UNIVERSIDADE FEDERAL DE PERNAMBUCO
CAMPUS AGRESTE
NÚCLEO DE TECNOLOGIA
CURSO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

MANOEL SEBASTIÃO DE MOURA NETO

PANORAMA BIBLIOMÉTRICO SOBRE AS PRINCIPAIS POLÍTICAS E PRÁTICAS DE SEGURANÇA CIBERNÉTICA EM PLATAFORMAS DE TELEMEDICINA

Caruaru
2025

MANOEL SEBASTIÃO DE MOURA NETO

PANORAMA BIBLIOMÉTRICO SOBRE AS PRINCIPAIS POLÍTICAS E PRÁTICAS DE SEGURANÇA CIBERNÉTICA EM PLATAFORMAS DE TELEMEDICINA

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Engenharia de Produção do Campus Agreste da Universidade Federal de Pernambuco – UFPE, na modalidade de monografia, como requisito parcial para a obtenção do grau de bacharel em Engenharia de Produção.

Área de concentração: Gestão da Informação

Orientadora: Thárcylla Rebecca Negreiros Clemente, DSc.

Caruaru

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Moura Neto, Manoel Sebastião de .
Panorama bibliométrico sobre as principais políticas e práticas de segurança cibernética em plataformas de telemedicina / Manoel Sebastião de Moura Neto. - Caruaru, 2025.
43 : il., tab.

Orientador(a): Thárcylla Negreiros Clemente
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro Acadêmico do Agreste, Engenharia de Produção, 2025.
Inclui referências.

1. Sistema de Telemedicina. 2. Cibersegurança. 3. Políticas de Segurança. 4. Segurança da Informação. I. Negreiros Clemente , Thárcylla . (Orientação). II. Título.

000 CDD (22.ed.)

MANOEL SEBASTIÃO DE MOURA NETO

PANORAMA BIBLIOMÉTRICO SOBRE AS PRINCIPAIS POLÍTICAS E PRÁTICAS DE SEGURANÇA CIBERNÉTICA EM PLATAFORMAS DE TELEMEDICINA

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Engenharia de Produção do Centro Acadêmico do Agreste do Campus Agreste da Universidade Federal de Pernambuco – UFPE, na modalidade de monografia, como requisito parcial para a obtenção do grau de bacharel**/**licenciado em bacharel em Engenharia de Produção.

Área de concentração: Gestão da Informação

Aprovada em: 21/055/2025

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
THARCYLLA REBECCA NEGREIROS CLEMENTE
Data: 23/05/2025 13:55:05-0300
Verifique em https://validar.iti.gov.br

_____ _____

Profª. Drª. Thárcylla Rebecca Negreiros Clemente (Orientadora)
Universidade Federal de Pernambuco

Documento assinado digitalmente
gov.br
AMANDA CARVALHO MIRANDA
Data: 23/05/2025 14:07:26-0300
Verifique em https://validar.iti.gov.br

_____ _____

Profa. Dra. Amanda Carvalho Miranda (Examinadora Interna)
Universidade Federal de Pernambuco

Documento assinado digitalmente
gov.br
MARINA DANTAS DE OLIVEIRA DUARTE
Data: 26/05/2025 10:32:45-0300
Verifique em https://validar.iti.gov.br

_____

Profa. Dra. Marina Dantas de Oliveira Duarte. (Examinadora Interna)
Universidade Federal de Pernambuco

Dedico esse trabalho aos meus pais, em especial minha mãe, que nunca desistiu de mim, independente das dificuldades, sempre me guiando e lembrando que o estudo liberta. Agradeço também aos irmãos que a vida me deu, Lucas Daniel Gomes Ribeiro, André Victor, Felipe Saballos e Anthony, por fazerem meus dias fora da faculdade mais leves. Agradeço também aos eternos companheiros que a Faculdade me deu, Dayvisson David, João Keven, Vivián Andrade e Jussara Souza, os quais foram responsáveis por aconselhar, acalentar e me ajudar imensamente durante minha passagem acadêmica. Também agradeço grandemente a minha fiel companheira, Ana Luísa Rocha, a qual me dá forças, me acolhe, me incentiva e me faz sentir como o homem mais feliz desse mundo. Por último, quero agradecer a Deus por me dar forças, me manter de pé e nunca me permitir desistir daquilo que amo e acredito, por mais difícil que seja.

AGRADECIMENTOS

Meus sinceros agradecimentos ao corpo docente da Universidade Federal de Pernambuco – Campus do Agreste. Agradeço desde o pessoal dos serviços gerais, que sempre mantiveram o local limpo e organizado para o conforto desenvolvimento intelectual dos alunos. Agradeço ao Sistema Público educacional, por me proporcionar uma formação de extrema qualidade, possibilitando me tornar o profissional e pessoa que sou hoje. E em especial gostaria de agradecer às professoras Dra. Thárcylla Negreiros Clemente, Dra. Cristina Medeiros e Dra. Marina Dantas. Essas que foram pessoas ímpares, extremamente humanas. Elas que me guiaram, mentoraram, aconselharam e transmitiram as coisas mais importantes que um aluno precisa e merece, conhecimento e empatia.

"Tudo o que é feito por amor está sempre além do bem e do mal." (NIETZSCHE, F. Além do Bem e do Mal, 1886, §153.)

