XII SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 12th INTERNATIONAL CONFERENCE

A cibersegurança, confiabilidade e velocidade nos procedimentos operacionais hospitalares

Cybersecurity, reliability and speed in hospital operational procedures

LUIZA VAZ DE DONNO
UNIVERSIDADE PRESBITERIANA MACKENZIE

Comunicação:
O XII SINGEP foi realizado em conjunto com a 12th Conferência Internacional do CIK (CYRUS Institute of Knowledge) e com o Casablanca Climate Leadership Forum (CCLF 2024), em formato híbrido, com sede presencial na ESCA Ecole de Management, no Marrocos.

A cibersegurança, confiabilidade e velocidade nos procedimentos operacionais hospitalares

Objetivo do estudo
Este estudo obteve como objetivo conhecer as etapas para viabilizar a implantação da cibersegurança nos processos operacionais hospitalares, de forma a aumentar a confiabilidade e velocidade nos procedimentos.

Relevância/originalidade
Sendo justificado pelo fato de o setor de saúde representar um terço dos ataques cibernéticos, ao serem mais propensos a pagarem resgate, uma vez que os dados e sistemas comprometidos podem custar vidas.

Metodologia/abordagem
A partir da pesquisa bibliográfica, foi viável compreender os principais desafios atuais do setor e levantar os conceitos hospitalares e de cibersegurança. Em seguida, foi realizada a etapa de coleta de dados, através de questionários, sendo analisados através da frequência de respostas.

Principais resultados
Dado que: profissionais de tecnologia da informação indicaram a necessidade da proteção de dados e sistemas; maioria dos profissionais hospitalares não obtêm treinamento de plano de contingência em caso de ciberataque; os pacientes afirmaram perder a confiança, caso o hospital sofra ciberataque.

Contribuições teóricas/metodológicas
Conhecimento sobre sistemas e softwares desenvolvidos para proteger o sistema operacional hospitalar, fatores para garantir o atendimento contínuo aos pacientes e demais operações da instituição. Em conjunto com a averiguação do conhecimento dos profissionais hospitalares em caso de parada sistêmica.

Contribuições sociais/para a gestão
Desta forma, a solução que o projeto apresentou é a implementação de um departamento de cibersegurança no ambiente hospitalar. Sendo possível assegurar a proteção do ambiente digital hospitalar, e, consequentemente, a continuidade operacional dos hospitais e a confiabilidade dos pacientes.

Palavras-chave: Ataques Cibernéticos, Cibersegurança, Confiabilidade, Hospital, Velocidade

Cybersecurity, reliability and speed in hospital operational procedures

Study purpose
This study aimed to understand the steps to enable the implementation of cybersecurity in hospital operational processes, in order to increase reliability and speed in procedures.

Relevance / originality
This is justified by the fact that the healthcare sector represents a third of cyber attacks, as they are more likely to pay a ransom, as compromised data and systems can cost lives.

Methodology / approach
Based on bibliographical research, it was possible to understand the main current challenges in the sector and raise hospital and cybersecurity concepts. Then, the data collection stage was carried out, using questionnaires, being analyzed based on the frequency of responses.

Main results
The main results are: IT professionals indicated the need to protect data and systems; most healthcare professionals do not receive contingency plan training in the event of a cyber attack; patients said they would lose confidence if the hospital suffered a cyberattack.

Theoretical / methodological contributions
It was possible to obtain knowledge about systems and softwares developed to protect the hospital operating system; factors to ensure continuous care for patients and other operations of the institution; investigating the knowledge of healthcare professionals in the event of systemic failures.

Social / management contributions
Therefore, the solution that the project presented is the implementation of a cybersecurity department in the hospital environment. It is possible to ensure the protection of the hospital digital environment, and, consequently, the operational continuity of hospitals and the reliability of patients.

Keywords: Cyber Attacks, Cybersecurity, Hospital, Reliability, Speed

A CIBERSEGURANÇA, CONFIABILIDADE E VELOCIDADE NOS PROCEDIMENTOS OPERACIONAIS HOSPITALARES

1 Introdução

De acordo com a Fortinet (2021), o Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, sendo este um aumento de mais de 950% em relação ao ano de 2020. Ainda segundo o relatório do laboratório de inteligência de ameaças, a República Federativa do Brasil ocupou o segundo lugar em número de ataques cibernéticos na América Latina e Caribe. Em função do setor de saúde representar um terço de todos os ataques cibernéticos, se torna importante a devida proteção contra acometimentos cibernéticos, segundo Sposito, para o Portal Hospitais Brasil (2022). Ademais, o setor de saúde é identificado como um alvo valioso e vulnerável, devido ao fato de organizações de saúde serem mais propensas a pagarem pedidos de resgate, uma vez que dados e sistemas comprometidos podem custar vidas.

Dentro desta narrativa há problemas como a perda e roubo de dados, prejudicando a habilidade dos profissionais ao atenderem os pacientes e a confiança que estes depositam na instituição, ao relatar Maia (2021). Segundo uma pesquisa realizada pelo Departamento de Saúde dos Estados Unidos, 60% dos hospitais de médio e grande porte tratam a cibersegurança como tema de segundo plano, o que por consequência reflete na falta de investimento em equipe e tecnologia. Sendo assim um cenário preocupante, uma vez que, prontuários eletrônicos, exames laboratoriais, diagnósticos de imagem e outros dados pessoais confidenciais dos pacientes não são protegidos de forma adequada.

Segundo InforChannel (2022), citando Amir Bar-El, fundador da CySource e especialista em cibersegurança, afirmou que o aumento das oportunidades de ciberataques no setor da saúde acontece devido à falta de proteção dos dispositivos médicos e IoT (Internet das Coisas) conectados. A partir de um estudo realizado pelo especialista, foi revelado que 21% dos dispositivos hospitalares utilizam senhas fracas, gerando um risco grave para a segurança do paciente, a confidencialidade dos dados e a continuidade operacional dos hospitais. Além disso, a falta de uma devida proteção aos dispositivos, em 2021, correspondeu a 500 casos de ataques cibernéticos e um prejuízo de mais de oito milhões de dólares, podendo gerar irreparáveis danos à saúde dos pacientes.

Conforme a empresa de cibersegurança Sentinel (2022), além das redes hospitalares estarem propícias a ataques cibernéticos, equipamentos médicos também podem ser hackeados. Dentre eles, foi apontado como os quatro mais perigosos: marca-passos, bombas de infusão de remédio, sistema de ressonância magnética e monitores de frequência cardíaca. Sendo assim, a partir de uma série de vulnerabilidades em dispositivos médicos conectados já descoberta, compreende-se que os dispositivos que utilizam frequência de rádio, tecnologia de rede ou que se conectem sem fio a outro equipamento, apresentam grandes chances de serem comprometidos.

Ademais, de acordo com a Agência de Segurança Cibernética e Infraestrutura (2023), conforme as organizações de saúde dependem cada vez mais de tecnologias digitais, se apresentam mais expostas a maiores riscos. Sendo dependente para o armazenamento de informações médicas e de pacientes, realização de procedimentos médicos, comunicação com pacientes e controle e registro das atividades ali presentes. Sendo assim, ao aludir Andrea Palm, secretária adjunta do Departamento de Saúde e Serviços Humanos dos Estados Unidos, afirma que durante os últimos anos é possível notar um aumento significativo no número e na gravidade dos ataques cibernéticos em hospitais. Expondo desta forma as vulnerabilidades dos sistemas, degradando a confiança dos pacientes e colocando a segurança destes em risco.

