superam o que poderia ser perdido. Quanto maior a tolerância ao risco de uma organização, mais disposto se está a encarar o risco e suas consequências. Já segundo Kure *et al*. (2018), a tolerância a riscos é diferente do apetite de risco, pois o apetite de risco está relacionado ao tamanho da incerteza que a organização está disposta a assumir para obter um benefício, enquanto a tolerância ao risco está relaciona ao tamanho do risco e, portanto, as consequências ou benefícios em potencial que a organização pode ganhar ou perder se o risco ocorrer.

Da mesma forma, os níveis de tolerância ao risco de cibersegurança devem ser fixados na linha de: sempre relatar incidentes de violação de segurança, desligamento da rede dentro do prazo de cinco minutos após conhecimento do ataque, substituir para procedimentos de rede *failover* (que é a é a comutação automática para recursos como sistema, *hardware* ou rede redundante) e enviar analistas dentro de prazos acordados previamente para discernir o tipo e gravidade do ataque e das possíveis perdas (ABRAHAM *et al*., 2019).

O PMI (2017) salienta que é imperativo que as organizações definam apetites e tolerância aos níveis de riscos, determinados e definidos como parte do processo de planejamento estratégico de cibersegurança. Essas avaliações antecipadas, refletem uma clareza de propósito e pavimentam um caminho garantindo uma organização eficaz no tratamento das ameaças cibernéticas.

Neste sentido, o processo de gerenciamento de risco, elimina-os até quase os extinguir. Entretanto, podem permanecer riscos residuais (riscos que ainda existem mesmo depois de serem tratados). Estes devem ser aceitos em um determinado nível, conforme algum parâmetro preestabelecido de mensuração acordado entre as partes responsáveis por riscos (KURE *et al*., 2018).

Logo, não há sistemas sem risco; portanto, faz-se necessário interpretar qual o nível de aceitação de risco da organização e quantificá-lo dentro de uma categoria e extensão. A Tabela 2, utiliza a probabilidade de ocorrência e impacto dos riscos com base em cinco categorias de riscos (KURE *et al*., 2018)

Tabela 2 – Categorização dos riscos

Item	Categoria	Extensão
1	**Extremo**	*0,81 – 1,00*
2	**Alto**	*0,61 – 0,80*
3	**Médio**	*0,41 – 0,60*
4	**Baixo**	*0,21 – 0,40*
5	**Muito Baixo**	*0,0 – 0,20*

Fonte: Kure *et al*. (2018).

Com os resultados dessa pontuação de avaliação da Tabela 2, a equipe de segurança cibernética pode aprofundar a aplicação e o gerenciamento de controles. Sendo que, a avaliação de risco ajuda a identificar as lacunas de controle que devem ser documentadas e disponibilizadas para fins de auditoria (BUSDICKER *et al*., 2017).

Igualmente importante, na visão de Ward *et al*. (2008) é conhecer e classificar todas as partes interessadas da organização. Neste sentido, o gerenciamento de risco moderno engloba todas as partes interessadas, sendo que na sua essência está a integração de toda a organização com as práticas de gerenciamento de riscos (ONDIEGE *et al*., 2017).

Segundo a ISO 31000 (2018) deve-se incluir também na análise dos riscos, o contexto externo em que a organização está inserida. Este pode incluir, mas não se limita a: o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local; os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e as relações com partes interessadas externas e suas percepções e valores.

Ainda segundo a ISO 31000 (2018) deve-se analisar o ambiente interno no qual a organização busca atingir seus objetivos. O contexto interno pode incluir, mas não se limita a:

a) Governança, estrutura organizacional, funções e responsabilidades;

b) Políticas, objetivos e estratégias implementadas para atingi-los;

c) Capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

d) Sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);

e) Relações com partes interessadas internas, e suas percepções e valores;

f) Cultura da organização;

g) Normas, diretrizes e modelos adotados pela organização; e

h) Forma e extensão das relações contratuais.

Neste sentido, todos os riscos conhecidos devem ser identificados e catalogados em um único documento para sua devida análise e tratamento. Os riscos podem ser classificados sob diversos parâmetros de segurança como: pessoal, infraestrutura, político, operacionais, não técnicos, técnicos e de governança ou regulatórios (WU *et al*., 2018).

Já segundo Kure *et al*. (2018), todos os riscos à segurança devem passar por uma avaliação apropriada, ressaltando a importância de combinar a segurança de aplicativos de energia e o suporte à segurança de infraestrutura no processo de avaliação dos riscos e fornece uma metodologia para avaliação de possíveis impactos.

Já o risco legal, é o risco relacionado a legislação, ou seja, da justiça de alguma maneira prejudicar as atividades de uma organização, por meio de multas, penalidades ou indenizações. O risco legal entra na categoria de risco operacional podendo ser causado pela quebra de termos contratuais firmados pelas organizações com outras partes, ou quanto o descumprimento da legislação. Os três principais tipos de risco legal são o litígio, regulatório e o de fraude (DANDAGE *et al*., 2018).

Com foco em riscos técnicos, pode-se classificá-los em seis tipos: risco de falsificação, adulteração, repúdio, divulgação de informações, negação de serviço e elevação de privilégio (NATSIAVAS *et al.*, 2018).

Posteriormente, o risco político aborda às complicações que organizações e governos podem enfrentar, decorrente do que é frequentemente mencionado como decisões políticas. Como qualquer mudança no âmbito político, as consequências previstas ou o valor de uma determinada ação econômica, pode alterar a probabilidade de alcançar os objetivos predeterminados (DANDAGE *et al*., 2018).

Ainda segundo Dandage *et al*. (2018), para as organizações os riscos políticos representam probabilidade de que eventos políticos possam prejudicá-las financeiramente por meio de impostos ou taxas, ou com a perda de custo de

oportunidade. Há dois tipos de riscos políticos, um em um nível macro e outro em um nível micro. Os riscos políticos macro têm consequências similares em todos os atores dentro de um determinado país. Os riscos políticos micro são os riscos específicos de determinados setores econômicos, organizações ou projetos.

Já os riscos pessoais, são todos aqueles que podem ocorrer com os colaboradores de uma organização, podendo ocasionar em um colaborador ou grupo de colaboradores reveses tais como: acidentes, lesões ou até mesmo a morte (DANDAGE *et al*., 2018).

Neste sentido, uma organização pode acabar sendo refém de um único colaborador que sabe determinada informação ou manusear determinado equipamento específico. Com isso caso este colaborador saia da empresa ou se ausente, ela fica submissa a esse revés (DANDAGE *et al*., 2018).

Os riscos podem também ser identificados de diversas maneiras. Uma das formas mais simples de identificar riscos é pela revisão da documentação de segurança cibernética fornecida pelo fabricante do dispositivo. Muitos profissionais usam a Plataforma de Avaliação de Risco de Dispositivos Médicos para realizar a avaliação de riscos nesse tipo de equipamento quando estão conectados (BUSDICKER *et al*., 2017).

Todos os atores da organização devem auxiliar a identificar os riscos na organização. Todos os riscos devem ser registrados em um único documento, denominado matriz de registro dos riscos (KURE *et al*., 2018, CORONADO *et al*., 2014, ABRAHAM *et al*., 2019).

As contramedidas contra ciberataques são propostas com base no método de uma matriz de risco com a sua classificação. Os valores adotados aos riscos foram introduzidos em um Sistema de Gerenciamento de Segurança da Informação (SGSI), e a avaliação quantitativa é realizada para uma avaliação detalhada dos riscos (ABRAHAM *et al*., 2019). Através de uma avaliação quantitativa dos riscos é possível observar que as contramedidas elaboradas, poderiam reduzir os riscos até determinado ponto (KURE *et al*., 2018). O Quadro 2, exemplifica uma matriz de registro dos riscos.

Quadro 2 - Exemplo de uma matriz de registro de riscos

ID	Risco	Gatilho	Causa	Impacto	Proprietário	Plano de Resposta
Identificador único para cada risco	Nome do risco identificado	Eventos que sinalizam que um risco está preste a ocorrer	Identificar a causa do risco	Identificar qual o impacto na instituição, caso o risco ocorra	Nome do responsável pelo risco	Possíveis respostas aos riscos identificáveis

Fonte: Adaptado de PMI (2017).

Uma técnica fundamental para identificar vulnerabilidades e ameaças do sistema é a modelagem de ameaças. Deve-se sempre utilizá-la nas organizações de saúde, pois ela exerce parte vital no processo do ciclo de vida em desenvolvimento da segurança. Além de identificar vulnerabilidade e ameaças do sistema ela também estabelece técnicas de mitigação apropriadas. A modelagem de ameaças deve ser empregada também na cadeia de suprimentos da organização, para identificar ameaças e vulnerabilidades em dispositivos específicos. (KURE *et al*., 2018).

A análise de risco fornece uma estrutura para a gerência conhecer e avaliar os perigos e vulnerabilidades da organização e com isso elaborar um plano de gerenciamento de riscos antes da ocorrência do evento de risco (BLANKE *et al*., 2016).

Em uma boa análise de riscos, faz-se necessário não apenas a priorização ou abordagem de apenas um grupo limitado de riscos, mas sim uma análise de todos os riscos quanto se é possível identificar. E se conhecer o quanto é necessário para reduzir esses riscos até um nível de aceitação pela organização (KWAK & STODDARD 2004).

Há três categorias básicas avaliar os riscos tais como: a) análise estatísticas em que a coleta e mensuração das informações são feitas na totalidade ou em uma determinada amostra da informação no intuito de descobrir padrões ou tendências; b) mineração de dados em que serão analisadas grandes quantidades de dados na busca de padrões ou associações para reconhecer vínculo entre os dados; e c) análises subjetivas em que a análise tem um cunho privativo, podendo ser por meio da opinião de especialistas, questionários e análises empíricas (WU *et al*., 2018).

Duas análises fundamentais para a identificação de riscos são a análise qualitativa e a análise quantitativa. A primeira é aquela que faz emergir os aspectos subjetivos de cada ator (como cada ator irá entender e qualificar o risco). É uma análise extraída da experiência dos atores. É usada na investigação da percepção ou entendimento de cada ator a respeito da natureza do risco, através de sua interpretação e experiencia (BLANKE *et al*., 2016 & PMI 2017).

Já a análise quantitativa, é a que atribui probabilidades numéricas a cada risco identificado, examinando seu potencial, impacto e consequências. Podem ser agrupadas por diversas categorias, conforme necessário. Este tipo de análise irá propor entender os riscos cibernéticos por meio de dados mensuráveis e quantificáveis, ou seja, numericamente (BLANKE *et al*., 2016 & PMI 2017).

Após todos os riscos serem identificados, avaliados quantitativamente e qualitativamente, analisada a sua probabilidade de ocorrência e verificados seus impactos, deve-se classificar essa matriz de riscos de acordo com a gravidade desse risco (KURE *et al*., 2018).

Da mesma forma, uma avaliação importante a ser executada é analisar a relação custo-benefício das contramedidas propostas, que compara os benefícios de uma ação em detrimento aos seus custos (ABRAHAM *et al*., 2019). Aqui deve-se utilizar objetivos claros, ter um domínio das aplicações propostas, dividir os estágios de gerenciamento de riscos em partes gerenciáveis, ter um domínio dos conceitos de gerenciamento, ter uma medição de impacto dos riscos e fontes de dados probabilísticos etc. (KURE *et al*., 2018).

A literatura mostra que, apesar de muitos métodos de avaliação de riscos, falta um que seja abrangente e envolva todas as etapas do processo de gerenciamento de riscos. Uma boa estratégia encontrada na literatura propõe uma abordagem para avaliar a vulnerabilidade das organizações a violações de segurança da informação usando o índice de impacto de ameaças e os índices de *cyber* vulnerabilidade com base na elaboração de árvores de vulnerabilidade (KURE *et al*., 2018).

Deste modo, a análise de árvore de falhas (FTA) pode uma ferramenta muito útil na análise de riscos. Sendo uma procedimento de cunho dedutivo que parte do geral para o específico, ou seja, *top-down*, essa ferramenta permite imaginar as interdependências entre os riscos e os sistemas. O princípio da árvore de falha é que se conheça o sistema que se está procurando proteger para prever os riscos que possam ocorrer (MANSOORZADEH *et al*., 2014).

Esse procedimento é baseado na identificação de um risco indesejado a ser analisado, denominado de evento principal. O desenvolvimento da árvore de falha prossegue com a identificação dos eventos relacionados a suas causas, até serem encontrados os riscos fundamentais. As relações entre eventos e causas são simbolizadas pela representação de portas lógicas (AND, OR, NOT, NAND etc.) (BOBBIO *et al*., 2001).

Segundo Dugan *et al*. (1992) com essa ferramenta é possível: a) Identificar os riscos e suas causas; b) Identificar os efeitos das consequências de erros de parte humana e de sistemas; c) Quantificar a probabilidade de riscos; e d) Priorizar os principais riscos.

Já a análise de probabilidades permite analisar ou mensurar numericamente as chances de ocorrer um determinado risco identificado. Com ela é possível verificar quais os riscos têm maiores chances de ocorrer em detrimentos de outros (BLANKE *et al*., 2016). Com essa classificação é possível identificar quais riscos devem ser tratados mediante sua probabilidade de ocorrência (PMI 2017).

Com o uso da ferramenta de FTA, a análise é efetuada em duas etapas distintas: a) uma etapa qualitativa em que as expressões lógicas do evento do topo são suas derivações em termos de implicantes primários e b) uma etapa quantitativa na qual probabilidades são atribuídas aos eventos de falha dos componentes básicos. A probabilidade de ocorrência do evento topo e de qualquer evento interno subsequente ao subsistema lógico é mensurado (BOBBIO *et al*., 2001).

Já a matriz de probabilidades e impacto é uma ferramenta visual excelente para analisar a probabilidade e impacto dos riscos. Com ela é possível adquirir uma compreensão coletiva e definição clara do risco, garantindo um nível de qualidade para o seu gerenciamento entre todos os envolvidos (MAROSIN *et al*., 2014).

Essa compreensão alcançada com a matriz de probabilidade e impacto dos riscos, obtém-se uma classificação de acordo com seu grau de priorização estabelecida por meio da junção de dois eixos. No vertical, a probabilidade é dividida em quantas categorias se considerem necessárias, e no horizontal em quantas categorias de impacto os responsáveis pela utilização dessa ferramenta acharem convenientes. Os riscos são categorizados como um ponto nessa matriz bidimensional de acordo com a junção das estimativas de probabilidade e impacto estabelecidas pelos responsáveis pela análise dos riscos

Da mesma forma, deve-se analisar o impacto, as consequências, os efeitos que os riscos catalogados podem causar na organização, classificando os impactos diretos e indiretos desses riscos. Deve-se fazer perguntas como: se esse risco se concretizar qual o impacto ele trará a organização? (BLANKE *et al*., 2016 & PMI 2017).

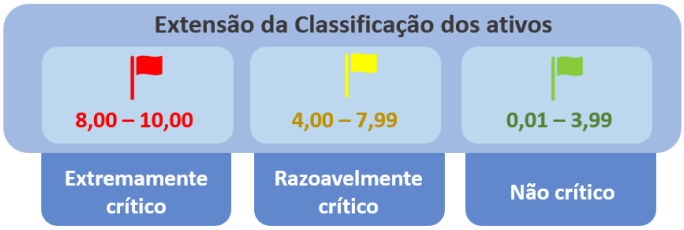
Também é essencial mensurar as informações em outros formatos como gráficos, que determinam quantitativamente a probabilidade de um ataque, o impacto do ataque e a redução do risco como resultado de uma contramedida específica para ajudar na tomada de decisões (KURE *et al*., 2018). Uma ferramenta como a Estrutura Analítica de Risco é fundamental para gerenciá-los (ABRAHAM *et al*., 2019).

Os ataques cibernéticos que manipulam ou destroem os dados podem prejudicar os sistemas de saúde, sem a consciência das organizações e têm potencial para danificar as infraestruturas críticas. Eles concentram-se basicamente, em identificar os ativos de infraestrutura da organização que são críticos para o pleno desenvolvimento das atividades diárias (KURE *et al*., 2018).

No gerenciamento de riscos, a identificação de ativos críticos é importante para que esses ativos obtenham proteção adequada. Consequentemente, eles necessitam de maior atenção e controle para não interromperem seu funcionamento. Ameaças cibernéticas contra a integridade dos dados são uma preocupação crescente que devem ser observados (KURE *et al*., 2018).

Também a criticidade é um indicador que identifica quão críticos são os ativos da organização. Esta tarefa combina o peso de um ativo com o valor de seu impacto para obter o nível crítico. Não há uma maneira padrão de combinar essas duas informações, já que não há como proteger todos os ativos críticos de todos os riscos existentes devido principalmente a restrições de recursos e orçamento limitado das organizações de saúde (ABRAHAM *et al*., 2019). Com isso, as organizações devem concentrar seus esforços nos ativos classificados como os mais críticos, em que a interrupção terá um sério impacto na segurança nacional, da saúde pública, da segurança ou da continuidade dos negócios da organização (CORONADO *et al*., 2014). A criticidade do ativo é estipulada com base na classificação do peso e na pontuação do valor de impacto. Em um ativo considerado mais importante, o fator de pontuação é maior. Já um ativo considerado menos importante, a pontuação é menor (KURE *et al*., 2018). O nível crítico do ativo pode ser classificado com base na descrição das três categorias conforme é demostrado na Figura 2:

Figura 2 - Classificação dos ativos



Fonte: Adaptada de Kure *et al*. (2018).

Neste sentido, a pontuação de ponderação do ativo é determinada de acordo com o nível em que um ativo é essencial para a continuidade das operações da organização. A categoria não define completamente a criticidade; no entanto, a criticidade de um ativo pode ser categorizada em extremamente crítico (ativos considerados mais valiosos para a continuidade das operações), razoavelmente crítico (ativos considerados com valor moderado) e não crítico (ativos consideras com valor baixo) dependendo do peso atribuído ao ativo conforme parâmetros mostrados na Figura 2 (CORONADO *et al*., 2014).

Já segundo Kure *et al*. (2018) e Coronado *et al*. (2014), uma pontuação de peso será atribuída a cada ativo, classificando-os com base no parecer subjetivo das partes interessadas da organização. A criticidade do ativo pode ser representada através de uma equação matemática conforme abaixo:

Criticidade de ativos (CA) **=** Pontuação do peso do ativo **×** Pontuação do valor do impacto

A criticidade irá caracterizar o que é mais crítico, urgente, fundamental devendo ser estabelecida previamente ao plano. É estabelecido como um parâmetro das consequências associadas à degradação ou perda de um ativo, sendo um dos principais indicadores utilizados pelas organizações para determinar qual ativo tem mais valor para a continuidade das operações (KURE *et al*., 2018).

Uma outra ferramenta importante é a decomposição. Ela consiste na divisão de itens maiores em itens menores, que são componentes mais adequados para gerenciar e controlar (PMI 2017).

As categorias exprimem os ativos de acordo com o nível dos requisitos de segurança, por meio de relações de criticidade de categoria, podendo ser classificados com categoria de grandeza como alta, média ou baixa. Ou com

categorias numéricas como 1, 2 ou 3. O cerne aqui é estabelecer quais os ativos mais valiosos para a organização, para criar estratégias para protegê-los de possíveis riscos (KURE *et al*., 2018 & CORONADO *et al*., 2014).

Outra ferramenta relevante encontrada na literatura é a Estrutura Analítica dos Riscos (EAR) que reúne os riscos em categorias por meio de uma hierarquização. Cada categoria dever ser fragmentada em níveis em que cada um especifica o risco do predecessor, proporcionando a visualização das relações dos riscos em vários níveis dentro de cada categoria (TAH & CARR 2000).

Como vantagens da EAR pode-se destacar: representar a causa raiz dos riscos, ilustrar as relações entre os riscos, aprofundar-se na relação dos riscos, expor as fontes mais relevante dos riscos e a possibilidade de encontra o maior número possível de riscos (PMI 2017).

Neste sentido, qualquer tratamento a riscos cibernéticos precisa contemplar no mínimo três fases distintas: a) identificação e conhecimento, b) avalição e c) respostas apropriadas aos riscos (WU *et al*., 2018). Planejar respostas aos riscos é o processo de concepção de ações para responder a riscos caso eles ocorram. Deve incluir a identificação e designação dos colaboradores que são responsáveis pelo risco caso ele ocorra. Já o processo de tratamento do risco pode envolver uma das ações a seguir ou uma combinação entre elas: alteração da probabilidade, do impacto, controle da ameaça ou redimensionamento das vulnerabilidades (PMI 2017). As atitudes da organização diante aos riscos são apresentadas no Quadro 3. Em que são exploradas quatro maneiras de lidar com os riscos cibernéticos.

Quadro 3 - Atitudes perante os riscos

Elemento	Definição
Prevenção	É um conjunto de medidas ou atividades que buscam evitar os riscos. É quando se age no risco antes que o mesmo ocorra. É evitar os riscos por completo, eliminando principalmente a causa dos eventos de riscos.
Mitigação	Procura reduzir a probabilidade de ocorrência de um evento de risco ou reduzir seu impacto a um nível aceitável pela organização. A mitigação de riscos envolve algumas etapas como: identifica o risco, planejar alternativas para evitá-lo ou reduzir seu impacto e planejar alternativas para evitá-lo ou reduzi-lo.
Transferência	A transferência não irá eliminar o risco. Consiste em transferir o risco e suas consequências negativas para terceiros. Com isso, o risco será transferido para empresas ou profissionais que irão saber lidá-lo da maneira mais apropriada.

Aceitação	Essa estratégia é utilizada quando não se é capaz de eliminar as ameaças de riscos. A aceitação pode ser passiva, quando é mais vantajoso aceitar os impactos do risco do que gastar tempo ou recursos para lidar com eles. E a aceitação ativa, que pode incluir o desenvolvimento de planos de contingências e reservas para ligar com os riscos.

Fonte: Adaptado de Blanke e McGrady (2016) e PMI (2017).

Já o Quadro 4, ilustra um exemplo de um controle de resposta aos riscos cibernéticos, em que foram acordadas três soluções para um risco identificado.

Quadro 4 - Controle de resposta aos riscos cibernéticos

ID	Risco	Gatilho	Causa	Impacto	Proprietário	Plano de Resposta
147C	Invasão do sistema	Sistema sobrecarregado	Acesso a portas E11 e F56	Perda de acesso a plataforma Phroteus por usuarios	Henrique	Reiniciar o sistema com protocolos padrões; Carregar firework protocolo H58C1; Fechar porta de acesso AWWPS após 05 segundos de carregamento dos protocolos.

Fonte: Adaptado de PMI (2017).

Segundo o PMI (2017) uma ferramenta também a ser utilizada é o grupo de discussões, que reúne as partes interessadas qualificadas e apropriadas para discutir sobre suas expectativas, entendimento e possíveis soluções para cada risco identificado, no intuito de construir soluções mais profundas e aprimoradas.

O sucesso ou fracasso do que for planejado é posto em prática na execução do plano de gerenciamento. Uma ferramenta encontrada na literatura científica é a *front-end planning* (FEP), que pode ser utilizada como uma significante ferramenta para sequenciar etapas em gerenciamento ou projeto de capital.

Segundo George *et al*. (2008) essa ferramenta sumariza as etapas de desenvolvimento de um projeto, pois determina os parâmetros para execução de cada etapa pré-estabelecida, almejando uma melhor qualidade em cada etapa, pois emprega as melhores prática em gestão. Ela contribui na otimização de pontos fortes e minimização de pontos tendem a impactar no correto desenvolvimento dos processos.

Ainda segundo George *et al*. (2008), a premissa dessa ferramenta é alicerçada sobre as etapas do processo de planejamento que devem ser corretamente definidas e desenvolvidas para não prejudicar as a fases do grupo de processo de execução.

Essa ferramenta enuncia que a etapa de planejamento seja concebida por profissionais aptos e qualificados na investigação e procura, visando atestar que o que for produzido ou almejado, encontra-se incorporado em especificações técnicas apropriadas (WEBSTER 2004).

Deste modo, o processo de FEP desenvolve informações estratégicas fortes que são utilizadas para eliminar riscos e envolver recursos para maximizar a plena execução de todas as etapas definidas (GEORGE *et al*., 2008).

Deve-se analisar e desenvolver algumas barreiras para garantir que elementos chave na execução sejam aprovados por responsáveis qualificados. Deste modo, cada barreira deve expor indagações apropriadas que tendem a causar algum resultado relacionada ao objetivo almejado (HONG *et al*., 2004).

Um outro item importante a ser observado é a comunicação, que dentro das organizações pode ser: interna, externa, com fornecedores e clientes. A comunicação também pode ser horizontal ou vertical (PMI 2017).

Uma comunicação eficiente refere-se ao fornecimento de informações no formato correto, ao público correto, no momento correto e com conteúdo correto. Uma comunicação eficiente é importante em qualquer organização, principalmente na elaboração da segurança cibernética. Na comunicação é imperativo sempre buscar uma conscientização e compreensão para mobilizar o apoio de toda a organização e dos usuários para criar e sustentar uma cultura proativa de segurança cibernética. Essa conscientização só será alcançada por meio de um nível de entendimento e consenso comum entre todos os envolvidos (ABRAHAM *et al*., 2019).

Neste sentido, dentro do plano de gerenciamento dos riscos, se faz necessário criar um plano de gerenciamento das comunicações, no qual deve-se determinar as necessidades de informação das partes interessadas pertinentes à riscos, tais como: quando, como e o que serão informados a elas. Os principais objetivos desse plano são: identificar todas as partes interessadas pertinentes a riscos da organização (internos e externos) (PMI 2017).

Ainda segundo o PMI (2017), faz-se necessário elaborar um registro com informações de contatos das partes interessadas, classificar qual o grau de informação necessária a cada uma, e, principalmente, qual é a meta da comunicação com cada membro desse plano.

Para Abraham *et al*. (2019), este plano deve esforçar-se para cativar a alta gerência a investir em determinadas iniciativas de segurança cibernética,

conscientizando-os sobre a importância da segurança digital, demostrando todos os perigos e consequências que um ataque pode proporcionar. Deve, ainda, esclarecer a todos os membros da organização, em todos os níveis, dos diversos cenários de ameaças à segurança digital, e como reagir a eles.