RESUMO

Nos últimos anos, os ambientes organizacionais passaram a adotar, de forma crescente, as Tecnologias da Informação e Comunicação (TIC) como ferramentas de suporte aos processos operacionais, gerenciais e estratégicos. No setor de serviços, destaca-se a ampliação do uso da plataforma web como meio para comunicação, divulgação e armazenamento de informações, especialmente na área da saúde. Nesse contexto, a telemedicina surge como alternativa eficiente para o atendimento remoto de pacientes por meio de dispositivos computacionais e sistemas digitais. Essa modalidade permite que unidades e centros médicos realizem diagnósticos e acompanhamentos a distância, promovendo maior acesso à assistência médica, inclusive em regiões remotas. Um dos principais benefícios desse modelo é o compartilhamento de dados clínicos entre diferentes profissionais, possibilitado por sistemas informatizados com acesso em rede. No entanto, o uso intensivo dessas tecnologias levanta preocupações quanto à privacidade, confidencialidade e segurança das informações sensíveis dos pacientes. Assim, torna-se necessário implementar políticas específicas de segurança da informação para garantir a integridade e a proteção dos dados envolvidos. O presente trabalho tem como objetivo realizar um levantamento bibliográfico sobre as principais políticas de segurança da informação adotadas em sistemas de telemedicina, analisando criticamente sua adequação ao contexto dos centros médicos brasileiros. O trabalho foi realizado a partir de uma análise bibliométrica na base de dados Scopus Elsevier, no recorte temporal de 1994 até 2022, a partir das análises, observou-se que de 2013 a 2016, os resultados indicam que as medidas de segurança eram mais básicas, demonstrando que era mais simples acessar seus arquivos em uma curva elíptica significava, já que toda a sua rede poderia ser considerada uma chave pública. Já no intervalo de 2017 a 2019, outras tecnologias foram desenvolvidas, como blockchain e criptografia homomórfica. Isso levou a uma integridade e privacidade maior dos dados. Nos últimos anos (2020-2022), a inteligência artificial combinada com o pensamento de zero trust (confiança zero) permitiu a avaliação de riscos em tempo real e uma melhor proteção das informações. Tal evolução vem de um esforço contínuo para equilibrar os sistemas de telemedicina, de modo a garantir que os dados estejam seguros enquanto o desempenho operacional permanece alto. Desse modo, essa pesquisa busca contribuir para o debate sobre a segurança

digital na saúde, destacando a importância de práticas normativas, técnicas e éticas que assegurem a confiança, segurança na coleta, transmissão e a eficácia dos atendimentos mediados por tecnologia.

Palavras-chave: Sistema de Telemedicina; Cibersegurança; Políticas de Segurança; Telemedicina; Segurança da Informação

ABSTRACT

In recent years, organizational environments have increasingly adopted Information and Communication Technologies (ICT) as tools to support operational, managerial, and strategic processes. In the service sector, the expanded use of web platforms stands out as a means for communication, dissemination, and storage of information, especially in healthcare. In this context, telemedicine emerges as an efficient alternative for remote patient care through computational devices and digital systems. This modality allows medical units and centers to conduct diagnoses and follow-ups remotely, promoting greater access to medical assistance, including in remote regions. One of the main benefits of this model is the sharing of clinical data among different professionals, enabled by networked computer systems. However, the intensive use of these technologies raises concerns about the privacy, confidentiality, and security of patients' sensitive information. Thus, it becomes necessary to implement specific information security policies to ensure the integrity and protection of the data involved. This study aims to conduct a bibliographic survey on the main information security policies adopted in telemedicine systems, critically analyzing their suitability for the context of Brazilian medical centers. The research was based on a bibliometric analysis of the Scopus Elsevier database, covering the period from 1994 to 2022. The analyses revealed that from 2013 to 2016, security measures were more basic, indicating that accessing files on an elliptic curve was simpler, as the entire network could be considered a public key. Between 2017 and 2019, other technologies were developed, such as blockchain and homomorphic encryption, leading to greater data integrity and privacy. In recent years (2020–2022), artificial intelligence combined with a zero-trust approach enabled real-time risk assessment and better information protection. This evolution stems from a continuous effort to balance telemedicine systems, ensuring data security while maintaining high operational performance. Thus, this research seeks to contribute to the debate on digital security in healthcare, emphasizing the importance of normative, technical, and ethical practices that ensure trust, security in data collection and transmission, and the efficacy of technology-mediated care.

Keywords: Telemedicine System; Cybersecurity; Security Policies; Telemedicine; Information Security

LISTA DE ILUSTRAÇÕES

Figura 1 –	Etapas da metodologia adotada por esta pesquisa	23
Gráfico 1 –	Representação gráfica da quantidade de documentos científicos publicados por ano entre 1994 e 2022	26
Gráfico 2 –	Representação gráfica da quantidade de periódicos por fonte do período temporal de 1996 a 2022	27
Figura 2 –	Representação gráfica da rede bibliométrica de conexões por autores	29
Figura 3 –	Representação gráfica reduzida da rede bibliométrica de conexões por autores	30
Figura 4 –	Representação gráfica da rede bibliométrica por critério de relevância de palavras-chaves	31
Figura 5 –	Representação gráfica de variação de densidade da rede bibliométrica	32

LISTA DE TABELAS

Tabela 1 – Listagem decrescente de autorias bibliométricas 28

LISTA DE ABREVIATURAS E SIGLAS

ECC	Criptografia de Curva Elíptica
GDPR	Regulamento Geral de Proteção de Dados
HIPAA	Lei de Portabilidade e Responsabilidade de Seguros de Saúde
LGPD	Lei Geral de Proteção de Dados
Ti	Tecnologia da Informação
TIC	Tecnologias da Informação e Comunicação
ANPD	Autoridade Nacional de Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO..... 14
1.1 JUSTIFICATIVA..... **15**
1.2 OBJETIVOS..... **17**
1.3 ESTRUTURA DO TRABALHO..... **17**
2 FUNDAMENTAÇÃO TEÓRICA..... 18
2.1 SISTEMAS DE TELEMEDICINA..... **18**
2.2 SEGURANÇA DA INFORMAÇÃO..... **19**
2.3 SEGURANÇA EM AMBIENTES DE TELEMEDICINA..... **20**
2.4 PERSPECTIVAS E TENDÊNCIAS EM CIBERSEGURANÇA NA SAÚDE DIGITAL..... **21**
3 METODOLOGIA..... 24
3.1 CLASSIFICAÇÃO DA PESQUISA..... **24**
3.2 PROCEDIMENTOS METODOLÓGICOS..... **24**
4 ANÁLISE BIBLIOMÉTRICA..... 26
4.1 ANÁLISE TEMPORAL DOS TRABALHOS SELECIONADOS..... **27**
4.2 ANÁLISE SOBRE OS PRINCIPAIS PERIÓDICOS DE PUBLICAÇÃO..... **28**
4.3 ANÁLISE SOBRE OS PRINCIPAIS AUTORES..... **29**
4.4 ANÁLISE SOBRE AS PALAVRAS-CHAVES UTILIZADAS..... **32**
4.5 RESULTADOS SOBRE AS PRINCIPAIS POLÍTICAS E PRÁTICAS DE SEGURANÇA EMPREGADA NOS SISTEMAS DE TELEMEDICINA..... **34**
5 CONSIDERAÇÕES FINAIS..... 36
5.1 CONCLUSÕES..... **36**
5.2 DISCUSSÕES E ANÁLISES..... **36**
5.3 RECOMENDAÇÃO PARA TRABALHOS FUTUROS..... **37**
REFERÊNCIAS..... 39