1.X OBJETIVOS

Identificar metodologias e processos que irão permitir o alcance da melhoria no aumento da confiabilidade e velocidade nos processos operacionais hospitalares, em relação aos seus pacientes. Tendo como objetivos específicos entender os aspectos de confiabilidade e velocidade voltados às operações hospitalares, relacionados com os aspectos positivos promovidos pela cibersegurança no ambiente.

2 Referencial Teórico

De acordo com Moss (2020) relatou um ataque cibernético ao hospital da Universidade de Dusseldorf, na Alemanha, o qual ocasionou a desabilitação do sistema geral, perda de informações dos pacientes, atraso nos procedimentos operacionais e o óbito de uma paciente. Devido a falta de habilidade dos profissionais presentes a prestarem os devidos socorros à paciente, a inatividade dos sistemas, dados inacessíveis e operações adiadas, a paciente teve que ser enviada para outro hospital. Este situava-se a mais trinta e dois quilômetros de distância, atrasando assim o tratamento que poderia ter salvado sua vida. Sendo assim, esta foi apontada como a primeira morte diretamente ligada a um ataque de segurança cibernética a hospitais (Moss, 2020).

Além disso, de acordo com Guimarães (2017), em junho de 2017, o Hospital de Câncer de Barretos foi alvo de ciberataque, ao ter seu sistema invadido por um ransomware. O qual, ao ultrapassar barreiras de proteção, de sistemas que apresentam vulnerabilidades, criptografa as informações e paralisa os sistemas. Neste caso, os hackers estavam exigindo um resgate de US$300,00 (trezentos dólares) em bitcoin, espécie de moeda digital, por máquina do hospital. Totalizando em US$360.000,00 (trezentos e sessenta mil dólares), na época convertendo para R$1,08 milhão (um milhão e oitenta mil reais). O hospital não precisou arcar com este custo financeiro, uma vez que o departamento de tecnologia da informação conseguiu recuperar 96% das máquinas em três dias. Porém, ainda de acordo com Guimarães (2017), os procedimentos hospitalares só foram normalizados seis dias depois. Dessa forma, atrasando três mil consultas e exames, em conjunto com o tratamento de radioterapia de trezentos e cinquenta pacientes do hospital.

Conforme a Agência de Segurança Cibernética e Infraestrutura (2021), um ataque cibernético no sistema hospitalar gera inúmeras implicações para as instituições de saúde. Entre elas, gera a falha na rede de tecnologia e informação e rompe a capacidade dos sistemas de saúde de acessarem registros eletrônicos de saúde, sendo necessário que pacientes em condições críticas sejam designados para outros hospitais. Ademais, o desvio de ambulâncias é uma importante interrupção no sistema, ocasionando atrasos no tratamento e tolerância de tempo, assim como diminuindo a qualidade do atendimento. A longo prazo, os hospitais que sofrem eventos cibernéticos têm maior probabilidade de sofrerem tensão hospitalar. A qual é definida pelo excesso de demanda por leitos em relação aos leitos hospitalares e a oferta de recursos. Sendo esta medida pela utilização de leitos de UTI, prejudicando os resultados de saúde e contribuindo para o aumento da mortalidade. Demonstrando que os ataques cibernéticos afetam toda a rede hospitalar, tanto internamente quanto externamente, sendo em relação às ambulâncias, qualidade e velocidade dos médicos em atendimentos, registros e controles de leitos e pacientes.

Ademais, segundo o Estadão (2022), com a implementação de tecnologias modernas e as legislações brasileiras, o setor de saúde apresentou diversas transformações ao decorrer dos anos. Ao ser decretado, através das Leis Nº13.787/2018 e Nº13.709/2018, sobre importância, padronização e proteção da digitalização, utilização de sistemas informatizados e proteção de dados sobre prontuários médicos e informações pessoais.

2.1 POLÍTICA DE CIBERSEGURANÇA NO SETOR DA SAÚDE

A partir disso, a AlcatelLucent Enterprise (2021) evidencia que é de suma importância que as empresas que atuam no setor da saúde desenvolvam um plano estratégico de segurança.

Uma vez que, consequências como interrupções operacionais, danos à reputação do hospital e multas por violações do Regulamento Geral de Proteção de Dados (RGPD), colocam em risco a vida dos pacientes. Sendo assim, é necessário um plano que deve gerenciar o risco de forma que atenda às demandas do contexto atual de transformação digital. Mantendo-se atualizado, de forma que considere a conformidade regulamentar como um ponto de partida e compreenda como a segurança impulsiona o valor do negócio. Obtendo assim uma abordagem de segurança e a implementação de um ecossistema para proteger o ambiente digital hospitalar.

De acordo com a Kaspersky (2023), a digitalização na área da saúde está expondo cada vez mais as organizações de saúde a ataques genéricos e direcionados. Em vista disso, a empresa de cibersegurança destacou a necessidade de um ecossistema de proteção englobando diversas etapas. Sendo essas: diversas camadas para endpoints, através de máquinas físicas e virtuais; conteinerização; dispositivos móveis; inteligência de ameaças assistida na nuvem e em algoritmos de Machine Learning, visando a proteção dos sistemas contra as diversas ameaças virtuais; troca segura de dados; e uma arquitetura definida por software. Sendo assim, conforme a Kaspersky (2023), desta forma é possível obter recursos exatos para a implementação de um ecossistema de segurança que auxilie na eficiência e velocidade dos sistemas e da infraestrutura de tecnologia da informação.

Além disso, ainda segundo Kaspersky (2023) é evidenciado a necessidade da devida proteção dos prontuários médicos de pacientes contra roubo, perda ou corrupção. Em conjunto com a importância de assegurar a disponibilidade dos serviços de saúde, por meio da promoção da continuidade operacional e minimizando o tempo de inatividade. Assim como, a necessidade de permitir que a propriedade intelectual se mantenha segura, através do ecossistema de cibersegurança adaptável para manter esses recursos seguros e protegidos. Sendo possível através da tecnologia da informação, auxiliando na redução de vulnerabilidades criadas pela IoT e, consequentemente, evitar a violação deste ecossistema (Kaspersky, 2023).

De acordo com Cooper (2023), os ataques generalizados de ransomware na cadeia hospitalar e a violação de dados de um prestador de cuidados de saúde, são considerados vulnerabilidades da infraestrutura desta área de saúde digital. Estes ataques, assim como comentado anteriormente, podem gerar consequências nos âmbitos da segurança do paciente, procedência de dados, desempenho operacional e na área financeira. Em vista disso, Cooper (2023) aponta o papel da cibersegurança para a área da saúde, a qual engloba fatores como a avaliações regulares de riscos, formação de funcionários, defesa em várias camadas, gestão de dispositivos, planejamento da resposta a incidentes e sistemas de backup. Por fim, o autor evidencia a importância da relação entre o fator humano e as tecnologias envolvidas, uma vez que o setor hospitalar está emergindo cada vez mais no domínio digital. Aumentando desta forma ao mesmo nível os riscos que este está exposto e colocando em risco a importância da confiança dos pacientes e a funcionalidade dos processos operacionais.

