SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS –
UEG COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO ESPECIALIZAÇÃO EM GERENCIAMENTO DE SEGURANÇA PÚBLICA

HUSTÊNIO ABÍLIO APPELT FILHO

CIBERSEGURANÇA: Desafios da saúde digital no contexto do Sistema Único de Saúde (SUS)

GOIÂNIA-GO

2024

HUSTÊNIO ABÍLIO APPELT FILHO

CIBERSEGURANÇA: Desafios da saúde digital no contexto do Sistema Único de Saúde (SUS)

Artigo científico apresentado como exigência para conclusão da disciplina Metodologia Científica do Curso Especialização em Gerenciamento de Segurança Pública (CEGESP) pela Secretaria de Segurança Pública de Goiás e a Universidade do Estado de Goiás, sob a orientação do Prof. Dra. Reycilane Carvalho Silva.

GOIÂNIA-GO

2024

CIBERSEGURANÇA:
Desafios da saúde digital no contexto do Sistema Único de Saúde (SUS)

CYBERSECURITY:
Challenges of digital health in the context of the Unified Health System (SUS)

Hustênio Abílio Appelt Filho[1]
Ricardo Barbosa de Lima[2]
Reycilane Carvalho Silva[3]

Resumo: Evolução Digital e Cibersegurança na Saúde Pública Brasileira. A transformação digital tem proporcionado avanços significativos no setor da saúde, resultando em diagnósticos mais precisos, tratamentos mais eficazes e maior acessibilidade aos serviços médicos. Contudo, essa evolução também trouxe à tona preocupações relacionadas à cibersegurança. O Brasil, assim como outras nações, tem investido em tecnologia e na capacitação de mão de obra qualificada para enfrentar os desafios da segurança digital na saúde, área que frequentemente é alvo de ataques cibernéticos com o objetivo de obter informações sensíveis da população. As informações de saúde, tanto administrativas quanto financeiras, presentes nos Sistemas de Informações em Saúde (SIS), junto com os dados gerenciais provenientes das demandas da Saúde Pública (DATASUS), são essenciais para o funcionamento do Sistema Único de Saúde (SUS). Este artigo busca entender os desafios enfrentados pelo governo brasileiro na proteção dos dados do SUS, avaliando as legislações vigentes e os riscos associados. A metodologia utilizada nesta pesquisa é de abordagem quali-quanti, integrando métodos qualitativos e quantitativos. Foi realizada uma revisão sistemática da literatura por meio de pesquisas on-line, abrangendo o período de 2010 a 2024. Esta revisão incluiu pesquisas bibliográficas e documentais, a fim de identificar tendências e soluções em cibersegurança no contexto da saúde pública. Além disso, a pesquisa incluiu um levantamento de dados estatísticos sobre óbitos ocorridos entre os anos de 2020 e 2024 nos municípios de Anápolis e Goiânia, no estado de Goiás. Os dados foram obtidos a partir do Sistema de Controle de Laudos (SCL) da Polícia Técnico-Científica de Goiás e do Sistema de Informação sobre Mortalidade (SIM). A abordagem adotada é tanto descritiva quanto exploratória. Descritiva ao detalhar o estado atual da cibersegurança no SUS e exploratória ao investigar novas estratégias e políticas para melhorar a proteção dos dados de saúde. Conclui-se que a cibersegurança no Brasil tem mostrado progressos significativos em termos de políticas e controle do ciberespaço. No contexto do Instituto Médico Legal (IML), sugere-se o desenvolvimento de um programa contínuo de treinamento para os profissionais que utilizam diariamente o SCL, com o objetivo de minimizar vulnerabilidades e prevenir ataques cibernéticos. Dessa forma, este artigo contribui para a compreensão dos desafios e avanços na proteção dos dados de saúde no Brasil, oferecendo insights valiosos para a implementação de medidas mais eficazes em cibersegurança.
Palavras-chave: Saúde; Segurança cibernética; SUS.

Abstract: Digital Evolution and Cybersecurity in Brazilian Public Health. Digital

[1] Bacharel em Medicina (UNIFENAS) – Especialista em Medicina da família e comunidade (SBMFC) – Especialista medicina do trafego (ABRAMET) – hustenio@hotmail.com.

[2] Professor do Programa de Pós-Graduação Interdisciplinar em Direitos Humanos/Mestrado (PPGIDH/PRPG) do Núcleo Interdisciplinar de Estudos e Pesquisas em Direitos Humanos (NDH/UFG), vinculado a Pró-Reitoria de Pesquisa e Inovação (PRPPI/UFG) e Cooperação Acadêmica entre UFG e SSPJGO - ricardobl@ufg.br

[3] Pós Doutoranda em Direitos Humanos pela Universidade Federal de Goiás (UFG) – Orientadora no Curso de Altos Estudos em Segurança Pública (CAESP) - Secretaria de Segurança Pública de Goiás (SSPGO) - reycechadud@gmail.com

transformation has brought significant advancements in the healthcare sector, resulting in more accurate diagnoses, more effective treatments, and greater accessibility to medical services. However, this evolution has also raised concerns related to cybersecurity. Brazil, like other nations, has been investing in technology and skilled labor to address the challenges of digital security in healthcare, a sector that is frequently targeted by cyber-attacks aimed at obtaining sensitive population information. Health information, both administrative and financial, found in the Health Information Systems (SIS), along with managerial data from public health demands (DATASUS), are essential for the functioning of the Unified Health System (SUS). This article seeks to understand the challenges faced by the Brazilian government in protecting SUS data, evaluating the existing legislation and associated risks. The methodology used in this research follows a quali-quantitative approach, integrating both qualitative and quantitative methods. A systematic literature review was conducted through online research, covering the period from 2010 to 2024. This review included bibliographic and documentary research to identify trends and solutions in cybersecurity within the context of public health. Additionally, the research involved gathering statistical data on deaths occurring between 2020 and 2024 in the municipalities of Anápolis and Goiânia, in the state of Goiás. Data were obtained from the Police Scientific Technical Control System (SCL) and the Mortality Information System (SIM). The approach adopted is both descriptive and exploratory. Descriptive by detailing the current state of cybersecurity in SUS and exploratory by investigating new strategies and policies to enhance the protection of health data. It is inferred that cybersecurity in Brazil has shown significant progress in terms of policies and control of cyberspace. In the context of the Medical Examiner's Office (IML), it is suggested to develop a continuous professional training program for those who handle the SCL daily, aiming to minimize vulnerabilities and prevent cyber-attacks. Thus, this article contributes to the understanding of the challenges and advances in the protection of health data in Brazil, providing valuable insights for the implementation of more effective cybersecurity measures.
Keywords: Health; Cybersecurity; SUS.

INTRODUÇÃO

Ao longo da história do Estado moderno e de forma mais profícua no contemporâneo, a tecnologia vem ocupando cada vez mais espaço e hoje em dia tem papel fundamental em todas as sociedades. Sua evolução transforma o mundo transpondo fronteiras, o que está aliado também ao crescente fluxo de dados e informações entre as mais diversas sociedades, uma realidade que certamente apresenta problemas e vulnerabilidades em termos de segurança. O risco de acessar redes e sites de todo o mundo traz perigos tanto para o usuário comum, quanto para organizações e instituições, tanto privadas quanto públicas (Caetano, 2023).

Numa perspectiva brasileira, a cibersegurança pode ser circunscrevida como pauta tanto de segurança e defesa do Brasil, quanto também em âmbito da ciência e do desenvolvimento tecnológico. O primeiro documento brasileiro que cita segurança cibernética, a Estratégia Nacional de Defesa (END) de 2008, ressalta que a estratégia de desenvolvimento nacional busca a “independência nacional, alcançada pela capacitação

tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear" uma vez que "não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento" (Brasil, 2008, s/p.).

Neste contexto, o termo 'ciberespaço' surgiu no final do século XX, sendo utilizado para definir todo o conjunto de redes de internet, o qual interliga usuários, sites, servidores, organizações, etc. Em decorrência a este termo e suas aplicações em diferentes âmbitos, surgiram também variações para ele, como o termo 'cibersegurança' ou 'segurança cibernética' (Caetano, 2023).

No cenário contemporâneo, a interconexão entre sistemas de informação e segurança pública se torna cada vez mais evidente e complexa. Com a rápida digitalização de serviços essenciais, como o Sistema Único de Saúde (SUS), a proteção de dados se tornou um aspecto fundamental da segurança pública. Como afirmado por Araújo (2024), a proteção de dados na área da saúde não é apenas uma questão de privacidade, mas também uma questão de segurança pública e bem-estar dos cidadãos.

O SUS, enquanto sistema de saúde universal e integral no Brasil, lida com uma quantidade imensa de informações sensíveis dos pacientes. A necessidade de proteger esses dados contra ameaças cibernéticas é incontestável, pois podem ter consequências devastadoras para os sistemas de saúde, comprometendo a integridade dos dados dos pacientes e colocando em risco a qualidade dos serviços de saúde (Figueredo; Varella, 2022).