1 INTRODUÇÃO

O avanço das Tecnologias de Informação e Comunicação (TIC) aplicadas aos contextos organizacionais vem apresentando implicações práticas que estimulam mudanças nos modelos de gestão e de negócios das organizações para atender necessidades e adaptações da sociedade por produtos diferenciados. Essas mudanças têm reflexo na abordagem de negócios conduzidos e gerenciados em ambientes virtuais, que tem sido vista como uma estratégia para assegurar maior dinamicidade no relacionamento entre os agentes da cadeia de suprimentos, com alta velocidade de disseminação de informações e mínimas barreiras de comunicação na era digital (SILVA; Oliveira, 2023, p. 47). O desempenho dos modelos de negócios virtuais, muitas vezes, ganha significativo apoio de tecnologias como a Internet que possibilita a comunicação interativa e a transmissão de dados, informações, documentos e arquivos multimídia entre diferentes fornecedores, clientes e consumidores ao redor do mundo.

Para diferentes organizações, atuar em ambientes virtuais oferece vantagens competitivas significativas, dentre elas a expansão do mercado e visibilidade em âmbitos globais, expansão da disponibilidade de recursos para a produção, maior dinamismo do estoque, maior velocidade na entrega de informações, menor custo nas operações, maior interação com os fornecedores, clientes e consumidores, a produção de grandes volumes de dados, velocidade na troca de informações, análises de dados e informações, criação de novos negócios digitais, conectividade entre diversos dispositivos e constantes interações com soluções voltadas para a Internet (CASTELLS, 2019).

Para empresas de prestação de serviços, além dessas vantagens, foi possível selaborar estratégias que auxiliem o ganho de índices de produtividade para que possam competir nos nichos de mercado específicos, explorando diferentes plataformas de comunicação, tais como sites, redes sociais, blogs, aplicativos e sistemas de informação integrados; e, fornecendo subsídios para uma gestão com redução de custos, maior disponibilidade dos produtos e maior eficiência no processamento das transações.

No entanto, algumas limitações são importantes de serem consideradas, em especial às relacionadas à segurança da informação. Nos últimos anos, as organizações têm voltado atenções ao aumento dos riscos que a falta de segurança

da informação causa na evolução e sobrevivência dos negócios, em especial devido à grande oferta de dispositivos tecnológicos e o crescente acesso e disseminação de dados e informações (STALLINGS; BROWN, 2018). A falta de segurança da informação evidencia muitos prejuízos para os diferentes agentes da cadeia de suprimentos de um negócio, em especial quando impacta negativamente a confiança dos clientes e fornecedores, a eficiência dos serviços, a disponibilidade das operações, a credibilidade do negócio e a imagem da empresa.

Neste sentido, há um incentivo para que as organizações adotem estratégias para evitar ocorrência de falhas de segurança causadas por hackers, spams, softwares maliciosos e outros tipos de ataques cibernéticos. Essas estratégias envolvem, muitas vezes, a proteção dos índices de desempenho e a manutenção da eficiência operacional do negócio, assegurando a integridade, disponibilidade e confidencialidade dos dados e informações (CABAJ *et al*., 2018).

Em particular, nos sistemas de telemedicina, as questões que envolvem segurança cibernética são ainda mais evidentes, pois a ineficiência das operações de segurança pode causar prejuízos sociais e morais, além dos prejuízos organizacionais. No entanto, ainda há uma lacuna na literatura sobre questões gerenciais relacionadas à segurança cibernética para unidades de saúde que operam em ambientes virtuais, especialmente para organizações atuantes em países emergentes, como o Brasil. Por essa perspectiva, foi oportuno o estudo sobre políticas e práticas de segurança cibernética para sistemas de telemedicina. A proposta do presente trabalho concentra-se na apresentação de estudos que apresentam modelos de gestão sobre potenciais políticas e práticas de segurança cibernética para sistemas de telemedicina. Para isso, uma análise bibliométrica da literatura será elaborada.

1.1 JUSTIFICATIVA

O avanço das TIC tem influenciado muitas organizações a adotarem recursos de prestação de serviços virtuais, dentre elas foi possível citar os serviços médicos que agregam TIC para oferecer atendimentos teleguiados de assistência médica aos pacientes com variadas patologias. No âmbito da telemedicina, as vantagens da utilização das TIC são indicadas pela ampliação do escopo de consulta de dados e

informações compartilhadas por diferentes especialistas ao redor do mundo (WHO, 2020).

Essa facilidade permite que pesquisas e diagnósticos médicos sejam elaborados com a composição de habilidades que agreguem valor a partir do compartilhamento e análises de registros históricos de saúde dos pacientes, imagens, laudos e diagnósticos de diferentes patologias, em uma infraestrutura de armazenamento de dados distribuída. Essa facilidade foi especialmente vantajosa para situações em que as patologias são desconhecidas em um determinado território e requerem o compartilhamento de experiências, ou quando os pacientes e os profissionais de saúde não conseguem ou não podem estar fisicamente no mesmo local.

