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.

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.

A partir do apontado pela 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.

2 PROBLEMA DE PESQUISA

Assim como afirmado pela 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.

Em concordância a isso, 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).

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.

2.1 OBJETIVO

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.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 POLÍTICA DE CIBERSEGURANÇA NO SETOR DA SAÚDE

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.

Conforme apontado por 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).

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.

3.2 CONFIANÇA E VELOCIDADE

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.

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.

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.

4 METODOLOGIA

4.1 MÉTODOS DE PESQUISA

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

4.2 UNIVERSO DA AMOSTRA

A amostra da pesquisa foi composta por sete profissionais hospitalares, três profissionais de tecnologia da informação e cem pacientes.

4.3 COLETA DE DADOS

A coleta de dados da pesquisa foi realizada a partir de dois instrumentos, sendo o principal o contato com os respondentes. Este foi concluído através de mídias sociais, onde foram identificados de acordo com a aderência aos temas de cibersegurança, hospitalares e pacientes. Após a realização do planejamento e pré-teste, definição do período de coleta de informações e de profissionais 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. Obtendo como finalidade transmitir os objetivos e apresentar uma padronização no processo de levantamento dos dados, visando obter uma melhor compreensão e tratamento destes. Sendo esta através da matriz de amarração, desenvolvida com base nas teorias envolvidas nas variáveis e elaborado questionamentos.

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

4.4 TRATAMENTO DE DADOS

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 dos pacientes.

A análise de dados foi realizada por frequência de respostas, para examinar 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.

5 ANÁLISE DOS RESULTADOS

A partir da análise de dados, foi compreendido que há um conjunto 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. Em conjunto com a disponibilidade dentro do ambiente, ou seja, evitar interrupções nos procedimentos operacionais hospitalares.

Para este sistema funcionar da devida forma, é exigido atendimento rigoroso às políticas e sistemas de cibersegurança, especialmente 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. Certificação da 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. Sendo esta uma constante, especialmente com o recente desenvolvimento de inteligência artificial nesta área. Apresentando também a necessidade de obter um plano documentado e uma equipe definida para resposta a incidentes, de forma a registrar e prevenir incidentes futuros. Por fim, é crucial realizar ajustes de segurança regulares e garantir atualização de recursos humanos adequados, educação e conscientização em segurança.

Em caso de ataque cibernético na instituição, é evidenciado a necessidade de obter um plano de contingência completo, envolvendo ativar a equipe de resposta a incidentes, avaliar os impactos e priorizar as atividades críticas. Permitindo assim implementar procedimentos manuais ou recuperar os *backups* dos sistemas, dados, serviços e infraestrutura, assim como, manter a comunicação interna e externa extremamente eficiente. Além disso, é preciso 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.

A partir da qualidade e detalhes das informações obtidas durante a análise de dados dos profissionais hospitalares e de tecnologia da informação, foram essenciais para o desenvolvimento detalhado de uma solução. Através do conhecimento sobre os sistemas, *softwares* e ecossistemas que atuam para a proteção do ambiente digital para este setor, em conjunto com outros fatores necessários para que os objetivos sejam alcançados. Este obtendo como finalidade proteger ou minimizar os impactos nas operações essenciais, bem como garantir o atendimento contínuo aos pacientes e demais operações da instituição. Garantindo também a confidencialidade e a integridade dos dados dos pacientes e demais envolvidos no âmbito hospitalar, em conjunto com a confiabilidade que estes depositam na organização.

6 CONSIDERAÇÕES FINAIS

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.

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.

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.

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

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.

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.

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.

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.

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.

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