Da mesma forma, o plano de comunicação deve sempre buscar conquistar a confiança da comunidade de usuários. Deve empenhar-se em proporcionar a todos a consciência e transparência, disseminando conhecimento sobre os perigos e as consequências da cibersegurança. Também deve identificar quais os treinamentos necessários para cada membro da organização, quando serão aplicados e como serão aplicados. Com um plano de gerenciamento das comunicações bem elaborado, a organização cultivará uma cultura de transparência e confiança de todos os colaboradores. Com isso todos estarão prontos para apoiar as medidas de segurança cibernéticas quando necessárias (ABRAHAM *et al*., 2019).

Neste sentido, a organização deve disseminar o plano de gerenciamento de riscos cibernéticos à toda organização por meio de sistemas de treinamento e conscientização de segurança sempre com foco na proteção das informações e dos dispositivos médicos. Todos os colaboradores da organização devem ser instruídos sobre preocupações e políticas de segurança da informação durante a orientação e lembrados no mínimo uma vez a cada ano. Todo novo problema na segurança da informação deve ser usado como exemplo para atualização de novas lacunas nas políticas e procedimentos existentes com treinamentos atualizados para aumentar continuamente a conscientização sobre segurança. (BLANKE *et al*., 2016).

Ao treinar e qualificar os colaboradores para enfrentar os riscos, são apresentadas as culturas, normas e padrões esperados. Possibilita a mudança de atitudes inadequadas e maximiza o desenvolvimento esperado, por meio da aquisição de novos conhecimentos e habilidades (HONG *et al*., 2004).

A técnica de segurança digital mais utilizadas na literatura científica é o treinamento adequado a todos os colaboradores da organização já que a maioria das violações de segurança é causada pelo acesso a arquivos maliciosos por colaboradores durante suas atividades rotineiras (KRUSE *et al*., 2017).

De maneira geral, a segurança cibernética deve ser incorporada à cultura da organização e deve ser inerente a todos os sistemas. A segurança, que é apenas reativa e que é avaliada somente após um incidente grave, é mais cara e menos eficaz (MARTIN *et al*., 2017).

Por meio de treinamentos específicos, a organização procura aflorar nos colaboradores a conscientização sobre cibersegurança, ao mesmo tempo em que os qualificam sobre as melhores práticas no seu combate (PMI, 2017).

Neste sentido, deve-se estabelecer políticas de segurança cibernética e garantir que ela se reflita no treinamento de todos na organização. A segurança cibernética e a conscientização sobre riscos devem ser obrigatórias igualmente a outros treinamentos já consolidados na cultura das organizações como combate e treinamento à incêndio e programas de controle médico de saúde ocupacional (MARTIN *et al*., 2017).

Conforme Huang *et al*. (2014), há pouco controle e governança regulatória, para novos sistemas computacionais considerados críticos para a segurança, de novos sistemas pois são caros e relativamente lentos para serem desenvolvidos, possuindo diferentes tipos de criticidade. Pode parecer evidente que, ao construir um novo sistema computacional, as informações desses devem ser preservadas por meio de mecanismos de controle de acesso, auditorias de segurança, controles de transações, criptografia de transmissão etc. Entretanto, conforme Bojanova *et al*. (2017), os programadores realizam apenas uma análise superficial da segurança e produzem requisitos de garantia bastante genéricos.

Ao desenvolver um novo produto, os requisitos de segurança são semelhantes entre os projetos, não são investidos recursos para explorar as necessidades em diferentes níveis do produto, ou para registrar os requisitos em nível individual para cada projeto. Muitas especificações de requisitos apenas possuem um único requisito de segurança, com algum dizer como “Somente usuários autorizados podem acessar essas informações”. É indispensável explorar os riscos encontrados e as vulnerabilidades do sistema ao nível do produto, arquitetar salvaguardas especificas e testá-las em todo o seu ciclo de vida (HUANG *et al*., 2014).

Entretanto, desenvolvedores de sistemas geralmente trabalham com cronogramas desafiadores, buscando cumprir prazos cada vez menores para suprir as necessidades do mercado e evitar perder a vantagem competitiva de seus produtos. Nesse processo de desenvolvimento acelerado a segurança do sistema é subestimada e é realizado com posteriores incrementos nos sistemas, como novos recursos (HABIBZADEH *et al*., 2019).

Conforme Abraham *et al*. (2019), o setor de saúde não está despreparado para lidar com a realidade das ameaças cibernéticas atuais. Porém, o setor tem a postura de que "se não está quebrado, não há necessidade de mexer”.

Neste sentido, não há um modo 100% eficaz de impedir todas as violações de cibercriminosos, mas a cibersegurança deve fazer parte dos processos de gestão das organizações de saúde. As organizações devem sempre buscar a resiliência cibernética que é uma visão holística do risco cibernético e que analisa, entre outras coisas, a cultura, os colaboradores, os processos, bem como a tecnologia da organização (COVENTRY *et al*., 2018).

Portanto, faz-se necessária a execução de requisitos mínimos de segurança cibernética por meio de um documento institucional, composto por procedimentos e ações fundamentais que devem serem executadas caso alguma ameaça à segurança cibernética seja constatada (ONDIEGE *et al*., 2017).

Como uma das principais atitudes a serem implantadas, consta a criptografia. Trata-se de um conjunto de regras para codificar a informação para que só o emissor e o receptor consigam decifrá-la. É uma técnica ampla, já utilizada há milênios pela humanidade e que vem sendo aperfeiçoada constantemente. Na cibersegurança, utiliza-se a técnica de chaves, mais conhecidas como chaves criptográficas. É um conjunto de *bit's* embasado em um algoritmo capaz de codificar e de decodificar informações. Caso o receptor utilize uma chave diferente do emissor não conseguirá obter a informação (ZHANG *et al*., 2017).

Alguns sistemas podem ser totalmente criptografados ou isso pode ser feito em arquivos específicos. A criptografia dos dados é uma solução versátil, podendo ser aplicada a dados específicos como senhas e usuários, ou a todos os dados de um sistema (BLANKE *et al*., 2016). Segundo Braga *et al*. (2019) é fundamental que essa ferramenta seja utilizada corretamente, pois, embora a criptografia seja um componente essencial da segurança cibernética, ela é uma das ferramentas mais incompreendidas no desenvolvimento de sistemas. Seu uso incorreto pode expor armadilhas e decisões de *design* que geram uma ampla fonte de vulnerabilidades nos sistemas.

Igualmente encontrado na literatura científica é a preparação e resiliência. Elas devem ser integradas nas métricas de qualidade locais e nacionais das organizações de saúde. Caso a organização ainda não as tenha, deve-se instituir uma comissão de qualidade da segurança cibernética, para promover melhorias contínuas e

responsabilizar explicitamente os líderes locais e nacionais, quanto a não conquista dos objetivos propostos. A resiliência da organização consiste em a organização estar preparada para enfrentar as dificuldades que toda organização enfrenta durante suas operações diárias (MARTIN *et al*., 2017).

A título de exemplo, funcionários que acessam os sistemas das organizações de saúde para extrair informações confidenciais de pacientes, para lucrar com a venda dessas informações é algo recorrente. Foi até criado o termo *insider*, para definir esse tipo de crime. Contudo, uma atitude que deve ser implanta é o treinamento. É essencial que as organizações apliquem treinamentos constantes a todos os colaboradores para que eles tenham conscientização que essas violações são graves, com resultados que incluem a demissão, multas e acionamento criminal (BLANKE *et al*., 2016).

Segundo Gordon *et al*. (2019) há estratégias para atenuar o risco cibernéticos, tais como: treinamento constante, mecanismos de detecção automáticos de *e-mails* de *phishing* que atuem antes de serem entregues ou o bloqueio de contas de *phishing*, são frequentemente usadas. Entretanto, os ataques continuam sendo um risco de segurança cibernética para as organizações de saúde em todo o mundo. Para lidar com essa ameaça, organizações implantaram programas de simulação de *phishing*, nos quais os colaboradores recebem *e-mails* falsos com *phishing* para educá-los sobre esse tipo de ataque. Caso algum colaborador clique nesses *e-mails*, recebem um breve treinamento sobre as ameaças de *phishing* ao serem direcionados para uma página temática sobre prevenção a essa ameaça

A segurança digital deve ser preservada nas quatro principais dimensões: preservação dos dados, acesso e modificação dos dados, troca de dados e interoperabilidade e conformidade dos dados (NATSIAVAS *et al*., 2018).

Igualmente relatado na literatura é o *hackathon*, que é uma atividade que vem crescendo em diversos setores da economia. Segundo Abraham, *et al*. (2019), o *hackaton* é uma ação inovadora e eficaz para combater ciberataques e promover soluções inovadoras. É um evento que agrupará programadores, desenvolvedores, *designers* e profissionais ligados à tecnologia e inovação, em uma maratona, com o objetivo de desenvolver soluções para problemas desafiadores da organização. As organizações devem utilizam os benefícios do *hackathon* para ajudar nas operações de segurança para identificar vulnerabilidades. Os *hackatons* estão se popularizando como uma evolução do *brainstorming* no setor de tecnologia. Devem ser contratados

consultores para realizar ataques à rede para expor vulnerabilidades através de testes de penetração, e sanar problemas das brechas nos sistemas. Esses consultores também são denominados como *white hats* ou *Ethical Hackers* que irão penetrar nos sistemas a procura de vulnerabilidades, para que elas sejam tratadas antes de reais ataques.

Igualmente encontrado na literatura científica é o *Backup,* que é o ato de copiar os dados fora do sistema principal em um armazenamento secundário e independente, com o intuito de conservar esses dados, caso o sistema principal venha a ter qualquer adversidade. Ele precisa ser feito em uma periodicidade acordada previamente por profissionais e gestores da organização. Com o crescente número de ataques aos sistemas, o *backup* vem a ser uma das soluções mais eficazes e baratas para a proteção de informações das organizações de saúde. Entretanto é uma solução negligenciada após as primeiras práticas (KHARRAZ *et al*., 2018).

Uma outra atividade são os seguros. Para enfrentar os desafios e ameaças expostos por cibercrimes, muitas organizações estão contratando os serviços de empresas de seguros. Esse mecanismo aumenta a resiliência da organização ao transferir os riscos com cibersegurança para uma empresa especializada. O seguro é um negócio em rápido crescimento, com vendas globais de US$ 2,75 bilhões somente em 2015. Deve-se desenvolver antecipadamente ao problema padrões e soluções específicas do setor de saúde, declarar responsabilidades e governanças, e comprometer os recursos adequados para suprir a segurança adequada (MARTIN *et al*., 2017).

Também a inteligência artificial (IA) é capaz de oferecer mais eficácia em diversos setores dentro das organizações, simplificar processos melhorar o desempenho e processar uma maior quantidade de dados. Na atualidade, a grande quantidade de dados que são processados dentro e fora das organizações é imensurável. Tratar esses dados se tornou um verdadeiro garimpo para o mercado, devido a revelarem conhecimentos preciosos sobre o cliente, mercado, setor, ameaças e oportunidades (MAIMÓ *et al*., 2019).

Diante de todo esse potencial que os dados podem proporcionar, muitas instituições estão utilizando a IA para processar as informações, visto que um banco de dados sem uma ferramenta adequada para tratá-los é ineficiente. As técnicas de aprendizado de máquina representam a capacidade das máquinas aprender sem ser explicitamente programadas para desenvolver dada função. Em vez de várias linhas

de código com instruções específicas para realizar uma tarefa específica, o IA possibilita treinar o algoritmo para que ele aprenda. Esse treinamento compreende a alimentação de grandes quantidades de dados, permitindo que o algoritmo aprenda, ajuste-se e se aprimore. A IA pode ser utilizada na detecção de anomalias detectadas em comunicações de rede ou na detecção de *ransomware* espalhados pelas redes ou pelos ambientes clínicos (MAIMÓ *et al*., 2019).

Também verificado na literatura é o descarte das informações de equipamentos médicos que podem ser comprometidos se feitos sem os devidos cuidados ou pela reutilização do equipamento. O descarte eficaz de dispositivos médicos, garante que dados confidenciais coletados durante o ciclo de vida do dispositivo não sejam afetados. Se faz necessário que todos os equipamentos médicos que contenham dados armazenados sejam examinados por profissionais qualificados antes de seu descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido extraídos adequadamente (LEBEDA *et al*., 2018).

É, portanto, necessário que estes dispositivos tenham as informações apagadas, destruídas ou sobregravadas por meio de técnicas adequadas que tornem as informações confidenciais irrecuperáveis. Essa preocupação deve ser contemplada também para transferência de equipamentos entre as diversas instalações da organização (BUSDICKER *et al*., 2017).

Os métodos e locais adequados para o descarte juntamente com toda a documentação necessária, deve ser contemplado no plano de gerenciamento de riscos. Por meio de uma governança rígida. Todas essas informações e registros de controles de segurança, devem ser registradas para as devidas auditorias (BUSDICKER *et al*., 2017).

Como salientado, os dispositivos médicos vêm ganhando a cada nova geração mais funcionalidades. Com isso faz-se necessária à sua devida proteção contra-ataques cibernéticos. A Tabela 3 apresenta onze requisitos de segurança para dispositivos do setor de saúde encontradas na literatura científica.

Tabela 3 - Lista de requisitos de segurança para dispositivos médicos.

Requisitos \ Autores	Abraham *et al.* (2019)	Blanke e McGrady (2016)	Braga *et al.* (2019)	Busdicker e Upendra (2017)	Coronado e Wong, (2014)	Ghafir *et al.* (2018)	Kharraz *et al.* (2018)	Kujawski *et al.* (2010)	Kure *et al.* (2018)	Maimó *et al.* (2019)	Martin *et al.* (2017)	Mostfa Kamal *et al.* (2016)	Natsiavas *et al.* (2018)	Ondiege *et al.* (2017)	Priestman *et al.* (2019)	Primo *et al.* (2018)	PMI (2017)	Pennock *et al.* (2002)	Zhang *et al.* 2017)
Todos os dispositivos médicos devem estar devidamente inventariados.		X			X														
Todos os dispositivos devem ser protegidos com senha, protetores de tela e *logoff* automático após um período pré-determinado.		X										X							
Todos os dispositivos devem conter senhas fortes, com uma combinação de oito caracteres e dígitos. Essas senhas devem ser alteradas a cada três meses.		X										X							
Todos os dispositivos portáteis, devem criptografar seus dados. Todas as chaves usadas para criptografia e descriptografia devem ser aprovadas previamente para possuírem requisitos de complexidade.		X	X		X		X						X						X
Todos os dispositivos portáteis, devem conter limpeza remota e rastreamento de localização geográfica.		X																	
Todos os dispositivos devem ter o bloqueio ativado após três falhas de tentativas no *login*.	X	X		X			X								X				
Todos os dispositivos devem ter seus sistemas operacionais, *software* e antivírus atualizados à medida que novos lançamentos e correções estiverem disponíveis.	X	X												X		X			
Todos os dispositivos devem ter *backup* de seus dados em local seguro com uma periodicidade previamente acordada por especialistas.	X	X				X	X				X					X			
Devem serem elaborar soluções de proteção de *endpoint* impedindo ataques internos ou externos.	X																		
Todos os sistemas devem serem monitoramento constante, na busca de invasores ou malwares.	X	X						X	X								X	X	
Devem serem implantar sistemas automatizados com inteligência artificial que detectam e impeçam ataques a redes e dispositivos.	X									X									
Total	**6**	**9**	**1**	**1**	**2**	**1**	**3**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**	**1**

Fonte: Autor.

Já a Tabela 4 apresenta as melhores práticas para evitar ataques cibernéticos encontradas na literatura científica.

Tabela 4 - Melhores práticas para segurança cibernética no setor de saúde.

Requisitos \ Autores	Abraham *et al.* (2019)	Ahmed e Ahmed (2019)	Blanke e McGrady (2016)	Bojanova e Voas (2017)	Busdicker e Upendra (2017)	Coronado e Wong, (2014)	Diggans e Leproust (2019)	Gordon *et al.* (2019)	Habibzadeh *et al.* (2019)	Huang (2014)	Kuerbis e Badiei (2017)	Kruse *et al.* (2017)	Lebeda *et al.* (2018)	Maimó *et al.* (2019)	Martin *et al.* (2017)	Mostfa Kamal *et al.* (2016)	Ondiege *et al.* (2017)	Priestman *et al.* (2019)	PMI (2017)
Ao contratar um novo colaborador (mesmo para meio período), deve-se verificar os antecedentes do colaborador.			X			X		X									X		
Deve ser concedido um acesso limitado ao sistema, com base na necessidade de acesso aos colaboradores, baseadas nas funções e responsabilidade da atividade exercida do cargo.			X			X											X		
O acesso de usuários aos bancos de dados, dever ser restrito e mediante ao vínculo do acesso a informações como nome do usuário, senha, informações acessadas, local e data do acesso.	X		X													X		X	
Deve ser usado a autenticação de dois ou três fatores para acessar o sistema da organização.	X		X		X	X												X	
As atividades devem ser auditadas e revisadas frequentemente, conforme a responsabilidade do colaborador.	X		X	X	X	X			X	X	X								
Deve ser revisado os registros das gravações, de toda a infraestrutura da organização para validar o acesso e uso individual.			X																
Deve se fornecer treinamentos constantes a todos os colaboradores da organização.	X		X			X		X				X		X	X				X
Deve-se prover a conscientização dos colaboradores sobre a segurança digital constantemente.	X		X		X	X													
Deve ser retirado o acesso ao sistema e a organização dos colaboradores que se desligarem da organização.	X		X		X		X												
Deve ser comunicado o desligamento do vínculo empregatício dos colaboradores desligados da organização com os fornecedores ou parceiros apropriados.		X	X				X												
Estacionamento e todas as áreas externas da organização, deve estar devidamente iluminada no período noturno.			X																
Todos os equipamentos e documentos físicos devem ser devidamente descartados.			X		X								X						

Deve ser configurado o bloqueio do terminal a cada ausência do colaborador, por mais breve que seja a ausência.			X																
Total	**6**	**1**	**13**	**1**	**5**	**6**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**1**

Fonte: Autor.

Segundo o PMI (2017) a etapa de monitoramento e controle dos riscos é o estágio em que os riscos identificados são observados, e se investiga novos riscos e riscos residuais. Buscando sempre analisar o êxito dos processos empregados, implantando ações preventivas e corretivas quando necessário.

Nesta fase de monitoramento, a equipe envolvida na gestão dos riscos deve procurar variações do que foi planejado para combater os riscos e a sua situação (KUJAWSKI *et al*., 2010). A real dinâmica do dia a dia ou o andamento das atividades tendem a modificar a prioridade e os efeitos dos riscos agrupadas durante as fases anteriores. Portanto, faz-se necessário acompanhar os riscos diariamente procurando por desvios (PENNOCK *et al*., 2002).

Neste sentido, o monitoramento dos riscos é um processo ininterrupto. Deve-se monitorar e avaliar os riscos identificados, monitorando os riscos residuais, identificando novos riscos (PMI 2017). Deve-se, ainda, identificar caso algum novo risco seja encontrado para inclui-lo na matriz de riscos e passar por todos os processos e avaliar caso ele se concretize (BLANKE *et al*., 2016)

Deve-se monitorar ativamente todos esses riscos e criar planos para mitigá-los, ou qualquer outra solução para contra-atacá-los. Os riscos são as possíveis consequências indesejadas do sistema e podem comprometer a segurança da organização e não atender às expectativas dos atores (KURE *et al*., 2018).

Neste sentido, o processo de monitoramento dos riscos e o seu gerenciamento, são dois processos que ocorrem simultaneamente. Enquanto o processo de monitoramento está confrontando os riscos constantemente, o gerenciamento está fazendo a sua avaliação, analisando os que forem residuais e avaliando a eficácia do plano de gerenciamento de riscos constantemente (BLANKE *et al*., 2016 & PMI 2017).

Todos esses processos devem interagir entre si, criando uma sinergia na gestão contra cibercriminosos. Cada processo pode envolver o esforço de uma ou várias pessoas, de acordo com as necessidades encontradas. Embora os processos sejam apresentados como elementos distintos neste trabalho, com um

sequenciamento definido, na prática eles vão se sobrepor e interagir entre si (PMI 2017).

O gerenciamento de riscos deve ter uma abordagem de integração, com uma combinação de vários componentes interdependente. Deve incluir todas os setores da organização, principalmente os setores que são alvos de atacantes e enfrentam diferentes tipos de riscos. Uma abordagem integrativa do gerenciamento de riscos moderna, deve possuir uma avaliação constante dos riscos em potencial em todos os níveis da organização. Deve conter todos os resultados reunidos em um único documento, tais como a identificação, avaliação e gerenciamento de riscos em toda a organização. a estrutura integrada de gerenciamento de riscos deve criar uma solução holística, considerando os aspectos técnicos e não técnicos dentro de uma organização (ONDIEGE *et al*., 2017).

A conhecida sigla “KPI” *(Key Performance Indicador)*, é um Indicador-chave de desempenho estabelecido pela organização. É uma forma de medir se as ações ou um conjunto de iniciativas está efetivamente atendendo aos objetivos propostos. Ao escolher os KPI’s a organização precisa analisar a sua relevância para atingir os objetivos propostos. Indicadores mal elaborados mostram performances erradas, pode-se ter a impressão de que está indo bem, mas na verdade não está (KURE *et al*., 2018).

De acordo com Kure *et al*. (2018) as organizações de saúde devem estabelecer KPI’s conforme oito categorias demostradas no Quadro 5.

Quadro 5 - Definições sobre KPI’s para o setor de saúde.

KPI	Definição
Confidencialidade	Está diretamente relacionado a proteção dos dados do sistema. Supervisiona os dados confidenciais contra indivíduos, entidades, processos ou usuários não autorizados, através de acessos não autorizados e atacantes maliciosos.
Disponibilidade	Refere-se a garantir que os ativos da infraestrutura estejam disponibilizados e acessíveis aos usuários, conforme acordado, ou quando e onde forem necessários.
Integridade	Refere-se à capacidade dos ativos críticos das organizações de infraestrutura de executar as funções necessárias de modo eficaz e eficiente, sem pausas, interrupções ou perda de suas funções.

Resiliência	Permite que as organizações lidem com problemas, adaptando-se as mudanças, superando obstáculos e resistindo às pressões de situações adversas encontradas no dia a dia.
Reputação	Reputação é a confiança que a organização ganhou pela coletividade, é a visão que a população ou comunidade têm de uma determinada organização.
Autenticidade	É a tecnologia empregada na identificação e verificação de um usuário autorizado, tendo a capacidade de distinguir os usuários autorizados dos não autorizados.
Não Repúdio	Fornece confirmações de que uma informação é entregue aos dois pontos da comunicação, garantindo que o remetente e o destinatário não abdiquem o envio e/ou o recebimento da informação em trânsito.
Manutenção	Está associada ao tempo médio de reparo de um determinado ativo, fazendo-o funcionar corretamente dentro de um período especificado, este tempo pode ser classificado em dia, semanas, meses ou conforme análises de especialistas.

Fonte: Adaptado de Kure, Islam e Razzaque (2018).

Deste modo, conforme Ondiege *et al*. (2017), é imperativo determinar metas e os principais KPIs que Identifiquem os objetivos organizacionais e de segurança como: Confidencialidade; Integridade; Disponibilidade e Reputação.

Esses principais indicadores de desempenho executam um papel essencial no gerenciamento de riscos das instituições. Deve-se sempre executar uma análise pontuando os pontos fortes e os pontos fracos, utilizando como base as metas organizacionais (KURE, *et al*., 2018). Faz-se necessária também a identificação das principais responsabilidades operacionais da infraestrutura para apoiar as atividades de segurança cibernética (CORONADO *et al*., 2014). Esses KPIs podem-se avaliar o alcance das metas, desempenho do gerenciamento de riscos e os processos da organização, além de permitir identificar avanços e necessidade de correções e ajustes (ABRAHAM *et al*., 2019).

Uma ferramenta tradicional, mas não muito sofisticada é o ciclo PDCA, acrônimo de *plan*, *do*, *check* e *act*. Ela é utilizada como um ciclo que garante excelência em seu uso buscando sempre a cada novo ciclo uma melhoria constante. A fase de planejamento possibilita explorar informações permitindo definir metas e ações para alcança-los. Já a fase de execução é a que coloca em prática o que foi planejado.Já a fase de checar compreende basicamente em comparar o que foi planejado com o que foi executado, procurando sempre desvios entre esses dois

elementos. Na etapa de ação do ciclo PDCA, os atores envolvidos implantam as ações corretivas caso aquelas adotadas não foram suficientes, se os dados levantados foram exíguos ou insuficientes ou as circunstâncias mudarem. E reutilizar/padronizar as atividades que tiveram o êxito planejado, garantindo uma máxima eficácia e eficiência. Na etapa de ação também deve-se disseminar os resultados obtidos na implantação nessa fase do ciclo, e estabelecer o que deu certo e o que pode ser melhorado para o início de um novo ciclo, buscando sempre uma melhoria contínua a cada aplicação do ciclo PDCA (VENKATRAMAN, 2007; MAAS; RENIERS, 2014; SILVA *et al*., 2017).

Neste sentido, os indicadores de resultados irão notificar as ações eficientes a partir da revisão das informações e padrões pré-estabelecidos, e o que está se caracterizando como ineficiente, possibilitando o devido ajuste do percurso para realinhar as estratégias e iniciando um novo ciclo dentro do sistema (MAAS & RENIERS 2014). Com a utilização dessa fase é possível corrigir o que não está sendo efetivo, determinar as causas raízes de problemas e a aplicação de ações para eliminar o que não está funcionando (BOZICKOVICI *et al*., 2012).

Ter uma postura proativa e não reativa, deve ser uma prática de gestão de todos os setores das instituições de saúde. Os danos causados às organizações podem ser extremamente prejudiciais ao funcionamento diário, como ser um golpe catastrófico à imagem da instituição. Portanto, se faz necessário possuir respostas corretas, possuir dados precisos e ser rápido no enfrentamento de uma crise cibernética. Com essas medidas, pode-se reverter uma situação de crise e minimizar seus danos (MARTIN *et al*., 2017).