Sendo assim, para compreender como estes ataques acontecem, é necessário conhecer as diversas categorias de cibersegurança, sendo estas: segurança de rede, segurança de informação, segurança operacional e segurança de aplicativos, segundo Almeida (2021). Ademais, é necessário compreender as principais ameaças que mais atingem o setor da saúde: tráfego de rede malicioso, phishing, sistema operacional vulnerável, ataque man-in-the-middle, malware, engenharia social e ransomware. A principal ameaça, de acordo com Almeida (2021) refere-se a coleta de dados confidenciais, em conjunto com o download de software não autorizado. Por outro lado, o ransomware é caracterizado como um softwaremalicioso, configurado para bloquear sistemas e acesso a arquivos de toda a rede digital, visando extorquir dinheiro do alvo, sendo este considerado uma espécie de sequestro de dados.

Conforme apontado pelo Codebit (2021), a Política de Segurança Informacional (PSI) é um fator essencial para o ambiente hospitalar, responsável pela segurança dos dados de pacientes e dos sistemas informacionais. Os quais estão protegidos de acordo com a Lei Geral

de Proteção de Dados 13.709/2018, definindo que as informações coletadas e armazenadas no ambiente hospitalar são dados pessoais sensíveis, sendo assim, é necessário que hospitais obtenham medidas especiais em relação a proteção durante a coleta, armazenamento, tratamento e manipulação das informações. A partir disso, Codebit (2021) expõe a necessidade de medidas de segurança física, humana, técnica e operacional, visando a proteção adequada contra acessos não autorizados, desvios de dados, interrupção de sistemas ou outras vulnerabilidades que o setor apresenta, uma vez que falhas e erros podem custar vidas.

Segundo Kuppe (2023), a Política de Segurança da Informação (PSI) é composta por diretrizes, regras e procedimentos que fazem parte e visam proteger e garantir os três princípios da segurança da informação. Estes são: a confiabilidade, disponibilidade e integridade. Sendo assim, a PSI pode ser elaborada através de documentos impressos ou digitais, plataformas de gestão de política e treinamentos e conscientização. Englobando aspectos como: controle de acesso físico, gerenciamento de incidentes, monitoramento e auditoria, padrões de comportamento, procedimento de segurança e restrição de acesso. Desta forma, a PSI garante a proteção de dados, conformidade com a Lei Geral de Proteção de Dados, otimização de processos de TI, maior transparência com colaboradores e a redução de custos. Sendo necessário realizar um diagnóstico, planejamento, criação de diretrizes, definição dos níveis de acesso e treinamento, para implementar uma PSI (Kuppe, 2023).

Em vista disso, a empresa Nova Leah (2023), líder mundial no fornecimento de soluções de segurança cibernética para fabricantes de dispositivos médicos e prestadores de cuidados de saúde, apresenta uma plataforma de gerenciamento de riscos de terceiros e monitoramento contínuo de segurança cibernética. Esta plataforma contém três princípios, sendo estes: identificação, avaliação e monitoramento. Abrangendo ciclos de gestão de relacionamento com terceiros mais curtos, consistência de avaliação, transparência das partes interessadas e confiabilidade do sistema. Sendo assim, a empresa cria um ambiente de saúde mais harmonioso, robusto, veloz e confiante. A partir da capacitação dos fabricantes de dispositivos médicos e os prestadores de cuidados de saúde para gerirem conjuntamente a segurança cibernética.

De acordo com EY Brasil (2023), ao realizar um benchmark sobre a vulnerabilidade do setor da saúde para os acometimentos cibernéticos e a adequação à LGPD, analisou que a maioria das instituições de saúde não obtêm um plano de continuidade de negócios definido para lidar com ciberataques. Passando a tratar apenas desse assunto como prioridade de gestão de risco e continuidade após experienciar um acometimento cibernético. Sendo assim, destacou que além das medidas básicas a serem tomadas, é necessário a realização de uma avaliação da postura e maturidade do programa de segurança cibernética por meio de cyber assessment. Este serve para identificar possíveis vulnerabilidades do sistema da rede hospitalar e endereçar as devidas correções e simulações de crises. Obtendo como intuito avaliar e aprimorar a resposta da instituição em caso de crises cibernéticas (EY Brasil, 2023).

A partir do apontado pela Agência Nacional de Vigilância Sanitária (2020), a cibersegurança é considerada uma responsabilidade compartilhada entre fabricantes de dispositivos médicos, agências de saúde e os usuários. Ainda de acordo com o apontado, esta apresenta como função proteger e fortalecer a eficácia e segurança de dispositivos médicos. Obtendo como objetivo minimizar os danos aos pacientes.

Assim como apontado por Lopes (2018), ao trazer dados de uma entrevista realizada pela KPMG, foi apontado que 81% das organizações ligadas à área da saúde já foram vítimas de ataques cibernéticos, ao ser relatado por seus gestores. Entre os gestores entrevistados, apenas metade relatou que sua organização estava preparada para se proteger de futuros ataques virtuais e 39% alegaram a falta de ferramentas confiáveis para a proteção de seus sistemas. Evidenciando assim a falta de implementação de sistemas de cibersegurança presente nas instituições, o que prejudicaria a coleta de informações sobre a melhoria na velocidade e confiabilidade no ambiente hospitalar, gerados pela presença da cibersegurança nas redes.

Além disso, outro problema presente é a ciência de ataques cibernéticos pela percepção de pacientes. Sendo que, ainda segundo Lopes (2018), é analisado que um a cada três pacientes irão sofrer roubo de seus dados pessoais das organizações médicas, tendo uma exposição de registros médicos maior do que 4,2 bilhões. Os quais, muitas vezes, não se tornam conhecimento específicos pelas vítimas, podendo assim afetar na análise da confiabilidade dos processos, uma vez que os pacientes podem não imaginar que os seus dados pessoais e a operação do hospital foram comprometidos.

Desta forma, a empresa de fabricação de equipamentos médicos Dräger (2022), um ataque cibernético no âmbito hospitalar pode ser uma questão de vida ou morte, em razão do risco no funcionamento de equipamentos. Assim como, o roubo de dados do hospital e dos pacientes podem ter efeitos prolongados. Apontando assim, que os hospitais devem tomar medidas cabíveis para proteger os sistemas de tecnologia da informação (TI), dados, equipamentos médicos e pacientes.

2.2 CONFIANÇA E VELOCIDADE

De acordo com Sennett (1999), a confiança depende de associação a longo prazo, de modo a tornar possível o estabelecimento de vínculos sedimentados por experiência positiva compartilhada. Tal raciocínio recebe apoio nos estudos inicialmente citados, sobre confiança geral e interpessoal, historicamente produzida. Sabe-se, porém, que condições de estabilidade temporal, capazes de sedimentar vínculos profundos e duráveis de confiança, são praticamente inalcançáveis, o que certamente compromete a qualidade dos relacionamentos e trocas sociais.

Conforme analisado o artigo de Sara Belfrage, Gert Helgesson e Niels Lynoe (2022), publicado na BMC Medical Ethics, a confiança tem sido reconhecida como um fator importante para uma interação bem-sucedida em relação a muitas instituições sociais. Considerando esta um agente extremamente importante no contexto dos cuidados de saúde, uma vez que se trata de um lugar onde as pessoas podem aparecer quando estão vulneráveis e precisam confiar nos outros em assuntos importantes e pessoais. Sendo assim, após algum acontecimento importante, como um ciberataque, a desconfiança pode reduzir a disposição dos pacientes em aceitar o acesso e o uso de seus dados pessoais por instituições. Acarretando um efeito erosivo sobre a confiança dos cidadãos nas estruturas nacionais da rede Internet, prejudicando a sua credibilidade, nível de segurança e funcionamento regular, especialmente nas que apresentam um histórico com acometimentos cibernéticos. Intensificando assim a importância de aplicar práticas que garantam os princípios essenciais de segurança da informação.