Apesar das vantagens da atuação em ambientes virtuais, algumas possíveis limitações exigem atenções dos gestores, tais como a necessidade de infraestrutura de rede, servidores e largura de banda suficientes para todos os agentes da cadeia de suprimentos, gestão integrada entre todos os sistemas de informação e operação, resposta sobre aspectos de regulamentação governamental sobre a troca de dados e itens em ambientes virtuais, quantidade de fornecedores, vendedores e compradores no nicho de mercado pretendido, e questões relacionadas à segurança, ou proteção, dos dados e informações (LAUDON; LAUDON, 2021).

Dentre as limitações, as questões relacionadas à segurança das informações foi uma das mais relevantes para o desempenho organizacional. A preocupação sobre a forma como as informações são protegidas deve fazer parte do planejamento estratégico de um negócio em ambiente virtual, pois a falta ou ineficiência da segurança dos dados e informações pode interferir em aspectos como a continuidade, os riscos, o retorno sobre o investimento e as oportunidades do negócio nesse ambiente (ISO/IEC 27001, 2022). A Internet, como o principal recurso utilizado pelas empresas virtuais, apresenta variados desafios para as organizações como as ameaças à integridade, disponibilidade e confiabilidade dos dados e informações, provocadas por ataques cibernéticos promovidos por hackers, spams, softwares maliciosos e corporações criminosas presentes na rede mundial de computadores. Essas ameaças são ainda mais graves para o setor da telemedicina que, em geral, lidam com dados e informações privados e pessoais dos fornecedores, clientes e consumidores, e podem apresentar recursos limitados para adquirir e implementar mecanismos de segurança cibernética (SCHNEIER, 2018).

Pela influência do tema, foi oportuno o desenvolvimento de uma pesquisa que permita o amplo conhecimento sobre políticas e práticas de segurança da informação adotadas em sistemas de telemedicina.

1.2 OBJETIVOS

O presente trabalho tem como objetivo geral: elaborar uma analise bibliométrica da literatura sobre os principais estudos científicos relacionados à segurança da informação para sistemas de telemedicina. Inicialmente, para o alcance do objetivo geral são listados os seguintes objetivos específicos:

- Selecionar artigos científicos que abordem a segurança da informação na telemedicina;
- Identificar os principais autores da área de estudo;
- Realizar uma análise sobre os principais conceitos abordados pelos estudos dos sistemas de telemedicina;
- Propor uma discussão sobre as ações para o processo de prevenção e detecção de falhas nos sistemas de telemedicina.

1.3 ESTRUTURA DO TRABALHO

O presente trabalho foi formado por cinco capítulos, sendo distribuídos como: No primeiro capítulo foi apresentada a Introdução, com uma discussão inicial sobre a proposta do trabalho, bem como a justificativa e os objetivos para sua elaboração. No segundo capítulo, são apresentados os principais conceitos teóricos e as principais referências bibliográficas utilizadas para a contextualização do trabalho. Em seguida, foi apresentada a metodologia utilizada para a elaboração do trabalho. No Capítulo 4, são apresentados os resultados e discussões. No Capítulo 5, são descritas as considerações finais.

Por fim, são listadas as referências utilizadas ao longo do trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

O aprofundamento conceitual foi fundamental para compreender os elementos que sustentam a problemática em estudo. Neste capítulo, são apresentados os fundamentos teóricos que envolvem a telemedicina e a segurança da informação, com ênfase na aplicação desses conceitos em ambientes digitais de atendimento em saúde. Essa análise foi essencial para a identificação dos desafios enfrentados pela gestão da informação em sistemas tecnológicos voltados à assistência médica remota.

2.1 SISTEMAS DE TELEMEDICINA

A transformação digital tem impactado profundamente o setor da saúde, especialmente no que se refere à ampliação do acesso e à descentralização dos serviços médicos. Nesse cenário, a telemedicina surge como uma alternativa estratégica que permite a oferta de atendimentos clínicos à distância, por meio do uso intensivo de Tecnologias da Informação e Comunicação (TIC).

De acordo com Ristevski e Chen (2018), os sistemas de telemedicina operam com base em infraestruturas tecnológicas capazes de processar, armazenar e transmitir informações clínicas, como imagens, laudos e registros eletrônicos, entre diferentes localidades. Essa estrutura permite que diagnósticos e condutas médicas sejam realizados remotamente, promovendo maior agilidade e alcance dos serviços de saúde. A funcionalidade desses sistemas depende de plataformas integradas, que garantam a troca segura e eficiente de dados entre profissionais, instituições e pacientes.

No entanto, conforme observado por Cabaj *et al*. (2018), o uso crescente de soluções digitais nesse setor implica em riscos significativos relacionados à segurança da informação. A interconexão entre sistemas distintos, muitas vezes pertencentes a diferentes entes da cadeia de saúde, exige o desenvolvimento de mecanismos que assegurem a confidencialidade, a integridade e a disponibilidade dos dados clínicos. Dessa forma, a confiabilidade das operações depende, também, da robustez dos sistemas de proteção empregados.

2.2 SEGURANÇA DA INFORMAÇÃO

O conceito de segurança da informação abrange o conjunto de práticas, normas e tecnologias voltadas à proteção dos dados contra acessos não autorizados, alterações indevidas e perdas acidentais. Segundo a norma brasileira NBR ISO/IEC 27002 (2013), os princípios fundamentais que norteiam essa segurança são a confidencialidade, a integridade e a disponibilidade das informações.

Em ambientes digitais de saúde, como os sistemas de telemedicina, esses princípios assumem importância central, considerando-se a natureza sensível dos dados tratados. Watzlaf *et al*. (2017) destacam que a exposição ou vazamento de informações médicas pode comprometer não apenas a reputação institucional, mas também acarretar prejuízos éticos, sociais e legais. A proteção de dados de pacientes deve, portanto, ser encarada como elemento estratégico de gestão e não apenas como uma exigência técnica.