O plano de gerenciamento de riscos deve ser utilizado, caso um risco já previamente identificado se torne real. As respostas já previamente elaboradas devem ser colocadas em prática para minimizar os danos. Eventos assim exigem decisões rápidas. Com isso faz-se necessário que as respostas sejam disponíveis e que todos os responsáveis por ela estejam cientes e preparados para tomar as ações necessárias (MARTIN *et al*., 2017).

Deste modo, Martin *et al*. (2017) elencam alguns itens que deve fazer parte dos planos de gerenciamento de riscos, conforme mostra o Quadro 6.

Quadro 6 - Elementos do plano de gerenciamento de riscos

Item	Descrição
1	Estabelecer os membros da equipe que irão integrar o comitê de crise, para serem acionado quando ocorrer um evento de risco
2	Documentar todos as respostas aos riscos identificados
3	Indicar o porta-voz em caso de crise, com o treinamento adequado em (*média training)*
4	Dispor de uma lista de contatos-chave de emergência, para serem localizados com rapidez, a qualquer hora em qualquer dia
5	Estabelecer um ponto de encontro de emergência padrão, para os envolvidos saberem onde devem ser agrupados
6	Estabelecer processos de simulação e testes para avaliar antecipadamente a eficácia do plano de gerenciamento de crises e atualizá-lo constantemente

Fonte: Adaptado de Martin *et al*. (2017).

Conclui-se que, no cenário atual, as informações ou “boatos” circulam em uma alta velocidade, e qualquer boato é capaz adquirir proporções inestimáveis. Consequentemente, o porta-voz que representa a organização deve estar devidamente preparado para enfrentar essa situação e compreender quais informações devem serem passadas à imprensa. Todos os envolvidos devem ter acesso ao plano de gerenciamento de riscos para identificar o processo de avaliação do incidente com sua potencial gravidade (MARTIN *et al*., 2017).

O próximo tópico demostra os principais modelos encontrados na literatura científica que inspiraram o modelo teórico-prático desenvolvido nesta dissertação.

2.4 MODELOS DE GESTÃO DE RISCOS DE CIBERSEGURANÇA NO SETOR DE SAÚDE

Diversas abordagens ou modelos de sistemas cibernéticos para cibersegurança em saúde foram encontradas na literatura científica, cujos critérios de busca e seleção estão descritos no Capítulo 3 - Métodos. Como resultado foram identificadas cinco principais modelos na revisão sistemática da literatura, que são descritas a seguir.

2.4.1 Modelo de treinamento *Anti-Phishing*

O modelo de treinamento *anti-phishing* foi proposto por Gordon *et al*. (2019). Ele afirma que a cibersegurança é um elemento cada vez mais importante nas organizações de saúde e que um dos principais meios de ataque tem sido o *phishing*, o qual influencia pessoas a divulgar informações confidenciais por meios enganosos.

Nesta sistemática é elaborado um modelo de treinamento para as organizações se blindarem contra esse tipo de ataque. Ele baseia-se no envio de *e-mails* falsos que simulam um ataque de *phishing* real. Os colaboradores que forem descuidados com esse tipo de *e-mail* imediatamente são encaminhados para um portal que informa sua ação e sua inscrição em um curso de conscientização para prevenir futuros problemas.

O modelo de treinamento sugerido dispõe de três etapas distintas: a) visão geral do *phishing*, em que é mostrado o conceito do que é *phishing*; b) os cenários de ataque do *phishing,* em que são demostrados os meios mais habituais de se atacar, e c) a identificação de análise de *phishing* em que são demostrados os malefícios causados à organização por esse tipo de ataque.

Após a conclusão do curso, os colaboradores são encaminhados para realizar um teste com dez questões pertinentes ao curso, conforme sintetizado no Quadro 7.

Quadro 7 – Questões pertinentes após o treinamento anti *phishing*

Descrição	**Exemplo**
Seção 01 Visão geral do *phishing*	Definição de engenharia social, anatomia de um *e-mail* de *phishing, d*emonstração de um ataque de *phishing*, impactos do *phishing,* como reportar um e-mail de *phishing*
Seção 02 Cenário de *phishing*	Identificação do alvo, estabelecendo a isca, fisgando o alvo, infecção em massa, comprometimento dos dados e consequências de um ataque de *phishing*
Seção 03 Identificação de *phishing*	Exemplos interativos de *e-mail* de *phishing*
Exame de verificação	10 questões

Fonte: Gordon *et al*. (2019).

Entretanto, conforme Gordon *et al*. (2019) os dados apresentados mostram que, mesmo depois de várias rodadas de treinamento, por um mesmo colaborador, ele acaba sendo sugestionado a clicar novamente, por curiosidade, nesse *malware.*

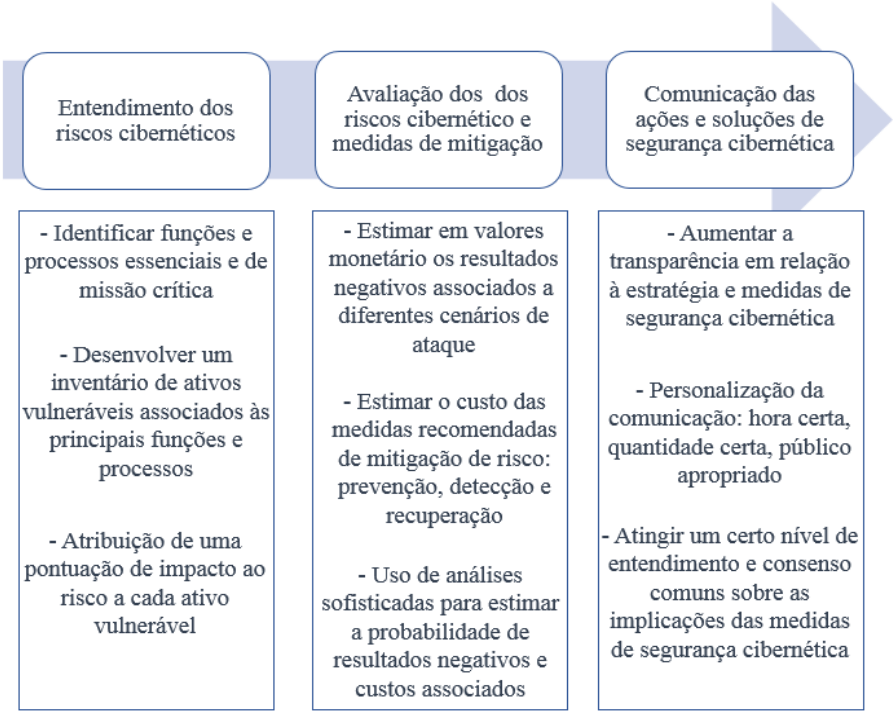
2.4.2 Modelo de gerenciamento de riscos de segurança cibernética em três etapas

Conforme Abrahan *et al*. (2019), o setor de saúde dos Estados Unidos não está preparado para enfrentar as atuais ameaças cibernéticas. A digitalização dos sistemas de saúde, por meio de sua interconectividade, torna o setor suscetível a vários *malwares*.

Segundo Abrahan *et al*. (2019) que foram os idealizadores deste modelo, ele está ancorado no equilíbrio, apresentando uma abordagem sistemática e holística para entender, avaliar e mitigar os riscos de cibernéticos.

O modelo proposto é dividido em um processo composto por três etapas. A primeira é fundamentada no aprofundamento para o entendimento dos riscos cibernéticos na organização. A segunda é composta pela avaliação dos riscos cibernéticos identificados na etapa anterior e por medidas de mitigação contra os riscos. A terceira e última fase é composta pela comunicação das ações e soluções encontradas para combater os riscos de segurança cibernética. A Figura 3 sintetiza todos os componentes dentro de cada uma das etapas:

Figura 3 - As três etapas do modelo proposto

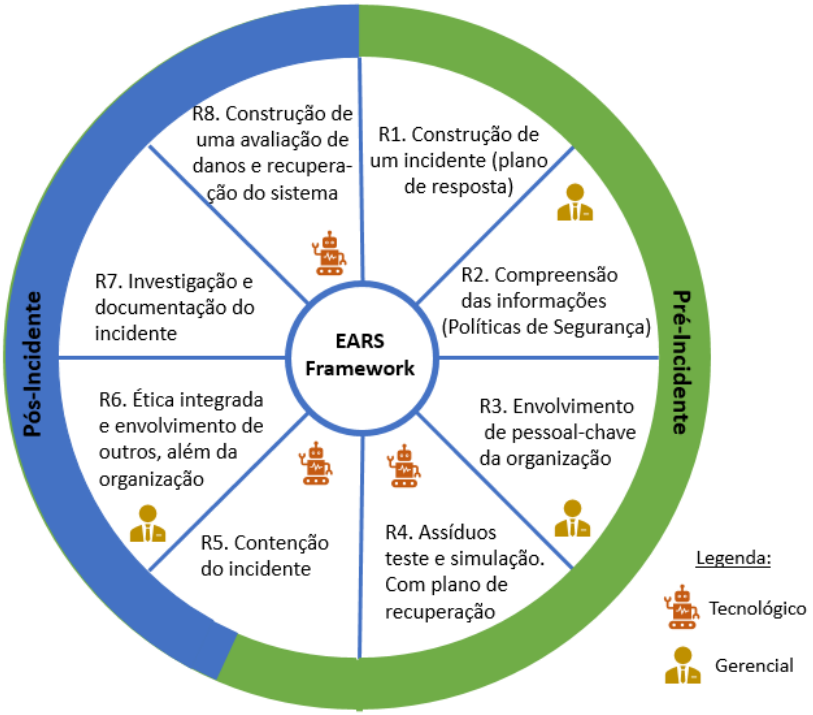


Fonte: Abrahan *et al*. (2019)

2.4.3 Modelo das oitos estratégias agregadas de resposta (EARS)

Conforme Jalali *et al*. (2019), idealizadores do modelo das oito estratégias agregadas de resposta (EARS), as organizações do setor de saúde são cada vez mais afetadas pela falta de segurança cibernética. Essa falta de segurança causa muitos efeitos deletérios em todos os setores das organizações. Por isso elas devem estabelecer respostas efetivas a esses males a fim de evitar prejuízos financeiros e principalmente a imagem das organizações. É sugerida uma estrutura de oito estratégias de resposta agregada EARS para incidentes cibernéticos, conforme Figura 4.

Figura 4- Modelo EARS



Fonte: Jalali *et al*. (2019).

Essas oito estratégias foram estruturadas em duas fases de respostas: pré-incidente e pós-incidente. E duas categorias de respostas: respostas de componentes tecnológicos e resposta de componentes gerenciais. Com um ciclo de oito passos a serem seguidos para enfrentar os desafios de manter as organizações protegidas de ataques. O Quadro 8 sintetiza o modelo proposto.

Quadro 8 – Etapas da EARS no combate a incidentes cibernéticos em organizações de saúde

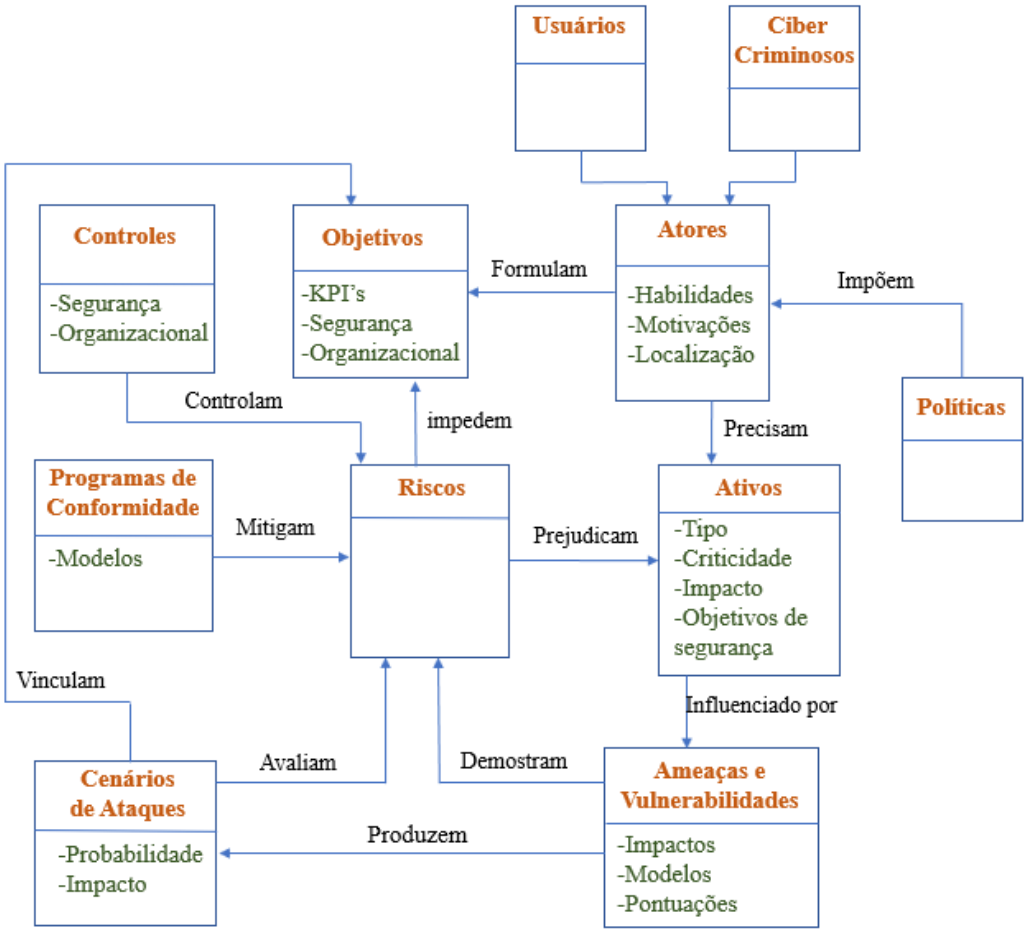
Etapa	Detalhe
R1	Um plano de resposta a incidentes deve ser elaborado antes de um incidente e deve incluir: Proteger toda a instituição. Possuir mecanismos de detecção. Métodos de investigação, por exemplo análise forense. Métodos corretivos para mitigação de danos e incidentes. Processos de contenção, entre outros.
R2	As políticas de segurança da informação são mostradas como tendo as seguintes efeitos se implementados antes de um incidente: Incentivar a notificação de incidentes e Incentivar a notificação da gravidade dos incidentes.
R3	As pessoas interessadas devem ter uma sólida compreensão dos seguintes itens antes de um incidente: A natureza crítica do incidente, os efeitos dos incidentes nas atividades diárias, os danos a imagem e reputação devido ao incidente entre outros.
R4	As rotinas de testes regulares antes de um incidente devem conter: *Backups e f*erramentas e processos restauradores.
R5a	Conter o incidente e evitar a propagação com as seguintes ações: seccionação da rede médica e hospitalar por prioridade e complexidade e inspeção dos dispositivos antes da nova conexão
R5b	Contenção do incidente e propagação adicional com as seguintes ações: desligar todos os dispositivos infectados, desconectar todos os dispositivos infectados da rede, desabilitar as funcionalidades de rede sem fio dos sistemas infectados e desligar toda a rede se houver uma ampla disseminação do ataque.
R6	A resposta ao incidente deve ser capaz de sustentar os seguintes valores éticos: preocupação com o bem-estar das pessoas, comunicação organizacional interna apropriada, notificação de todos os membros afetados pela violação, práticas de negócios assertivas, contato e envolvimento do pessoal chave entre outros.
R7	Medidas investigativas para um incidente devem incluir: proteger qualquer evidência encontrada, análise forense do incidente por um especialista, documentação de toda resposta.
R8	Algoritmos de avaliação dos danos, com a capacidade de: realização de ações sequenciais, recebimento de um conjunto de transações maliciosas de um IDS, seleção dos ID's mínimo de conexão, análise do sistema para encontrar alterações de dados entre outros.

Fonte: Jalali *et al*. (2019).

2.4.4 Modelo de gerenciamento integrado de riscos cibernéticos

Esse modelo proposto por Conforme Kure *et al*. (2018), compreende um conjunto de conceitos essenciais juntamente com suas relações para alcançar o gerenciamento de risco em segurança cibernética. A Figura 5 sintetiza essa relação entre os conceitos.

Figura 5 - Metamodelo de relação entre conceitos de segurança cibernética.



Fonte: Kure *et al*. (2018).

Segundo Kure *et al*. (2018), os usuários e os cibercriminosos são dois conjuntos paralelos, que mesmo não se comunicando, estão no mesmo nível de classificação, podendo ser representado por um usuário. Cada um desses diversos atores tem seus próprios objetivos estratégicos específicos, dentro de seu próprio ambiente organizacional, executando assim atividades específicas.

Ainda segundo seus idealizadores, as metas são os objetivos gerais de um ator. Essas metas apoiam os interesses e garantem a continuidade dos negócios. Muitas dessas metas são fundamentadas em KPIs, segurança e objetivos organizacionais. Com base nos KPIs os atores da organização irão planejar suas ações.

Os riscos são os resultados indesejados. Embora eles sejam inevitáveis nas organizações, é responsabilidade dos atores garantir que os riscos sejam controlados para atingir as metas. Deve-se identificar todos os riscos possíveis, e elaborar

respostas a eles, tais como: mitigação, planos de respostas ou qualquer outra solução para contra-atacá-los.

Os ativos podem ser: pessoas, serviços, instalações, processos, procedimentos, equipamentos etc. Podem ser elementos tangíveis ou intangíveis, necessários e com valor para a organização. A identificação dos principais ativos e a valorização dos principais é um importante processo. Os ativos podem ser classificados quanto a sua criticidade e sua categoria. As criticidades são associadas à degradação ou perda de um ativo, sendo o principal indicador das organizações para determinar qual ativo tem mais valor para a continuidade dos negócios. A categoria classifica os ativos de acordo com seu nível de sensibilidade e requisitos de segurança. A criticidade de uma categoria de ativo pode ser elencada por exemplo como alta, média ou baixa.

Controle é a proteção ou conjuntos de proteções ou contramedidas em segurança cibernética, para impedir ou minimizar a segurança dos riscos na organização. Os controles são mecanismos usados para fornecer segurança. São a combinação de técnicas e controles para impedir ameaças e vulnerabilidades.

Os programas de conformidade são conjuntos de requisitos projetados para proteger as organizações com a criação de modelos a serem seguidos.

Os cenários de ataques cibernéticos são um evento que leva a um impacto negativo nos ativos da organização. Há alguns componentes que irão determinam um ciberataque em uma organização, tais como: tipos de ameaças, habilidade, capacidade e localização do ator, ativos, eventos e tempo. É necessário que as organizações desenvolvam vários resultados possíveis para aumentar sua capacidade de se proteger contra-ataques cibernéticos.

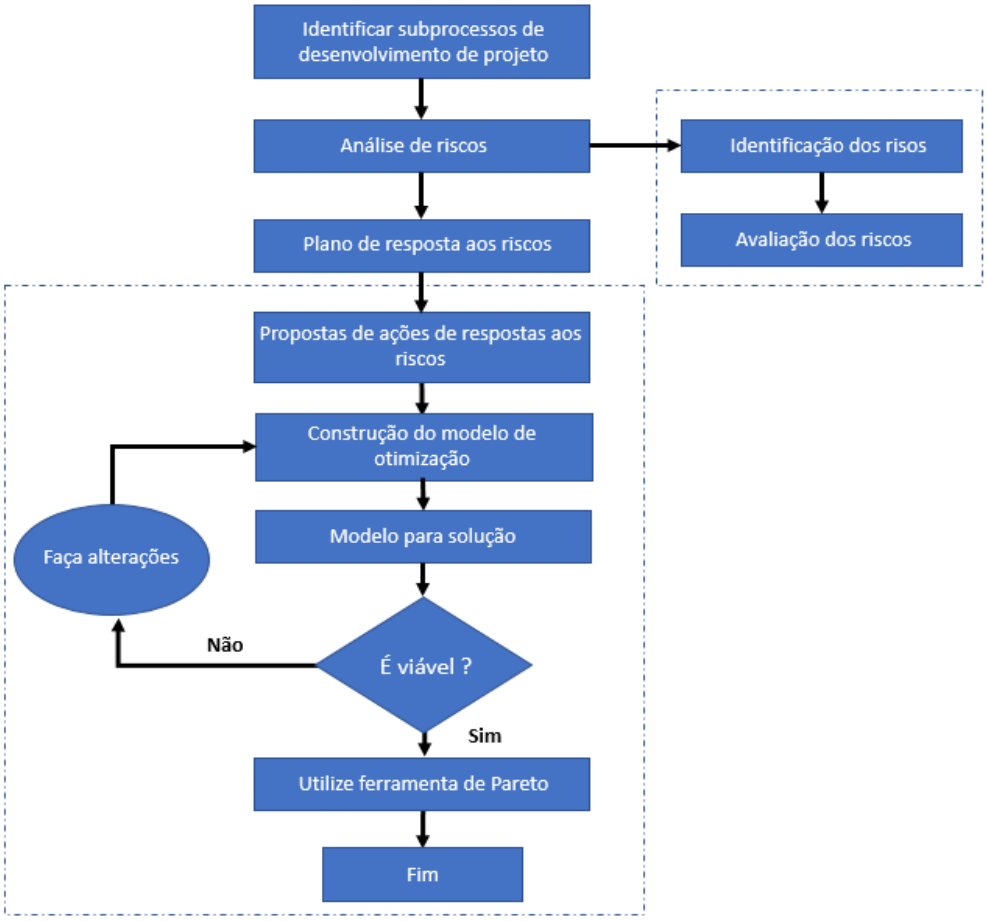
As políticas são os princípios que norteiam as ações das organizações. Há várias políticas de segurança cibernética, tais como: controle de acesso, *backup*, treinamento etc.

Ameaças e vulnerabilidades são as fraquezas de um programa de segurança da organização que é explorado por uma ameaça de obter acesso não autorizado a um ativo em que há três propriedades, ou seja, impacto, tipo e pontuação de peso.

2.4.5 F*ramework* para gerar respostas ao plano de gerenciamento de riscos

Segundo WU *et al*. (2018), o *framework* proposto fornece um fluxograma que demostra sistematicamente um sequenciamento para produzir um plano de resposta a riscos. O modelo baseia-se nas atividades em paralelo de: analisar, identificar e avaliar os riscos, passando para as etapas de: criação de um plano, propostas e modelos para tratar os riscos. Sequencialmente é feita uma análise para averiguar o êxito da solução. Ainda segundo seus idealizadores, esse ciclo é repetido para todos os riscos identificados, na busca de respostas adequadas para o devido tratamento dos riscos. A Figura 6 demostra o *framework* proposta pelo autor.

Figura 6 - *Framework* para gerar respostas ao gerenciamento de riscos



Fonte: WU, *et al*. (2018).

O próximo tópico, apresenta um resumo dos cinco principais modelos e conceitos apresentados por este estudo.

2.4.6 Síntese dos modelos e conceitos observados na literatura científica.

No desenvolvimento dessa dissertação foram encontrados diversos modelos na literatura científica e incluído cinco sistemáticas que formam a base dos modelos destes estudos. A Tabela 5, apresenta uma síntese desses modelos.

Tabela 5 – Síntese dos modelos observados na literatura científica.

Itens \ Autores	Gordon *et al.* (2019)	Abrahan *et al.* (2019)	Jalali *et al.* (2019)	Kure *et al.* (2018)	WU, *et al.* (2018)
Quantidade de etapas do modelo	**3**	**3**	**2**	**2**	**2**
Cibersegurança é um item primordial	x	x	x	x	x
Modelo utiliza treinamentos	x			x	
Modelo procura blindar a organização	x	x	x	x	x
Modelo possui uma visão geral do problema	x	x	x	x	x
Modelo inclui Disseminação das ações para toda equipe		x	x	x	
Modelo utiliza *Framework*					x
Modelo utiliza organograma				x	
Modelo em etapas circular			x	x	x
Modelo em etapas unidirecionais	x	x			
Total	**5**	**5**	**5**	**7**	**5**

Fonte: Autor.

A Tabela 6, demostra os autores que contribuíram com cada uma das quatorze etapas que compõem a estrutura teórica desenvolvida nessa dissertação e será demostrada no próximo capítulo, conforme a legenda utilizada nas colunas na tabela: **A=** Produzir o plano de gerenciamento dos riscos; **B=** Definir e entender o que são riscos cibernéticos; **C=** Identificar os riscos cibernéticos; **D=** Avaliar os riscos cibernéticos; **E=** Analisar a probabilidade e impacto dos riscos cibernéticos; **F=** Classificar os riscos cibernéticos; **G=** Conceber respostas aos riscos cibernéticos; **H=** Disseminação do plano de gerenciamento de riscos; **I =** Treinamento e qualificação; **J=** Adequar a organização com as ações de riscos acordadas; **L=** Execução de requisitos de sistemas *cyber* no setor de saúde; **M=** Monitorar os riscos cibernéticos; **N=** Verificação dos riscos cibernéticos residuais; **O=** Implantação de ações corretivas a ameaças encontradas.

Tabela 6 – Autores que contribuíram para a estrutura teórico-prática

Etapa / Autores	A	B	C	D	E	F	G	H	I	J	L	M	N	O
Abraham *et al*. (2019)	X	X	X	X	X	X		X		X	X		X	
Blanke *et al*. (2016)	X			X	X		X	X			X	X	X	
Bobbio *et al*. 2001				X	X									
Bojanova *et al*. (2017)										X				
Bozickovici *et al*. (2012)														X
Braga *et al*. (2019)											X			
Bubnov *et al*. (2015)					X									
Busdicker *et al*. (2017)	X	X	X								X			
Coronado *et al*. (2014)	X	X	X			X					X		X	
Coventry *et al*. (2018)										X				
Dandage *et al*. (2018)			X											
Dugan *et al*. 1992				X										
Gordon *et al*. (2019)											X			
Habibzadeh *et al*. (2019)										X				
Hong *et al*. (2004)									X					
Huang *et al*. (2014)										X				
ISO 31000 (2018)		X												
Kharraz *et al*. (2018)											X			
Kruse *et al*. (2017)									X					
Kure *et al*. (2018)	X	X	X	X	X	X						X	X	
Kwak *et al*. (2004)				X										
Lebeda *et al*. (2018)											X			
Maas *et al*. (2014)														X
Maimó *et al*. (2019)											X			
Mansoorzadeh *et al*. (2014)				X										
Marosin *et al*. (2014)	X				X									
Martin *et al*. (2017)	X								X		X			X
Natsiavas *et al*. (2018)		X	X								X			
Ondiege *et al*. (2017)	X	X									X		X	
PMI (2017)	X	X	X	X	X	X	X	X				X	X	
Silva *et al*. (2017)														X
Tah *et al*. (2000)						X								
Ward *et al*. (2008)		X												
Wu *et al*. (2018)			X	X			X							
Zhang *et al*. (2017)											X			
Total	**9**	**9**	**8**	**9**	**7**	**5**	**3**	**3**	**3**	**5**	**13**	**3**	**6**	**4**

Fonte: Autor.