Segundo Corrêa e Corrêa (2017), ao dissertarem sobre a velocidade como um dos aspectos do desempenho nos processos de produção e operação, demonstram sua importância para obter acesso, atendimento, cotação e entrega. Sendo esta vantagem utilizada para ganho de acesso à operação, dar início ao atendimento, cotar preço, prazo e especificação e entrega do produto.

Em concordância com o afirmado, a partir do artigo realizado pela RedFox (2023), foi compreendido que, para os profissionais da saúde, o uso de tecnologia adequadas complementam, dão suporte e substituem processos repetitivos. Acarretando assim em um processo mais ágil e eficiente, permitindo aos médicos mais tempo para darem a atenção devida aos pacientes, através de ferramentas de automação, como prontuários, agendas e prescrições eletrônicas.

Análise sustentada por Baltzan (2016), ao defender que a utilização de redes sem fios gera diversos benefícios para a funcionalidade dos médicos. Citando entre eles: o aumento da capacidade de localização e monitoramento, fornecimento de acesso imediato aos dados, melhora do fluxo de trabalho e aumento da mobilidade. Além disso, a rede hospitalar armazena versões digitais de ótima qualidade de diversos exames, tais como: raios X, ressonância magnética e tomografias computadorizadas, podendo ser rapidamente acessadas pelos médicos do hospital, fomentando assim a progressão na qualidade do atendimento.

Além disso, segundo Negri (2020), em seu artigo publicado no Centro de Pesquisa em Ciência, Tecnologia e Sociedade, o uso da tecnologia de informação tornou-se uma alternativa promissora em relação à diminuição de custos para a melhoria e ampliação dos serviços de saúde. Juntamente com o afirmado por Bouronikos (2020), no Instituto de Desenvolvimento do Empreendedorismo, a tecnologia na área da saúde permite que os profissionais armazenem e recuperem dados relacionados com registros de saúde de pacientes. Aprimorando assim a comunicação das informações do paciente, através de um método uniforme, e reduzindo a chance de erros médicos, melhorando a saúde e a segurança do paciente no âmbito hospitalar.

Não obstante, a cibersegurança é de suma importância para o ramo hospitalar para proteger os benefícios gerados pela utilização da IoT (Internet das Coisas). De acordo com o Grupo Gerenciar (2022), algumas das vantagens são: fácil recuperação de informações em caso de desastres; compartilhamento de registros médicos com profissionais de saúde para melhorar o atendimento; fluxo de trabalho clínico aprimorado em todas as funções de prática; organização eficiente dos registros; e acesso rápido ao histórico médico do paciente e revisar dados. Demonstrando assim a importância e consequências da cibersegurança para os procedimentos operacionais hospitalares.

A partir disso, segundo Wetsman (2021), uma das evidências mais claras de um ataque ransomware é o atraso nas operações hospitalares, prejudicando todo o funcionamento da organização. Ao aludir ao Josh Corman, conselheiro sênior da Agência de Segurança Cibernética e Infraestrutura dos Estados Unidos, afirma que é necessário que as organizações parem de fingir que não há danos à vida humana causados por ataques cibernéticos. Dentre eles é dada pertinência ao revés na velocidade dos procedimentos hospitalares, podendo causar atendimento degradado ou atrasado, diagnóstico inadequado, piora no quadro do paciente e até óbito de pacientes. Ademais, ao remeter a Mark Jerrett, destaca que os médicos em geral tendem a pensar nos ciberataques como uma questão de tecnologia da informação, quando na verdade é uma questão de segurança do paciente, diretamente relacionada com a confiança deste na organização.

De acordo com a Agência de Segurança Cibernética e Infraestrutura (2023), conforme as organizações de saúde dependem cada vez mais de tecnologias digitais para armazenar as informações médicas e de pacientes, realizar procedimentos médicos, comunicar-se com os pacientes, ter controle e registro sobre das atividades ali presentes, estas estão cada vez mais expostas a maiores riscos. Sendo assim, ao aludir Andrea Palm, secretária adjunta do Departamento de Saúde e Serviços Humanos dos Estados Unidos, afirma que durante os últimos anos é possível notar um aumento significativos no número e na gravidade dos ataques cibernéticos em hospitais, expondo as vulnerabilidades dos sistemas, degradando a confiança dos pacientes e colocando a segurança destes em risco.

Em concordância, Wetsman (2021), ao realizar um relatório com seiscentas organizações de saúde dos Estados Unidos da América, sobre o histórico destas em relação a ciberataques, chegou a conclusão de que, apenas quase 40% comentou que tiveram um ataque ransomware em um período de dois anos. Estes acometimentos cibernéticos congelam o sistema da rede do hospital e demandam pagamento para desbloquear, o que interrompe ou impede a capacidade das organizações de saúde de cuidar dos pacientes. Dentre as unidades que sofreram com ciberataques, 70% afirmaram que obtiveram atrasos em resultados de testes ou procedimentos e levaram a internações hospitalares mais longas. Além disso, 36% afirmaram obter complicações nos procedimentos médicos e 22% relataram que a taxa de mortalidade aumentou. O estudo de Wetsman (2021) concluiu que os hospitais geralmente são relutantes ao compartilhar informações sobre tais acometimentos, uma vez que podem gerar impactos sobre a reputação da organização e confiabilidade dos pacientes, dado que, mais da metade das organizações demonstraram não serem capazes de lidar com os ataques ransomware.

A partir do apontado pela Agência de Segurança Cibernética e Infraestrutura (2021), é possível analisar uma forte relação entre ciberataques, excesso de demanda por leitos em relação aos leitos hospitalares e a oferta de recursos. O estudo ilustra a capacidade reduzida e o estresse externo que os ataques cibernéticos podem causar nas infraestruturas de saúde, principalmente durante um padrão de atendimento para crises. Constatando um modelo de efeitos em cascata de como os aumentos no volume de pacientes hospitalares levam a uma degradação sistêmica mais ampla. Tais como comunicação interrompida, desvio de ambulâncias, cirurgias atrasadas ou canceladas, inabilidade de acessar registros médicos de pacientes, demanda registro manual do progresso e do tratamento dos pacientes, atrasos no processamento e comunicação dos resultados de exames, perda do controle e aumento do número de leitos e a incapacidade de atendimento a pacientes de alto risco.

Em um curto período as consequências dos ataques cibernéticos é a interrupção da capacidade dos sistemas de saúde de acessar registros eletrônicos de saúde e serviços baseados em rede, como tecnologia cardíaca e oncológica, ainda de acordo com a Agência de Segurança Cibernética e Infraestrutura (2021). Por outro lado, em um período de longo tempo, os registros médicos de pacientes podem permanecer limitados, complicando o atendimento a pacientes de longo prazo que possuem registros detalhados que determinam os tratamentos. Uma vez que a equipe médica passa mais tempo para achar os dados do paciente, reduzindo o número de leitos que a equipe pode atender e potencialmente levando a piores resultados. Desta forma, um ataque ransomware nas instituições de saúde geram consequências prejudiciais durante o momento e a curto e longo prazo, principalmente em relação aos procedimentos médicos, leitos hospitalares e pacientes em unidade de terapia intensiva (UTI).

3 Metodologia

3.1 MÉTODOS DE PESQUISA

De acordo com Richardson (2017), pode-se descrever um método de pesquisa como a escolha de procedimentos sistemáticos, com o objetivo de descrever e explicar fenômenos. Tal procedimento se aproxima do método científico, devido ao fato de delimitar um problema, realizar observações e interpretá-las nas relações encontradas, contanto também com a fundamentação destas em teorias, se possível.