Acredita-se que 90% das organizações do setor de saúde 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), como por exemplo o treinamento inadequado ou até mesmo inexistente e baixo investimento na segurança de dados. Para os cibercriminosos, o setor de saúde é um alvo atraente e vulnerável por dois motivos: é uma fonte rica de informações valiosas da população e é um alvo extremante vulnerável (Martin *et al*., 2017).

Além disso, ataques cibernéticos bem-sucedidos contra o sistema de saúde podem ter sérias consequências para a saúde pública, como interrupções nos serviços de atendimento médico, comprometimento da qualidade do tratamento e até mesmo riscos à vida dos pacientes, destacando a importância crítica da cibersegurança para a sociedade como um todo. Portanto, a inadequação na cibersegurança pode resultar não apenas no comprometimento dos dados, mas também no comprometimento de dispositivos vitais à vida. É essencial que haja conscientização de todos os envolvidos no setor de saúde sobre a responsabilidade da segurança cibernética, pois ela vai além dos fabricantes de dispositivos

médicos, mas envolve os servidores e inclusive do usuário final (Natsiavas *et al*., 2018).

Do ponto de vista acadêmico, a cibersegurança no setor de saúde tem sido tratada como tópico importante por autores brasileiros e estrangeiros (Abraham *et al*. 2019, Alexander *et al*. 2019, Coronado *et al*. 2014, Ghafir *et al*. 2018, Gordon *et al*. 2019, Martin *et al*. 2017, Ondiege *et al*. 2017), sendo comum a todos eles que as informações geradas por este setor são valiosas, mas que os estados têm realizado ações insuficientes na proteção de dados da saúde e que não há investimentos significativos em cibersegurança, sendo uma área por muitas vezes negligenciada.

Portanto, é necessário avançar em estudos para aumentar a conscientização sobre a cibersegurança e construir uma cultura nas instituições públicas e privadas orientadas à cibersegurança (Natsiavas *et al*., 2018). Nos últimos anos o Brasil foi alvo de diversos ataques cibernéticos que afetaram instituições públicas e privadas. Em particular, o setor de saúde tem sido alvo de ataques de *ransomware*[4] e vazamentos de dados. Diante desse cenário, torna-se evidente a importância de um estudo aprofundado sobre a cibersegurança no contexto do SUS. O presente trabalho tem como tema os desafios enfrentados pelo governo brasileiro para proteção de dados do Sistema Único de Saúde (SUS), já que ele é utilizado pela grande maioria dos cidadãos brasileiros.

O presente trabalho tem como objetivo geral avaliar os desafios enfrentados pelo governo brasileiro na proteção dos dados do Sistema Único de Saúde (SUS). A crescente digitalização no setor da saúde trouxe não apenas benefícios em termos de eficiência e acessibilidade, mas também a necessidade de fortalecer a cibersegurança para proteger informações sensíveis da população. Nesse contexto, é essencial entender as principais dificuldades e as ações tomadas para garantir a segurança dos dados no SUS.

Primeiramente, o trabalho busca identificar os maiores desafios atuais para a gestão da segurança cibernética no Brasil. Este objetivo específico envolve a análise das vulnerabilidades existentes no sistema de saúde e dos riscos associados a possíveis ataques cibernéticos. A complexidade e a magnitude do SUS, que atende milhões de brasileiros, tornam a proteção de dados um desafio significativo, exigindo uma infraestrutura robusta e atualizada para prevenir e mitigar ataques.

Em segundo lugar, o trabalho pretende evidenciar as iniciativas governamentais voltadas para a segurança dos dados dos cidadãos no SUS. Esta análise inclui a avaliação de

[4] software malicioso que criptografa os dados de um computador ou de uma rede, tornando-os inacessíveis aos usuários

políticas públicas, investimentos em tecnologia e programas de capacitação para profissionais da saúde. É crucial entender como o governo tem atuado para fortalecer a cibersegurança e quais medidas estão sendo implementadas para proteger as informações sensíveis dos pacientes.

Por fim, o trabalho busca conhecer a legislação brasileira referente à proteção de dados e cibersegurança. A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, é um marco importante na regulamentação da proteção de dados no Brasil. Este objetivo específico envolve a análise da LGPD e de outras normativas relacionadas, com o intuito de compreender como a legislação brasileira está sendo aplicada no contexto da saúde pública e quais são as lacunas e desafios ainda existentes.

Assim, este trabalho contribui para uma compreensão abrangente dos desafios e das iniciativas do governo brasileiro na proteção dos dados do SUS. Ao abordar os aspectos técnicos, políticos e legais da cibersegurança na saúde, busca-se oferecer uma visão detalhada e crítica das estratégias e das políticas adotadas para garantir a segurança das informações de saúde no Brasil.

Para tanto a metodologia utilizada concentra-se no cunho qualitativo com a análise da gestão da segurança cibernética brasileira, seus desafios e legislação pertinente. As consequencias de ataques cibernéticos foram demonstradas a partir de exemplos identificados em literatura. Adicionalmente foram analisados os dados gerados pelo Instituto Médico Legal - IML e pelo DATASUS em relação aos óbitos ocorridos entre os anos de 2020-2024 nos municípios de Anápolis e Goiânia, no estado de Goiás. Os dados foram comparados para enfatizar a importância da informação gerada pelo IML para estudos sobre melhoria e implementalção de políticas de segurança pública e cibernética.

O trabalho foi estruturado em tópicos para proporcionar um detalhamento mais minucioso do assunto. Primeiramente, no tópico 1.1, aborda-se a cibersegurança de forma geral e sua aplicação no setor da saúde. Este segmento discute o conceito de cibersegurança e explora como ele se relaciona com os sistemas de saúde, destacando a importância da proteção de dados sensíveis e a prevenção de ataques cibernéticos que podem comprometer a integridade e a privacidade das informações médicas.

No tópico 1.2, o foco se volta para o DataSUS, descrevendo detalhadamente as ferramentas utilizadas pelo Estado para organizar o sistema digital de saúde. O DataSUS é uma plataforma essencial para a gestão de dados de saúde no Brasil, e este tópico examina suas funcionalidades, a infraestrutura tecnológica envolvida e os mecanismos de segurança implementados para garantir a proteção dos dados armazenados e processados.

Por fim, o tópico 1.3 trata da legislação e das estratégias brasileiras relacionadas à proteção de dados gerais e em saúde. Este segmento detalha as principais leis desenvolvidas no Brasil com o objetivo de alcançar a segurança cibernética na saúde, como a Lei Geral de Proteção de Dados (LGPD) e outras normativas específicas do setor. São analisadas as estratégias e políticas adotadas pelo governo para fortalecer a cibersegurança, bem como os desafios e as lacunas ainda presentes na legislação e na prática.

Ao dividir o trabalho nesses tópicos, busca-se fornecer uma compreensão abrangente e detalhada dos diversos aspectos que envolvem a cibersegurança no setor da saúde, desde os conceitos fundamentais e as ferramentas utilizadas até a legislação e as estratégias implementadas pelo governo brasileiro para proteger os dados de saúde da população.Diante da relevância social, econômica e acadêmica da cibersegurança no sistema de saúde brasileiro, este estudo se apresenta como uma contribuição significativa para a compreensão dos desafios e soluções já alcançadas pelo Brasil, abrindo espaço para a busca de futuras soluções nesse campo e fortalecimento da segurança dos dados de saúde dos cidadãos brasileiros.

1 REVISÃO TEÓRICA

O Sistema Único de Saúde (SUS) é uma das maiores e mais complexas redes de saúde pública do mundo, estruturado para garantir acesso universal, integral e equitativo a serviços de saúde para toda a população brasileira. Criado pela Constituição Federal de 1988 e regulamentado pela Lei nº 8.080/1990, o SUS é organizado em três níveis de gestão: federal, estadual e municipal.

No nível federal, o Ministério da Saúde é responsável por formular políticas nacionais, coordenar programas de saúde pública, definir diretrizes e repassar recursos financeiros aos estados e municípios. As secretarias estaduais de saúde, por sua vez, atuam na coordenação e execução de políticas de saúde no âmbito estadual, complementando as ações federais e prestando apoio técnico e financeiro aos municípios. No nível municipal, as secretarias de saúde são responsáveis pela gestão e execução direta dos serviços de saúde, incluindo unidades básicas de saúde, hospitais e programas de saúde da família.

A política pública de saúde no Brasil, sob a administração do SUS, envolve a implementação de programas e ações que visam a promoção, prevenção e recuperação da saúde. A gestão eficiente e a tomada de decisões baseadas em dados confiáveis são essenciais para a

eficácia dessas políticas. Com a crescente digitalização dos serviços de saúde, o armazenamento e a gestão de dados se tornaram uma necessidade crítica. Nesse contexto, a plataforma GOV.br, um portal unificado do governo brasileiro, facilita o acesso a serviços e informações digitais, inclusive na área da saúde.

A integração digital proporcionada pela plataforma GOV.br é crucial para a melhoria da gestão de dados de saúde no SUS, oferecendo vários benefícios. Em primeiro lugar, permite a centralização de dados de saúde em um único sistema, facilitando o acesso e a gestão de informações pelos diferentes níveis de gestão do SUS. Além disso, o acesso a dados integrados e atualizados possibilita uma melhor análise e planejamento das políticas de saúde, permitindo respostas mais rápidas e eficientes a crises sanitárias e outras demandas da saúde pública.