O próximo capítulo irá demostrar a estrutura teórico-prática desenvolvida por este dissertação.

3. ELABORAÇÃO DA ESTRUTURA TEÓRICO-PRÁTICA

Neste capítulo, são apontadas as inspirações, fundamentações e conceitos teóricos referentes ao desenvolvimento da estrutura teórico-prática desenvolvida para gestão de riscos de cibersegurança para instituições de saúde do Brasil, com o objetivo de auxiliar a gerência dessas instituições a identificar, avaliar, responder e monitorar os riscos de cibersegurança que estas instituições estão expostas.

Deste modo, a estrutura de gerenciamento de risco proposta procura gerar uma condução bem-sucedida por meio de vários fatores, que aproximam as organizações a atingirem os objetivos de cibersegurança pretendidos. A estrutura teórico-prática desenvolvida, proporciona uma ferramenta de gestão de riscos cibernéticos por meio de elementos essenciais encontrados na literatura científica, com seu arcabouço inspirado na técnica do ciclo (*plan*) planejar, (*do*) aplicar, (*check*) verificar e (*action*) agir, mais conhecida pela sigla (PDCA). Conforme Nidd *et al*. (2016), a utilização dessa técnica proporciona soluções expressivas para as organizações que a empregam.

A utilização do ciclo PDCA pode se converter em uma ferramenta relevante para auxliar as instituições de saúde do Brasil a combaterem as atuais ameaças cibernéticas que estas instituições estão expostas. Desta forma, segundo Nidd, Thorn e Porter (2016); Venkatraman (2007); Maas e Reniers (2014); Silva *et al*. (2017) e Bozickovici *et al*. (2012) a técnica do ciclo PDCA é uma das ferramentas mais poderosas na *Total Quality Management* (TQM) – gestão da qualidade total – utilizada para se obter controle e melhorias contínuas em processos e produtos.

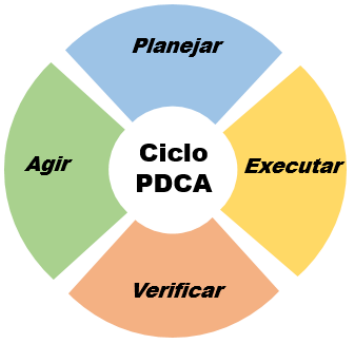
O ciclo PDCA, foi concebida em 1930 por Walter A. Shewhart, cujos conceitos foram ampliados por William Edward Deming em 1950 na utilização do conceito na restruturação de empresas japonesas no pós segunda guerra, oportunidade na qual o ciclo PDCA também ficou conhecido como Ciclo de Deming (SILVA *et al*., 2017).

Ainda segundo Silva *et al*. (2017), a princípio, o ciclo PDCA foi empregado para fiscalizar a qualidade de produtos, porém foi observada sua potencialidade como uma técnica para desenvolver melhorias contínua em processos. Em outras palavras, o ciclo PDCA almeja melhorar produtos ou processos, sendo uma ferramenta simples, porém eficaz.

Essa ferramenta é figurada muitas vezes como uma filosofia na busca de sempre estar melhorando a cada nova aplicação de um ciclo, produzindo evolução e melhorias constantes (BOZICKOVICI *et al*., 2012).

A Figura 7, demostra graficamente a divisão do ciclo PDCA nas suas quatro fases.

Figura 7, Representação gráfica do ciclo PDCA.



Fonte: Autor.

A Tabela 7, traduz uma análise dos elementos básicos necessários para cada fase do ciclo PDCA encontrados na literatura científica.

Tabela 7 - Elementos básicos do ciclo PDCA encontrados na literatura.

Atividade / Autor	Jones *et al.* (2010)	Soković *et al.* (2009)	Lupan *et al.* (2005)	Matsuo e Nakahara (2013)	Wang *et al.* (2018)	**Total**
Planejar						
1) Identificar os problemas;	x	x		x	x	**4**
2) Avaliar as causas dos problemas;	x			x		**2**
3) Criar metas realistas;			x	x		**2**
4) Elaborar planos de ações realistas.			x			**1**
Executar						
1) Capacitação da instituição e dos colaboradores para alcançar as metas estabelecidas na fase anterior;	x		x	x	x	**4**
2) Executar o plano de ação desenvolvido na fase anterior.					x	**1**
Verificar						
1) Checar se o plano de ação está sendo executado de acordo com o planejado;	x	x		x		**3**
2) Verificar se os resultados são satisfatórios.		x	x		x	**3**

Agir						
1) Correção do que deu errado;	x					1
2) Padronização do que deu certo;		x	x			2
3) Compartilhamento do aprendizado;	x					1
4) Reiniciação de um novo ciclo.			x	x		2

Fonte: Autor.

Por consequência, a Tabela 8, apresenta as principais armadilhas encontradas na literatura científica em relação a utilização do ciclo PDCA, que devem ser evitadas para se extrair melhores resultados com a aplicação desta técnica.

Tabela 8 - Principais armadilhas na utilização do ciclo PDCA encontradas na literatura

Atividade / Autor	Jones *et al.* (2010)	Soković *et al.* (2009)	Lupan *et al.* (2005)	Matsuo e Nakahara (2013)	Wang *et al.* (2018)	**Total**
Planejamento						
1) Não encontrar a causa raiz do problema;				x	x	2
2) Definir metas sem planos para alcançá-lo;	x					1
3) Definir metas irreais.			x			1
Execução						
1) Executar sem o devido planejamento;	x		x	x	x	4
2) Não capacitação da equipe;		x				1
3) Não capacitação da organização;					x	1
4) Não disseminar corretamente o que precisa ser feito.		x				1
Verificação						
1) Executar e não checar;					x	1
2) Não reportar os indicadores as partes interessadas.			x			1
Ação						
1) Não corrigir o que está errado;	x				x	2
2) Não padronizar ações eficazes;			x			1
3) Completar o ciclo PDCA apenas uma única vez.	x				x	2

Fonte: Autor.

Na sequência, serão apresentados os quatorze elementos essenciais encontrados na literatura científica que compõem as quatro fases da estrutura teórico-

prática aqui proposta, desenvolvendo um plano de gerenciamento de riscos cibernético completo para instituições de saúde do Brasil.

3.1 FASE 1 – ELABORAÇÃO DO PLANO DE GERENCIAMENTO DE RISCOS

A estrutura teórico-prática foi desenvolvida e estruturada em quatro fases distintas, porém entrelaçadas. A **Fase 1** denominada **Elaboração do Plano de Gerenciamento de Riscos,** é a fase em que são planejadas, analisadas e definidas as ações que devem ser exercidas para combater os riscos cibernéticos na instituição de saúde.

De acordo com a literatura científica, um plano de gerenciamento de riscos é uma das melhores soluções para combater as atuais ameaças cibernéticas (BUSDICKER *et al*., 2017; ABRAHAM *et al*., 2019; MAROSIN *et al*., 2014; ONDIEGE *et al*., 2017; PMI, 2017; KURE *et al*., 2018; NATSIAVAS *et al*., 2018 e WARD & CHAPMAN, 2008).

Nesta fase são estabelecidos os objetivos e metas com a criação e elaboração de caminhos e soluções para atingi-los (BUSDICKER *et al*., 2017). Todo esse planejamento é fundamentado com a visão, missão e valores da organização (ABRAHAM *et al*., 2019). Todas as etapas a seguir estão conectadas, sendo cada uma complementar a outra.

Na **Etapa 1**: intitulada **Produzir o Plano de Gerenciamento dos Riscos,** é responsável por documentar, definir, ordenar, integrar e coordenar todos as ações para proteger a organização contra os crimes cibernéticos (BUSDICKER *et al*., 2017).

São utilizadas três entradas:

1) *Políticas organizacionais*, que são guias, orientações, diretrizes, regimentos e regras que direcionam a organização (ABRAHAM *et al*., 2019).

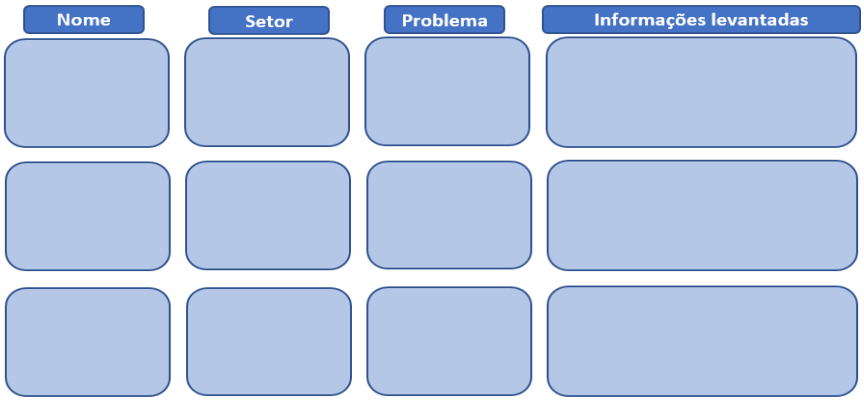
2) *Fatores ambientais da organização*, que é o levantamento das crenças e expectativas da organização mediante aos riscos cibernéticos (PMI, 2017).

3) *Ativos de processos organizacionais*, que é o levantamento de todos os documentos, contratos, declaração e processos que vigoram na organização (PMI, 2017).

São empregadas quatro ferramentas & técnicas:

1) *Opinião de especialistas*, que é proporcionada por pessoas, grupos ou instituições que têm treinamentos, conhecimentos, habilidades ou experiência especificas sobre o risco da organização (ONDIEGE *et al*., 2017). Serão levantadas as opiniões dos especialistas referentes a proteção cibernética da instituição e compiladas no banco de dados conforme demostrado na Figura 8.

Figura 8 - Compilação da opinião dos especialistas da instituição

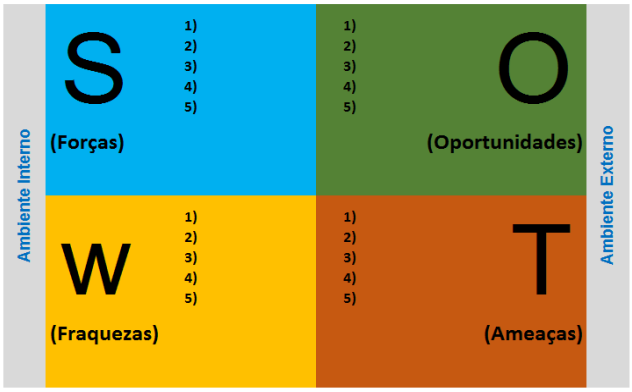


Fonte: Adaptado de PMI (2017).

2) *Análise SWOT:* utilizada para identificar os pontos fortes, os pontos fracos, as oportunidades e ameaças referente aos riscos cibernéticos da organização (HELMS & NIXON, 2010).

A Figura 9 demostra um modelo da *análise SWOT*.

Figura 9 - Análise das Forças, Fraquezas, Oportunidades e ameaças da instituição.



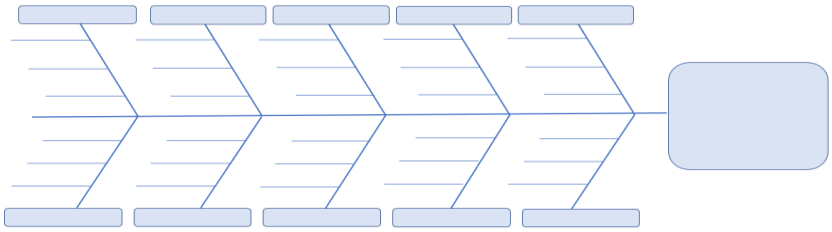
Fonte: Adaptada de Helms e Nixon (2010).

3) *Técnicas de diagramas*, são utilizadas três diagrama básicos como: *diagrama de causa e efeito,* para expor causas e os efeitos dos riscos identificados

(ANDERSSON *et al.*, 2002). *Fluxograma,* para diagramar e representar de forma esquemática elementos que compões os riscos identificados (PMI 2017) e o *diagrama de Pareto,* para priorizar ações que apresentem um melhor efeito a respeito dos riscos cibernéticos (KAYNAK, 2003).

Serão utilizadas técnicas de diagrama, como o *diagrama de causa e efeito* demostrado na Figura 10.

Figura 10 - Diagrama de causa e efeito



Fonte: Adaptada de Kaynak (2003).

4) *Revisão de documentações*, é fundamental para analisar se toda as informações referentes aos riscos cibernéticos foram analisadas e documentas adequadamente (PMI, 2017).

Obtém-se como saída dessa etapa:

O *plano de gerenciamento dos riscos cibernéticos*, que é um documento técnico composto da base é fundamentações para gerenciar todas as demais fases da estrutura teórico-prática, que será utilizado por todos as demais etapas (MARTIN *et al.*, 2017).

Na **Etapa 2,** denominada **Definir e Entender o que são Riscos Cibernéticos,** são estabelecidas fundamentações básicas entre toda a equipe de gerenciamento de riscos cibernéticos buscando um devido alinhamento entre toda a equipe (KURE *et al.*, 2018). Deve ser alinhada a tolerância e o apetite dos riscos da organização (PMI, 2017). Deve-se entender: o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico e competitivo da organização (KURE *et al.*, 2018). Em suma, deve-se alinhar, estabelecer e interpretar os riscos organizacionais, decifrando sua extensão e impacto na organização (CORONADO & WONG, 2014). Além de estabelecer a equipe e as atribuições de cada colaborador.

São utilizadas duas entradas:

1) *Nível e tolerância e aceitação dos riscos da organização*, que é o grau, quantidade e nível de um determinado risco que a organização está predisposta a aceitar (PMI, 2017).

2) *Plano de gerenciamento dos riscos cibernéticos*, que fomenta essa etapa alinhando todos com o entendimento mais profundo sobre os riscos cibernéticos.

São empregadas duas ferramentas & técnicas:

1) *Opinião dos especialistas*, que é proporcionada por pessoas, grupos ou instituições que têm treinamentos, conhecimentos ou habilidades especificas sobre o risco em questão (ONDIEGE *et al*., 2017). O objetivo é alinhar com todos os membros da equipe o que será considerado como riscos e o que não será aplicado como ameaça.

2) *Reuniões*, o objetivo dessa ferramenta é discutir e regrar o que será tolerado e combativo referente ao tratamento dos riscos cibernéticos. Quem serão a equipe que irá desenvolver o plano de gerenciamento dos riscos e quais papéis cada colaborador irá desempenhar no processo (PMI, 2017).

Obtém-se como saída dessa etapa:

O *registro dos riscos cibernéticos*, detalhando todos os riscos identificados, incluídos, excluídos, categoria, causas etc.

Na **Etapa 3,** denominada **Identificar os Riscos Cibernéticos,** busca-se a identificação e catalogação de todos os riscos cibernéticos em um documento próprio para sua apropriada análise e tratamento (WU *et al*., 2018). Deve-se utilizar um indicador único para cada risco, agrupando-o de acordo com sua categoria (KURE *et al*., 2018). Deve-se Identificar, discernir, diferenciar e documentar todos os riscos cibernéticos da organização (ABRAHAM *et al*., 2019).

São utilizadas quatro entradas:

1) *Plano de gerenciamento dos riscos*, é a criação do documento composto por uma descrição da situação da organização em referência aos riscos cibernéticos e todas as medidas para monitorá-lo, controlá-lo extingui-lo etc. (BUSDICKER *et al*., 2017).

2) *Políticas organizacionais*, é o levantamento das diretrizes, regimentos e regras que orientam as ações da organização. São baseadas nos objetivos da organização em atingir suas metas (DANDAGE *et al*., 2018).

3) *Fatores ambientais da organização*, que é o levantamento das crenças e expectativas da organização mediante aos riscos cibernéticos (PMI, 2017).

4) Ativos de processos organizacionais, que é o levantamento de todos os documentos, contratos, declaração e processos que vigoram na organização (PMI, 2017).

São empregadas quatro ferramentas e técnicas:

1) *Técnicas de diagramas*, são utilizadas três diagrama básicos como: *diagrama de causa e efeito,* para expor causas e os efeitos dos riscos identificados (ANDERSSON *et al.*, 2002). *Fluxograma,* para diagramar e representar de forma esquemática elementos que compões os riscos identificados (PMI, 2017) e o *diagrama de Pareto,* para priorizar ações que apresentem um melhor efeito a respeito dos riscos cibernéticos (KAYNAK, 2003).

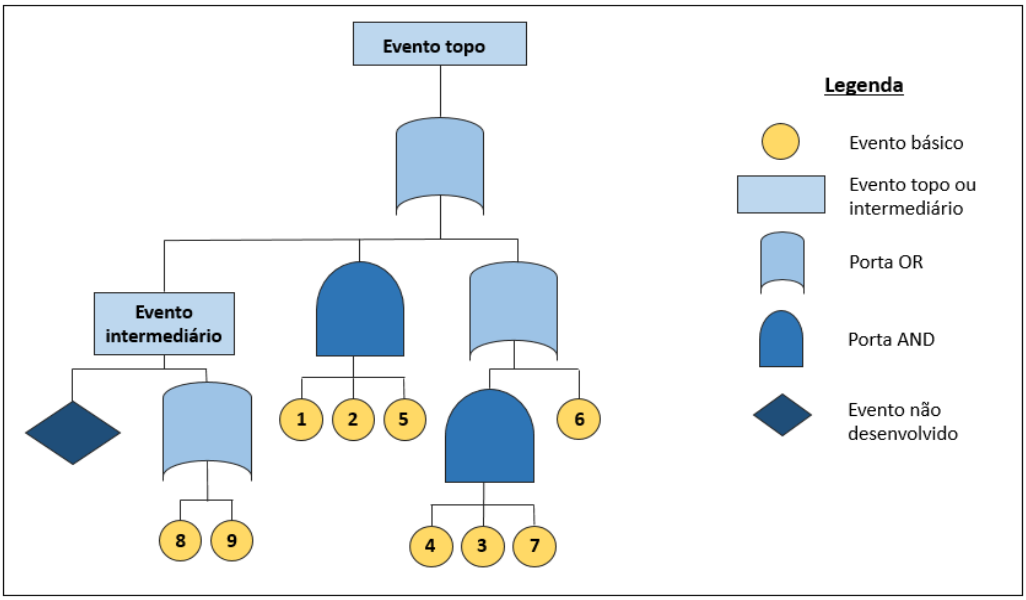
2) *Técnicas de coleta de informações,* são utilizadas técnicas de coletas de informações como *brainstorming* para descobrir riscos cibernéticos e ações para controlá-los e erradicá-los e entrevistas com grupo de colaboradores envolvidas no combate aos riscos (PMI 2017).

3) Análise *SWOT*, ferramenta utilizada para identificar os pontos fortes, os pontos fracos, as oportunidades e ameaças referente ao tratamento dos riscos cibernéticos (HELMS & NIXON, 2010).

4) *Análise da uma árvore de falhas,* deve ser utilizada esta ferramenta para sequenciar as conexões dos riscos topo até riscos básicos, obtendo uma amostragem mais rica dos riscos. A ação “análise de árvore de falhas” demostra claramente todas as conexões para se chegar do evento topo até o evento básico. Com isso realiza uma percepção completa dos riscos envolvidos em um sistema (MANSOORZADEH *et al*., 2014).

A Figura 11, demostra um exemplo da análise da árvore de falhas:

Figura 11 - Análise de uma árvore de falhas



Fonte: Adaptada de Bobbio *et al*. (2001).

Obtém-se como saída dessa etapa:

Uma *Matriz de Registro dos Riscos Cibernéticos*, que busca identificar todos os riscos cibernéticos possíveis.

A Figura 12, demostra um exemplo de uma matriz de registro dos riscos.

Figura 12- Matriz de registro de riscos.

ID	Descrição do risco	Categoria do risco	Probabilidade	Impacto	Responsável	Resposta	Observações

Fonte: Adaptada de PMI (2017).

Na **Etapa 4** denominada **Avaliar os Riscos Cibernéticos**, são feitas as avaliações pertinentes a cada risco identificado para entendê-lo e compreendê-lo, rastreando sua origem, causa raiz e consequências (KWAK & STODDARD 2004).

São utilizadas duas entradas:

1) *Plano de gerenciamento dos riscos*, que serve como um guia para esta etapa (BUSDICKER & UPENDRA, 2017).

2) *Matrix de registro dos riscos*, sendo a matéria prima para essa etapa os riscos já identificados para sua devida avaliação (PMI, 2017).

São empregadas três ferramentas e técnicas:

1) *Análise qualitativa*, tem um cunho subjetivo. Tem como base desta análise a opinião, convicções, experiência dos especialistas interpretadas pela equipe de desenvolvimento do plano de gerenciamento de riscos (BLANKE *et al*., 2016).

2) *Análise dos custos-benefícios,* utiliza essa ferramenta para explorar os custos despendidos em detrimento dos benefícios que serão atingidos (PMI, 2017).

3) *Avaliação da urgência dos riscos cibernéticos*, é categorizado todos os riscos mediante sua urgência e importância de resposta (ABRAHAM *et al*., 2019).

Obtém-se como saída dessa etapa:

Uma atualização dos documentos de riscos, tais como a *matriz de registro dos riscos* e o *plano de gerenciamento de riscos* (PMI, 2017).

Na **Etapa 5,** denominada **Analisar a Probabilidade e Impacto dos Riscos Cibernéticos**, são analisadas a probabilidade da ocorrência de cada risco identificado mediante o impacto e consequência que será resultante na organização (BLANKE *et al*., 2016).

São utilizadas duas entradas:

1) *Plano de gerenciamento dos riscos cibernéticos*, que serve como um guia para esta etapa (BUSDICKER & UPENDRA, 2017).

2) *Matriz de registro dos riscos*, sendo a matéria prima para essa etapa os riscos já identificados para sua devida análise (PMI, 2017).

São empregadas duas ferramentas e técnicas:

1) *Analisar da probabilidade dos riscos cibernéticos*, para calcular a probabilidade da ocorrência de todos os riscos identificados (MAROSIN *et al*., 2014).

2) *Analisar o impacto dos riscos cibernéticos*, para calcular o impacto da ocorrência de todos os riscos identificados (BUBNOV *et al*., 2015).

Com base nos riscos identificados serão analisados a probabilidade para os riscos ocorrerem e os seus impactos caso ele ocorra, com isso é possível ter uma visão maior sobre os riscos (ABRAHAM *et al*., 2019).

A Figura 13, demostra a uma matriz de probabilidade e impacto dividida em categorias.

Figura 13 - Representação de uma matriz de probabilidade e impacto

PROBABILIDADE \ IMPACTO		baixo → alto				
		IRRELEVANTE	BAIXO	MODERADO	ALTO	EXTREMO
alta ↑	QUASE CERTO	Significante	Pouco Crítico	Crítico	Muito Crítico	Muito Crítico
	MUITO PROVÁVEL	Significante	Muito Significante	Pouco Crítico	Crítico	Muito Crítico
	POUCO PROVÁVEL	Pouco Significante	Significante	Muito Significante	Pouco Crítico	Crítico
	IMPROVÁVEL	Insignificante	Pouco Significante	Significante	Muito Significante	Pouco Crítico
baixa	RARO	Insignificante	Insignificante	Pouco Significante	Significante	Muito Significante

Fonte: Adaptada de Fauziyah *et al*. (2020) e PMI (2017).

Obtém-se como saída dessa etapa:

A obtenção da *matriz de probabilidade e impacto*, que demostra a probabilidade de todos os riscos em cinco categorias (raro, improvável, pouco provável, muito provável e quase certo) e o impacto também em cinco categorias (irrelevante, baixo, moderado, alto e extremo) (FAUZIYAH *et al*., 2020).

Na **Etapa 6,** denominada **Classificar os Riscos Cibernéticos**, são categorizados os riscos cibernéticos em grupos de acordo com a classe de risco e sua criticidade (KURE *et al*., 2018).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos*, que serve como um guia para esta etapa (BUSDICKER & UPENDRA, 2017).

São empregadas duas ferramentas e técnica:

1) *Opinião dos especialistas,* que é proporcionada por pessoas, grupos ou instituições que têm treinamentos, conhecimentos ou habilidades especificas sobre o risco em questão. O objetivo é alinhar com todos os membros da equipe o que será considerado como riscos e o que não será aplicado como ameaça (ONDIEGE *et al*., 2017).

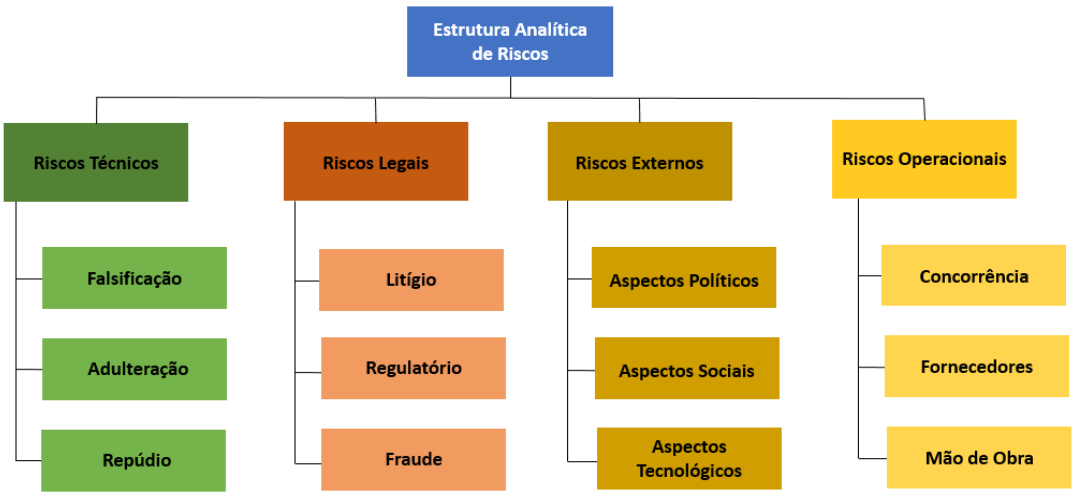
2) *Categorização e Decomposição*, é a classificação e subdivisão dos riscos cibernéticos em componentes menores e melhores gerenciados (PMI, 2017).