Ainda de acordo com Richardson (2017), é possível considerar que há três métodos de pesquisa, sendo estes o quantitativo, o qualitativo e o misto. O método quantitativo é definido pela utilização deste para testar teorias objetivas, presente tanto na coleta de informações, quanto no tratamento delas, utilizando técnicas estatísticas para analisar os dados obtidos. Por outro lado, o método qualitativo é a análise de dados, de uma forma adequada, para compreender a natureza de um fenômeno social, através de entrevistas, análises de documentos, observação e outros. Por fim, o método misto se caracteriza pela combinação ou associação dos métodos quantitativo e qualitativo, a partir da coleta, análise e exploração de ambos os tipos de dados.

Neste sentido, este estudo foi realizado a partir da análise descritiva dos elementos necessários para a implantação da cibersegurança, junto aos procedimentos hospitalares.

3.2 UNIVERSO DA AMOSTRA

Segundo Vergara (2015), o universo da amostra é uma parte selecionada a partir de um critério de representatividade, considerando-se assim o conjunto de elementos que possuem as características que serão utilizadas como objeto de estudo.

Posto isso, a amostra da pesquisa foi composta por sete profissionais hospitalares, três profissionais de tecnologia da informação e cem pacientes. A análise de dados foi realizada por frequência de respostas, para analisar o sistema de cibersegurança nos procedimentos hospitalares, em conjunto com a confiabilidade e velocidade. A partir disso, obteve-se conhecimento sobre a utilização e importância da cibersegurança em hospitais, como esta

implica na velocidade dos atendimentos médicos e quais fatores afetam os níveis de confiabilidade dos pacientes.

3.3 COLETA DE DADOS

A coleta de dados da pesquisa foi realizada a partir de dois instrumentos, sendo o principal o contato com os entrevistados. Concluído através de mídias sociais, onde foram identificados de acordo com a aderência aos temas de cibersegurança, hospitalares e pacientes, por meio de questionamentos direcionados para cada área envolvida.

Após a realização do planejamento e pré-teste, definição do período de coleta de informações e as instituições estabelecidas para participar da pesquisa, foi possibilitado o início à aplicação de questionários abertos e fechados direcionados. Através de questões elaboradas para percepção dos três públicos participantes e, em seguida, perguntas específicas para os participantes de cada área. Utilizando a matriz de amarração, Apêndice A. Obtendo como finalidade transmitir os objetivos e apresentar uma padronização no processo de levantamento dos dados, visando obter uma melhor compreensão e tratamento destes, assim como apontado por Richardson (2017).

Por fim, o segundo instrumento utilizado foi a pesquisa bibliográfica, fundamentada através de leituras e análises de artigos científicos, livros, meios digitais e relatórios.

3.4 TRATAMENTO DE DADOS

De acordo com Bardin (2010), a análise de conteúdo tem como objetivo conhecer aquilo que está por trás das palavras sobre as quais se debruçam. A análise visa o conhecimento de variáveis de ordem histórica, psicológica, sociológica, através de um mecanismo de dedução com base em indicadores reconstruídos a partir de uma amostra (Bardin, 2010).

Posto isso, visando a confiabilidade e velocidade no âmbito das operações hospitalares, pretende-se apresentar métodos que viabilizem o processo de implantação da cibersegurança nesses procedimentos. Para tanto, foi utilizado como base, a percepção dos envolvidos nos processos de operações hospitalares. Sendo este na visão de especialistas hospitalares, profissionais de tecnologia da informação e automação, e dos pacientes. Os resultados informacionais obtidos foram avaliados pela frequência das respostas direcionadas ao tema.

4 Análise dos Resultados e Discussões

4.1 CIBERSEGURANÇA

Quando o tema tratado foi a cibersegurança, as respostas da questão 1, indicada no Apêndice A – Matriz de Amarração, pelos profissionais de saúde e da área de TI indicaram regras de manuseio, normas e regras de segurança. Foi afirmado pela maioria dos profissionais do setor da saúde o conhecimento sobre existência de regras de manuseio de equipamentos de informática no ambiente de trabalho. Sendo estas: mudança de senha frequente; acesso aos sistemas somente no local de trabalho ou via VPN; configuração de acesso aos sistemas conforme o perfil do usuário; desautorizando o acesso de redes sociais pessoais.

Por outro lado, na percepção dos profissionais de TI, o mesmo questionamento apontou um mix de fatores necessários para a segurança da informação neste setor. Evidenciando a necessidade de uma forte governança corporativa, política de segurança da informação, criptografia de dados e controle de acesso físico. Sendo necessário que as políticas e procedimentos de segurança da informação estejam definidos corretamente, implementação de segurança da infraestrutura e dos servidores e softwares, proteção dos dados com sistemas de criptografia, promoção de avaliações e auditorias regularmente e, por fim, promover desenvolvimento/treinamento contínuo de todos os usuários para o uso correto dos sistemas. Garantindo desta forma a confidencialidade e a integridade dos dados dos pacientes e demais envolvidos no âmbito hospitalar, os resultados contidos nas normas e políticas de segurança da informação e a disponibilidade dentro do ambiente, ou seja, evitar interrupções nos procedimentos operacionais hospitalares.

Ao abordar a necessidade de implementação de um departamento de cibersegurança, a maior parte dos profissionais hospitalares afirmaram que é necessário que as instituições de saúde insiram um controle adicional de acesso aos equipamentos e relatórios médicos. Os profissionais de TI, afirmaram que é fundamental que o departamento seja implementado e organizado para abranger os aspectos relacionados à proteção do ambiente digital e dos dados confidenciais. Esta em função da criticidade e da responsabilidade do departamento de cibersegurança em um hospital. Sendo necessário considerar uma estrutura compatível com as necessidades e tamanho da organização, além de adotar as melhores práticas em cibersegurança, como afirmado na questão anterior. Isto inclui profissionais bem qualificados, atualizados e especializados nas diversas funções e atuações deste departamento.

Ao questionar os profissionais hospitalares sobre a questão 3, a maior parte respondeu que há uma Política de Segurança Informacional Hospitalar. Ao detalhar sobre o assunto, apenas mencionaram a Lei Geral de Proteção de Dados e a existência de protocolos, como exemplo a necessidade de autorização administrativa para acesso a certas informações. Em relação à quarta questão para este grupo, a maior parte dos entrevistados afirmaram não obter conhecimento sobre testes de segurança no sistema informacional.

As respostas da questão 3 dos profissionais de TI, indicaram a necessidade de diversos fatores. Os entrevistados apontaram que este setor requer o atendimento rigoroso na identificação de ativos e requisitos de segurança. Sendo crucial a realização de análise dos riscos e vulnerabilidades, utilizando ferramentas de varredura e testes de penetração, em conjunto com o teste de eficácia das medidas de segurança, através de testes e de auditorias planejadas. Destacando a importância de certificar a implementação das medidas de segurança, como firewalls, IPS/IDS, antivírus, criptografia e outros. Assim como, assegurar a monitoração e análise dos eventos de segurança em tempo real, integrando uma inteligência de análise de ameaças - uma constante, especialmente com o recente desenvolvimento de inteligência artificial nesta área. Mencionando também a importância de obter um plano documentado e uma equipe definida para resposta a incidentes, de forma a registrar e prevenir incidentes futuros. Por fim, destaca a necessidade de realizar ajustes de segurança regulares e garantir atualização de recursos humanos adequados, educação e conscientização em segurança.