Outro benefício significativo é a segurança de dados. A proteção dos dados de saúde é uma prioridade, e o uso de plataformas seguras como o GOV.br ajuda a minimizar os riscos de vazamentos e ataques cibernéticos, garantindo a privacidade e a integridade das informações dos cidadãos. A integração de sistemas de saúde com a plataforma GOV.br também facilita a interoperabilidade entre diferentes sistemas e bases de dados, promovendo uma comunicação mais eficiente entre unidades de saúde e órgãos de gestão.

Apesar dos avanços, o SUS enfrenta desafios significativos em termos de infraestrutura e recursos humanos capacitados para gerenciar e proteger grandes volumes de dados. A necessidade de investimentos contínuos em tecnologia e treinamento é crucial para assegurar que os dados armazenados sejam utilizados de forma eficaz e segura. Além disso, a legislação, como a Lei Geral de Proteção de Dados (LGPD), impõe diretrizes rigorosas para a proteção e o uso de dados pessoais, o que exige uma adaptação constante das políticas e práticas de armazenamento de dados dentro do SUS.

A estrutura do SUS, aliada à política pública do Estado e às novas necessidades de armazenamento de dados, evidencia a importância da digitalização e da segurança cibernética na gestão da saúde pública. A plataforma GOV.br representa um passo significativo nessa direção, promovendo a centralização, segurança e eficiência na gestão dos dados de saúde, essencial para a melhoria contínua dos serviços oferecidos à população brasileira.

A internet ajudou o crescimento econômico e se tornou um recurso para a sociedade, disponibilizando novas oportunidades e sendo a infraestrutura crítica para muitos serviços. Logo, ataques em ambiente virtual promovem perigo à esses serviços, pois *hackers*[5] utilizam

[5] Indivíduos com habilidades avançadas em computação e tecnologia, que utilizam seus conhecimentos para explorar sistemas informáticos, redes e software.

das vulnerabilidades existentes no ciberespaço para prejudicar os sistemas de informação (Nunes, 2012). Neste contexto, foi criado o conceito de cibersegurança, isto é, a segurança do ciberespaço. O objetivo da cibersegurança é controlar o acesso às informações de forma que pessoas não autorizadas não consigam obter acesso a esses dados. Além disso, ela busca encontrar formas de verificar mensagens, bem como garantir sua autenticidade, para que se possa ter certeza com quem se está falando ou quem enviou uma determinada mensagem (Teles, 2015).

A evolução digital na esfera da saúde trouxe uma série de benefícios, incluindo diagnósticos mais acurados, tratamentos mais efetivos e uma maior acessibilidade aos serviços médicos. Contudo, essa transição também despertou a preocupação com a cibersegurança. Conforme os sistemas de saúde se tornam cada vez mais dependentes da tecnologia, os perigos associados aos ataques cibernéticos, capazes de comprometer severamente a segurança dos pacientes e a integridade dos dados médicos, também se intensificam (Araújo, 2024).

Dentro da dinâmica do ciberespaço e da cibersegurança, é fundamental que as nações possuam capacidades internas para se projetarem com tecnologias próprias e, principalmente, mão de obra qualificada. Infelizmente no Brasil os ataques cibernéticos são comuns e cresceram espantosos 950% em relação a 2021, segundo relatório da Fortinet, uma empresa multinacional da California – Estados Unidos da América – que desenvolve e comercializa sortware, produtos e serviços de cibersegurança. Atualmente, a área da saúde é a que mais sofre com os ataques, que são realizados para gerar visibilidade, já que é tema de interesse da população; para pedir pagamento de resgate de dados; porque ainda há baixa capacitação em segurança, dentre outras razões.

A cibersegurança no Sistema Único de Saúde (SUS) apresenta uma série de desafios e questões complexas. A crescente digitalização dos serviços de saúde, aliada à sensibilidade dos dados dos pacientes, cria um ambiente propício para ameaças cibernéticas que podem comprometer a integridade e segurança das informações (Figueredo; Varella, 2022).

Diante deste contexto, a Organização Mundial da Saúde (OMS) fixou o período de cinco anos (a partir de 2020) para estados membros estabelecerem uma abordagem segura em meio à saúde digital. Este prazo expira em 2025, ou seja, diversas nações, inclusive o Brasil, precisam criar ou já estão desenvolvendo legislações mais robustas para resguardar dados sensíveis de seus cidadãos em pouco tempo.

1.1 Cibersegurança geral e no setor da saúde

Governar ou administrar a cibersegurança abrange todos os métodos de governança, incluindo nações, estados regionais, mercados, desenvolvedores de *software*[6] e *hardware*[7], proprietários de sistemas e equipamentos, e usuários finais (Kuerbis *et al*., 2017). Segundo Natsiavas *et al*. (2018), a interação dessas diversas formas de governança sobre a segurança cibernética resulta em uma governança fragmentada e confusa. No entanto, as nações devem encarar a cibersegurança como uma questão de segurança nacional, dada sua importância e relevância (Kuerbis *et al*., 2017).

Martin *et al*. (2017) identificam três pilares fundamentais no cerne do problema: uma governança fragmentada, onde falta clareza sobre as responsabilidades para proteger sistemas e dados; uma cultura no setor que se concentra apenas no atendimento aos clientes; e a falta de investimentos significativos na proteção dos sistemas.

Conforme Berger e Schneck (2019), a cibersegurança reflete os riscos enfrentados à medida que a internet cresce e se diversifica. Como a internet foi originalmente desenvolvida sem preocupações com a segurança, o armazenamento ou tráfego de dados, a cibersegurança tornou-se uma preocupação posterior.

Mostfa *et al*. (2016) afirmam que todos os setores econômicos devem se proteger contra vários tipos de ameaças, como *malware*[8], *phishing*[9], engenharia social (obtenção de informações confidenciais por meio da persuasão dos usuários), negação de serviço (sobrecarga dos recursos dos sistemas, como processamento de dados e/ou tráfego de rede), *botnet*[10] e *ransomware*.

De acordo com Alexander *et al*. (2019), garantir a cibersegurança é uma tarefa desafiadora em qualquer setor na era da informação atual, e o setor de saúde se destaca como um dos alvos mais suscetíveis a ataques cibernéticos devido à sua infraestrutura antiquada e não adaptada especificamente para suas necessidades. Assim como em outros setores, o campo da saúde está continuamente adotando inovações tecnológicas para atender às demandas atuais

---

[6] Programas de computador, ou conjunto de instruções, que permitem ao usuário realizar tarefas específicas em um computador ou dispositivo eletrônico

[7] Componentes físicos de um computador ou dispositivo eletrônico que podem ser tocados e manipulados.

[8] Abreviação para "software malicioso" (malicious software) e refere-se a qualquer tipo de programa ou código de computador desenvolvido com o objetivo de causar danos, roubar dados, comprometer a segurança ou operação de sistemas computacionais sem o consentimento do usuário.

[9] técnica para enganar os usuários e obter informações confidenciais

[10] invasão de vários sistemas por meio de "robôs" que os controlam sem o conhecimento dos usuários

dos cuidados de saúde, tanto dentro quanto fora do ambiente hospitalar (Wethington *et al*., 2018).

Os registros tradicionais dos pacientes foram substituídos por Registros Médicos Eletrônicos, nos quais são armazenadas todas as informações pessoais e clínicas dos pacientes. Isso amplia ainda mais a superfície de ataque e apresenta desafios significativos para a segurança digital das instituições (Gordon *et al*., 2019). Apesar dos benefícios como a rápida transmissão de informações clínicas para os médicos e o gerenciamento em tempo real da terapia, a conectividade generalizada pode expor os pacientes a vulnerabilidades em termos de segurança cibernética (Alexander *et al*., 2019).

Também é importante considerar a telessaúde, um conceito abrangente que engloba várias atividades distintas, como serviços remotos, diagnósticos, pesquisas e educação. Dentro desse contexto, está o telediagnóstico, que permite diagnosticar doenças à distância, com o "paciente e médico em locais distintos" (Dias, 2021). Essas novas ferramentas trazem benefícios para pacientes, profissionais e gestores do setor de saúde. Cada vez mais, os pacientes utilizam seus próprios dispositivos móveis, que se integram aos sistemas médicos, permitindo um gerenciamento colaborativo de doenças e a coordenação de cuidados (Handler, 2018).

Com todos esses avanços, a cibersegurança torna-se cada vez mais crucial na infraestrutura das organizações de saúde. Ataques sofridos por essas instituições impactaram negativamente suas operações, resultando em perda de informações, cancelamentos de consultas e procedimentos clínicos, e altos custos financeiros, além de um custo intangível que é a reputação negativa das instituições (Gordon *et al*., 2019). No entanto, apenas recentemente a cibersegurança se tornou um tópico importante dentro do setor de saúde, como resultado do potencial de comprometimento dos dispositivos médicos (Coronado *et al*., 2014).

Além disso, de acordo com a literatura científica, os profissionais especializados em cibersegurança são escassos e caros. Por essa razão, as organizações de saúde frequentemente não conseguem pagar as taxas de mercado por esses serviços e acabam contando com equipes que não estão adequadamente preparadas para enfrentar os desafios atuais (Martin *et al*., 2017).