Serão novamente levantadas as opiniões dos especialistas e salvas na compilação da opinião dos especialistas da instituição e a categorização e decomposição dos riscos.

Obtém-se como saída dessa etapa:

A criação da estrutura analítica dos riscos *(*EAR*),* que classifica todos os riscos por categoria. A Figura 14, demostra um exemplo de uma EAR.

Figura 14 - Demonstração da EAR.



Fonte: Adaptada de PMI (2017); Carr e Tah (2001).

Na **Etapa 7,** denominada **Conceber Respostas aos Riscos Cibernéticos**, com a conclusão das etapas anteriores é possível conceber soluções para os riscos cibernéticos identificados, priorizando os riscos críticos, mediante alternativas e ações para maximizar as oportunidades e minimizar as ameaças dos riscos, relacionando os riscos a proprietários na sua solução e acompanhamento (WU *et al*., 2018).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos*, que serve como um guia para esta etapa (BUSDICKER; UPENDRA, 2017).

São empregadas duas ferramentas e técnicas:

1) *Opinião dos especialistas,* que é proporcionada por pessoas, grupos ou instituições que têm treinamentos, conhecimentos, habilidades ou experiência especificas sobre o risco em questão. O objetivo é encontrar soluções por meio da prevenção, mitigação, transferência ou aceitação dos riscos cibernéticos identificados (ONDIEGE; CLARKE; MAPP, 2017).

2) *Grupo de discussões,* é utilizado essa ferramenta para agrupar as partes interessadas qualificadas e apropriadas para debater a respeito de suas expectativas,

entendimento e soluções para cada risco identificado com o objetivo de construir soluções apropriadas para os riscos cibernéticos identificados (PMI, 2017).

Obtém-se como saída dessa etapa:

Contramedidas e respostas pertinentes e apropriadas para o devido tratamento e combate dos riscos cibernéticos na organização que servirão como guia para as próximas fases e etapas (BLANKE & MCGRADY, 2016).

A Tabela 9, demostra um resumo da **Fase 1** do modelo teórico-prático.

Tabela 9 – Resumo da Fase 1.

FASE 1 - ELABORAÇÃO DO PLANO DE GERENCIAMENTO DE RISCOS					
ETAPAS	**AUTORES**	**OBJETIVOS**	**ENTRADAS**	**FERRAMENTAS & TÉCNICAS**	**SAÍDAS**
1- PRODUZIR O PLANO DE GERENCIAMENTO DOS RISCOS	Abraham *et al*. (2019) Natsiavas *et al*. (2018) WARD *et al*. (2008) PMI (2017)	Estruturar, documentar, definir, ordenar, integrar e coordenar todas as ações para proteger a organização referente aos riscos cibernéticos	Políticas organizacionais; Fatores ambientais da organização; Ativos de processos organizacionais.	Opinião de especialistas; Análise SWOT; Técnicas de diagramas; Revisão de documentações.	Plano de gerenciamento dos riscos cibernéticos
2- DEFINIR E ENTENDER O QUE SÃO RISCOS CIBERNÉTICOS	Busdicker *et al*. (2017) Ondiege *et al*. (2017) Kure *et al*. (2018) Coronado *et al*. (2014) Abraham *et al*. (2019) Natsiavas *et al*. (2018) WARD *et al*. (2008) PMI (2017) ISO 31000 (2009)	Alinhar, estabelecer e interpretar os riscos organizacionais. Entendendo sua extensão e impacto na organização	Plano de gerenciamento dos riscos cibernéticos. Nível e tolerância de aceitação dos riscos da organização;	Opinião de especialistas; Técnicas de diagramas.	Registro dos riscos
3- IDENTIFICAR OS RISCOS CIBERNÉTICOS	Kure *et al*. (2018) Abraham *et al*. (2019) Coronado *et al*. (2014) Natsiavas *et al*. (2018) Dandage *et al*. (2018) Busdicker *et al*. (2017) Ondiege *et al*. (2017) PMI (2017)	Identificar, discernir diferenciar e documentar todos os riscos cibernéticos da organização.	Registro dos Riscos; Políticas organizacionais; Fatores ambientais da organização; Ativos de processos organizacionais.	Técnicas de diagrama; Técnicas de coleta de informações; Análise SWOT; Análise da uma árvore de falhas.	Matriz de registro dos riscos cibernéticos

ETAPAS	AUTORES	OBJETIVOS	ENTRADAS	FERRAMENTAS & TÉCNICAS	SAÍDAS
4- AVALIAR OS RISCOS CIBERNÉTICOS	Blanke *et al*. (2016) Kure *et al*. (2018) Abraham *et al*. (2019) Coronado *et al*. (2014) PMI (2017)	É uma análise sistemática de todos os aspectos dos riscos em todos os setores, atividades e equipamentos da organização. Avaliando quantativamente, qualitativamente e o custo-benefício.	Matriz de registro dos riscos cibernéticos	Análise qualitativa; Análise dos custos benefícios; Avaliação da urgência dos riscos cibernéticos.	Atualização dos documentos de riscos
5- ANALISAR A PROBABILIDADE E IMPACTO DOS RISCOS CIBERNÉTICOS	Blanke *et al*. (2016) PMI (2017) Kure *et al*. (2018) Abraham *et al*. (2019)	Analisar e calcular as possiblidades, impactos e consequências dos riscos cibernéticos identificados podem causar na organização.	Plano de gerenciamento dos riscos cibernéticos; Registro dos riscos.	Analisar as probabilidades dos riscos cibernéticos; Analisar o impacto dos riscos cibernéticos.	Matrix de probabilidade e impacto
6- CLASSIFICAR OS RISCOS CIBERNÉTICOS	Coronado *et al*. (2014) Kure *et al*. (2018) Abraham *et al*. (2019) PMI (2017)	Distribuir em classes ou grupos, de acordo com o sistema ou método ou classificação dos riscos cibernéticos.	Matrix de probabilidade e impacto	Opinião de especialistas; Categorização e Decomposição.	Estrutura analítica dos riscos-EAR
7- CONCEBER RESPOSTAS AOS RISCOS CIBERNÉTICOS	Blanke *et al*. (2016) PMI (2017)	Desenvolver alternativas e ações para maximizar as oportunidades e minimizar as ameaças dos riscos cibernéticos das organizações. Dedica-se a dar soluções aos riscos identificados, mediante a prioridade do risco. Definindo um proprietário a cada risco.	Estrutura analítica dos riscos EAR	Opinião de especialistas; Grupo de discussões.	Atualização dos documentos de riscos

Fonte: Autor.

3.2 FASE 2 – EXECUÇÃO DO PLANO DE GERENCIAMENTO DE RISCOS

A **Fase 2,** denominada **Execução do Plano de Gerenciamento de Riscos,** tem como objetivo pôr em ação o que foi planejado na fase um (GEORGE *et al*., 2008). É composta por quatros etapas: disseminar, treinar, adequar e executar conforme a seguir:

Na **Etapa 8,** denominada **Disseminação do Plano de Gerenciamento de Riscos,** a proposta é externar as informações corretas, ao pessoal adequado no momento preciso (PMI 2017 e ABRAHAM *et al*., 2019).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernéticos*, que declara as informações que devem ser disseminadas como, quando e para quem (BUSDICKER & UPENDRA, 2017).

São empregadas duas ferramentas e técnicas:

1) *Reuniões*, que é uma ferramenta de comunicação para difundir o plano de gerenciamento de riscos para o entendimento comum a quem de direito na organização (PMI, 2017).

2) *Métodos de comunicação,* nesta etapa são utilizados os métodos de comunicação como: reuniões, telefonemas, videoconferência e e-mails para disseminar o plano de gerenciamento de riscos cibernéticos (ABRAHAM *et al*., 2019).

Obtém-se como saída dessa etapa:

A garantia de que o que foi acordado e planejado para a execução correta no plano de gerenciamento dos riscos seja do entendimento e conhecimento dos usuários, colaboradores e instituições pertinentes (KURE *et al*., 2018, ABRAHAM *et al*., 2019).

Na **Etapa 9,** denominada **Treinamento e Qualificação**, são qualificados os colaboradores para enfrentar os riscos cibernéticos, são expostas as culturas, normas e padrões esperados. Possibilitando a mudança de atitudes inadequadas e maximizando o desenvolvimento esperado, por meio da aquisição de novos conhecimentos e habilidades quando necessários (HONG *et al*., 2004).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernéticos*, que declara as informações que devem ser disseminadas como, quando e para quem (BUSDICKER e UPENDRA, 2017).

São utilizadas duas ferramentas e técnicas:

1) *Treinamento*, com essa ferramenta é apresentado os conhecimentos, habilidades e competências que foram constatadas como carentes no plano de gerenciamento nos sistemas, instalações, equipamentos, colaboradores e usuários da organização (HONG *et al*., 2004).

2) *Reconhecimento e recompensas*, com a execução de políticas para reconhecer e valorizar os colaboradores que estão se dedicando a combater os riscos cibernéticos na organização por meio de celebrações de seus esforços, como o anúncio público de seus esforços e prêmios simbólicos como pequenos itens de valor (PMI, 2017).

Obtém-se como saída dessa etapa:

Um maior engajamento dos colaboradores da organização na busca incessante de proteger as organizações contra crimes cibernéticos. Obtém-se com isso propósitos claros, melhores relacionamentos interpessoais e motivação por desafios (MARTIN *et al*., 2017).

Na **Etapa 10,** denominada **Adequar a Organização com as Ações de Riscos Acordadas,** busca-se os mesmos objetivos da etapa anterior, porém o foco dessa etapa é atuar na adequação da organização (BOJANOVA *et al*., 2017). Adaptando-a com as ações necessárias e acordados para preservar a organização no combate aos riscos cibernéticos (HUANG *et al*., 2014).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernético*, utiliza o plano que contém informações, das políticas organizacionais, política de gestão de riscos, fatores ambientais das organizações e os ativos de processos organizacionais (BUSDICKER e UPENDRA, 2017).

São utilizadas duas ferramentas e técnicas:

1) *Auditorias de qualidade*, que adequa a organização com o plano de gerenciamento dos riscos. Por meio da comparação dos elementos que não estão de acordo com o plano (DEFOND e ZHANG, 2014).

2) *Análise de processos*, que adequa a organização com os processos que estão adequados e a extinção de processos inadequados no combate aos cibercrimes (PMI, 2017).

Obtém-se como saída dessa etapa:

Uma melhor proteção da organização com seu devido enquadramento as melhores normas e padrões de segurança cibernética (COVENTRY *et al*., 2018).

Na **Etapa 11,** denominada **Execução de Requisitos de Sistemas *Cyber* no Setor de saúde,** são executados os requisitos mínimos de cibersecurity para proteger a organização no combate a cibercrimes (ONDIEGE *et al*., 2017).

É utilizada apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernéticos*, utiliza o plano que contém informações, dos itens mínimos que devem ser executados na organização para sua devida proteção (BUSDICKER e UPENDRA, 2017).

São utilizadas duas ferramentas e técnicas:

1) *Auditorias de qualidade*, que adequa a organização com os critérios mínimos de cibersecurity. Por meio da comparação dos elementos que não estão de acordo com o plano (DEFOND e ZHANG, 2014).

2) *Análise de processos*, que adequa a organização com os processos que estão adequados e a extinção de processos inadequados no combate aos cibercrimes mediante a melhores práticas desenvolvidas (PMI, 2017).

Obtém-se como saída dessa etapa:

A utilização dos elementos mínimos de cibersegurança listadas na Tabelas 8 e 9 e 10 é plausível uma proteção mínima, porém adequada dos dispositivos médicos.

A Tabela 10, demostra um Lista de requisitos mínimos de segurança cibernética para dispositivos médicos encontradas na literatura científica.

Tabela 10- Lista de requisitos de segurança para dispositivos médicos

Item	**Requisitos** / **Autores**	Abraham *et al.* (2019)	Blanke e McGrady, (2016)	Braga *et al.* (2019)	Busdicker e Upendra, (2017)	Coronado e Wong, (2014)	Ghafir *et al.* (2018)	Kharraz *et al.* (2018)	Martin *et al.* (2017)	Mostfa *et al.* (2016)	Natsiavas *et al.* (2018)	Ondiege *et al.* (2017)	Priestman *et al.* (2019)	Primo *et al.* (2018)

1	Todos os dispositivos devem ter *backup* de seus dados em local seguro com uma periodicidade previamente acordada por especialistas.	X	X				X	X	X					X
2	Todos os dispositivos portáteis, devem criptografar seus dados. Todas as chaves usadas para criptografia e descriptografia devem ser aprovadas previamente para possuírem requisitos de complexidade.		X	X		X		X			X			
3	Todos os dispositivos devem ter o bloqueio ativado após três falhas de tentativas no login.	X	X		X			X					X	
4	Todos os dispositivos devem ter seus sistemas operacionais, *software* e antivírus atualizados à medida que novos lançamentos e correções estiverem disponíveis.	X	X									X		X
5	Todos os dispositivos médicos devem estar devidamente inventariados, contendo qual o tipo de informação o dispositivo armazena.		X			X								
6	Todos os dispositivos devem ser protegidos com senha, protetores de tela e *logoff* automático após um período pré-determinado.		X							X				
7	Todos os dispositivos devem conter senhas fortes, com uma combinação de oito caracteres e dígitos. Essas senhas devem ser alteradas a cada seis meses.		X							X				
8	Todos os dispositivos portáteis, devem conter limpeza remota e rastreamento de localização geográfica.		X											
9	Implantar sistemas automatizados com inteligência artificial que detectam e impeçam ataques a redes e dispositivos.	X												
10	Monitoramento constante das redes e sistemas.	X												
11	Elaborar soluções de proteção de endpoint impedindo ataques internos ou externos.	X												
12	Auditoria constante dos provedores de serviços em nuvem com os padrões de auditoria como SAS 70 e FIPS 200.	X												
Total		**7**	**8**	**1**	**1**	**2**	**1**	**3**	**1**	**2**	**1**	**1**	**1**	**2**

Fonte: Autor.

Foi considerado para a utilização no modelo teórico-prático os sete itens da Tabela 10, representados com a cor verde, que tiveram no mínimo duas citações na literatura científica. Os itens representados na cor vermelha não serão utilizados por só terem uma citação.

A Tabela 11, apresenta as melhores práticas para evitar ataques cibernéticos encontradas na literatura científica.

Tabela 11 - Melhores práticas para segurança cibernética no setor de saúde.

Item	Requisitos / Autores	Abraham *et al.* (2019)	Ahmed e Ahmed, (2019)	Blanke e McGrady, (2016)	Bojanova e Voas, (2017)	Busdicker e Upendra, (2017)	Coronado e Wong, (2014)	Diggans e Leproust, (2019)	Gordon *et al.* (2019)	Habibzadeh *et al.* (2019)	Huang, (2014)	Kruse *et al.* (2017)	Kuerbis e Badiei, (2017)	Lebeda *et al.* (2018)	Maimó *et al.* (2019)	Martin *et al.* (2017)	Mostfa Kamal *et al.* (2016)	Ondiege *et al.* (2017)	PMI, (2017)	Priestman *et al.* (2019)
1	As atividades devem ser auditadas e revisadas frequentemente, conforme a responsabilidade do colaborador.	X		X	X	X	X			X	X		X							
2	Deve se fornecer treinamentos constantes a todos os colaboradores da organização.	X		X			X		X			X			X	X			X	
3	Deve ser usado a autenticação de dois ou três fatores para acessar o sistema da organização.	X		X		X	X													X
4	Ao contratar um novo colaborador (mesmo para meio período), deve-se verificar os antecedentes do colaborador.			X			X		X									X		
5	O acesso de usuários aos bancos de dados, dever ser restrito e mediante ao vínculo do acesso a informações como nome do usuário, senha, informações acessadas, local e data do acesso.	X		X													X			X
6	Deve-se prover a conscientização dos colaboradores sobre a segurança digital constantemente.	X		X		X	X													
7	Deve ser retirado o acesso ao sistema e a organização dos colaboradores que se desligarem da organização.		X	X		X		X												
8	Deve ser concedido um acesso limitado ao sistema, com base na necessidade de acesso aos colaboradores, baseadas nas funções e responsabilidade da atividade exercida do cargo.			X			X											X		
9	Deve ser comunicado o desligamento do vínculo empregatício dos colaboradores desligados da organização com os fornecedores ou parceiros apropriados.		X	X				X												
10	Todos os equipamentos e documentos físicos devem ser devidamente descartados.			X		X								X						
11	Deve ser revisado os registros das gravações, de toda a infraestrutura da organização para validar o acesso e uso individual.			X																

12	Estacionamento e todas as áreas externas da organização, deve estar devidamente iluminada no período noturno.			X																
13	Deve ser configurado o bloqueio do terminal a cada ausência do colaborador, por mais breve que seja a ausência.			X																
Total		**5**	**2**	**13**	**1**	**5**	**6**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**2**

Fonte: Autor.

Foi considerado para a utilização no modelo teórico-prático os dez itens da Tabela 11, representados com a cor verde, que tiveram no mínimo três citações na literatura científica. Os itens representados na cor vermelha, não serão utilizados por só terem uma citação.

Desta forma, a Tabela 12, demostra um resumo da **Fase 2** do modelo teórico-prático.

Tabela 12- Resumo da Fase 2.

FASE 2 - EXECUÇÃO DO PLANO DE GERENCIAMENTO DE RISCOS					
ETAPAS	**AUTORES**	**OBJETIVOS**	**ENTRADAS**	**FERRAMENTAS & TÉCNICAS**	**SAÍDAS**
8- DISSEMINAÇÃO DO PLANO DE GERENCIAMENTO DE RISCOS	Abraham *et al*. (2019) PMI (2017)	Proliferação de informações referentes a geração, coleta, compartilhamento, retenção, recuperação e distribuição final, referentes ao plano de gerenciamento de riscos, de forma apropriada e adequada.	Plano de gerenciamento dos riscos cibernéticos	Reuniões; Métodos de comunicação.	Atualização dos documentos de riscos
9- TREINAMENTO E QUALIFICAÇÃO	Kruse *et al*. (2017) Martin *et al*. (2017) Coronado *et al*. (2014) Abraham *et al*. (2019) PMI (2017)	Treinar e qualificar os colaboradores das organizações sobre as melhores práticas no combate a cibercrimes. Buscando aflorar a conscientização sobre cibersegurança, ao mesmo tempo que os qualificam.	Plano de gerenciamento dos riscos	Treinamento; Reconhecimento e recompensas.	Avaliação do desempenho da equipe
10- ADEQUAR A ORGANIZAÇÃO COM AS AÇÕES DE RISCOS ACORDADAS	Abraham *et al*. (2019) Huang *et al.* (2014) Bojanova *et al*. (2017) Habibzadeh *et al*. (2019) Martin *et al*. (2017) Coventry *et al*. (2018) PMI (2017)	Adaptar a organização com os atos necessários e acordados para proteger a organização contra riscos cibernéticos	Avaliação do desempenho da equipe	Auditorias de qualidade; Análise de processos.	Atualização dos documentos de riscos

ETAPAS	AUTORES	OBJETIVOS	ENTRADAS	FERRAMENTAS & TÉCNICAS	SAÍDAS
11- EXECUÇÃO DE REQUISITOS DE SISTEMAS *CYBER* NO SETOR DE SAÚDE	Abraham *et al*. (2019) Zhang *et al*. (2017) Blanke *et al*. (2016) Braga *et al*. (2019) Natsiavas *et al*. (2018) Martin *et al*. (2017) Gordon *et al*. (2019) Kharraz *et al*. (2018) Kruse *et al*. (2017) Maimó, *et al*. (2019) Busdicker *et al*. (2017) Lebeda *et al*. (2018) Coronado *et al*. (2014) PMI (2017)	Executar na organização padrões mínimos de segurança cibernética	Plano de gerenciamento dos riscos cibernéticos	Auditorias de qualidade; Análise de processos.	Atualização dos documentos de riscos

Fonte: Autor.

3.3 FASE 3 – MONITORAMENTO DO PLANO DE GERENCIAMENTO DE RISCOS

A **Fase 3,** denominada **Monitoramento do Plano de Gerenciamento dos Riscos,** tem como objetivo monitorar os riscos identificados na fase um, monitorar a implementação das etapas adequar a organização com as ações de riscos acordadas e execução de requisitos de sistemas *cyber* no setor de saúde, monitorar os riscos residuais, identificar novos riscos e avaliar a eficácia do processo no combate aos riscos cibernéticos (PENNOCK *et al*., 2002). É composta com duas etapas conforme segue:

A **Etapa 12**, denominada **Monitorar os riscos cibernéticos**, compreende a acompanhar os riscos cibernéticos desde o primeiro momento em que se inicia os processos na instituição. É uma etapa que mesmo estando na fase três deve ser praticada em todos os momentos dentro das instituições (KUJAWSKI *et al*., 2010).

É utilizado apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernéticos*, utiliza-se o plano que contém informações, dos itens mínimos que devem ser executados, os registros dos riscos e as respostas aos riscos cibernéticos (BUSDICKER e UPENDRA, 2017).

São utilizadas três ferramentas e técnicas:

1) *Opinião de especialistas*, que trabalham na organização e conhecem os sistemas, instalações e equipamentos (ONDIEGE, CLARKE & MAPP, 2017).

2) *Reavaliação dos riscos*, a sua utilização pode prover na identificação de novos riscos cibernéticos, revisão dos riscos encontrados e conclusão dos riscos não mais válidos (PMI, 2017).

3) *Auditoria de riscos*, monitora a eventualidade da eficiência dos processos na busca de um melhor controle dos riscos cibernéticos. Buscando melhorar a estrutura teórico-prática proposta para sua devida eficácia (XIAO & XIAO, 2013).

Obtém-se como saída dessa etapa:

A coleta do *status* de desempenho do gerenciamento de riscos cibernéticos. É possível medir a efetividade e o comportamento das ações tomadas na organização. Gerando informações suficientes para ajustar as ações necessárias (KURE *et al*., 2018).

A **Etapa 13,** é denominada **Verificação dos Riscos Cibernéticos Residuais.** Com o desenvolvimento da etapa anterior é possível detectar se há riscos cibernéticos

derivados ou remanescentes das ações empregadas para combatê-los (ONDIEGE *et al*., 2017).

São utilizadas duas entradas:

1) *Plano de gerenciamento dos riscos cibernético*, que atesta as ações executadas e os resultados esperados, possibilitando identificar riscos residuais (BUSDICKER e UPENDRA, 2017).

2) *Relatório de desempenho*, que coleta, expõe e distribui as informações sobre o desempenho das ações aplicadas (PMI, 2017).

São utilizadas três ferramentas e técnicas:

1) *Opinião de especialistas,* que tenham experiencia do comportamento da organização para perceber alterações dos resultados esperados (ONDIEGE, CLARKE e MAPP, 2017).

2) *Reavaliação dos riscos*, que deve ser constante na organização para reavaliar as ações empregadas e constatar se as soluções planejadas ainda são viáveis para os problemas de cibersegurança (PMI, 2017).

3) *Análise de variação e tendências*, que faz uma avaliação entre o que foi planejado com os resultados reais na organização. Buscando variações ou tendências que indiquem o desvio da rota planejada (KURE *et al*., 2018).

Obtém-se como saída dessa etapa:

Um controle efetivo na organização em relação a efetividade das ações para proteger a organização. São atualizados os documentos de segurança cibernética, podendo ser solicitadas mudanças no plano e a elaboração de relatórios de desempenho (KURE *et al*., 2018).

A Tabela 13, demostra um resumo da **Fase 3** do modelo teórico-prático.

Tabela 13- Resumo da Fase 3.

FASE 3 - MONITORAMENTO DO PLANO DE GERENCIAMENTO DOS RISCOS					
ETAPAS	**AUTORES**	**OBJETIVOS**	**ENTRADAS**	**FERRAMENTAS & TÉCNICAS**	**SAÍDAS**
12- MONITORAR OS RISCOS CIBERNÉTICOS	Blanke *et al*. (2016) Kure *et al*. (2018) Coronado *et al*. (2014) Abraham *et al*. (2019) PMI (2017)	Monitorar os riscos cibernéticos dentro da organização	Plano de gerenciamento dos riscos cibernéticos	Opinião de especialistas; Reavaliação dos riscos; Auditoria de riscos.	Atualização dos documentos de riscos Solicitação de mudanças Relatórios de desempenho
13- VERIFICAÇÃO DOS RISCOS CIBERNÉTICOS RESIDUAIS	Blanke *et al*. (2016) Ondiege *et al*. (2017) Kure *et al*. (2018) Coronado *et al*. (2014) Abraham *et al*. (2019) PMI (2017)	Gerenciar os riscos cibernéticos residuais da organização	Plano de gerenciamento dos riscos cibernético; Relatório de desempenho.	Opinião de especialistas; Reavaliação dos riscos; Análise de variação e tendências.	Atualização dos documentos de riscos Solicitação de mudanças Relatórios de desempenho

Fonte: Autor.

3.4 FASE 4 – IMPLANTAÇÃO DAS CONTRAMEDIDAS NECESSÁRIAS PARA CONTER OS RISCOS

Com isso, dá-se início a **Fase 4**, intitulada **Implantação das Contramedidas Necessárias para Conter os Riscos** que deve refletir a respeito das ações estruturadas se foram adequadas nas soluções do combate aos cibercrimes.