Em seguida, os profissionais, ao responderem à questão 4, demonstraram que o principal é que existam medidas corretivas e melhorias contínuas na segurança da rede hospitalar. Envolvendo uma combinação de métodos e ferramentas de varredura e testes de penetração, como *pentests*, uma revisão periódica e avaliação das políticas de segurança da instituição, a verificação de configurações de segurança, auditorias de controle de acesso e gerenciamento de identidades, os próprios testes regulares de invasão e detecção e ainda o monitoramento de eventos de segurança para identificar e prevenir padrões fora das operações regulares.

Após serem questionados sobre a implementação de um ecossistema de segurança, os profissionais de TI afirmaram a necessidade da utilização de softwares avançados de detecção de ameaças e possíveis anomalias de rede em tempo real. Comentando também sobre a importância de ter definido os requisitos e políticas de segurança alinhadas com normas e regulamentos, obter as melhores tecnologias e soluções de segurança e garantir que as soluções de segurança selecionadas estejam instaladas. Mencionando também a necessidade de realizar o monitoramento periódico, melhorias adequadas e treinamentos e conscientização para os usuários do hospital.

As respostas da questão 6, indicaram que as medidas mais essenciais para esta finalidade requerem que a área de cibersegurança da instituição hospitalar tenha uma solução pertinente para antecipação de futuros ataques. É necessário ação proativa de inteligência de ameaças, com a implementação dos sistemas de detecção de intrusões e prevenção. Este atuando em conjunto com a realização de testes de penetração e de simulações de incidentes. Sendo

essencial obter o monitoramento e análise de logs e eventos, assim como as interfaces de trocas de informações de segurança.

A última questão para os profissionais de TI, sobre cibersegurança, demonstrou que se utiliza uma abordagem estruturada com revisão e atualização regular dessa documentação. Os entrevistados afirmaram que podem ser consideradas ações de definição do escopo, a análise de riscos, o planejamento da arquitetura de segurança, as políticas de segurança e procedimentos, a seleção e implementação de tecnologias e soluções, o monitoramento e controle, as avaliações e os ajustes contínuos. Sendo assim, o quesito de segurança e boas práticas estão envolvidos desde a fase de desenvolvimento até a sustentação desse software.

Em relação ao tema cibersegurança, os pacientes, ao serem questionados se obtêm conhecimento sobre as consequências de um ataque cibernético no setor hospitalar, 57% afirmaram que não obtém conhecimento suficiente, 23% não obtém conhecimento algum e 20% disseram que obtém conhecimento. Em seguida, ao questionar se já presenciaram um acometimento cibernético no hospital, 5% afirmaram que sim.

4.2 OPERAÇÕES HOSPITALARES

Ao tratar das operações hospitalares, a maioria dos profissionais hospitalares responderam que obtêm conhecimento, em relação à questão 5. Em seguida, as respostas para a questão 6 indicaram que quatro profissionais afirmaram haver protocolos relacionados à acometimentos cibernéticos em sua instituição. Dentre os entrevistados, ao responderem a questão 7, apenas um profissional hospitalar atuou e uma organização que sofreu tentativa de acesso ilegal, obtendo como consequência a paralização dos sistemas por uma semana. Os profissionais de saúde, ao serem questionados se realizaram algum treinamento de contingência, em caso de ciberataque, a maior parte afirmou que não.

Os profissionais de TI, ao serem questionados sobre a questão 8, relataram que um plano de contingência completo envolve ativar a equipe de resposta a incidentes, em seguida avaliar os impactos e priorizar as atividades críticas. Permitindo assim a equipe a implementar procedimentos manuais e/ou recuperar os backups dos sistemas, dados, serviços e infraestrutura, assim como, a manter comunicação interna e externa extremamente eficiente. Além disso, é necessário realizar uma avaliação pós incidente para identificar causas e prevenir incidentes futuros, precavendo-se de novas ocorrências e paralisações sistêmicas. Assim como, proteger a integridade dos dados confidenciais e a continuidade do atendimento aos pacientes e demais pessoas no ecossistema do hospital. Por fim, os entrevistados defenderam que é de suma importância a organização obter um plano de contingência funcional, bem definido e atualizado, uma vez que este é vital no ambiente hospitalar.

Em relação à questão 3, os três cenários mais apontados pelos pacientes foram: atrasos no processamento e comunicação dos resultados de exames e comunicação interrompida, com 78 votos cada, e inabilidade de acesso a registros médicos de pacientes, com 76 votos. O quarto cenário mais apontado, com 66 votos, foi o atraso ou cancelamento de cirurgias e exames. Em seguida, a demanda de registro manual do progresso e do tratamento dos pacientes obteve 59 votos. Por fim, a perda do controle de leitos, recebeu 49 votos; a incapacidade de atendimento a pacientes de alto risco, obteve 48 votos; e o desvio de ambulâncias obteve apenas 47 votos.

4.3 CONFIABILIDADE

Ao tratar da confiabilidade, as respostas da questão 9, tanto para os profissionais hospitalares, quanto para os profissionais de TI, todos responderam que a confiabilidade faz parte do processo de investimento em segurança da informação. Em relação aos pacientes, a resposta da questão 4, apenas 31% dos pacientes responderam que continuariam confiando na infraestrutura de um hospital, após um ataque cibernético. Por outro lado, 69% dos pacientes afirmaram que não continuariam confiando mais a sua vida no hospital.

4.4 VELOCIDADE

Por fim, ao tratar da velocidade, a maior parte dos profissionais de saúde afirmaram que o avanço tecnológico contribuiu para a velocidade no ambiente de trabalho. Foi mencionado o aprimoramento no sistema de prontuário eletrônico; sistema de agendas e comunicação de agendamentos; confirmações de consultas; comunicação e cuidados com paciente e familiares; e na segurança do paciente. Em contrapartida, um dos entrevistados afirmou que não houve contribuição na velocidade, devido às camadas de proteção do sistema.

Por outro lado, do ponto de vista dos profissionais de TI, para que não haja interrupções nos sistemas, é necessário a identificação de riscos na instituição, em conjunto com a proteção de dados confidenciais. Estas estão ligadas à adoção de estratégias e práticas de engenharia de software. Sendo este de forma a detectar, resistir, responder e permitir uma rápida recuperação em casos de ataques de cibersegurança. Para tal, é preciso que haja uma cultura de segurança, plataformas seguras, análises regulares de riscos e de testes de segurança. Em conjunto com o monitoramento e resposta a incidentes, as atualizações e patches de segurança, isto é, uma constante. Além disso, é necessário a proteção de dados, uma vez que o setor hospitalar possui dados muito sensíveis, e a devida integração com os diversos sistemas de compartilhamento/interoperabilidade de informações e de imagens de saúde, sem deixar de considerar a expansão corrente da Telemedicina. Para mais, é importante que o software esteja sempre atualizado, configurado e apresente medidas de segurança desde o início do desenvolvimento.

Ao questionar os pacientes sobre o conhecimento em leis que abordam a digitalização e utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de pacientes, a maior parte dos entrevistados apontaram não obter conhecimento sobre as leis apresentadas, sendo este um total de 91% dos pacientes. Desta forma, os pacientes não demonstraram obter conhecimento de como uma ferramenta que pode auxiliar na velocidade dos procedimentos médicos, pode ser o mecanismo utilizado para gerar uma parada sistêmica na instituição.