Segundo a perspectiva de Abraham *et al*. (2019), apenas 40% dos altos executivos do setor de saúde possuem um entendimento profundo dos protocolos de segurança cibernética. Isso sugere que a alta administração não está assumindo a liderança ou a responsabilidade de garantir uma governança forte em segurança cibernética. Além disso, é demonstrado um baixo comprometimento de recursos, geralmente variando de 0% a 3% do orçamento total de TI, dedicados à gestão da cibersegurança.

De acordo com Maimó *et al*. (2019), os mecanismos de proteção cibernética existentes,

como antivírus, sistemas de detecção de intrusões (IDS), *firewalls*, filtros da web, VPNs etc., não são suficientes para defender os sistemas organizacionais de ataques cibernéticos. Isso ocorre devido ao fato de que os sistemas atuais transformam dados em informação, essa informação em conhecimento e, consequentemente, em metadados.

1.2 O DATASUS

A Saúde Pública no Brasil passou por diversas transformações ao longo dos anos, e um ponto crucial desse processo foi a realização da 8ª Conferência Nacional de Saúde em 1986, sediada em Brasília. Esse evento representou um marco significativo, pois teve um papel fundamental na estruturação do Sistema Único de Saúde (SUS). A partir dessa conferência, foram estabelecidas diretrizes para a prestação de cuidados de saúde baseados em princípios de universalidade, acesso equitativo e participação ativa da sociedade nas decisões. A implementação dessas diretrizes requer a administração e supervisão dos serviços em todos os níveis governamentais, seguindo padrões éticos e morais, visando promover o bem-estar coletivo (Brasil, 2006).

Portanto, esse paradigma demanda não apenas líderes capazes de introduzir políticas e normas de atendimento inovadoras, mas também requer habilidades e competências para enfrentar os desafios que surgem durante esse processo de transição. Além disso, esse modelo exige que os gestores de saúde sejam sensíveis, decididos, práticos, responsáveis, perspicazes e que possuam estratégias claras de planejamento, organização, coordenação e supervisão (Martins; Waclawovsky, 2015).

Acesso a dados precisos, oportunos e facilmente acessíveis é, portanto, essencial para a formulação de políticas, organização, monitoramento e controle dos serviços de saúde prestados à comunidade. Isso se deve ao fato de que o acesso aos registros de saúde pública desempenha um papel crucial na identificação da exposição ambiental a doenças e, também, na monitoração do progresso e eficácia das intervenções (Martins; Waclawovsky, 2015).

Diante desse contexto emergente, o Ministério da Saúde, com o objetivo de fomentar e apoiar a gestão, tem colaborado com o Departamento de Informática do Sistema Único de Saúde (DATASUS) para criar uma variedade de recursos destinados a garantir o acesso à informação e comunicar as atividades dentro do SUS (BRASIL, 2014).

O DATASUS é responsável por fornecer aos órgãos do SUS os sistemas de informação e o suporte computacional essenciais para o planejamento, execução e monitoramento dos planos de saúde. Atualmente, o departamento desempenha um papel significativo como

provedor de soluções de *software* para as secretarias estaduais e municipais de saúde, adaptando seus sistemas de acordo com as necessidades dos gestores e incorporando novas tecnologias à medida que a descentralização administrativa se consolida (Brasil, 2002).

Estabelecido pelo Decreto Nº 100, de 16 de abril de 1991, publicado no Diário Oficial da União (D.O.U.) em 17 de abril de 1991 e retificado conforme publicado no D.O.U. de 19 de abril de 1991, o DATASUS tem a competência de especificar, desenvolver, implantar e operar sistemas de informações relacionados às atividades finais do SUS, em conformidade com as diretrizes do órgão setorial (Brasil, 2007).

Atualmente, o DATASUS é responsável por uma vasta quantidade de informações do Sistema Único de Saúde (SUS). As informações em saúde, administrativas e financeiras dos atuais Sistemas de Informações em Saúde (SIS), juntamente com as informações gerenciais produzidas a partir das demandas dos Gestores (Municipal, Estadual e Federal) da Saúde Pública, constituem um de seus principais ativos, sendo informações cruciais para o funcionamento do SUS. O Departamento é de fato responsável pela implementação do Sistema Nacional de Informação em Saúde (SNIS) do Ministério da Saúde (Brasil, 2007).

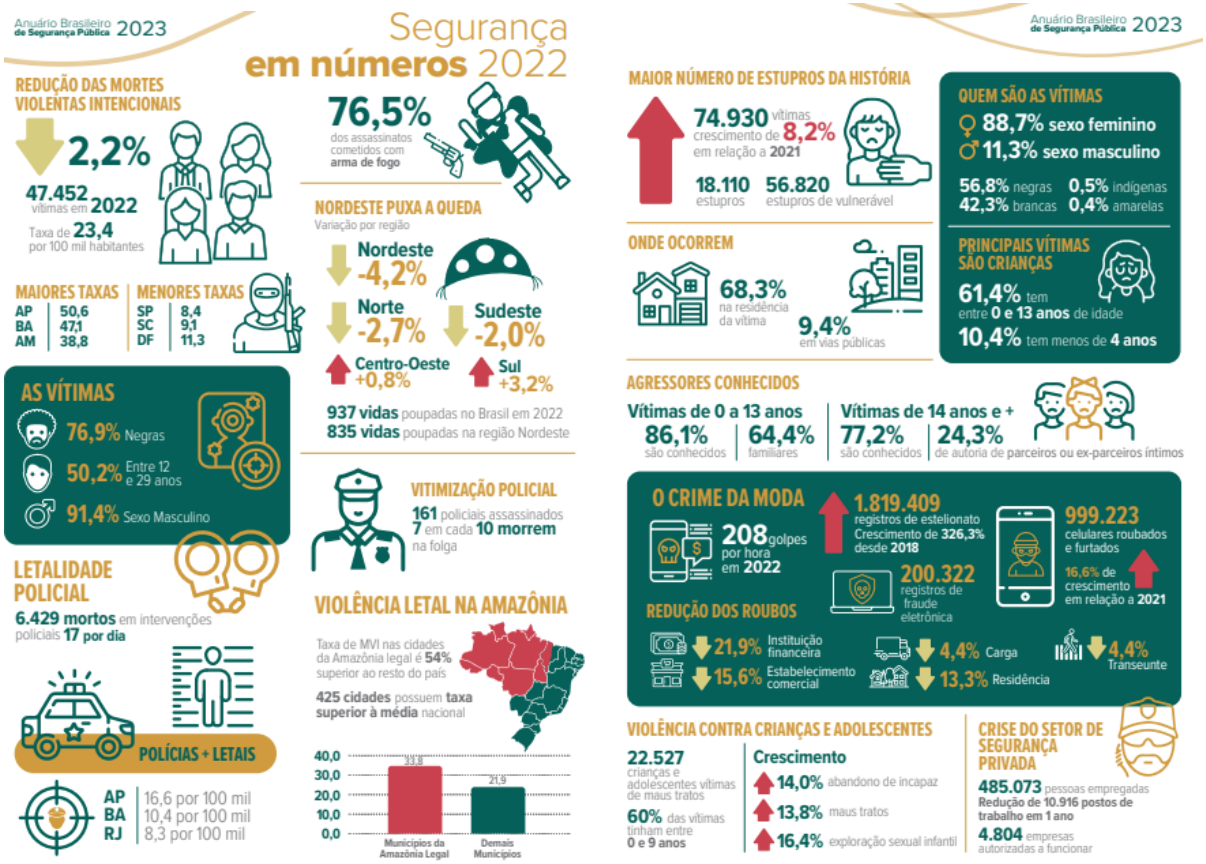
Ainda sim, o Departamento gera uma vasta gama de dados sobre a saúde pública no país. Esses dados são fundamentais para a gestão, planejamento e avaliação de políticas de saúde. Os principais tipos de dados gerados pelo DataSUS incluem: Dados de Mortalidade (SIM - Sistema de Informação sobre Mortalidade), Dados de Nascidos Vivos (SINASC - Sistema de Informações sobre Nascidos Vivos), Dados de Internações Hospitalares (SIH - Sistema de Informações Hospitalares), Dados de Notificações de Agravos (SINAN - Sistema de Informação de Agravos de Notificação), Dados de Assistência Ambulatorial (SIA - Sistema de Informações Ambulatoriais), entre outros.

Neste sentido, os médicos legistas são fundamentais para a geração de dados de alta qualidade no DataSUS, o que, por sua vez, sustenta a saúde pública no Brasil. Sua atuação permite uma compreensão mais aprofundada da mortalidade e das suas causas, influenciando diretamente na formulação de políticas públicas, na pesquisa científica e na melhoria contínua dos serviços de saúde.