Além dos riscos inerentes à manipulação digital de dados, os sistemas de saúde estão sujeitos a diversas formas de ataques cibernéticos, incluindo invasões, interceptações de comunicações e ações de ransomware. Os ataques de ransomware utilizam malware para impedir que as vítimas acessem ou criptografem seus dados ou, pior ainda, para distribuir o caos operacional. E os criminosos que os realizam exigem pagamentos para restaurar o acesso aos arquivos. Isso apresenta grandes riscos para a segurança e privacidade dos sistemas de saúde.

No campo da telemedicina, em particular, há ansiedade em relação a volumes de material sensível – como registros de pacientes e dados pessoais – escondidos em muitos megabytes.

Além disso, analisando sob a perspectiva da privacidade, constatamos que empresas de tecnologia utilizam esses dados. Algumas dessas empresas coletam, armazenam e empregam diversas formas de informação médica e pessoal para fins como algoritmos de inteligência artificial, marketing direcionado ou análise comportamental. Esta prática levanta questões éticas e legais.

Se esses dados forem mal geridos, os pacientes podem sofrer vazamentos ou danos. Eles também prejudicam o direito dos pacientes à privacidade, bem como a confiança na sociedade.

Portanto, é crucial que as plataformas de telemedicina sejam dotadas de recursos robustos de proteção de dados e de arranjos que não permitam que terceiros se apropriem indevidamente ou vazem qualquer informação relacionada aos pacientes.

Para minimizar tais riscos, autores como Kritzinger e Von Solms (2010) e Ben-Asher e Gonzalez (2015) enfatizam a necessidade de políticas organizacionais claras, treinamentos regulares para os colaboradores e o desenvolvimento de uma cultura voltada à segurança digital. Boyson (2014) complementa essa visão ao afirmar que a segurança da informação deve ser incorporada às decisões estratégicas das instituições, integrando-se aos objetivos organizacionais de continuidade e inovação.

2.3 SEGURANÇA EM AMBIENTES DE TELEMEDICINA

Em um ambiente regulatório como a Lei Geral de Proteção de Dados (LGPD), a complexidade dos sistemas de telemedicina adiciona desafios à proteção de dados clínicos. Ou seja, há incontáveis pontos de troca estabelecidos entre diferentes atores e o fluxo de informações é contínuo entre eles – hospitais, médicos, pacientes e prestadores de serviços médicos. Esses sistemas poderiam facilmente se tornar centros de violações de privacidade ou de ciberataques. Dey *et al*. (2017) identificam que, ao longo da última década, diversas abordagens foram desenvolvidas com o intuito de proteger essas estruturas, como o uso de criptografia, protocolos seguros e autenticação robusta.

Apesar da variedade de métodos existentes, alguns autores alertam para as limitações dessas técnicas. Nyeem et al. (2013), por exemplo, ressaltam que certos mecanismos oferecem apenas proteção parcial ou podem ser facilmente comprometidos em caso de gestão ineficiente das chaves de segurança. Nesse contexto, Thanki, Borra e Mandal (2018) propuseram o uso de técnicas de ocultação de dados (esteganografia) como alternativa para garantir tanto a segurança quanto a integridade das informações médicas compartilhadas entre sistemas.

Contudo, observa-se uma lacuna significativa na literatura no que diz respeito à formulação de políticas específicas voltadas à cibersegurança em serviços de telemedicina. Mahmood *et al*. (2013) defendem que a ausência de diretrizes

estratégicas claras compromete a capacidade de resposta das instituições diante de incidentes, além de dificultar a construção de ambientes mais resilientes.

Isso nos leva aos desafios brasileiros de garantir a integridade e confiabilidade dos dados, a principal legislação que regula a proteção de dados pessoais é a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD estabelece diretrizes para coleta, armazenamento, tratamento e compartilhamento de dados pessoais, garantindo os direitos dos titulares e impondo obrigações às organizações que lidam com essas informações.

Na questão da saúde, a LGPD faz uma distinção importante, pois por tratar de dados sensíveis há exigência de uma proteção adicional. Ela regula, por exemplo, o tratamento de dados médicos, genéticos e de saúde, reforçando a necessidade de consentimento explícito e de medidas de segurança robustas. Além disso, a legislação prevê que os profissionais e instituições de saúde devem implementar políticas de privacidade compatíveis com suas atividades específicas, assegurando confidencialidade, integridade e disponibilidades dessas informações.

Em termos de avanços regulamentários, o país já passou por discussões e implementações significativas, como a regulamentação de direitos dos titulares, classificação de dados sensíveis, obrigações de relato de incidentes de segurança, além do fortalecimento de aspectos relacionados à transferência de dados para o exterior. Recentemente, a Autoridade Nacional de Proteção de Dados (ANPD) tem emitido orientações e normas complementares para detalhar esses pontos, promovendo maior entendimento e fiscalização do cumprimento da LGPD

2.4 PERSPECTIVAS E TENDÊNCIAS EM CIBERSEGURANÇA NA SAÚDE DIGITAL

A digitalização da saúde, impulsionada pela adoção de tecnologias emergentes como inteligência artificial, computação em nuvem e blockchain, tem ampliado os horizontes da assistência médica, ao mesmo tempo em que introduz novos riscos à segurança da informação. Segundo Sharma e Bashir (2021), a própria inteligência artificial pode ser utilizada por agentes mal-intencionados para

gerar ataques sofisticados e personalizados, ampliando os desafios enfrentados pelas equipes de segurança.

Além disso, dispositivos móveis e vestíveis *(wearables)*, cada vez mais utilizados no monitoramento contínuo da saúde, apresentam vulnerabilidades relacionadas à coleta e transmissão de dados em tempo real. Como ressaltado por Mosenia e Jha (2017), esses dispositivos, muitas vezes com recursos limitados de proteção, requerem soluções específicas que garantam a segurança de ponta a ponta na cadeia de informações.