5 Conclusões/Considerações finais

A metodologia do estudo permitiu atingir parcialmente os objetivos deste. O método de abordagem para os entrevistados foi realizado através de mídias sociais e seleção de perfil, de acordo com a aderência aos temas. Sendo possível identificar o perfil dos respondentes, segmentando entre profissionais hospitalares, profissionais de tecnologia da informação e pacientes. Devido à complexidade das informações e período de pesquisa de campo, não foi possível entrevistar cinco profissionais de tecnologia da informação, como estabelecido anteriormente. Em contrapartida, o universo da amostra relacionado aos profissionais hospitalares foi maior do que o pré-estabelecido.

As teorias levantadas deram um bom panorama sobre as operações hospitalares, cibersegurança e ciberataques. Sendo possível compreender e diferenciar quais as etapas a serem realizadas por profissionais de cada área, tanto para a prevenção, proteção e retenção de danos nos sistemas e equipamentos hospitalares. Assim como, os pontos necessários para desenvolvimento nos hospitais, como uma proteção eficiente para o ambiente digital, em conjunto com o treinamento de seus colaboradores em caso de parada sistêmica. Desta forma, preservando a qualidade e velocidade dos procedimentos hospitalares, em conjunto com a confiança dos pacientes na instituição.

Os objetivos do estudo foram alcançados parcialmente, uma vez que a pesquisa obteve abordagem qualitativa, sendo possível apenas gerar evidências. Englobando a necessidade de um ecossistema para proteger o ambiente digital hospitalar, treinamentos e conscientização constante nesta área para os usuários do hospital, forte governança corporativa e política de segurança da informação. Evidenciando também as consequências, prejuízos e danos que um ataque cibernético pode causar nesse setor.

6 Referências

AGÊNCIA DE SEGURANÇA CIBERNÉTICA E INFRAESTRUTURA. **CISA, HHS Release Collaborative Cybersecurity Healthcare Toolkit**. Cybersecurity & Infrastructure Security Agency, 2023. Disponível em: https://www.cisa.gov/news-events/news/cisa-hhs-release-collaborative-cybersecurity-healthcare-toolkit. Acesso em: 12 jan. 2024.

AGÊNCIA DE SEGURANÇA CIBERNÉTICA E INFRAESTRUTURA. **Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm**. Cybersecurity & Infrastructure Security Agency, 2021. Disponível em: https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf. Acesso em: 10 jan. 2024.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA - ANVISA. **Princípios e práticas de cibersegurança em dispositivos médicos**. ANVISA, 2020. Disponível em: https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2020/saiba-mais-sobre-ciberseguranca-em-dispositivos-medicos/guia-38.pdf. Acesso em: 15 jan. 2024.

ALCATELLUCENT ENTERPRISE**. Cibersegurança para redes de saúde na era da Transformação Digital**. AlcatelLucent Enterprise, 2021. Disponível em: https://www.al-enterprise.com/-/media/assets/internet/documents/healthcare-cybersecurity-brochure-ptbr.pdf. Acesso em: 05 nov. 2023.

ALMEIDA, Lucas. **Cibersegurança: protegendo os dados da sua instituição de saúde**. Nexxto, 2021. Disponível em: https://nexxto.com/ciberseguranca-protegendo-os-dados-da-sua-instituicao-de-saude/. Acesso em: 17 nov. 2023.

BALTZAN, Paige. **Tecnologia Orientada para Gestão**. Porto Alegre: Grupo A, 2016. E-book. ISBN 9788580555493. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788580555493/. Acesso em: 14 jan. 2023.

BARDIN, Laurence. Análise de Conteúdo. São Paulo: Edições 70, 2011. Acesso em: 22 jan. 2023.

BELFRAGE, S.; HELGESSON, G.; LYNOE, N. **Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden**. BMC Medical Ethics, 2022. Disponível em: https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-022-00758-z. Acesso em: 16 dez. 2022.

BOURONIKOS, Vasilis. **Importance of Technology in Healthcare**. Institute of Entrepreneurship Development, 2020. Disponível em: https://ied.eu/blog/importance-of-technology-in-healthcare/. Acesso em: 10 jan. 2023.

CERBERUS SENTINEL. **Most Dangerous Hacked Medical Devices**. Disponível em: https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices/. Acesso em: 20 nov. 2022.

CODEBIT. **Segurança da Informação Hospitalar: uma prática essencial**. Codebit, 2021. Disponível em: https://codebit.com.br/blog/hospitais-e-clinicas/seguranca-informacao-hospitalar-pratica-essencial. Acesso em: 11 out. 2023.

COOPER, Verena. **A importância da cibersegurança na saúde**. SplashTop, 2023. Disponível em: https://www.splashtop.com/pt/blog/importance-of-cybersecurity-in-healthcare. Acesso em: 11 out. 2023.

CORRÊA, Henrique L.; CORRÊA, Carlos A. **Administração de Produção e de Operações - O Essencial**, 3ª edição. São Paulo: Grupo GEN, 2017. E-book. ISBN 9788597013788. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597013788/. Acesso em: 29 mar. 2023.

CRESWELL, John W.; CLARK, Vicki L P. **Pesquisa de métodos mistos. (Métodos de pesquisa)**. Porto Alegre: Grupo A, 2013. E-book. ISBN 9788565848411. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788565848411/. Acesso em: 26 fev. 2023.

DRÄGER. **A importância da segurança de equipamentos médicos**. Disponível em: https://www.draeger.com/pt-br_br/Hospital/Cybersecurity-In-Healthcare. Acesso em: 08 dez. 2022.

DRUMMOND, Virgínia S. **Confiança e Liderança nas Organizações**. São Paulo: Cengage Learning Brasil, 2012. E-book. ISBN 9788522109722. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788522109722/. Acesso em: 10 dez. 2022.

ESTADÃO. **Por que clínicas e hospitais precisam investir em cibersegurança?**. Estadão, 2022. Disponível em: https://summitsaude.estadao.com.br/saude-humanizada/por-que-clinicas-e-hospitais-precisam-investir-em-ciberseguranca/. Acesso em: 10 out. 2023.

EY BRASIL. **Quais os desafios econômicos e tendências do setor de saúde no Brasil**?. EY Brasil, 2023. Disponível em: https://www.ey.com/pt_br/health/como-empresas-de-saude-no-brasil-enfrentam-desafios#chapter-1335947979. Acesso em: 18 jan. 2024.

FORTINET. **Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 02 dez. 2022.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. São Paulo: Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555060164/. Acesso em: 12 jan. 2023.

GRUPO GERENCIAR. **Importância da digitalização de documentos médicos para hospitais e clínicas**. Grupo Gerenciar, 2022. Disponível em: https://grupogerenciar.com.br/2022/10/importancia-da-digitalizacao-de-documentos-medicos-para-hospitais-e-clinicas/. Acesso em 12 jan. 2023.

GUIMARÃES, Keila. **Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais**. BBC Brasil, 2017. Disponível em: https://www.bbc.com/portuguese/brasil-40870377. Acesso em: 31 out. 2023.

INFORCHANNEL. **Hackers invadem hospitais e colocam a vida de pacientes em risco**. InforChannel, 2022 Disponível em: https://inforchannel.com.br/2022/02/09/hackers-invadem-hospitais-e-colocam-a-vida-de-pacientes-em-risco/. Acesso em: 04 dez. 2022.

KASPERSKY. **Cibersegurança para o setor de saúde**. Kaspersky, 2023. Disponível em: https://www.kaspersky.com.br/enterprise-security/healthcare. Acesso em: 05 nov. 2023.