Um exemplo disso são os dados gerados pelo Anuário Brasileiro de Segurança Pública, que é uma publicação anual que reúne, analisa e divulga dados e informações sobre a segurança pública no Brasil (FBSP, 2023). Ele é produzido pelo Fórum Brasileiro de Segurança Pública (FBSP), uma organização não governamental que se dedica a promover a transparência e a eficiência na gestão da segurança pública no país. Informações como “Estatísticas de Criminalidade”, “Violência contra Grupos Vulneráveis” são baseados em dados gerados

também pelo DATASUS. No ano de 2023 foi publicado a análise de segurança pública brasileira do ano de 2022, dados que foram compilados e resumidos nas Figuras 1 e 2 abaixo, sendo exemplos da importância dos dados gerados sobre saíde e segurança pública no país.

Figura 1: Mapa da violência: dados sobre número de mortes, características das vítimas, regiões de ocorrencia e sobre a ocorrencia de estupros no ano de 2022.



Fonte: Anuário Brasileiro de Segurança Pública 2023.

1.3 Legislação e estratégias brasileiras relacionadas à proteção de dados gerais e em saúde

A proteção da privacidade individual é consagrada como um dos direitos fundamentais pela Constituição Federal de 1988 e é também um dos princípios fundamentais do Marco Civil da Internet (Brasil, 2014), uma legislação que aborda interações no ambiente digital. Até meados de 2018, o Brasil carecia de legislação específica sobre a proteção de dados pessoais. Entre as leis relevantes neste contexto, destacam-se a Lei do Habeas Data (Lei nº 9.507, de 12 de novembro de 1997), o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) e o Marco Civil da Internet (Lei nº

12.965, de 23 de abril de 2014). Apenas com a promulgação da Lei nº 13.709, de 14 de agosto de 2018, o Brasil passou a dispor de uma Lei Geral de Proteção de Dados Pessoais.

Recentemente, esse direito tornou-se um dos pilares da Lei Geral de Proteção de Dados (LGPD), que regula a coleta, proteção e transferência de dados pessoais no país. Essa legislação foi implementada com o objetivo de aumentar o controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para o uso e coleta de dados, e garantindo que os usuários tenham opções para acessar, corrigir e excluir essas informações. No contexto da LGPD, há uma atenção especial aos dados relacionados à saúde, considerados sensíveis devido à sua alta vulnerabilidade e potencial para discriminação (Boni, 2018).

A orientação sobre a Proteção e Utilização de Dados Relacionados à Saúde (United Nations, 2019), desenvolvida pela força-tarefa da Organização das Nações Unidas (ONU) responsável pela privacidade e proteção de dados ligados à saúde, esclarece a definição de "dados relacionados à saúde". Segundo o documento, esses dados englobam todas as informações pessoais relacionadas à condição física ou mental de um indivíduo, incluindo registros de serviços médicos que revelem aspectos sobre seu histórico, estado atual ou prognóstico de saúde. Além disso, os dados genéticos são igualmente considerados dados de saúde conforme essa recomendação. Os dados de saúde provenientes de testes, como diagnósticos pré-natais, diagnósticos de pré-implantação ou identificação de características genéticas, mesmo que não diretamente relacionados à saúde da mãe, devem receber proteção equivalente a outros dados de saúde.

Nesse contexto, estão inclusos o tratamento de dados pessoais ligados à saúde, realizado por profissionais de saúde ou entidades sanitárias, assim como o tratamento de dados pessoais para fins de pesquisa científica, por exemplo. Essas informações são consideradas sensíveis e requerem mecanismos específicos para assegurar sua proteção, segurança e confidencialidade. No campo da saúde, o princípio da confiança vai além das questões éticas e estabelece-se como a base fundamental da relação entre o paciente e os profissionais responsáveis por seu tratamento, o que influencia diretamente sua qualidade de vida.

No entanto, é crucial destacar que a transmissão desses dados sensíveis envolve uma variedade de serviços que ultrapassam a relação médico-paciente, incluindo seguradoras, laboratórios e prestadores de serviços terceirizados, entre outros (United Nations, 2019). Em 2016, foi estabelecida a Política Nacional de Informação e Informática em Saúde (PNIIS), com o intuito de guiar as iniciativas de tecnologia da informação e comunicação (TIC) em todo o sistema de saúde brasileiro (BRASIL, 2016). A questão da privacidade é abordada inicialmente na apresentação dos princípios fundamentais da política, os quais

englobam a confidencialidade, o sigilo e a privacidade das informações de saúde pessoal como direitos individuais. Posteriormente, a privacidade é associada à utilização de certificação digital e, por fim, é mencionada como uma das principais barreiras para a implementação de projetos de TI em saúde, evidenciando vulnerabilidades e incertezas quanto aos meios de garantia na prática.

No ano subsequente, uma abordagem mais prática em relação à saúde digital foi delineada através do documento chamado Estratégia e-Saúde para o Brasil, aprovado pela Resolução CIT nº 19, de 22 de junho de 2017, emitida pela Comissão Intergestores Tripartite (CIT). Esse documento estabeleceu diretrizes e princípios para o Sistema Único de Saúde (SUS), e discutiu a política brasileira de governo eletrônico, com foco na proposta de Saúde Digital e nas estratégias para integrá-la ao SUS. De acordo com o referido documento, a e-Saúde deveria ser incorporada ao SUS como uma dimensão fundamental até o ano de 2020, com o objetivo de melhorar substancialmente os serviços de saúde através da disponibilização e utilização de informações completas, precisas e seguras. As tecnologias empregadas seriam consideradas como um meio para alcançar um padrão superior de qualidade na prestação de cuidados de saúde e nos processos relacionados à saúde, em todas as esferas governamentais e no setor privado, beneficiando pacientes, cidadãos, profissionais de saúde, gestores e organizações de saúde (Brasil, 2020).

Como forma de concretizar a visão delineada para a saúde digital no Brasil, o programa do governo federal conhecido como Conecte SUS (CONECT SUS, 2021) foi destacado. Este programa consiste em um sistema integrado destinado a promover o suporte à informatização e à troca de informações entre os estabelecimentos de saúde. Implementado através de um aplicativo disponível para uso tanto por profissionais de saúde quanto por cidadãos em geral, o Conecte SUS adere aos mesmos padrões de política de privacidade dos aplicativos do Ministério da Saúde e estabelece uma série de diretrizes com o objetivo de preservar a confidencialidade das informações armazenadas em seu sistema. Além disso, ele fornece um documento informativo aos titulares dos dados de saúde, esclarecendo questões relevantes sobre o acesso às informações e até mesmo sobre a possibilidade de recusar o compartilhamento dos dados de saúde.

O Ministério da Saúde caracterizou o Conecte SUS como um programa em constante desenvolvimento, sujeito a monitoramento e avaliação sistemáticos (CONECT SUS, 2021). Para este fim, durante a 34ª Reunião Ordinária do Comitê Gestor da Estratégia de Saúde Digital, foi aprovado o Plano de Ação, Monitoramento e Avaliação, concebido para identificar, priorizar e integrar de maneira coordenada os programas, projetos e ações de saúde, com o intuito de

implementar as iniciativas que compõem o sistema Conecte SUS (CONECT SUS, 2021). No mesmo período, também foi proposto o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com o objetivo de organizar e apresentar a estratégia de TIC e os resultados esperados durante o período de 2019 a 2021 do DATASUS do Ministério da Saúde. Esse plano enfatizou a importância da segurança e privacidade como princípios orientadores das atividades de governança digital, e expressamente recomendou a formulação de um marco legal de e-saúde no país.

Recentemente, no Brasil, foi publicada a Portaria GM/MS nº 3.632, com data de 21 de dezembro de 2020, que apresenta a versão mais atualizada da Estratégia de Saúde Digital para o Brasil 2020-2028 (BRASIL, 2020). Este documento, fundamentado nos avanços obtidos pelos projetos que compõem o Programa Conecte SUS, reitera a proposta original enquanto busca organizar e consolidar as ações realizadas ao longo da última década. Além disso, ele introduz uma visão futura na qual a Rede Nacional de Dados em Saúde (RNDS) será estabelecida e reconhecida como a principal plataforma digital para informações, inovação e serviços de saúde.

2 METODOLOGIA

Para responder ao objetivo proposto, foi realizada uma revisão sistemática da literatura, um método que objetiva identificar o maior número possível de estudos sobre um determinado fenômeno de forma organizada, resultando em uma análise reflexiva, crítica e compreensiva a respeito do material selecionado. O estudo foi realizado por meio de pesquisas *on-line* por meio de busca em artigos científicos, livros, reportagens e periódicos, entre os anos de 2010 e 2024. Literaturas publicadas antes de 2010 não foram consideradas neste estudo.

A busca bibliográfica foi realizada em cinco bases de dados nacionais e internacionais: Biblioteca Virtual em Saúde Brasil (BVS), Literatura Latino-Americana e do Caribe em Ciências da Saúde (LILACS), Portal de Periódicos Capes, Scientific Electronic Library Online (SCIELO) e U.S. National Library of Medicine (PUBMED). Nas bases nacionais foram utilizados os descritores: "sistema de informação em saúde", "cibersegurança" e "informatização do SUS" e adaptações. Nas bases internacionais os descritores utilizados foram: "health information system", "cybersecurity" and "SUS computerization". Foram selecionados artigos em português, inglês e espanhol.