Diante dos desafios impostos pelo uso crescente dessas tecnologias aplicadas a serviços de saúde, torna-se fundamental desenvolver e implementar estratégias de cibersegurança robustas. Essa necessidade reforça a importância de estabelecer políticas específicas que garantam a proteção eficaz dos dados sensíveis, promovendo a confiança nos sistemas digitais de saúde e assegurando a continuidade e a eficiência dos atendimentos médicos, mesmo diante de ameaças cada vez mais sofisticadas.

Ao mesmo tempo, as medidas de segurança para sistemas de telemedicina passaram por mudanças significativas na última década. Isso se deve tanto à crescente complexidade das modalidades de ataque quanto ao desenvolvimento mais rápido da tecnologia de proteção. Os principais tipos, divididos por períodos, mostram uma tendência de melhoria de tecnologia e conceito.

No período de 2013-2016, temos os Mecanismos de Autenticação Simples, Criptografia de Baixo Nível, onde, primeiro, uma série de medidas de proteção relativamente simples foram implementadas. Tradicionalmente, o sistema justificadamente exigia login e senha como elementos-chave privados para garantir que usuários autorizados pudessem acessá-lo. Mas estas medidas, embora necessárias, apresentavam algumas das fraquezas inerentes à tecnologia base. Como um ataque anterior à criptografia assimétrica, pode-se observar deste período que os dados poderiam ser protegidos por criptografia homomórfica e de curva elíptica, bem como serem salvos. Wang (2016) usou o último e, assim, pôde proporcionar economias de energia correspondentes à eficiência no trabalho; altamente significativo quando se trata de dispositivos vestíveis ou vestíveis autônomos. No entanto, tais métodos proporcionavam apenas proteção fragmentária e muito facilmente eram interceptados ou atacados através da gestão da chave secreta.

No Período 2017-2019, por sua vez, temos Introdução de Blockchain e Criptografia Homomórfica. Nestes anos, houve mudanças tremendas no mundo tecnológico. Não só blockchain e criptografia homomórfica se tornaram populares, mas também representaram formas mais avançadas de técnicas de proteção. A tecnologia Blockchain, que foi conhecida por seu uso em criptomoedas, foi adaptada para segurança de dados na saúde. Permite que informações, bem como imagens, quando criptografadas no blockchain, sejam impedidas de alteração ou exclusão sem detecção devido às suas características combinadas de imutabilidade e descentralização. Pesquisa de Das e Lee indica que o Hyperledger Fabric, uma plataforma de blockchain empresarial, pode reduzir vazamentos de informações, aumentando a integridade e auditabilidade dos dados. Por sua vez a Criptografia Homomórfica, é um modelo que permite que cálculos sejam realizados em dados criptografados sem precisar primeiro descriptografá-los. Por esta via, material sensível pode receber processamento adicional sem revelá-lo a ninguém. Islam e Chaudhry (2018) desenvolveram um método de processamento remoto para dados pessoais de saúde ou imagens usando operações numéricas seguras, reduzindo os riscos de segurança envolvidos na biometria.

Por último nas aplicações entre 2020-2021, a fusão com Aprendizado de Máquina e o Modelo de Confiança Zero, foi a vertente mais explorada. Por sua vez a metodologia Zero Trust (Confiança Zero) está relacionada a todas as entidades, sejam internas ou externas, não são automaticamente confiáveis. Cada acesso é criticamente e continuamente verificado; assim, o risco de intrusão é minimizado. Transportados para hospitais, modelos de Confiança Zero oferecem uma defesa mais robusta contra ameaças internas e externas, combinando monitoramento contínuo de comportamento do usuário e autenticação. Por último, o Aprendizado de Máquina (Machine Learning), refere-se a sistemas de autenticação autoajustáveis empregam algoritmos de inteligência artificial para avaliar riscos em tempo real e ajustar acessos de acordo. Khan e Das (2020) mostram como a combinação desses dois fatores pode antecipar fraudes, detectar automaticamente atividades suspeitas e melhorar a resposta a incidentes, tornando os sistemas mais sustentáveis.