KUPPE, Fernanda. **Política de segurança da informação: como implementar na sua empresa**. VCX, 2023. Disponível em: https://vcx.solutions/politica-de-seguranca-da-informacao-como-implementar/. Acesso em: 16 nov. 2023.

LOPES, Eduardo Bernuy. **Saúde: a importância de se investir na segurança da informação dos pacientes**. Portal Saúde Business, 2018. Disponível em: https://www.saudebusiness.com/ti-e-inovao/sade-importncia-de-se-investir-na-segurana-da-informao-dos-pacientes. Acesso em: 10 dez. 2022.

MAIA, Ubirajara. **Se a saúde é um dos principais alvos de ataques cibernéticos, por que o setor não dá tanta importância ao assunto?.** Future Health, 2021. Disponível em: https://futurehealth.cc/saude-principais-alvos-ataques-ciberseguranca/. Acesso em: 16 jan. 2023.

MOSS, Sebastian. **Patient dies after German hospital IT systems were hacked**. Data Center Dynamics, 2020. Disponível em: https://www.datacenterdynamics.com/en/news/patient-dies-after-german-hospital-it-systems-were-hacked/. Acesso em: 20 nov. 2022.

NEGRI, Fernanda De. **As tecnologias da informação podem revolucionar o cuidado com a saúde?**. Instituto de Pesquisa Econômica Aplicada, 2020. Disponível em:

https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/107-as-tecnologias-da-informacao-podem-revolucionar-o-cuidado-com-a-saude. Acesso em: 10 jan. 2023.
NOVA LEAH. **The Complete Medical Device Cybersecurity Third Party Risk Management and Continuous Monitoring Platform**. Nova Leah, 2023. Disponível em: https://www.novaleah.com/selectevaluate-for-healthcare-providers/. Acesso em: 08 dez. 2023.
PORTAL HOSPITAIS BRASIL. **Setor de Saúde torna-se alvo prioritário dos ataques cibernéticos**. Portal Hospitais Brasil, 2022. Disponível em: https://portalhospitaisbrasil.com.br/setor-de-saude-torna-se-alvo-prioritario-dos-ataques-ciberneticos/. Acesso em: 05 dez. 2022.
REDFOX. **Transformação digital na Saúde: saiba como funciona**. Disponível em: https://redfox.tech/blog/transformacao-digital-na-saude-o-que-e-e-como-promover-a-saude-digital/. Acesso em: 14 jan. 2023.
RICHARDSON, Roberto J. **Pesquisa Social - Métodos e Técnicas**, 4ª edição. São Paulo: Grupo GEN, 2017. E-book. ISBN 9788597013948. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597013948/. Acesso em: 14 jan. 2023.
SENNETT, Richard. **A Corrosão do Caráter: consequências pessoais do trabalho no novo capitalismo**. Rio de Janeiro: Record, 1999. Acesso em: 20 jan. 2023.
SILVEIRA, Aline M.; VILSEKE, Abel J.; PEZZATTO, Alan T.; et al. **Confiabilidade de sistemas**. Porto Alegre: Grupo A, 2018. E-book. ISBN 9788595028456. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595028456/. Acesso em: 23 jan. 2023.
VERGARA, Sylvia C. **Métodos de Pesquisa em Administração**, 6ª edição. São Paulo: Grupo GEN, 2015. E-book. ISBN 9788522499052. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788522499052/. Acesso em: 11 jan. 2023.
WETSMAN, Nicole. **Hospitals say cyberattacks increase death rates and delay patient care**. The Verge, 2021. Disponível em: https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patient. Acesso em: 20 mar. 2023.
WETSMAN, Nicole. **The pandemic revealed the health risks of hospital ransomware attacks.** The Verge, 2021. Disponível em: https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks. Acesso em: 10 jan. 2024.

APÊNDICE A – Matriz de Amarração

Teoria	Perguntas - Profissionais da Saúde	Perguntas - Profissionais de Tecnologia da Informação	Pacientes
Cibersegurança	1. Existem regras de manuseio dos equipamentos de informática na sua unidade hospitalar? Se sim, cite quais são? 2. No seu entender deveria ter um controle adicional de acesso aos equipamentos e	1. Quais são as regras de segurança da informação para manter o cuidado com os dados e garantir a melhoria contínua para o âmbito hospitalar? 2. Como deve ser englobado um departamento de cibersegurança responsável pela	1. Você possui conhecimento sobre as consequências que um ataque cibernético poderia gerar para um hospital? 2. Você já esteve presente em um ambiente durante

	relatórios médicos para todos os usuários? 3. Existe uma Política de Segurança Informacional Hospitalar utilizada pelo seu hospital? Comente sobre. 4. Durante os seus anos de carreira a organização já comentou sobre algum procedimento de teste do sistema informacional?	proteção do ambiente digital do hospital - dados pessoais, equipamentos médicos, sistema informacional e relatórios médicos? 3. Como deve ser realizado e desenvolvido a identificação e monitoramento, visando uma cibersegurança completa para o sistema de rede da organização? 4. Como é avaliado o sistema de proteção de uma rede de dispositivos, visando identificar os riscos presentes? 5. Como é realizada a implementação de um ecossistema de segurança que auxilie na eficiência e velocidade dos sistemas e da infraestrutura de tecnologia da informação? 6. Como é desenvolvido um sistema de antecipação a futuros ataques, problemas ou eventos cibernéticos? 7. Como é desenvolvido a documentação de planejamento de gerenciamento de cibersegurança do ciclo de vida do produto?	um ataque cibernético?
Operações Hospitalares	5. Você obtém conhecimento se existe um plano de gerenciamento de cibersegurança do hospital? 6. No padrão de atendimento para crises há um regulamento sobre acometimentos	8. Em caso de uma parada sistêmica em uma rede hospitalar, qual o plano de contingência?	3. Quais dos seguintes cenários você julgaria como consequência de um ataque cibernético? Sendo estas: comunicação interrompida, desvio de ambulâncias,

	cibernéticos? Se sim, comente sobre. 7. Você já atuou ou atua em alguma instituição médica que já sofreu tentativa ilegal de acesso as informações presentes no sistema? Se sim, qual foi a Gestão de Risco e Continuidade de Negócios? 8. Você já passou por um treinamento de contingência caso o hospital sofra um ataque cibernético? Se sim, quais procedimentos seriam utilizados?		cirurgias e exames atrasados ou cancelados, inabilidade de acesso a registros médicos de pacientes, demanda de registro manual do progresso e do tratamento dos pacientes, atrasos no processamento e comunicação dos resultados de exames, perda do controle de leitos e a incapacidade de atendimento a pacientes de alto risco.
Confiabilidade	9. Confiabilidade para os clientes/pacientes é algo que faz parte do processo de investimento em segurança da informação?	9. Confiabilidade para os clientes/pacientes é algo que faz parte do processo de investimento em segurança da informação e cibersegurança?	4. Você continuaria confiando a sua vida em um hospital após ele ter sofrido um ataque cibernético?
Velocidade	10. Você identifica que o avanço tecnológico contribui para a velocidade no ambiente de trabalho? Sendo sobre prontuários, exames, atendimento, agendas, controle de paciente, comunicação, cirurgias e diversos outros. Se sim, qual você identifica como os mais importantes?	10. Como é possível garantir que um software seja capaz de detectar, resistir, responder e se recuperar de ataques de cibersegurança, a fim de manter seu desempenho essencial?	5. Você obtém conhecimento sobre as Leis Nº13.787/2018 e Nº13.709/2018? Sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.