Este estudo empregou uma abordagem rigorosa na seleção de artigos empíricos, focando

em quatro áreas específicas relacionadas à cibersegurança no contexto brasileiro. Os critérios de inclusão foram direcionados para garantir a relevância e a aplicabilidade dos resultados à realidade nacional, enquanto os critérios de exclusão foram meticulosamente aplicados para manter o foco nos desafios específicos enfrentados pelo Brasil no campo da cibersegurança na saúde.

Inicialmente, foram incluídos artigos que abordavam a legislação brasileira pertinente à cibersegurança, destacando as regulamentações específicas que impactam diretamente os sistemas de saúde do país. A análise dessas legislações é crucial para compreender o arcabouço legal que orienta a proteção de dados sensíveis e a prevenção de violações cibernéticas no setor da saúde.

Além disso, foram considerados estudos que exploravam as políticas públicas já implementadas no Brasil para mitigar os riscos cibernéticos, especialmente aquelas voltadas para fortalecer a segurança dos sistemas de saúde. A avaliação dessas políticas proporciona insights sobre as estratégias adotadas pelo governo brasileiro para enfrentar os desafios emergentes em cibersegurança.

Outro ponto de interesse foram os artigos que identificaram e discutiram os principais desafios enfrentados pelo Brasil em relação à cibersegurança na área da saúde. Esses estudos oferecem uma visão crítica das vulnerabilidades existentes, como a falta de infraestrutura adequada e a necessidade de capacitação contínua dos profissionais de saúde em questões de segurança digital.

Por fim, foram examinados artigos que investigaram cibercrimes específicos ocorridos no setor de saúde brasileiro. Essas análises são fundamentais para compreender os tipos de ataques cibernéticos mais comuns, os impactos desses incidentes na prestação de serviços de saúde e as medidas necessárias para prevenir futuras ocorrências.

Os critérios de exclusão foram aplicados rigorosamente para garantir a relevância e a coerência dos estudos incluídos. Foram excluídos estudos que se concentravam em políticas públicas de outros países, cibersegurança não relacionada aos sistemas de saúde, cibercrimes fora do contexto da saúde, trabalhos em idiomas que não fossem português, inglês ou espanhol, além de literatura publicada antes de 2010.

Ao seguir esses critérios, o estudo assegurou uma análise aprofundada e focada nos desafios específicos enfrentados pelo Brasil em sua jornada para fortalecer a cibersegurança no setor de saúde, contribuindo para o desenvolvimento de estratégias mais eficazes e adaptadas às necessidades locais.O levantamento bibliográfico foi realizado em março de 2024, e uma nova busca para atualização da revisão foi realizada entre abril e maio de 2024. No total, foram

encontradas 523 publicações, das quais 107 foram selecionadas. Os trabalhos encontrados foram selecionados a partir do exame dos títulos e palavras-chave e, posteriormente, da leitura dos resumos. Após a leitura completa dos artigos, considerando os critérios de inclusão e exclusão, 42 referências foram incluídas na revisão. Com os dados bibliográficos compilados, eles foram agrupados de acordo com sua relevância e discutidos à luz da literatura científica, visando atender aos objetivos propostos neste trabalho.

Adicionalmente, foram incluídos neste estudo dados sobre os óbitos ocorridos nos municípios de Anápolis e Goiânia entre os anos de 2020-2024, neste último especificamente até o dia 21/05/2024, data em que os dados foram levantados pelo primeiro autor deste artigo. Os dados foram retirados do banco de dados SCL (Sistema de Controle de Laudos da Polícia Tecnico-científica do estado de Goiás). Foram incluídas neste estudo informações estatísticas sobre a mortalidade ocorrida nos citados municípios e subdivididas nos seguintes parâmetros: morte acidental, homicídio, morte suspeita, morte natural, sem histórico informado e suicídio. Os dados obtidos não fazem distinção de sexo, idade, estado civíl, raça, profissão, ou outro parâmetro, sendo considerados apenas os números de óbitos ocorridos e sua causa generalista.

Estas informações foram comparadas aos dados de mortalidade do Serviço de Informação de Mortalidade (SIM), criado pelo Departamento de Informática do Sistema Único de Saúde (DATASUS), afim de comparação de dados. Essa base de dados anônimos é de acesso digital e público, disponível a partir do link < https://datasus.saude.gov.br/informacoes-de-saude-tabnet/>.

3 RESULTADOS E DISCUSSÃO

Nunca antes na história houve uma quantidade tão significativa de informações geradas e processadas digitalmente como nos dias atuais, resultado de uma rápida disseminação de dados (Guo, 2010). Com a popularização da internet, as pessoas passaram a acessar informações de forma instantânea, deixando um rastro digital de todas as atividades realizadas, tanto online quanto offline (Dias, 2021).

De acordo com Blanke (2016), o setor de saúde tornou-se um alvo para ciberataques devido ao seu tamanho econômico e às vulnerabilidades presentes nos sistemas das instituições de saúde, que muitas vezes negligenciam investimentos em cibersegurança. Não são apenas os computadores que estão vulneráveis a ataques cibernéticos, mas qualquer dispositivo que tenha acesso à internet, como dispositivos inteligentes e câmeras de segurança. As diversas inovações

que buscam conectar dispositivos médicos com a *internet*, os registros eletrônicos de pacientes e atendimentos pela internet abrem as portas para novos ataques (Dias et al., 2021). Por esse fato, dispositivos médicos conectados à internet ou a rede de um hospital também estão em risco de ataques.

Um exemplo disso foi o ataque conhecido como Mirai, um *malware* que se se destacou por explorar falhas de segurança em dispositivos, que em 2016 infectou vários dispositivos inteligentes, se espalhando como um *worm*[11] pela rede. Com vários dispositivos infectados, criou-se uma rede zumbi com 100 mil dispositivos, os quais foram utilizados para realização de ataques de negação de serviço distribuído (Cloudflare, 2024; Greene, 2016; Buxton, 2022). Em 2017, um ataque de *ransomware* conhecido como *Wanna Cry* comprometeu a rede de equipamentos radiológicos de diversos hospitais, provocando reagendamentos dos exames já marcados (News, 2022).

Kessler *et al*. (2019) demonstraram que nos Estados Unidos, entre 2009 e 2018, houve um aumento exponencial nas violações cibernéticas na área da saúde, expondo os dados de mais de 176 milhões de pacientes. Segundo o mesmo estudo, 70% dessas violações de dados são causadas diretamente ou indiretamente por descuido dos colaboradores das próprias instituições. A este respeito nota-se que, a negligência e o descuido de funcionários são características que não podem ser totalmente corrigidas por meio de tecnologia ou legislação, mas sim por meio de treinamentos e políticas internas das organizações (Brody; Chang; Schoenberg, 2018). Ainda sim, em estudos feitos nos Estados Unidos sobre a resiliência do setor de saúde contra cibercriminosos em 22 grandes cidades do país, observaram a ausência de um modelo padrão de segurança cibernética adequado para proteger as instituições (AL-Muhtadi *ET AL*., 2019). Portanto, as considerações críticas derivadas desses relatos de pesquisa apontam para a urgência de investimentos contínuos em educação e treinamento para os funcionários da saúde, bem como para o desenvolvimento de políticas internas robustas e a implementação de modelos de segurança cibernética mais eficazes. Somente através de uma abordagem integrada, que combine conscientização, políticas organizacionais claras e tecnologias adequadas, será possível mitigar os riscos crescentes associados às violações de dados na área da saúde.

Um exemplo recente e nacional ilustra essa vulnerabilidade: ocorrido em fevereiro de

[11] São um tipo de vírus autorreplicador que entra nas redes explorando vulnerabilidades, movendo-se rapidamente de um computador para o outro. Por isso, os *worms* podem se propagar e se espalhar rapidamente – não apenas localmente, mas com o potencial de afetar sistemas em diversos locais.

2020, em Foz do Iguaçu, Paraná, antes mesmo do registro oficial do primeiro caso de Covid-19 no Brasil. Um paciente que deu entrada em uma Unidade de Pronto Atendimento com suspeita de gripe teve sua suspeita de Covid-19 registrada no prontuário pelo médico responsável pelo atendimento. Logo em seguida, uma cópia do documento começou a circular na internet, gerando pânico na população (Clickfoz, 2021).

Embora haja diversos estudos sobre segurança cibernética no setor de saúde em diferentes países, incluindo América do Norte, Europa e Ásia, ainda existe uma lacuna na literatura científica em pesquisas nacionais sobre esse tema.

No Brasil, somente em 2022, foram registradas 103,16 bilhões de tentativas de ataques cibernéticos (Security report, 2023). Além disso, ocorreram diversos incidentes cibernéticos que afetaram a prestação de serviços públicos, como os ataques ao ConecteSUS[12] e ao FormSUS[13], impactando o controle vacinal e expondo dados pessoais sensíveis de pacientes. Autores como Abraham *et al*. (2019), Berger *et al*. (2019), Coronado *et al*. (2014) e Gordon *et al*. (2019) já apontavam em seus estudos que a cibersegurança no setor da saúde é negligenciada no Brasil, e que não há investimentos significativos para uma saúde digital efetiva.