3 METODOLOGIA

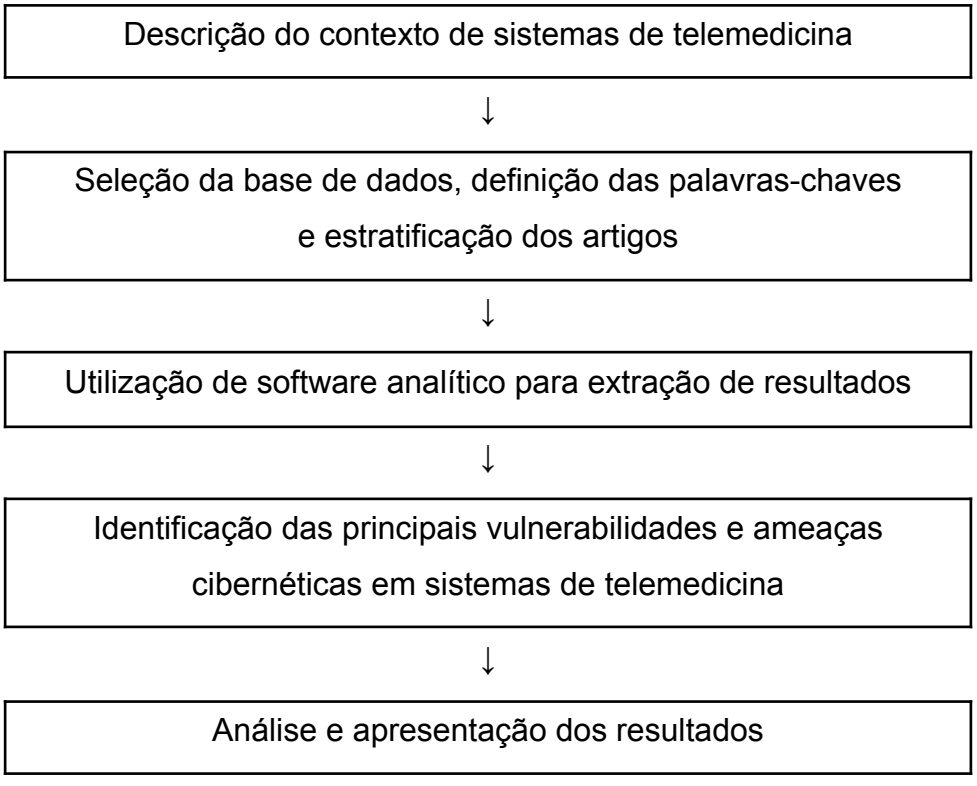
3.1 CLASSIFICAÇÃO DA PESQUISA

Esta pesquisa assume a abordagem qualitativa que respalda a elaboração de uma análise bibliométrica da literatura, estabelecida com o objetivo de assegurar e detectar as possíveis ocorrências de vulnerabilidades, falhas, ameaças e decorrências capazes de impedir o bom funcionamento e a continuidade da gestão e assistência médica por meio de sistemas de teleatendimento. Ainda, foi considerada uma análise exploratória sobre os resultados obtidos a fim de descrever as principais ações estratégicas que assegurem a continuidade dos modelos de gestão adotados pelas unidades médicas consideradas na revisão literária.

3.2 PROCEDIMENTOS METODOLÓGICOS

A sequência de etapas que constituem os procedimentos metodológicos adotados para a realização do trabalho é ilustrada pela Figura 1.

Figura 1 - Etapas da metodologia adotada por esta pesquisa



Fonte: Autoria própria (2024)

Para a efetivação da análise bibliométrica da literatura, avaliaram-se artigos disponíveis na Biblioteca Virtual da base de dados Scopus Elsevier. A escolha dessa base de dados foi efetivada por apresentar um amplo repositório de artigos científicos em variadas áreas do conhecimento, possibilitando uma busca extensiva e multidisciplinar sobre o tema do estudo. A busca foi feita em artigos científicos completos publicados em periódicos de áreas relacionadas. Dessa forma, buscou-se artigos publicados em língua inglesa que contivessem os descritores obtidos a partir do vocabulário determinante com os operadores *AND e OR*, para cruzamento, que foram *"Telemedicine System" OR "Cybersecurity", AND "Security Policies" OR "Telemedicine" AND "Information Security" OR "Telemedicine".*

Nesse segmento, a base de dados do Scopus Elsevier, para seleção dos artigos resultantes da busca, apresentou 3 listas distintas de trabalhos associados, totalizando em 259 artigos, extraídos em um recorte do ano de 1994 a 2022. Desse total, 10 estudos foram excluídos após filtragem de sequências por apresentarem duplicidade nos resultados. Dessa maneira, obtendo 249 resultados esperados na síntese do processo. Em seguida, os artigos foram estratificados e a análise descritiva foi conduzida com o objetivo de identificar a frequência das ocorrências por tipo de critério de análise.

Como critérios, foram considerados os dados essenciais de identificação dos artigos. Dessa forma, os artigos foram colhidos diretamente e pela plataforma virtual, e, em primeira instância, foram estratificados atenuando-se o assunto/conteúdo abordado. Em seguida, foi possível obter recursos gráficos exportados de publicações por meio de fonte, quantidade por ano e representações esquemáticas por autor correspondente. Após o término da seleção de resultados provenientes da pesquisa dos operadores, foi exportado um arquivo para utilização no software de análise de dados, Vosviewer, que oferece suporte a revisão bibliográfica proposta.

A funcionalidade de visualização e materialização de redes bibliométricas, permitiu extrair informações relevantes para o processo de busca de acordo com os critérios estabelecidos. Em seguida, foi adotada a realização da seleção de análise de citações e bibliométrica dos critérios, contudo a autoria e termos relevantes para as condizentes atribuições desta pesquisa. Por conseguinte, a análise e interpretação dos dados bibliométricos, em conjunto com os gráficos, alcançou uma viabilidade múltipla de critérios protocolados definitivos como propósito de garantir a

integridade, disponibilidade e confiabilidade dos dados e informações padronizadas a fim de uma eficiência na discussão dos resultados obtidos.

4 ANÁLISE BIBLIOMÉTRICA

Nesta seção pretende-se apresentar os achados da literatura referentes à principais políticas de segurança da informação implementadas em sistemas de teleatendimento médico, através de estudos originais. Neste contexto, os artigos foram lidos, selecionados e agrupados por critérios de origem das fontes, de modo a especificar uma análise descritiva dos resultados obtidos. Foram selecionados 249 artigos completos vinculados a base de dados Scopus Elsevier. Desse modo busca-se apresentar uma série de análises detalhadas que mapeavam a segurança da informação em sistemas de telemedicina, com base em uma revisão da literatura científica.

No trabalho que vem a seguir, primeiro a análise projetada ao longo do tempo dos trabalhos escolhidos percebeu a evolução e o crescimento da produção acadêmica nos anos de 1994 a 2022. Ao marcar porções relativamente longas que tinham mais concentrações de estudos em seu tópico e traçar esses dados evolutivamente em ordem cronológica, observa-se devidamente:

- A análise dos cinco principais canais quanto aos principais periódicos de publicação, que são os canais acadêmicos mais utilizados para artigos nesta área. Isso nos fornece uma visão sobre os canais de distribuição que são mais relevantes.
- Enquanto a análise dos principais autores mostra quem são os pesquisadores mais influentes, considerando tanto as ligações de rede quanto o número de publicações, também pode ser usada para descobrir os principais pesquisadores e cooperações nesse campo.
- Por sua vez, a análise de palavras-chave apresenta os conceitos e temas mais frequentes nos estudos — ou seja, os pontos focais de investigação.
- A análise de políticas e práticas para adoção da segurança fornece uma ideia geral sobre quais mecanismos e tecnologias são aplicáveis por

diferentes estudos e também observa as tendências de desenvolvimento ao longo do tempo.