Na **Etapa 14,** intitulada **Implantação de Ações Corretivas a Ameaças Encontradas.** A equipe envolvida irá implantar ações corretivas caso as ações concebidas não foram suficientes, se os dados levantados foram exíguos ou insuficientes ou as circunstâncias mudarem. E reutilizar/padronizar as atividades que tiveram o êxito planejado, garantindo uma máxima eficácia e eficiência (SILVA *et al*., 2017).

É utilizado apenas uma entrada:

1) *Plano de gerenciamento dos riscos cibernético*, que contém todas as ações e previsões no combate ao cibercrime (BUSDICKER e UPENDRA, 2017).

São utilizadas duas ferramentas e técnicas:

1) *Reuniões*, para discutir sobre a efetividade das ações e novos planos de ações caso necessários (PMI, 2017).

2) *Opinião de especialistas*, que possuem a expertise necessária para jugar as ações e resultados obtidos (ONDIEGE, CLARKE e MAPP, 2017).

Obtém-se como saída dessa etapa:

Uma padronização do que que está dando certo e sua devida repetição em um novo ciclo e a exclusão das atividades ineficientes com seu devido realinhamento evitando sua reutilização (BOZICKOVICI *et al*., 2012). Com essas ações obtém-se uma atualização nos documentos do projeto, solicitações de mudança nas ações ineficientes e a atualização dos relatórios de desempenho (PMI, 2017).

Ao chegar nessa etapa se inicia um novo ciclo de ações com informações suficientes do que está dando certo e o que deve ser excluído ou melhorado no plano de gerenciamento dos riscos (ABRAHAM *et al*., 2019).

A Tabela 14, resume a **Fase 4** do modelo teórico-prático.

Tabela 14- Resumo da Fase 4.

FASE 4 - IMPLANTAÇÃO DAS CONTRAMEDIDAS NECESSÁRIAS PARA CONTER OS RISCOS					
ETAPAS	**AUTORES**	**OBJETIVOS**	**ENTRADAS**	**FERRAMENTAS & TÉCNICAS**	**SAÍDAS**
14- IMPLANTAÇÃO DE AÇÕES CORRETIVAS A AMEAÇAS ENCONTRADAS	Martin *et al*. (2017) PMI (2017)	Reflexão e realinhamento do plano de gerenciamento de crises da organização	Plano de gerenciamento dos riscos cibernético	Reuniões; Opinião de especialistas.	Atualização dos documentos de riscos Solicitação de mudanças Relatórios de desempenho

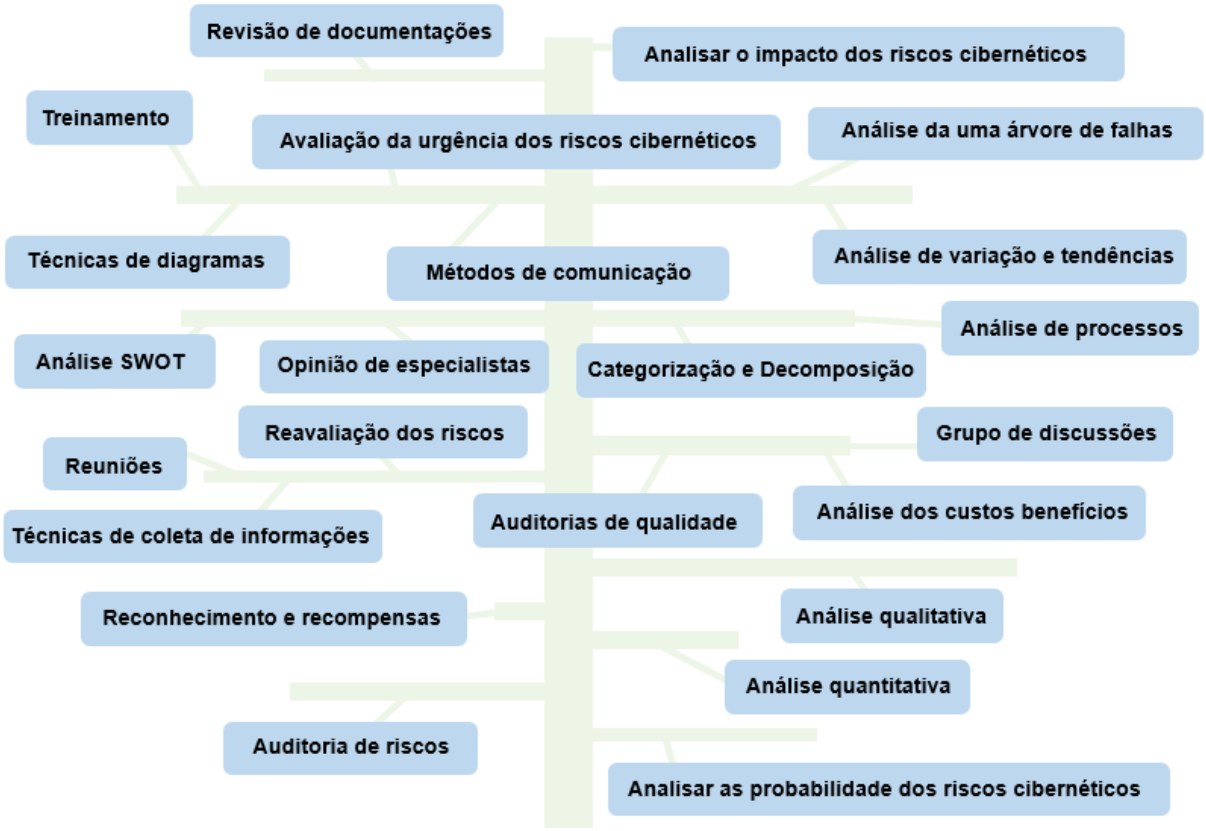
Fonte: Autor.

3.5 ESTRUTURA TEÓRICO-PRÁTICA PROPOSTA PARA GESTÃO DE RISCOS DE SISTEMAS DE CIBERSEGURANÇA NO SETOR DE SAÚDE

A estrutura teórico-prática desenvolvida é um plano de gerenciamento de riscos cibernéticos completo para instituições de saúde do Brasil. Sequenciada logicamente e utilizando as 23 melhores ferramentas e técnicas junto com as melhores prática encontradas na literatura científica.

A Figura 15, demostra as ferramentas e técnicas utilizadas.

Figura 15 – Ferramentas e técnicas utilizadas na estrutura teórico-prática.



Fonte: Autor.

Desta forma, essa estrutura inspira-se no ciclo PDCA para criar um plano de gerenciamento de riscos completo dividida em quatro fases com quatorze elementos conforme apresentação dos capítulos anteriores.

A Figura 16, demostra a representação essa estrutura.

Figura 16 - Proposição da estrutura teórico-prática

Fonte: Autor.

4. METODOLOGIA DA PESQUISA

Neste capítulo, será demostrada a abordagem metodológica e os princípio científicos que regem e norteiam está dissertação. São abordados as sequencias e o desenho dessa pesquisa de mestrado.

De acordo com Ghauri e Gronhaug (2005), a pesquisa científica é um processo rigoroso, uma caminhada regrada por procedimentos sólidos e relevantes, necessitando comprovar seu desenvolvimento com a austeridade suscetível de verificação ou averiguação.

4.1 DEFINIÇÃO DO PROBLEMA E REVISÃO DA LITERATURA CIENTÍFICA

A primeira etapa de uma pesquisa científica é a revisão bibliográfica, sendo ela essencial pois irá permitir interpretar o estado da arte e os conhecimentos existentes a respeito do tema em questão Cauchick Miguel *et al*., (2012).

Consequentemente, conforme análise da literatura científica em busca do estado da arte, foram encontradas asserções que concluíram na interpretação dos objetivos desta dissertação, tais como são apresentadas na Tabela 1 desta dissertação.

Também foi constatado o atual patamar tecnológico das organizações, resultado de grande parte dos processos atuais serem exercidos por meio digital (HOFMANN & RÜSCH, 2017). Tornando o setor de saúde um alvo chamativo, devido sua falta de investimentos em cibersegurança, abundância de informações pessoais, grandeza econômica e brechas na segurança digital (BLANKE *et al*., 2016).

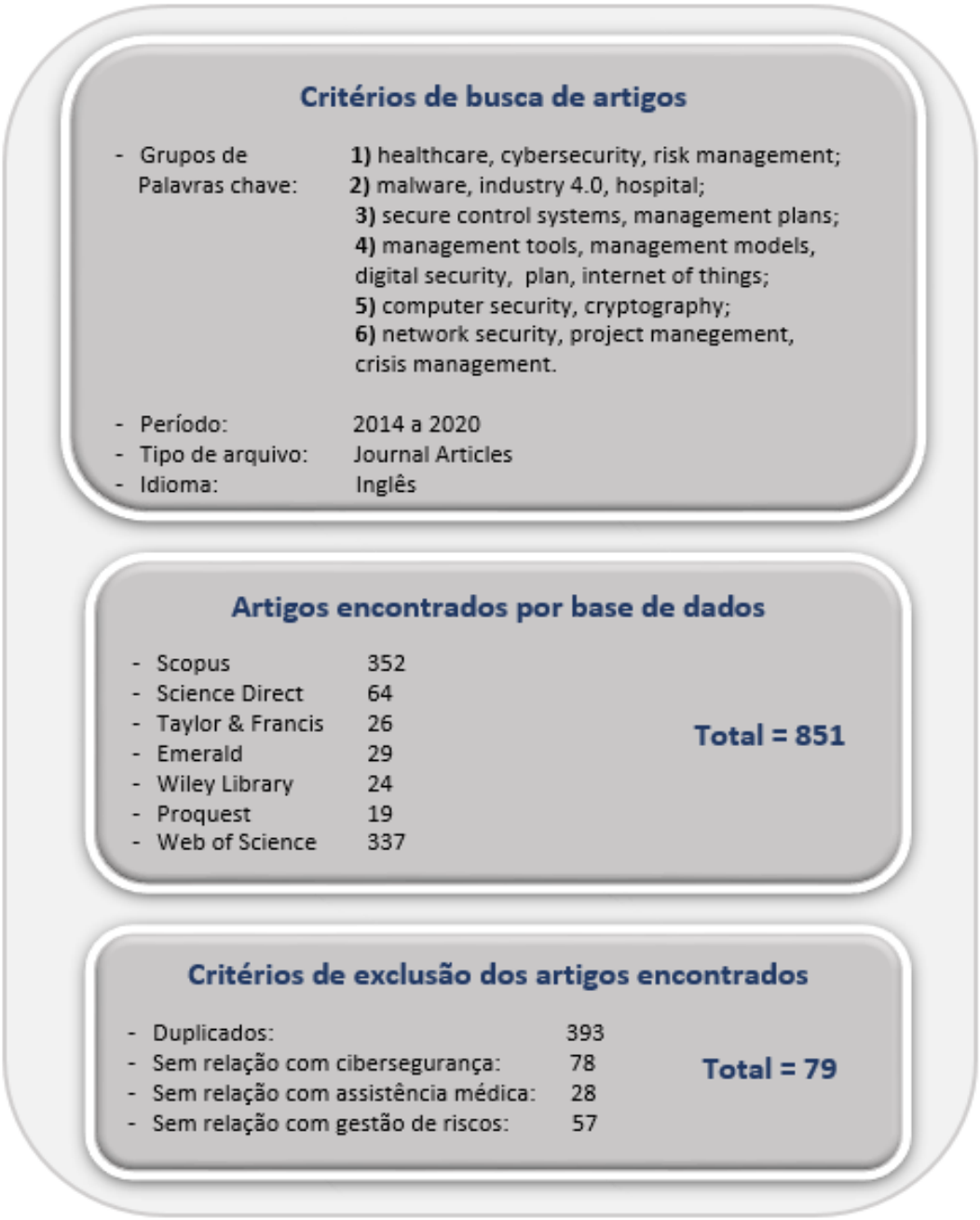
Inicialmente, os esforços foram concentrados em artigos de revisão da literatura, como os artigos de: Pesapane *et al.* (2018); Kruse *et al.* (2017); Coventry e Branley, (2018) e Martin *et al.* (2017), para um primeiro contato com a área. Na qual foram identificadas e catalogados as principais palavras-chave que foram consideradas as mais assertivas, combinadas entre si para a busca dos demais artigos acadêmicos.

Consequentemente, para ordenação da revisão da literatura a abordagem metodológica emprega a revisão sistemática da literatura, sendo um processo que reúne informações necessárias por meio de procedimentos organizados, compreensíveis e replicáveis (MOHER, LIBERATI, *et al.*, 2009).

Preocupou-se com a análise de quais bases de dados *on-line* representam o amplo espectro para a montagem de um referencial teórico sólido e consistente da literatura científica. Após a consulta a dois especialistas sobre o assunto, chegou-se à conclusão que as sete bases de dados apresentadas na Figura 17, conseguem cumprir de forma satisfatória essa tarefa.

A Figura 17 sintetiza os critérios de inclusão e exclusão dos artigos utilizados por esta dissertação.

Figura 17 – Critérios de seleção e exclusão de artigos



Fonte: Autor.

Desta forma, foi concentrado os esforços por meio de uma análise vertical, dos 79 artigos inicialmente selecionados, objetivando definir as linhas de pesquisas as lacunas apresentadas e os principais elementos bibliográficos. Por consequência, tornou-se possível elaborar as questões de pesquisa apresentadas nesta dissertação.

Além disso, foi empregada a avaliação e análise dos textos, onde empregou-se técnicas de análise de conteúdo apresentadas por Bardin (1986). Conforme o autor a análise de conteúdo deve ser ordenada em: pré-análise, exploração dos textos e interpretação dos resultados. Ainda segundo o autor, é fundamental a seleção dos documentos, a codificação dos documentos e a interpretação dos resultados.

Consequentemente, utilizou-se a análise temática no qual é possível contemplar do que se trata o artigo, como é problematizado, qual o posicionamento dos autores perante os problemas de pesquisa e quais os temas e subtemas que são abordados. Finalmente, utilizou-se a análise interpretativa, para estabelecer a unidade lida, situar sobre o contexto cultural e filosófico dos artigos contemplados para os autores dessa dissertação formularem um juízo próprio e crítico dos artigos analisados.

Portanto, conforme a literatura científica, defender o setor de saúde contra cibercrimes, é um obstáculo as organizações no século XXI, também é constatado que, não há uma solução cem por cento infalível para o problema, entretanto, foi demostrado que uma estrutura de gestão de riscos é a solução mais adequada para combater as ações de cibercriminosos.

4.2 DEFINIÇÃO DOS OBJETIVOS PARA SOLUCIONAR O PROBLEMA

Com os atuais avanços tecnológicos, há uma maior conexão entre a *internet* das coisas (IoT) e uma comunicação máquina a máquina (M2M) entre outras, entretanto, implementar/utilizar toda essas novas tecnologias/comodidades é um processo complexo (HOFMANN *et al*., 2017).

Nesse novo cenário, a segurança da informação desempenha um papel central, por meio de uma estrutura legal, desenvolvimento de novos colaboradores, desenvolvimento de novos modelos de negócio e desenvolvimento de novas pesquisas (SHARPE *et al*., 2019).

Logo, para se inserir nessa nova etapa da interação/produção global, faz se necessário proteger as instituições contra os atuais cibercrimes. A segurança da informação deve ser ancorada como um fator-chave das cadeias de valor e padrões internacionais, como igualmente na conscientização e competência das organizações (LEE *et al*., 2019).

Nesse contexto, o setor de saúde, está constantemente incorporando inovações tecnológicas para satisfazer as necessidades atuais aos cuidados de saúde dentro e fora do ambiente hospitalar (WETHINGTON, *et al*., 2018).

Desta forma, foram definidos os objetivos de estudar a gestão de riscos e a segurança de dados no setor de saúde, com base na literatura científica, desenvolver um método de gestão de riscos com foco em sistemas de segurança de dados para o setor e testar e avaliar a sistemática, do método de gestão de riscos em sistemas de segurança de dados, em grandes instituições de saúde do Brasil.

Consequentemente, foi desenvolvido uma estrutura teórico-prática apresentada na Figura 16, que contempla as melhores práticas e ações encontradas na literatura científica. O próximo tópico irá argumentar o *design* da estrutura teórico-prática proposto para esta dissertação.

4.3 *DESIGN* E DESENVOLVIMENTO DA ESTRUTURA TEÓRICO-PRÁTICA DESENVOLVIDA

A estrutura teórico-prática proposta, é um plano de gerenciamento de riscos baseado na metodologia do ciclo PDCA, com a ideia de planejar as ações necessárias, aplicá-las na instituição de saúde, descobrir possíveis falhas nas ações, solucionar desvios do planejado e verificar os resultados.

Conforme Busdicker *et al*. (2017); Abraham *et al*. (2019); Marosin *et al*. (2014); Ondiege *et al*. (2017); Martin *et al*. (2017) e PMI, (2017) a elaboração de um plano de gerenciamento de riscos cibernéticos é uma solução adequada para o problema da segurança cibernética no setor de saúde.

Segundo Nidd, Thorn e Porter (2016); Venkatraman (2007); Maas e Reniers (2014); Silva *et al*. (2017) e Bozickovici *et al*. (2012) o ciclo PDCA é uma das ferramentas mais poderosas em gestão da qualidade e melhoria de processos.

Na busca de melhorar a cada novo ciclo de aplicação da metodologia, a estrutura teórico-prática proposta foi estruturado em quatro fases conforme são descritos em detalhes no capítulo três.

A próximo tópico, irá mostrar a testagem da estrutura teórico-prática por meio de estudo de caso.

4.4 TESTAGEM DA ESTRUTURA TEÓRICO-PRÁTICA POR MEIO DE ESTUDO DE CASO

Inicialmente este trabalho optou por duas outras metodologia de estudo que se provaram inadequados para esta pesquisa. Com isso, concluiu-se que a metodologia mais adequada a ser utilizada é o estudo de caso.

Para Yin (2001), o estudo de caso trabalho de cunho empírico que investiga um fenômeno atual dentro do contexto da vida real em que os limites entre esse fenômeno e o contexto não são nitidamente definidos.

O qual este trabalho está trabalhando com múltiplo casos para uma melhor compreensão e empregabilidade do modelo proposto.

Segundo Yin (2001), não há um número mínimo de casos requeridos para a aplicação da metodologia, o mais importante é a aplicação da metodologia em casos que demostrem os fatos e fenômenos para obter os objetivos e resultados desejados.

4.5 AVALIAÇÃO DA ESTRUTURA TEÓRICO-PRÁTICA E SUA APLICAÇÃO

A estrutura teórico-prática desenvolvida, foi apresentada a três instituições de saúde por meio de seus representantes para avaliar sua viabilidade e eficácia, foram apresentadas as quatro fases e quatorze elementos juntamente com o objetivo pretendido em cada elemento as entradas, ferramentas e técnicas utilizadas e as saídas esperadas.

Avaliou-se a estrutura *in loco* com a sua total implementação para mensuração de seus resultados e eficácia e avaliação se a estrutura soluciona os problemas de cibersegurança na instituição selecionada.

4.6 COMUNICAÇÃO DOS DADOS

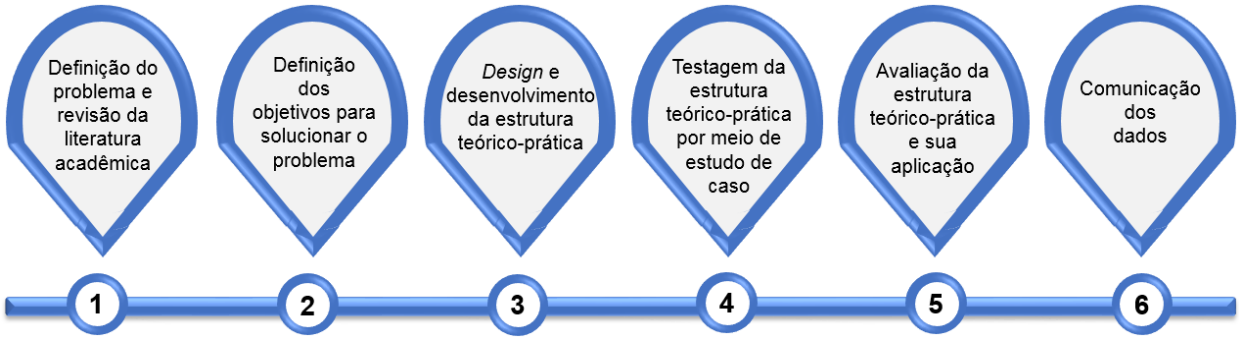
As contribuições e resultados inicialmente adquiridos, foram compartilhados com a instituições analisadas, expostas nesta dissertação de mestrado e devidamente disseminados por meio de publicações no formato de artigos acadêmicos em revistas de grande impacto.

O primeiro artigo intitulado “*Risk Management Focusing on the Best Practices of Data Security Systems for Healthcare*“ sobre a revisão da literatura foi submetido

a revista "*International Journal of Innovation* (IJI)" a qual foi aceito para publicação na primeira edição de 2021.

A Figura 18, representa o sequenciamento descrito.

Figura 18- Sequenciamento das etapas



Fonte: Autor.

Já o próximo tópico, irá discutir sobre a análise metodológica desta pesquisa.

4.7 ESTRUTURA METODOLÓGICA DA PESQUISA

Segundo Marconi e Lakatos (2003), está dissertação é de natureza aplicada por gerar conhecimentos de conteúdo prático, envolvendo interesses dispostos na sociedade em que ela esta inserida.

Já conforme Cauchick Miguel *et al*. (2012), o desenvolvimento de novos conhecimentos em pesquisas de Engenharia de Produção é a finalidade a ser alcançada, convertendo conhecimentos existentes em novos conhecimentos para a sociedade. Ainda segundo a visão dos autores, esta dissertação é definida conforme seus objetivos de pesquisa como uma pesquisa explicativa, sendo um tipo de pesquisa que examina o conhecimentos sobre a realidade, explicando seu porque sua razão. Basendo-se em trabalhos já existentes para poder ser embasada, no qual este trabalho procura clarificar a relação como um método de gestão de riscos em seguraça cibernética pode auxiliar o setor de saúde a se proteger das ameaças e desafios contemporâneos.

A coleta dos dados apoiou-se na primeira fase em uma pesquisa bibliográfica por meio da revisão da literatura e interpretação do estado da arte, dos principais *journals* a fim de obter dados e informações a respeito do tema proposto, que permitiu um relacionamento direto com o objetos de estudo deste trabalho, no sentido de

desenvolver um método de gestão de riscos de cibersegurança. E em uma segunda fase em entrevistas semi-estruturadas aplicadas a especialistas da área em grandes instituição de saúde do Brasil.

Conforme Creswell (2007), é utilizada a abordagem qualitativa, em que o pesquisador coleta os dados no ambiente real, analisando e interpretando esses dados subjetivamente, por meio da heterodoxia no estágio da investigação.

De acordo com Cauchick Miguel *et al*. (2012), após desenvolver o modelo teórico, o pesquisador deve selecionar o método de pesquisa para testar o modelo desenvolvido, sendo que a escolha desse método de pesquisa resulta de alguns elementos distintos, tais como: recursos, tempo, natureza do problema de pesquisa, viabilidade do acesso aos dados, etc.

A principio o método de pesquisa proposto para estabelecer as bases lógicas ao conhecimento científico foi o estudo de caso. Conforme Yin (2001), o estudo de caso é um estudo de essencia empírica que analisa um fenômeno atual em situações reais inseridos em seu próprio contexto. Sendo que o estudo de caso tem a possibilidade de tratrar uma vasta quantidade de indícios tais como: documentos, artefatos, dispositivos, entrevistas e observações.

A Figura 19, demostra uma sintese da estrutura metodologica desta pesquisa.

Figura 19 – Estrutura metodológica da pesquisa.

Fonte: Autor.

4.7.1 Método de Pesquisa

Esta dissertação utiliza como método teórico o estudo de caso. Conforme Yin (2001), o estudo de caso é utilizável para pesquisar novos conceitos, como para analisar e aplicar na prática elementos teóricos sugeridos, sendo útil quando o fenômeno é amplo ou complexo, não podendo ser pesquisado afastado das circunstâncias em que ele acontece naturalmente.

Ainda segundo o mesmo autor, o estudo de caso é um estudo de característica empírica, na qual irá procurar definir ou testar uma teoria, utilizando muitas das vezes os instrumentos de pesquisa tais como: entrevistas, observações direta, observação participante e dados secundários.

Conforme Marconi e Lakatos (2003), não há a principio uma estrurura aprioristicamente, ou engessada para conduzir o estudo de caso, podendo ser utilizada muitas técnicas de pesquisa. Segundo (GIL, 2002), não há um conformidade quanto as etapas a serem adotadas no estudo de caso.

Esta dissertação utiliza o sequenciamento sugerido por Cauchick Miguel *et al*. (2012) para conduzir esse estudo. A Figura 20, demostra as seis etapas do sequenciamento utilizado nessa dissertação.

Figura 20 - Sequenciamento do estudo de caso

Fonte: Baseado de Cauchick Miguel *et al*. (2012)

Na etapa **Definição da estrutura** conceitual teórica foi feito o levantamento da literatura científica, organização da literatura e compreensão do estado da arte como já esclarecido no início desse capítulo.

Na etapa **Planejamento do caso**, foram feitos contatos com grandes instituições de saúde da grande São Paulo para averiguação da possibilidade de testar esta pesquisa. Foram escolhidas três grandes instituições não públicas de saúde.

Conforme Cauchick Miguel *et al*. (2012), é utilizado nesta etapa da pesquisa um estudo de caso longitudinal, em que a pesquisa investiga o presente em detrimento ao estudo de caso retrospectivo.

Foram selecionadas três técnicas de coletas de dados: formulário, entrevista semiestruturada e observação *in modus operandis*. A utilização de várias técnicas de coletas de dados e a interação do pesquisador com os elementos pesquisados e a elaboração de constructos a partir da literatura científica proporciona que a pesquisa obtenha uma melhor validade (EISENHARDT, 1989).