Até a primeira metade de 2018, não havia legislação específica sobre a proteção de dados pessoais no Brasil. Nesse sentido, vários autores concordam que há uma falta de ações dos Estados na proteção de dados do setor de saúde, ou que as ações existentes ainda são ineficientes (Abraham *et al*., 2019; Handler *et al*., 2018; Kruse *et al*., 2017; Stern *et al*., 2019).

Diante destes fatos, é possível entender que a cibersegurança ainda precisa se adequar à realidade de cada país, não sendo diferente no Brasil. Ainda que muitos casos de cibercrimes sejam cometidos sobre o Sistema de Saúde do Brasil, as políticas públicas estão evoluindo para amenizarem tal realidade e controlar o ciberespaço com maior efetividade. Ainda há muito o que ser desenvolvido, mesmo que muito já tenha sido realizado em prol da segurança de dados da população brasileira. O desafio é para todos os usuários: pacientes, médicos, profissionais de diagnósticos, etc.

Além da segurança dos dados relacionado à privacidade, as informações produzidas por médicos legistas são fundamentais para a justiça criminal, uma vez que trazem informações sobre a causas e circunstâncias de mortes, lesões e outros tipos de violência e fornecendo

[12] Plataforma digital desenvolvida e utilizada no contexto do Sistema Único de Saúde (SUS) no Brasil. Essa plataforma foi criada para integrar e facilitar o acesso a informações e serviços relacionados à saúde pública.

[13] Sistema utilizado no Brasil no âmbito do Sistema Único de Saúde (SUS). Essa plataforma é utilizada para a coleta de informações e dados relacionados aos serviços de saúde prestados pelo SUS.

evidências valiosas para a tomada de decisões judiciais .

Com uma função essencial na Segurança Pública, os médicos legistas também atuam nas perícias em pessoas vivas, incluindo vítimas e suspeitos de crimes. Eles são responsáveis por realizar exames de lesão corporal, avaliações periciais em casos de acidentes de trânsito, perícias para constatação de Danos Pessoais Causados por Veículos Automotores de Via Terrestre(DPVat), exames cautelares em custodiados, bem como avaliações indiretas em prontuários e a avaliação pericial de embriaguez. Os médicos legistas também são fundamentais na investigação de crimes de violência contra mulheres, crianças e idosos, bem como em casos de crimes sexuais, produzindo laudos que podem comprovar a materialidade desses crimes.

3.1 Dados gerados a partir de Institutos Médicos Legais – IML

O DataSUS é alimentado por diferentes unidades notificadoras, sendo elas: estabelecimentos de saúde, institutos médico-legais, serviços de verificação de óbitos, cartório do registro civil e os próprios médicos, que seguem as determinações dos conselhos federal e regionais de medicina sobre o assunto.

Em relação a óbitos, por exemplo, nos Institutos Médicos Legais o médico responsável preenche uma Declaração de Óbito (DO) e posteriormente implementa os dados no banco de dados SCL (Sistema de Controle de Laudos da Polícia Tecnico-científica do estado de Goiás). O preenchimento deve abranger informações confiáveis, como tipo de óbito, sexo, idade, município de ocorrência e residência, etc. A partir de dados produzidos por médicos legistas do estado de Goiás, informações estatísticas sobre numero de mortes, causa de mortes e lesões corporais são produzidas. a partir de relatórios estatísticos do Instituto Médico Legal - IML. Após o registro das informações no IML, os dados são enviados à Secretaria de Saúde do Estado, a qual então envia as informações ao DataSUS.

Os municípios de Anápolis e Goiânia foram analisados em relação ao número de óbitos dos últimos cinco anos, afim de relacionar tais dados com a importancia e relevancia das informações geradas pelo IML a partir dos Dos produzidos pelos Médicos Legistas. Os dados podem ser analisados na Tabela 1 abaixo:

Tabela 1: Número de óbitos nos municípios de Anápolis e Goiânia entre os anos de 2020-2024, SLC-IML.

Município	**Causa do óbito**	**2020**	**2021**	**2022**	**2023**	**2024 (até 21/05)**
Goiânia	Morte acidental	1.014	1.164	1.149	1.146	391

	Suicídio	145	169	207	208	72
	Sem histórico informado	17	3	13	5	19
	Morte natural	229	268	323	280	114
	Morte suspeita	22	129	137	167	59
	Homicídio	715	491	414	418	152
	Mortes totais	**2.118**	**2.222**	**2.243**	**2.224**	**796**
Anápolis	Morte acidental	273	258		239	96
	Suicídio	41	60	60	53	18
	Sem histórico informado	14	19	16	20	35
	Morte natural	51	63	67	51	19
	Morte suspeita	33	35	36	32	11
	Homicídio	163	168	133	72	23
	Mortes totais	**575**	**603**	**566**	**477**	**202**

Fonte: O Autor (2024).

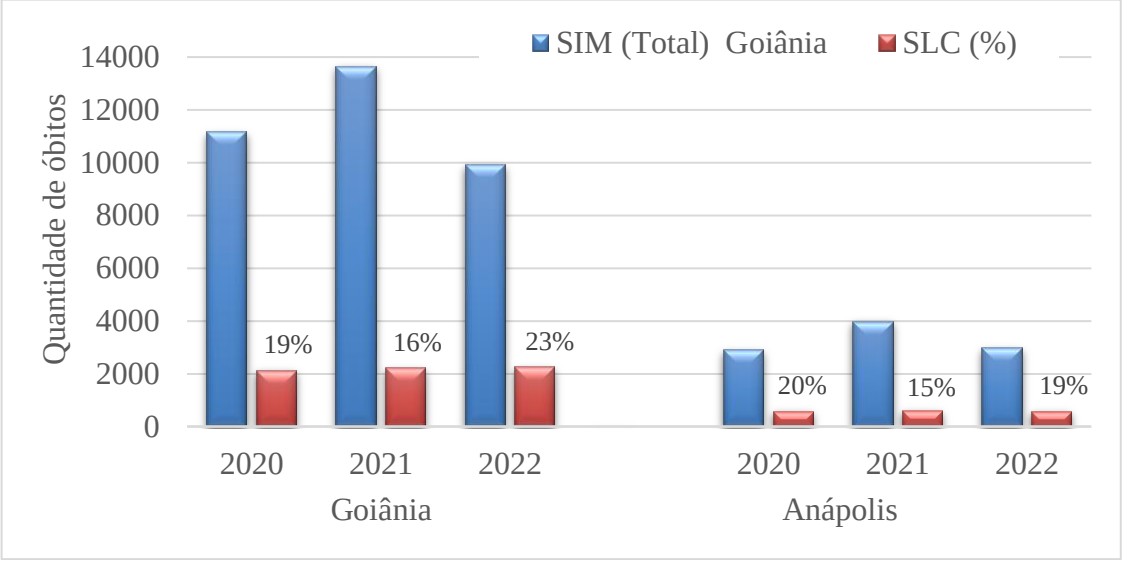
Já em relação aos dados encontrados no SIM (Sistema de Informação Sobre Mortalidade), apesar das informação sobre numero de óbitos estarem disponíveis apenas até o ano de 2022, observa-se maior número de ocorrencia de óbitos para os municípios de Anápolis e Goiânia em relação ao SLC, como demonstrado na Tabela 2, devido ser um sistema de informação nacional incorporado a partir de oitro outos sistemas e fontes de dados, e não apenas o SLC.

Tabela 2: Número de óbitos para Goiânia e Anápolis entre 2020-2022 de acordo com o SIM.

Município	**2020**	**2021**	**2022**
Goiânia	11.150	13.642	9.916
Anápolis	2.893	3.989	2.972

Fonte: Sistema de Informação Sobre Mortalidade – SIM.

Gráfico 1: Relação entre a quantidade de óbitos no SIM e SLC, para Anápolis e Goiânia, para os anos de 2020, 2021 e 2022.



Fonte: O autor (2024).

Em comparação aos dados disponíveis no SLC com os dados do SIM, para os anos de 2020, 2021 e 2022, é possível observar que os dados produzidos pelo Instituto Médico

Legal representam, em média, 20% do total de informações inseridas no SIM, o que pode ser observado no Gráfico 1, acima. Estes dados demostram o quão importante para o SIM são os dados produzidos pelo IML, uma vez que eles são a base para o desenvolvimento de políticas públicas voltadas à segurança pública, além de dados demográficos, análise da violência no país, feminicídio, estupros, entre outros.

4 CONSIDERAÇÕES FINAIS

O aumento das preocupações com a confidencialidade dos direitos à saúde e à privacidade tem despertado a atenção do Estado para a necessidade de garantir a proteção de dados. As novas práticas geram dados pessoais sensíveis que carecem de proteção específica devido às sérias consequências da divulgação indevida. A exposição não autorizada de dados de saúde pode resultar em prejuízos significativos, exigindo respostas do Poder Judiciário. Informações coletadas em ambientes de saúde pública, especialmente em procedimentos realizados por empresas privadas, necessitam de termos e condições claros para sua utilização, acesso, compartilhamento, armazenamento, descarte e possíveis responsabilizações.

Um treinamento mais eficiente das pessoas que acessam os sistemas de saúde é fundamental para mitigar os riscos de exposição indevida de dados sensíveis. A digitalização crescente na área da saúde aumenta a necessidade de capacitação contínua dos profissionais, especialmente aqueles que lidam diariamente com informações críticas. Treinamentos regulares e específicos sobre segurança cibernética e boas práticas no manuseio de sistemas como o SCL (Sistema de Controle de Laudos) são essenciais para reduzir vulnerabilidades e proteger a integridade dos dados.

A restrição do amplo acesso às funcionalidades que não deveriam ser acessadas por todos os usuários também se mostra crucial. Implementar políticas de acesso baseadas em funções e necessidades específicas pode limitar inadvertências e acessos não autorizados, mitigando os riscos de violações de privacidade e segurança. A definição clara de permissões de acesso, alinhada com as diretrizes de segurança da informação, é fundamental para garantir que apenas pessoal autorizado possa manipular informações sensíveis dentro dos sistemas de saúde, como o SCL, fortalecendo assim as defesas contra potenciais ataques cibernéticos.

As implicações e restrições do emprego de tecnologias na área da saúde ainda apresentam uma série de incertezas, tanto em relação aos potenciais benefícios e progressos projetados para o futuro quanto aos perigos decorrentes da exposição indevida de informações. É digno de nota nas disposições sobre a legislação e regulação da saúde digital

o reconhecimento explícito da necessidade de uma norma capaz de oferecer segurança jurídica a todos os envolvidos, protegendo direitos fundamentais como confidencialidade e privacidade de dados, corroborando as diretrizes do PDTIC de 2019 e a previsão de estabelecimento e adoção de normas e padrões para a representação, armazenamento, troca e utilização de dados de saúde, incluindo terminologias clínicas e aspectos legais relacionados ao uso da informação, como previsto na LGPD.

Neste contexto, a LGPD representa um avanço ao abordar procedimentos de organização, tratamento e sistemas de dados, embora não forneça regulamentação específica para a saúde. Apesar dos esforços, vazamentos de dados pessoais de saúde são frequentes, alimentando golpes e fraudes. A gestão de informações pessoais em saúde vai além de prontuários e exames, exigindo uma abordagem ampla. O alto custo regulatório para aplicar e fiscalizar os procedimentos de conformidade com a norma é um desafio para as organizações de saúde, que lidam com uma ampla gama de informações.

Portanto, é necessário uma revisão profunda tanto na documentação quanto nas práticas operacionais para cumprir as exigências da LGPD e implementar as atividades prioritárias da Estratégia de Saúde Digital para o Brasil. O desafio para o Estado é reconhecer os impactos das tecnologias na promoção do direito à saúde e suas ramificações, enquanto equilibra sigilo, dignidade e segurança com o progresso tecnológico e acesso à informação, reduzindo a vulnerabilidade do indivíduo ao fornecer dados pessoais com a expectativa de privacidade protegida, conforme preconizado pela legislação nacional e seu planejamento técnico.

As iniciativas de saúde digital devem ser guiadas pela Lei Geral de Proteção de Dados, e para alcançar essa conformidade, são propostas as seguintes atividades: identificação dos pontos críticos que necessitam de alinhamento com a LGPD para a expansão da Rede Nacional de Dados em Saúde (RNDS) e a identificação de modelos de compartilhamento seguro de dados de saúde em conformidade com a LGPD. Com isso, é garantido a segurança jurídica, assegurando a privacidade e confidencialidade dos dados, o que beneficia não apenas usuários, profissionais, gestores e organizações, mas também fortalece a credibilidade da Saúde Digital.

No caso do médico legista do IML e a partir das análises realizadas neste trabalho, conclui-se que, em um cenário de avanço acelerado da digitalização na área da saúde, a segurança cibernética emerge como uma prioridade incontestável, e o dominio de manuseio do sistema pelos profissinais que lidam diariamente com digitalização de dados é imprescindível. A interconexão de sistemas de saúde, como exemplo o DATASUS, resulta

no armazenamento massivo de dados médicos e a crescente adoção de tecnologias inovadoras elevaram os riscos de possíveis ataques. Apesar de haver possibilidade de ataques de *hackers* ao Sistema utilizado, o melhor programa a ser desenvolvido para melhoria da segurança do trabalho de digitalização de dados pelo Médico Legista seria de Treinamentos Funcionais para todos aqueles que tem acesso ao SCL, sendo estes treinamentos frequentes e rígidos, acompanhando as atualizações do sistema e objetivando o domínio de quem o manipula. A vulnerabilidade, muitas vezes, está relacionada com o baixo treinamento e pelo baixo domínio das ferramentas disponíveis pelo SLC, o que dá margem para equivocos que vunerabilizam a séria tarefa de digitalização dos dados fornecidos pelo IML.

REFERÊNCIAS

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

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

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.

ARAÚJO, G. Desafios e prioridades da cibersegurança no setor de saúde: protegendo vidas e Dados em um mundo digital. 18 de janeiro de 2024. Disponível em: < Desafios e prioridades da cibersegurança no setor de saúde: protegendo vidas e Dados em um mundo digital - Inforchannel>. Acesso em: 21 de março de 2024.

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.

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.

BRASIL. Conselho Nacional de Secretários de Saúde. SUS: avanços e desafios. Brasília: CONASS, 2006.

BRASIL. CONSELHO NACIONAL DE SECRETÁRIOS DE SAÚDE; Ciência e Tecnologia em Saúde. – Coleção Progestores – Para entender a gestão do SUS, 4; Brasília: CONASS, 2007. Disponível em: http://www.conass.org.br.

BRASIL. Decreto nº 6.703. **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

BRASIL. Estratégia de Saúde Digital para o Brasil 2020-2028 [recurso eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília : Ministério da Saúde, 2020.

BRASIL. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do Sistema Único de Saúde. DATASUS trajetória 1991-2002. Brasília: Ministério da Saúde; 2002.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. eMAG: modelo de acessibilidade em governo eletrônico. Brasília: Ministério do Planejamento; 2014.

BRASIL. Política Nacional de Informação e Informática em Saúde. Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília: Ministério da Saúde, 2016.

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

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

BUXTON, O. What Is the Mirai Botnet? 2022. Disponível em: https://www.avast. com/c-mirai.

CAETANO, J. V. F. **Ciberespaço, cibersegurança e os desafios da implantação da tecnologia 5g no Brasil.** (Monografia). Universidade Federal de Uberlândia, Minas gerais. 70p. 2023.

CLICKFOZ. Secretaria de Saúde desmente caso de Coronavírus em Foz do Iguaçu. **ClickFoz**. 2021.

CLOUDFLARE. O que é a botnet Mirai? 2024. Dispon´ıvel em: https://www.cloudflare. com/pt-br/learning/ddos/glossary/mirai-botnet/

CONECT SUS. **Plataforma de saúde para o cidadão, profissionais e gestores de saúde do Sistema Único de Saúde Brasileiro**, 2021.

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.

DIAS, F. M. et al. Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saude. Universidade Nove de Julho, 2021.

DIAS, F., M. **Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saúde**. Dissertação (Mestrado) – Universidade Nove de Julho - UNINOVE, São Paulo, 132p., 2021.

FIGUEIREDO, V. B. N.; VARELLA M. D. Dimensões da privacidade das informações em saúde no Brasil**. Direitos Fundamentais & Justiça**, ano 16, n. 47, p. 319-343, jul./dez. 2022.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf.

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

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.

GREENE, T. DDoS attack takes down Krebs site. 2016. Disponível em: https://www.csoonline.com/article/3123785/ largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html.

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

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

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

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 CatholicUniversity**, v. 19, p. 466-492, 2017.

MAIMÓ, *et al*. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. **Sensors (Switzerland)**, vol.19, n.5, p.1114, 2019.

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

MARTINS CC, WACLAWOVSKY AJ. Problemas e desafios enfrentados pelos gestores públicos no processo de gestão em saúde. **Rev Gestão Sist Saúde**. 4(1):100-109. 2015.

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.

NEWS, T. H. Are Medical Devices at Risk of Ransomware Attacks? 2022. Disponível em: https://thehackernews.com/2022/01/are-medical-devices-at-risk-of.html.

NHS. Sharing your health records. About the NHS, 2018.

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

PARLAMENTO EUROPEU – CONSELHO EUROPEU. **Directiva 2002/58/CE, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas** (Directiva sobre la privacidad y las comunicaciones electrónicas). Diario Oficial de las Comunidades Europeas. 2002. Disponível em: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF.

SECURITY REPORT. Brasil sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado. **Security Report**, 1 mar. 2023. Disponível em: <https://www.securityreport.com.br/overview/brasil-sofreu-10316-bilhoesde-tentativas-de-ataques-ciberneticos-em-2022/>. Acesso em: 20 mar. 2024.

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

UNITED NATIONS. Special Rapporteur on the Right to Privacy. Draft Recommendation on the protection and use of health-related data. p. 06, 2019.

VARGAS, M.; RODRIGUES, E. Ministério da Saúde sofre nova invasão de ‘hacker sincero’: ‘Arrumem esse site porco’. Disponível em: <https://www.estadao.com.br/saude/ministerio- da-saude-sofre-nova-invasao-de-hackersincero-arrumem-esse-site-porco/>. Acesso em: 21 março 2024.

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.