Desta forma, formam selecionados formulários para serem respondidos por representantes do departamento de tecnologia da informação (TI). Conforme Marconi e Lakatos (2003), o formulário é uma guia formal destinada a reunir dados e informações relevantes de indagações propostas, da qual o preenchimento é exercido pelo próprio pesquisador. Entrevistas semiestruturadas, para questionamentos referentes a cibersegurança da instituição. Conforme Marconi e Lakatos (2003), a entrevista é o encontro entre duas pessoas, com o propósito de se adquirir informações sobre um determinado tema mediante um colóquio formal. E a observação, na qual são analisados os meio de proteção contra crimes cibernéticos da instituição de saúde. Ainda segundo Marconi e Lakatos (2003), na observação o pesquisador faz a investigação recolhendo dados sobre a questão de pesquisa mediante a observação direta ou indireta de fatos, ações ou fenômenos.

Na etapa **Conduzir o caso** é realizado um teste piloto para testar e verificar os procedimentos, validar a metodologia desenvolvida e visar seu aprimoramento. Os testes da estrutura teórico prática desenvovida foram realizados com três grandes instituições de saúde da cidade de São Paulo- Brasil, os quais constataram sua efacácia.

Na etapa de **Coleta dos dados**, os dados são recolhidos utilizando as três técnicas de coleta selecionadas: formulário, entrevista semiestruturada e observação. Conforme Yin (2001), nessa etapa o pesquisador deve: buscar praticar questões apropriadas aos objetivos da pesquisa, procurando sempre interpretar as respostas recebidas da melhor forma possível, eliminar qualquer tipo de preconceito previamente concebido, procurar sempre ser um bom ouvinte, estar bem fundamentado sobre o tema da pesquisa, estar aberto a contraposições de ideias e ser adaptativo a qualquer situação vivenciada.

Na etapa **Analisar os dados**, após a coleta dos dados é realizado uma codificação dos dados, conforme Cauchick Miguel *et al*. (2012) é o primeiro passo para reduzir o conteúdo dos dados. Nesta codificação dos dados, também serão considerados conforme os mesmos autores, todos os *insights* durante a coleta dos dados. Somente o que for essencial e relevante positivamente ou negativamente para os objetivos dessa pesquisa serão incluídos nessa dissertação. Após a codificação e inserção das informações apropriadas aos objetivos dessa pesquisa, as mesmas serão comparadas com os dados teóricos levantados.

Na etapa **Divulgar os dados**, todas as informações pertinentes são incluídas nesta dissertação e publicadas em um revista de impacto do setor para validação da comunidade científica.

Concluí-se o sequenciamento das etapas do estudo de caso, na sequencia será demostrado como será a avaliação da estrutura teórico-prática e sua aplicação.

4.7.2 Escolha das Instituições de Saúde para Aplicar o Estudo de Caso

Patton (2002), recomenda no estudo de caso, escolher instituições em que se possa retirar quantidades relevantes de informações sobre o tema da pesquisa, para extrair o máximo possivel de informações úteis para a pesquisa.

Ainda segundo o mesmo autor, é necessário elaborar critérios válidos, para selecionar as instituições em que sera exercido o estudo de caso.

Está dissertação trabalha com os critérios selecionados abaixo:

a) Escolheu-se, três grandes instituições de saúde, já consolidadas no mercado nacional, que tenham departamentos responsáveis por combater e proteger a segurança cibernética da instituição;

b) Filtrou-se, instituições que permitissem o contato com os responsáveis pela área desejável;

c) Filtrou-se, instituições que permitissem o acesso a organização para a devida aplicação da estrutura teórico-prática, comparando-a com as ferramentas utilizadas nessas instituições.

Três grandes instituições de saúde na cidade de São Paulo- Brasil foram selecionadas para aplicação da pesquisa, conforme abaixo:

a) Instituição privada de saúde com mais de 100 anos de atuação, localizada na cidade de São Paulo- Brasil, referência em diversas especialidades cirurgicas, oncologica e ginecologica com mais de 400 leitos hospitalares.

b) Instituição privada de saúde com mais de 100 anos de atuação, localizada na cidade de São Paulo- Brasil, com quase 400 leitos hospitalares. Atendendo a mais de 50 especialidades médicas.

c) Instituição privada de saúde com quase 50 anos de atuação, localizada na cidade de São Paulo- Brasil, com mais de 700 leitos hospitalares. Atendendo a dezenas de especialidades médicas.

Desta forma, o próximo capítulo irá debater sobre a análises dos resultados encontrados nestas três instituições de saúde.

5. ANÁLISE DOS RESULTADOS E DISCUSSÕES

Conforme Thompson e Perry (2004), para a análise dos resultados e a devida garantia da qualidade da pesquisa, qualquer método de pesquisa científica deve ser guiado pela confiabilidade e validade dos resultados.

Os primeiros resultados gerados foram obtidos por meio da revisão da literatura conforme são apresentados a seguir.

5.1 MENSURAÇÃO DA LITERATURA CIENTÍFICA.

Com a revisão da literatura foi possível mensurar, interpretar e extrair informações tais como: os principais autores e *journals* da área, as principais soluções, lacunas e métodos de estudos científicos.

Desta forma, foi possível observar uma evolução das publicações do tema apresentado nos últimos anos e sua importância para a comunidade. Foi possível observar a internacionalidade dos artigos da amostra, sendo possível observar uma hegemonia de autores dos EUA, China e Índia.

Conforme Thomé *et al*. (2016) a frequência de citação de uma palavra nos artigos permite uma primeira leitura dos temas em uma determinada área. Dos 294 conjuntos de palavras-chave dos artigos pertencentes a esse estudo, os três vocábulos mais presente foram: *cybersecurity* presente 30 vezes, *security* presente 05 vezes e *privacy* presente 05 vezes.

Foi possível observar um predomínio, de publicações de artigos com a colaboração de mais de uma instituição de pesquisa em detrimento a publicações de apenas uma única instituição. Comprova-se com esses dados uma ciência sem fronteiras praticada por pesquisadores em diferentes partes do globo, com o objetivo de desenvolvimento do conhecimento humano.

Foi possível verificar os *journals: Ieee Access, International Journal Of Project Management e Engineering, Construction And Architectural Management* como os mais representativos, referente ao tema cibersegurança no setor de saúde.

Os três artigos mais relevantes analisados têm mais de 100 citações. Encabeçado pelo pesquisador Chan, Albert P.C., da *Hong Kong Polytechnic University* (China), com 189 citações, o pesquisador Keil, Mark de *Georgia State*

University (EUA) com 172 citações e o pesquisador Kruegel, Christopher da *University of Florida* (EUA) com 171 citações.

Os próximos tópicos apresentam os principais resultados encontrados nas três instituições de saúde analisadas nesta pesquisa. As mesmas serão apresentadas como instituição de saúde A, B e C.

5.2 ANÁLISES INTRA-CASOS

A análise intra-casos se concretiza por meio da comparação dos elementos relevantes analisados nesta pesquisa das três instituições de saúdes investigadas, com o foco em cada uma das instituições isoladamente.

5.2.1 Instituição de saúde A

A instituição de saúde A, conta com um padrão de excelência comparável a grandes instituições médicas internacionais. Conforme Cooper (2020), está entre as quinze melhores instituições de saúde do país. É centenária na área da saúde, privada, localizada na cidade de São Paulo, sendo uma referência em diversas especialidades cirúrgicas, oncológica e ginecológica e constituída com mais de 400 leitos hospitalares. O setor pesquisado de segurança da informação, pertence a área de tecnologia da informação (TI), sendo o setor composto por nove colaboradores.

O primeiro ponto observado a ser mencionado a respeito dos resultados da pesquisa na instituição consiste em que eles nunca presenciaram problemas referentes a cibersegurança.

Foi constatado também que a instituição emprega grandes esforços para sempre possuir os melhores equipamentos e *softwares* disponíveis no mercado para a instituição. Também foi observado que, na instituição os equipamentos são trocados regularmente por novas versões e todas as atualizações são feitas regularmente. Outro ponto observado é que, todos os colaboradores do setor pesquisado têm curso superior e experiência no mercado.

Foi constatado que a instituição considera eficiente para a proteção e integridade de seus sistemas e dados apenas software antivírus e sistemas de *firewall*. Eles acreditam que a instituição está completamente segura com esses dois elementos utilizados. Ainda, relataram que a estrutura teórico-prática desenvolvida é

eficiente, bem estruturada e possui boas ferramentas de controle a segurança cibernética. Entretanto, acreditam que somente a utilização das duas ferramentas já utilizadas e mencionadas anteriormente seja suficiente para proteger a instituição.

Conforme análise da estrutura teórico-prática pela instituição, os entrevistados acreditam que é uma solução bem desenvolvida e estrutura é eficiente para combater ameaças cibernéticas. Não sugeriram nenhuma inclusão ou exclusão de seus elementos/estrutura, pois acreditam que está bem projetada.

A Tabela 15, apresenta os critérios analisados da instituição.

Tabela 15 – Critérios analisados na instituição de saúde A.

INSTITUIÇÃO A			
Categoria	**Itens Analisados**	**Resultado**	**Observações**
Incidentes Cibernéticos	Interrupção dos sistemas/serviços	Nunca	0
	Perda de dados	Nunca	0
	Problemas com colaboradores internos	Nenhum	0
	Controle de acesso ao sistemas e dados	Sim	NA
Sistemas de Proteção Cibernéticos	Atualização de equipamentos e *softwares*	Regularmente	A cada nova versão
	Backups dos sistemas e dados	Regularmente	Semanalmente
	Antivírus	Sim	*full time*
	Sistemas de *firewalls*	Sim	*full time*
	Criptografia dos dados	Não	0
	Inteligência artificial	Não	0
Políticas e Treinamentos	Políticas de combate a cibersegurança	Sim	NA
	Treinamentos sobre cibersegurança	Sim	Apenas na contratação
	Padrões de segurança cibernética	Sim	Vários padrões
Gestão de Riscos Cibernéticos	Plano de gerenciamento de riscos cibernéticos	Não	Não utilizam
	Plano de gerenciamento de crises	Não	Não utilizam
	Auditoria de segurança cibernética	Não	Não utilizam
Estrutura Teórico-Prática Desenvolvida	Aprovou a estrutura teórico-prática	Sim	NA
	Sugestão de alterações/aperfeiçoamentos	Nenhuma	NA
	Avalia como necessária para a instituição	Sim	Sim
	Adotaria a estrutura teórico-prática na instituição	Sim	Sim, caso fosse necessária

Fonte: Autor.

5.2.2 Instituição de saúde B

A instituição de saúde B conta com um padrão de excelência Europeu. É também centenária na área da saúde, privada, localizada na cidade de São Paulo, atende a mais de cinquenta especialidades médicas e constituída com quase 400 leitos hospitalares. E conforme Cooper (2020) também consta nas entre as quinze melhores instituições de saúde do Brasil. O setor pesquisado de segurança da informação pertence à área de TI, sendo o setor composto por seis colaboradores.

O primeiro ponto observado a ser mencionado é que a instituição nunca presenciou problemas referentes a cibersegurança. Também foi constatado que a instituição investe grandes esforços para possuir os melhores equipamentos e *softwares* disponíveis no mercado. Foi observado que os equipamentos são atualizados regularmente. Todos os colaboradores do setor pesquisado têm curso superior e experiência no mercado.

Foi notado que a instituição considera suficiente para a proteção e integridade de seus sistemas e dados apenas *softwares*, antivírus e sistemas de *firewall*. Eles acreditam que a instituição está completamente segura com esses dois elementos utilizados.

Foi relatado que, a estrutura teórico-prática desenvolvida e apresentada para avaliação é eficiente, bem estruturada e possui ferramentas apropriadas de controle a segurança cibernética. Entretanto, a exemplo da empresa A, acreditam que somente a utilização das duas ferramentas já utilizadas e descritas seja suficiente para proteger a instituição.

Conforme avaliação da estrutura teórico-prática, os entrevistados acreditam que ela é uma solução eficiente e não sugeriram nenhuma inclusão, exclusão ou alteração de seus elementos/estrutura.

A Tabela 16, apresenta os critérios analisados da instituição.

Tabela 16 – Critérios analisados na instituição de saúde B.

INSTITUIÇÃO B			
Categoria	**Itens Analisados**	**Resultado**	**Observações**
Incidentes Cibernéticos	Interrupção dos sistemas/serviços	Nunca	0
	Perda de dados	Nunca	0

	Problemas com colaboradores internos	Nenhum	0
	Controle de acesso ao sistemas e dados	Sim	NA
Sistemas de Proteção Cibernéticos	Atualização de equipamentos e *softwares*	Regularmente	A cada nova versão
	Backups dos sistemas e dados	Regularmente	Diariamente
	Antivírus	Sim	*full time*
	Sistemas de *firewalls*	Sim	*full time*
	Criptografia dos dados	Sim	0
	Inteligência artificial	Não	0
Políticas e Treinamentos	Políticas de combate a cibersegurança	Sim	NA
	Treinamentos sobre cibersegurança	Sim	Apenas na contratação
	Padrões de segurança cibernética	Sim	Vários padrões
Gestão de Riscos Cibernéticos	Plano de gerenciamento de riscos cibernéticos	Não	Não utilizam
	Plano de gerenciamento de crises	Não	Não utilizam
	Auditoria de segurança cibernética	Não	Não utilizam
Estrutura Teórico-Prática Desenvolvida	Aprovou a estrutura teórico-prática	Sim	NA
	Sugestão de alterações/aperfeiçoamentos	Nenhuma	NA
	Avalia como necessária para a instituição	Não	Sim, caso fosse necessário
	Adotaria a estrutura teórico-prática na instituição	Sim	Sim, caso fosse necessária

Fonte: Autor.

5.2.3 Instituição de saúde C

A instituição de saúde C, conta com um padrão de excelência comparável a excelentes instituições médicas internacionais. Tem quase 50 anos na área da saúde, privada, localizada na cidade de São Paulo, sendo uma referência em diversas especialidades médicas e constituída com mais de 700 leitos hospitalares. E conforme Cooper (2020), também consta entre as quinze melhores instituições de saúde do Brasil. O setor pesquisado de segurança da informação, pertence a área de tecnologia da informação (TI), sendo o setor composto por cinco colaboradores.

O primeiro ponto observado e a ser mencionado a respeito dos resultados da pesquisa na instituição consiste que eles nunca presenciaram problemas referentes a cibersegurança.

Foi constatado também que a instituição investe para possuir os melhores equipamentos e *softwares* disponíveis no mercado. Também foi observado que os

equipamentos são trocados regularmente por novas versões e todas as atualizações são feitas regularmente. Outro ponto observado é que todos os colaboradores do setor pesquisado têm curso superior e experiência no mercado.

Foi constatado ainda que, a instituição considera eficiente para a proteção e integridade de seus sistemas e dados apenas software antivírus e sistemas de *firewall*. Eles acreditam que a instituição está completamente segura e protegida com a utilização desses dois elementos utilizados. Os entrevistados relataram que a estrutura teórico-prática analisada é eficiente, bem estruturada e possui boas ferramentas de controle a segurança cibernética. Entretanto, acreditam que somente a utilização das duas ferramentas utilizadas e já mencionadas seja o suficiente para proteger a instituição.

Conforme análise da estrutura teórico-prática pela instituição, acreditam que é uma solução eficiente e não sugeriram nenhuma inclusão ou exclusão de seus elementos/estrutura.

A Tabela 17, apresenta os critérios analisados da instituição.

Tabela 17 – Critérios analisados na instituição de saúde C.

INSTITUIÇÃO C			
Categoria	**Itens Analisados**	**Resultado**	**Observações**
Incidentes Cibernéticos	Interrupção dos sistemas/serviços	Nunca	0
	Perda de dados	Nunca	0
	Problemas com colaboradores internos	Nenhum	0
	Controle de acesso ao sistemas e dados	Sim	NA
Sistemas de Proteção Cibernéticos	Atualização de equipamentos e *softwares*	Regularmente	A cada nova versão
	Backups dos sistemas e dados	Regularmente	Semanalmente
	Antivírus	Sim	*full time*
	Sistemas de *firewalls*	Sim	*full time*
	Criptografia dos dados	Não	0
	Inteligência artificial	Não	0
Políticas e Treinamentos	Políticas de combate a cibersegurança	Sim	NA
	Treinamentos sobre cibersegurança	Sim	Apenas na contratação
	Padrões de segurança cibernética	Sim	Vários padrões
Gestão de Riscos Cibernéticos	Plano de gerenciamento de riscos cibernéticos	Não	Não utilizam

	Plano de gerenciamento de crises	Não	Não utilizam
	Auditoria de segurança cibernética	Não	Não utilizam
Estrutura Teórico-Prática Desenvolvida	Aprovou a estrutura teórico-prática	Sim	NA
	Sugestão de alterações/aperfeiçoamentos	Nenhuma	NA
	Avalia como necessária para a instituição	Não	Não, analisa como necessária
	Adotaria a estrutura teórico-prática na instituição	Sim	Sim, caso fosse necessária

Fonte: Autor.

5.3 ANÁLISES ENTRE-CASOS

Nesta seção, será apresentada por meio de uma triangulação os resultados mais relevantes obtidos nas três instituições de saúdes analisadas. Conforme Ellram (1996), é importante uma pré-esturutração dos casos para uma melhor análise qualitativa além de melhorar a revisão e a síntese dos dados analisados.

Já na visão de Miles e Huberman (1994), a organização e apresentação dos casos é de relevante para os resultados da pesquisa, sendo que os dados devem ser exibidos de modo a facilitar as conexões e relações entre os casos analisados na pesquisa. Ainda, segundo os mesmos autores, se faz necessária a criação de uma matriz com a subdivisão das principais categorias identificadas entrelaçadas entre linhas e colunas por meio de suas similaridades e proporções, diferenças e contrates, e por último por padrões identificados entre os casos analisados.

Sengundo Cooper (2020), as três instituições de saúde em que a pesquisa foi aplicada então entre as melhores instituições de saúde do Brasil.

A Tabela 18 traz uma análise comparativa geral entre os três estudos de casos.

Tabela 18 – Comparativo entre os estudos de caso.

Categorias	Itens Analisados	Instituição A	Instituição B	Instituição C
Perfis das Instituições	Tipo	Privada	Privada	Privada
	Tempo de operações no Brasil	mais de 100 anos	mais de 100 anos	quase 50 anos
	Leitos	mais de 400	quase 400	mais de 700
	Porte	Grande	Grande	Grande
	Investem em cibersegurança	sim	sim	sim

Elaboração do Plano de Gerenciamento de Riscos	Definir e entender o que são riscos cibernéticos	sim	não	não
	Identificar os riscos cibernéticos	não	não	não
	Avaliar os riscos cibernéticos	sim	não	não
	Analisar a probabilidade dos riscos cibernéticos	não	não	não
	Verificar o impacto dos riscos cibernéticos	não	não	não
	Classificar os riscos cibernéticos	sim	não	não
	Planejar respostas aos riscos cibernéticos	sim	sim	sim
Execução do Plano de Gerenciamento de Riscos	Disseminação do plano de gerenciamento de riscos	não	não	não
	Treinamento e qualificação	sim	sim	sim
	Adequar a organização com as ações de riscos acordadas	sim	sim	sim
	Execução de requisitos de sistemas *cyber* no setor de *healthcare*	sim	sim	sim
Monitoramento do Plano de Gerenciamento de Riscos	Monitorar os riscos cibernéticos	sim	sim	sim
	Gerenciar os riscos cibernéticos residuais	sim	não	não
Implantação das Contramedidas Necessárias para Conter os Riscos	Executar o plano de gerenciamento de crises	não	não	não
Efeitos	Aprovaram a estrutura teórico-prática	sim	sim	sim
	Irão utilizá-la na instituição	não	não	não
	Deram sugestão de melhorias na estrutura teórico-prática	não	não	não

Fonte: Autor.

Como se observa na análise da comparação dos três casos analisado, há uma semelhança bastante relevante entre as condutas relativas à cibersegurança nas três instituições analisadas.

O que mais chama a atenção é o fato de todas elas acreditam que, ao adotarem *softwares*, antivírus e *firewalls*, estão totalmente protegidas contra eventuais ataques cibernéticos e outros problemas semelhantes de segurança de suas informações. Talvez o fato de nunca terem experimentado problemas sérios nessa área dê as instituições de saúde a falsa impressão de que tais instrumentos são suficientes. Porém, o fato relevante é que em termos de segurança das informações todas as três

instituições encontram-se altamente vulneráveis. Se nunca tiveram problemas é porque ninguém ainda se interessou em interferir em seus sistemas e bancos de dados. Para corroborar essa afirmação, basta lembrar o que Sanger, Perlroth e Schmitt (2020) relataram: “O Departamento de Estado, o Departamento da Segurança Interna e partes do Pentágono dos Estados Unidos, foram invadidos por *hackers* russos e tiveram boa parte dos seus dados comprometidos”.

Se as organizações mencionadas, que estão entre as melhores protegidas do mundo, são atacadas e comprometidas por um ataque cibernético, por certo não será um simples antivírus associado a um *firewall* que irá evitar que o mesmo aconteça com as instituições avaliadas.

Complementado a análise, a Tabela 19 apresenta uma comparação entre as catorze principais asserções encontradas na literatura científica levando em conta os resultados encontrados nos três estudos de casos nas instituições de saúde do Brasil.

Tabela 19 – Comparação entre as principais asserções encontradas na literatura científica em detrimento as resultados dos três estudos de casos.

Asserções \ Autores	Abraham *et al.* (2019)	Ahmed *et al.* (2019)	Alexander *et al.* (2019)	Al-Muhtadi *et al.* (2019)	Blanke *et al.* (2016)	Coronado *et al.* (2014)	Coventry *et al.* (2018)	Diggans *et al* (2019)	Gordon *et al.* (2019)	Koppel *et al* (2019)	Kruse *et al.* (2017)	Kure *et al.* (2018)	Lechler *et al* (2017)	Leung *et al.* (2019)	Maimó *et al.* (2019)	Martin *et al.* (2017)	Ondiege *et al.* (2017)	Pesapane *et al.* (2018)	PMI (2017)	**Total**	**Instituição A**	**Instituição B**	**Instituição C**
Cibersegurança é um componente que se torna cada vez mais importante na infraestrutura de segurança das organizações de saúde	x	x	x		x		x		x		x	x			x	x	x	x		**12**	Concorda	Concorda	Concorda
Alerta as instituições de saúde sobre as vulnerabilidades relacionadas as novas tecnologias e as incentiva a tomarem medidas para aprimorar a segurança de seus dispositivos e banco de dados	x	x	x	x	x	x	x	x		x	x			x			x			**12**	Não acredita que a instituição está vulnerável	Não acredita que a instituição está vulnerável	Não acredita que a instituição está vulnerável
Um grande problema é o tempo de detecção de uma invasão aos sistemas, muitas vezes podendo ser executada sem que os responsáveis pelo sistema tenham consciência do ataque	x					x	x	x			x				x					**6**	Acreditam que é muito difícil a invasão ao sistema	Acreditam que é muito difícil a invasão ao sistema	Acreditam que é muito difícil a invasão ao sistema
As instituições de saúde devem se empenhar em soluções e técnicas de proteção de dados, mecanismos de controle de acesso, *firewalls*, sistemas de detecção de intrusão, mecanismos de criptografia, filtros de *spam*, conscientização e treinamento do usuário. Porém, não são suficientes para defender os sistemas de ataques cibernéticos.													x		x	x				**3**	Concorda	Acreditam que apenas com as técnicas relatadas já é o suficiente para se protegerem	Acreditam que apenas com as técnicas relatadas já é o suficiente para se protegerem
Acredita-se que atualmente a principal razão de ataques cibernéticos a instituições de saúde é para o ganho financeiro							x				x					x				**3**	Concorda	Não acredita que a instituição está vulnerável a este problema	Não acredita que a instituição está vulnerável a este problema

Devido à natureza crítica dos dispositivos médicos e sua capacidade de impactar a saúde do paciente, o potencial de dano em uma violação da segurança cibernética é catastrófico, a vulnerabilidade identificada neste segmento é extremamente complexa	x	x	x			x					x					x	x	x		**8**		Concorda	Acredita que a instituição está protegida e não teria problema em recuperar os dados	Acredita que a instituição está protegida e não teria problema em recuperar os dados
Acredita-se que não há um modelo padrão de segurança cibernética adequado que proteja 100% as instituições de saúde	x			x		x	x				x							x		**6**		Concorda	Acredita que apenas com antivírus e firewall a instituição está protegida	Acredita que apenas com antivírus e firewall a instituição está protegida
Predomina nas instituições de saúde equipamentos desatualizados ou ultrapassados facilitando que *hackers* ou *malwares* explorem essas vulnerabilidade desse sistema						x	x				x									**3**		Não concorda com a afirmação, relata que a instituição tem os melhores equipamentos disponíveis no mercado	Não concorda com a afirmação, relata que a instituição tem os melhores equipamentos disponíveis no mercado	Não concorda com a afirmação, relata que a instituição tem os melhores equipamentos disponíveis no mercado
Há a falta de profissionais qualificados em cibersegurança atuando no setor de saúde. Muito dos profissionais que atuam no setor são inexperientes e despreparados para suprir as dificuldades enfrentadas pelo setor						x	x				x									**3**		Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com qualificação e experiência adequada as necessidades do mercado	Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com qualificação e experiência adequada as necessidades do mercado	Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com qualificação e experiência adequada as necessidades do mercado
Os especialistas em cibersegurança são caros e escassos. As organizações de saúde geralmente não podem arcar com as taxas de mercado por seus serviços e acabam dispondo de equipes sem o devido preparo							x				x					x				**3**		Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com ganhos financeiros adequados ao mercado	Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com ganhos financeiros adequados ao mercado	Não concorda com a afirmação, relata que a instituição tem ótimos profissionais com ganhos financeiros adequados ao mercado
Apenas recentemente a cibersegurança tornou-se um tópico importante dentro do setor de saúde	x					x												x		**3**		Acredita que a cibersegurança não é um tópico recente, mas, já conhecido a muito tempo	Acredita que a cibersegurança não é um tópico recente, mas, já conhecido a muito tempo	Acredita que a cibersegurança não é um tópico recente, mas, já conhecido a muito tempo

As organizações de saúde, devem possuir uma estrutura de cibersegurança baseada em risco	x	x		x	x	x			x		x		x			x	x			**10**		Concorda	Não concorda. Acredita que somente com antivírus e firewall a instituição está protegida	Não concorda. Acredita que somente com antivírus e firewall a instituição está protegida
No âmago do problema pode-se destacar a falta de investimentos significativos para proteger os sistemas/dados	x					x										x				**3**		Não concorda. Acredita que a instituição tem investimentos significativos e suficientes para se proteger de ciberataques	Não concorda. Acredita que a instituição tem investimentos significativos e suficientes para se proteger de ciberataques	Não concorda. Acredita que a instituição tem investimentos significativos e suficientes para se proteger de ciberataques
Uma solução simples e eficiente é o treinamento nas instituições de saúde regularmente	x					x			x		x					x			x	**6**		Concorda. A organização pratica essa prática regularmente	Concorda. Porém, a instituição só a emprega na contratação de um novo colaborador	Concorda. Porém, a instituição só a emprega na contratação de um novo colaborador

Fonte: Autor.

Conclui-se com um ceticismo perigoso e imprudente das instituições de saúde nacionais em relação a cibersegurança. Em que, as mesmas, acreditam estarem totalmente seguras contra ciberataques. Observou-se também um ceticismo semelhante em um passado recente em instituições de saúde internacionais por diversos estudos encontrados na literatura científica. O que ocasionou nestas instituições internacionais diversos contratempos como perda da credibilidade da marca da instituição, paralisação das atividades médicas que são essenciais a vida, perdas financeiras e o extravio de informações sigilosas entre outras.

É importante que o mercado nacional tenha ciência desses problemas para não cometerem os mesmos erros de suas equivalentes no mercado internacional.

A próxima seção, irá proporcionar as conclusões encontradas nesta pesquisa sobre o tema cibersegurança em instituições de saúde.

6. CONCLUSÃO

Conforme constatado por esta pesquisa, em nenhum outro momento na história há tantas informações geradas e processadas digitalmente como nos presentes dias, visto que a tendência é que cada vez mais estes números aumentem exponencialmente. Isso traz como subproduto um aumento no número de ataques cibernéticos a órgãos, instituições e empresas para desviar essas informações.

Também foi constatado que, grande parte das violações referentes a cibersegurança está diretamente relacionada à negligência e/ou descuido das instituições. Do mesmo modo observou-se que, o setor de saúde é um dos mais vulneráveis a estas invasões, visto que um dos fatos constatados é que o orçamento total empregados para a gestão de cibersegurança das instituições de saúde é em média de 0% a 3% do orçamento total do departamento de TI. De maneira oposta outros setores da economia chegam a empregar em média de 4% a 10% de seus orçamentos a esta mesma questão.

Também foi verificado que, somente os mecanismos de proteção cibernéticas padrões como: antivírus, sistemas de detecção de intrusões (IDS), *firewalls*, *webfilters*, VPN's etc., não são suficientes para defender os sistemas das organizações. Entretanto, nesta pesquisa, observou-se que as instituições nacionais semelhantemente às internacionais, erroneamente têm uma falsa sensação de proteção, apenas com a utilização daqueles mecanismos. Consequentemente, a estratégia para lidar com os riscos cibernéticos empregada é uma remediação que ocorre somente após o fato ocorrido.

Adicionalmente, esta pesquisa contribui com a teoria, pois com uma revisão da bibliografia, qual foi possível selecionar os melhores artigos e autores referentes ao tema de estudo com maior relevância e valor. Como resultado, observou-se uma lacuna de pesquisa já que não há uma literatura específica sobre cibersegurança em instituições de saúde nacionais, pois todo o conteúdo teórico disponível refere-se a pesquisa de grandes instituições norte americanas, europeias e asiáticas. Portanto, o desenvolvimento de uma estrutura teórico-prática para cibersegurança em instituições brasileiras, acrescenta conhecimento à literatura que trata do tema.

Igualmente, esta pesquisa gera contribuições à prática. Por meio de estudo de casos foi possível testar uma melhor visão para a proteção das instituições de saúde, proporcionando uma ferramenta com melhores informações, agilidade e praticidade

para o setor de saúde no qual as instituições analisadas corroboraram a eficiência e potencialidade da estrutura desenvolvida e analisada. Entretanto, estas não a consideram necessária Já que não enfrentaram problemas com a estrutura precária de segurança que usam no momento. Com base na literatura analisada, os ataques cibernéticos a essa instituições é a penas uma questão de tempo.

Como conclusão global desta pesquisa é demostrado que, este julgamento das instituições nacionais corrobora pesquisas internacionais quanto a falta de consciência das instituições julgando estarem protegidas apenas com proteções como *firewall* e antivírus. Isso demostra uma grande vulnerabilidade das instituições nacionais às atuais adversidades impostas pelo atual desenvolvimento tecnológico que a humanidade desfruta.

Do mesmo modo, as contribuições para a sociedade, encontradas corroboram, como já dito, as principais pesquisas internacionais. Com uma cibersegurança inadequada, resulta não somente no comprometimento de informações pessoais de pacientes, mas também, no comprometimento de dispositivos vitais à vida utilizados por estas instituições. Igualmente, os reflexos dos ataques trazem diversos problemas tanto às instituições como para a população que necessita de atendimento, impactaram no funcionamento da instituição, resultando em perda de informações, cancelamentos de consultas e procedimentos clínicos vitais a vida.

Consequentemente, a significativa dimensão econômica é uma advertência às instituição de saúdes nacionais que, devido ao seu tamanho e despreparo em proteger seus sistemas, poderão torna-se um alvo extremamente atraente. Isso impacta além da perda de informações sigilosas com reflexos de alto custos monetários causados com a perda da credibilidade da instituição, as perdas causadas com a paralisação das atividades e com uma possível maior despesa por meio de *ransomwares* (bloqueio do sistema da instituição liberando-o somente após um pagamento exigido pelo invasor). Neste sentido, muitos dos custos são incalculáveis devido a criticidade do setor e dos possíveis danos causados à população.

Também se observa que, como já salientado nesta pesquisa, informações médicas são de 20 a 50 vezes mais valiosas para os cibercriminosos do que informações furtadas no setor financeiro. Atualmente a principal razão de ataque é o ganho financeiro. Contudo, não se deve descartar motivações políticas cujo objetivo é tirar vidas, em uma forma de guerra silenciosa que são projetadas por especialistas como uma evolução das tradicionais guerras armadas.

Identificou-se como limitação desta pesquisa que o presente estudo considerou apenas três das melhores instituições do país, o que não permite generalizações. É sugerido como trabalhos futuros avançar em outros estudos sobre cibersegurança junto a mais instituições de saúdes nacionais para aumentar a conscientização sobre a cibersegurança.

Finalmente, conclui-se que a estrutura teórico-prática desenvolvida para gestão de riscos em cibersegurança é eficiente e minimiza os riscos cibernéticos das instituições de saúde, no qual foram empregados métodos de gerenciamento de riscos modernos incluindo requisitos regulatórios existentes tais como: NIST, ISO31000, ISO27001, HIPAA e PMBOK. Com a estrutura de gerenciamento de riscos orientada a objetivos, esses padrões fornecem diretrizes para as atividades de gerenciamento de riscos.

Com esta ferramenta, as instituições de saúde podem se preparar e dar respostas eficientes aos riscos expostos, estando aptas a reduzi-los drasticamente e/ou até mesmo eliminá-los completamente.

REFERÊNCIAS BIBLIOGRÁFICAS

31000, I. **Risk management – Principles and guidelines**. [S.l.]. 2018.

ABDELHAMID, M.; KISEKKA, V.; SAMONAS, S. Mitigating e-services avoidance: the role of government cybersecurity preparedness. **Information and Computer Security**, 27, 2018. 26-46.

ABRAHAM, ; CHATTERJEE, ; SIMS, R. Muddling through cybersecurity: Insights from the U.S. healthcare industry. **Business Horizons**, v.62, n. n.04, 2019. 539-548.

AHMED, A. A.; AHMED, W. A. An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. **Sensors**, v. 19 n.17, 2019.

ALEXANDER, ; HASEEB, ; BARANCHUK,. Are implanted electronic devices hackable? **Trends in Cardiovascular Medicine**, 2019. 476-480.

AL-MUHTADI, J. *et al*. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. **Health Informatics Journal**, v. 25, p. 315-329, 2019.

ANDERSSON, J. O. *et al*. Thermo-Calc & DICTRA, computational tools for materials science. **Calphad: Computer Coupling of Phase Diagrams and Thermochemistry**, 26 n.2, 2002. 273-312.

ASKAR, A. J. Healthcare management system and cybersecurity. **International Journal of Recent Technology and Engineering**, p. 237-248, 2019.

BARDIN, L. **El Analisis de Contenido**. 70. ed. São Paulo: Almedina Brasil, 2011.

BERGER, M.; SCHNECK,. National and transnational security implications of asymmetric access to and use of biological data. **Frontiers in Bioengineering and Biotechnology**, v. 7, 2019.

BILEK, M.; MUSCIONICO; AMIEL,. A primer on the regulation and development of M-Health products. **Regulatory Rapporteur**, p. https://www.scopus.com/record/display.uri?eid=2-s2.0-85032879397&origin=inward&txGid=408ced46814b35c8bd8454243cf24e2d, 2017.

BISSONNETTE, L.; BERGERON, M. G. Portable devices and mobile instruments for infectious diseases point-of-care testing. **Expert Review of Molecular Diagnostics**, p. 471-494, 2017.

BLANKE, J.; MCGRADY,. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. **Journal of healthcare risk management**, p. 14-24, 2016.

BOBBIO, A. *et al*. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. **Reliability Engineering and System Safety**, 71, 2001. 249–260.

BOJANOVA, ; VOAS,. Trusting the Internet of Things. **IT Professional**, v. 19 n.5, p. 16-19, 2017.

BOZICKOVICI, R. *et al*. Integration of simulation and lean tools in effective production systems - Case study. **Journal of Mechanical Engineering**, 58, 2012. 642-652.

BRAGA, *et al*. Understanding How to Use Static Analysis Tools for Detecting Cryptography Misuse in Software. **IEEE Transactions on Reliability**, p. 1384-1403, 2019.

BRODY, R. G.; CHANG, H. U.; SCHOENBERG, E. S. Malware at its worst: death and destruction. **International Journal of Accounting & Information Management**, 2018.

BUBNOV, G. *et al*. Increasing Flexibility of Risk Management in it Projects with Isorisk Curves and Risk Mapping. **International Workshop on Computer Science and Engineering**, 2015. 314-317.

BUSDICKER, M.; UPENDRA, P. The role of healthcare technology management in facilitating medical device cybersecurity. **Biomedical Instrumentation and Technology**, p. 19-25, 2017.

CAGLIANO, A. C. *et al*. Risk Management in Hospital Wards: The Case of Blood Procurement and Handling. **IFAC-PapersOnLine**, 50 n.1, 2017. 4648-4653.

CAUCHICK MIGUEL, P. *et al*. **Metodologia de Pesquisa em Engenharia de Produção e Gestão de Operações**. Rio de janeiro: Elsevier Editora Ltda., 2012.

CHAN, A. P. C.; SCOTT, D.; LAM, E. W. M. Framework of success criteria for design/build projects. **Journal of Management in Engineering**, v. 18 n.3, p. 120-128, 2002.

CLELAND-HUANG, J. How well do you know your personae non gratae? **IEEE Software**, v. 31, p. 28-31, 2014.

COOPER, N. The Wold's Best Hospital 2020. **Newsweek**, n. 2020 Ed., 2020. Disponivel em: <https://www.newsweek.com/best-hospitals-2020/brazil>.

CORONADO, A. J.; WONG, T. L. Healthcare cybersecurity risk management: Keys to an effective plan. **Biomedical Instrumentation and Technology**, v. 48, p. 26-30, 2014.

COVENEY, P. V.; DOUGHERTY, E. R.; HIGHFIELD, R. R. Big data need big theory too. **Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences**, 374, 2016.

CRESWELL, J. W. **Projeto de pesquisa métodos qualitativo, quantitativo e misto**. Porto Alegre : Artmed Bookman, 2007.

DANDAGE, R.; MANTHA, S. S.; RANE, S. B. Ranking the risk categories in international projects using the TOPSIS method. **International Journal of Managing Projects in Business**, v. 11, p. 317-331, 2018.

DEFOND, M.; ZHANG, J. A review of archival auditing research. **Journal of Accounting and Economics**, 58 n. 2, 2014. 275-326.

DIGGANS, ; LEPROUST,. Next steps for access to safe, secure DNA synthesis. **Frontiers in Bioengineering and Biotechnology**, v. 7, 2019.

DUGAN, J. B.; BAVUSO, S. J.; BOYD, M. A. Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems. **IEEE Transactions on Reliabilit**, 41, 1992. 363-377.

EISENHARDT, K. M. Building Theories from Case Study Research. **Academy of Management Review**, v. 14 n.4, p. 532-550, 1989.

ELIZABETH, M. J.; JOBIN, J.; DONA, J. A fog based security model for electronic medical records in the cloud database. **International Journal of Innovative Technology and Exploring Engineering**, 8 n.7, 2019. 2552-2560.

ELLRAM, L. M. The use of the case study method in logistics research. **Journal of Business Logistics**, 17 n.2, 1996. 93-138.

FAUZIYAH, S. *et al*. Evaluating and mitigating risk of an automated people mover system project: A case study. **Journal of Physics: Conference Series**, 1444, 2020.

FRONTONI, E. *et al*. Sharing health data among general practitioners: The Nu.Sa. project. **International Journal of Medical Informatics**, 129, 2019. 267-274.

GEORGE, R.; BELL, L. C.; BACK, W. E. Critical Activities in the Front-End Planning Process. **Journal of Management in Engineering**, 24 n.2, 2008. 66-74.

GHAFIR, I. *et al*. BotDet: A System for Real Time Botnet Command and Control Traffic Detection. **IEEE Access**, p. 38947-38958, 2018.

GHAURI, P.; GRONHAUG, K. **Research Methods in Business Studies:** A Practical Guide. 3º. ed. London: Prentice Hall, 2005.

GIL, A. C. **Como Elaborar Projeto de Pesquisa**. São Paulo: Atlas S.A, 2002.

GONCHAROV, E.; KRUGLOV, K.; DASHCHENKO, Y. Five ICS cybersecurity myths based on Kaspersky Lab ICS CERT experience. **At-Automatisierungstechnik**, 67, 2019. 372-382.

GORDON, W. J. *et al*. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. **Journal of the American Medical Informatics Association**, p. 547-552, 2019.

GRIMES, S.; WIRTH, A. Holding the Line: Events that Shaped Healthcare Cybersecurity. **Biomedical instrumentation & technology**, 2017.

GUO, S. From printing to internet, are we advancing in technological application to language learning? **British Journal of Educational Technology**, 41 n.2, 2010. E10-E16.

HABIBZADEH, *et al*. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. **Sustainable Cities and Society**, v. 50, 2019.

HANDLER,. Data Sharing Defined-Really! **Computer**, p. 36-42, 2018.

HELMS, M. M.; NIXON, J. Exploring SWOT analysis – where are we now?: A review of academic research from the last decade. **Journal of Strategy and Management**, 3 n. 3, 2010. 215-251.

HOFMANN, E.; RÜSCH, M. Industry 4.0 and the current status as well as future prospects on logistics. **Computers in Industry**, p. 23-34, 2017.

HONG, P.; NAHM, A. Y.; DOLL, W. J. The role of project target clarity in an uncertain project environment. **International Journal of Operations and Production Management**, 24 n.12, 2004. 1269-1291.

HUTCHINS, M. J. *et al*. Framework for Identifying Cybersecurity Risks in Manufacturing. **Procedia Manufacturing**, 1, 2015. 47-63.

JALALI, S. *et al*. EARS to cyber incidents in health care. **Journal of the American Medical Informatics Association**, v. 26, p. 81-90, 2019.

JONES, E. C.; PARAST, M. M.; ADAMS, S. G. A framework for effective Six Sigma implementation. **otal Quality Management and Business Excellence**, 21 n.4, 2010. 415-424.

KAYNAK, H. The relationship between total quality management practices and their effects on firm performance. **Journal of Operations Management**, 21 n. 4, 2003. 405-435.

KEIL, M.; WALLACE, L.; RAI, A. Understanding software project risk: A cluster analysis. **Information and Management**, v. 42 n.1, p. 115-125, 2004.

KESSLER, S. R. *et al*. Information security climate and the assessment of information security risk among healthcare employees. **Health informatics Journal**, 2019.

KHARRAZ, ; ROBERTSON , ; KIRDA,. Protecting against Ransomware: A New Line of Research or Restating Classic Ideas? **IEEE Security and Privacy**, v. 16, p. 103-107, 2018.

KING, *et al*. Digital Diabetes Congress 2018. **Journal of Diabetes Science and Technology**, p. 1231-1238, 2018.

KOPPEL, R.; KUZIEMSKY, C. Healthcare data are remarkably vulnerable to hacking: Connected healthcare delivery increases the risks. **Studies in Health Technology and Informatics**, p. 218-222, 2019.

KRUEGEL, *et al*. A comprehensive approach to intrusion detection alert correlation. **IEEE Transactions on Dependable and Secure Computing**, v. 1 n.3, p. 146-168, 2004.

KRUSE, C. S. *et al*. Cybersecurity in healthcare: A systematic review of modern threats and trends. **Technology and Health Care**, v. 25, p. 1-10, 2017.

KUERBIS, B.; BADIEI, F. Mapping the cybersecurity institutional landscape. **Australian Catholic University**, v. 19, p. 466-492, 2017.

KUJAWSKI, E.; ANGELIS, D. Monitoring Risk Response Actions for Effective Project Risk Management. **Systems Engineering**, 13 n.4, 2010. 353-368.

KURE, H. I.; ISLAM, S.; RAZZAQUE, M. A. An integrated cyber security risk management approach for a cyber-physical system. **Applied Sciences (Switzerland)**, 2018.

KWAK, Y. H.; STODDARD, J. Project risk management: lessons learned from software development environment. **Technovation**, 24, 2004. 915-920.

LEBEDA, F. J.; ZALATORIS, J. J.; SCHEERER, J. B. Government Cloud Computing Policies: Potential Opportunities for Advancing Military Biomedical Research. **MILITARY MEDICINE**, v. 183, p. 438-447, 2018.

LECHLER, ; WETZEL,. Conceptualizing the silent risk of inadvertent information leakages. **Computers and Electrical Engineering**, p. 67-75, 2017.

LEE, J.; AZAMFAR, M.; SINGH, J. A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. **Manufacturing Letters**, 2019. 34-39.

LEUNG, *et al*. Patient and family member readiness, needs, and perceptions of a mental health patient portal: A mixed methods study. **Studies in Health Technology and Informatics**, p. 266-270, 2019.

LOI, M. *et al*. Cybersecurity in health –disentangling value tensions. **Journal of Information, Communication and Ethics in Society**, p. 229-245, 2019.

LUPAN, R. *et al*. A relationship between Six Sigma and ISO 9000:2000. **Quality Engineering**, 17 n.4, 2005. 719-725.

MAAS, S.; RENIERS, G. Development of a CSR model for practice: connecting five inherent areas of sustainable business. **Journal of Cleaner Production**, 64 n.1, 2014. 104-114.

MAIMÓ, *et al*. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. **Sensors (Switzerland)**, 2019.

MANSOORZADEH, S. *et al*. A Comprehensive and Practical Framework for Reliable Scheduling in Project Management. **Advanced Materials Research**, 903, 2014. 378-383.

MARCONI, A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 5º Edição. ed. São Paulo: Atlas S.A, 2003.

MAROSIN, D.; LINDEN, D.; SOUSA, S. A Collaborative Risk Management Framework for Enterprise Architecture, 2014.

MARTIN , G. *et al*. Cybersecurity and healthcare: How safe are we? **BMJ (Online)**, 2017.

MASSEY, J. E.; LARSEN, J. P. Crisis Management in Real Time: How to Successfully Plan for and Respond to a Crisis. **Journal of Promotion Management**, 12/3, 2006.

MATSUO, M.; NAKAHARA, J. The effects of the PDCA cycle and OJT on workplace learning. **The International Journal of Human Resource Management**, 24 n.1, 2013. 195-207.

MEKHILEF, M.; CARDINAL, J. S. L. A pragmatic methodology to capture and analyse decision dysfunctions in development projects. **Technovation**, 25 n.4, 2005. 407-420.

MILES, M. B.; HUBERMAN, A. M. **Qualitative Data Analysis**. 2ª Ed. ed. London: SAGE Publications, v. 16 n. 7, 1994. 575-582 p.

MOHER, D. *et al*. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. **PLoS Medicine**, 6 n.7, 2009.

MOSTFA KAMAL, S. U. *et al*. Survey and brief history on malware in network security case study: Viruses, worms and bots. **ARPN Journal of Engineering and Applied Sciences**, p. 683-698, 2016.

NATSIAVAS, P. *et al*. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. **BMC Medical Informatics and Decision Making**, v. 18 n.1, 2018.

NIDD, P.; THORN, T.; PORTER, M. K. Chasing perfection -The proactive imp PDCA (+E) review. **The American Society of Mechanical Engineers**, 2, 2016. 1-9.

ONDIEGE, B.; CLARKE, M.; MAPP, G. Exploring a new security framework for remote patient monitoring devices. **Computers**, v. 6 n.1, 2017.

PATTON, M. Q. **Qualitative Research & Evaluation Methods**. 3º. ed. California -EUA: Sage Publications, 2002.

PENNOCK, M. J.; HAIMES, Y. Y. Principles and guidelines for project risk management. **Systems Engineering**, 5 n.2, 2002. 89-108.

PESAPANE , F. *et al*. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. **Insights into Imaging**, 2018.

PMI, P. M. I. **Project Management Body of Knowledge -PMBOK**. [S.l.]: Global Standard, 2017.

POURSOLTAN, M.; MASMOUDI, M.; ALBERT, P. Application of Risk Management for Discrete Event Simulation Projects in Healthcare Systems. **Engineering Management Journal**, 2020. 1-13.

PRIESTMAN, *et al*. Phishing in healthcare organisations: threats, mitigation and approaches. **BMJ Health & Care Informatics**, v. 26, e100031, 2019.

PRIMO, H. *et al*. 10 Steps to Strategically Build and Implement your Enterprise Imaging System: HIMSS-SIIM Collaborative White Paper. **Journal of Digital Imaging**, v. 32, p. 535-543, 2018.

ROMANIUK, S. IoT – review of critical issues. **INTL Journal of Electronics and Telecommunications**, 2018. 95-102.

SANGER, D. E.; PERLROTH, N.; SCHMITT, E. Scope of Russian hacking becomes clear: multiple U.S. agencies were hit. **The New York Times**, New York, 14 Dez. 2020. Disponivel em: <https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>. Acesso em: 14 Dez. 2020.

SHARPE, R. *et al*. An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components. **Computers in Industry**, 2019. 37-44.

SHNEIDERMAN, B.; PLAISANT, C. Sharpening analytic focus to cope with big data volume and variety. **IEEE Computer Graphics and Applications**, 2015.

SILVA, A. S.; MEDEIROS, C. F.; VIEIRA, R. K. Cleaner Production and PDCA cycle: Practical application for reducing the Cans Loss Index in a beverage company. **Journal of Cleaner Production**, 150 n.1, 2017. 324-338.

SOKOVIĆ, M. *et al*. Basic Quality Tools in Continuous Improvement Process. **Journal of Mechanical Engineering**, 55 n.5, 2009. 1-9.

STERN, A. D. *et al*. Cybersecurity features of digital medical devices: An analysis of FDA product summaries. **BMJ Open**, v. 9 n.6, 2019.

SWEDE, M. J.; SCOVETTA, V.; EUGENE-COLIN, M. Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. **Journal of Allied Health**, 48 n.2, 2019. 148-155.

TAH, J. H. M.; CARR, V. A proposal for construction project risk assessment using fuzzy logic. **Construction Management and Economics**, 18 n.4, 2000. 491-500.

TAYLANA, *et al*. Construction projects selection and risk assessment by fuzzy AHPand fuzzy TOPSIS methodologies. **Applied Soft Computing**, 17, 2014. 105-116.

THAW, D. The Efficacy of Cybersecurity Regulation. **Georgia State University Law Review**, v. 30, p. 287-374, 2014. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241838>.

THOMÉ, M. T. *et al*. Similarities and contrasts of complexity, uncertainty, risks, and. **International Journal of Project Management**, p. 1328-1346, 2016.

THOMPSON, F.; PERRY, C. Generalising results of an action research project in one work place to other situations: Principles and practice. **European Journal of Marketing**, 38 n.3, 2004. 401-417.

VENKATRAMAN, S. A framework for implementing TQM in higher education programs, 15, 2007. 92-112.

WANG, T. C.; TANG, T. W.; CHENG, J. S. Art-oriented model of hotel service innovation. **International Journal of Contemporary Hospitality Management**, 30 n.1, 2018. 160-177.

WARD, ; CHAPMAN, C. Stakeholders and uncertainty management in projects. **Construction Management and Economics**, v. 26 , p. 563-577, 2008.

WEBSTER, J. Project Planning: Getting it Right the First Time. **IEEE Aerospace Conference Proceedings**, 6, 2004. 3924-3930.

WETHINGTON, E. *et al*. Establishing a Research Agenda on Mobile Health Technologies and Later-Life Pain Using an Evidence-Based Consensus Workshop Approach. **Journal of Pain**, p. 1416-1423, 2018.

WORLD ECONOMIC FORUM. The Global Risks Report 2017. **World Economic Forum**, Janeiro 2017. Disponivel em: <https://www.weforum.org/reports/the-global-risks-report-2017>.

WU, D. *et al*. A multiobjective optimization method considering process risk correlation for project risk response planning. **Information Sciences**, 467, 2018. 282-295.

XIAO, Z.; XIAO, Y. Security and Privacy in Cloud Computing. **IEEE Communications Surveys & Tutorials**, 15 n.2, 2013. 843-859.

YIN, R. K. **Estudo de Caso - Planejamento e Métodos**. 2º Edição. ed. Porto Alegre: Bookman, 2001.

ZHANG, *et al*. Cryptographic key protection against FROST for mobile devices. **Cluster Comput**, p. 2393-2402, 2017.