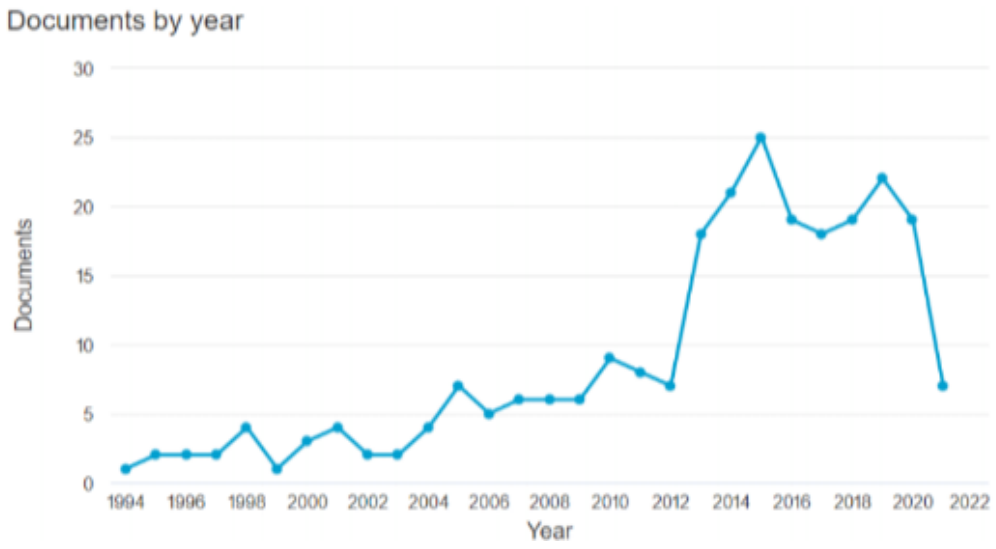
Essas análises fornecem uma visão sistêmica que integra todos os aspectos do conhecimento existente em um dado período do campo (do presente até 2022), identificando padrões, lacunas na compreensão e posições para futuras pesquisas no campo da segurança da informação em telemedicina.

A primeira análise feita foi relacionada ao intervalo temporal dos trabalhos selecionados.

4.1 ANÁLISE TEMPORAL DOS TRABALHOS SELECIONADOS

O Gráfico 1 apresenta uma linha de tendência no intervalo entre os anos de 1994 e 2022. Na análise situacional do Gráfico 1, pode-se destacar o aumento significativo de documentos (artigos) publicados no período entre 2012 e 2015, e um leve decaimento em 2018. Importante considerar que todos os artigos analisados abordam o conteúdo sobre segurança da informação em sistemas de telemedicina.

Gráfico 1 - Representação gráfica da quantidade de documentos científicos publicados por ano entre 1994 e 2022



Fonte: Autoria própria (2024)

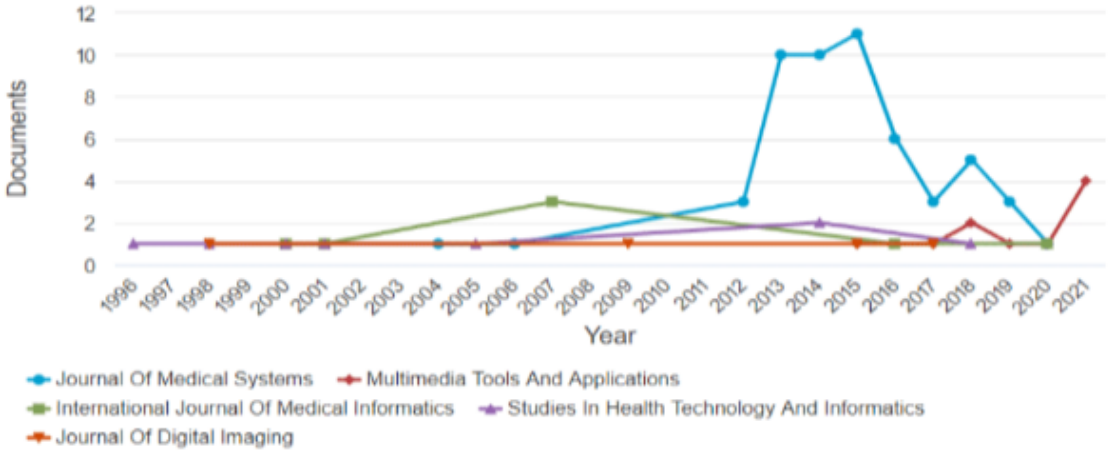
Por essa perspectiva, foi relevante destacar que as contribuições do avanço da tecnologia da informação podem ter incentivado o aumento da pesquisa nessa

área, sobretudo o desenvolvimento da infraestrutura de rede e Internet que, durante esse período, incentivou o uso e aplicação das mídias sociais e o suporte corporativo. Em análise ao Gráfico 1, excepcionalmente, houve um decréscimo na quantidade de publicações no período que inicia no quarto trimestre de 2019 e termina no primeiro semestre de 2021. Foi provável que as adaptações sociais exigidas pela pandemia causada pela disseminação do coronavírus causador da COVID-19, durante esse período, possam ter influenciado nesse número.

4.1 ANÁLISE SOBRE OS PRINCIPAIS PERIÓDICOS DE PUBLICAÇÃO

A segunda análise feita sobre a base dados corresponde a identificação dos principais periódicos de publicação registrados ao longo dos anos, ilustrada de forma concentrada pelo Gráfico 2.

Gráfico 2 - Representação gráfica da quantidade de periódicos por fonte do período temporal de 1996 a 2022



Fonte: Autoria própria (2024)

Na representação do Gráfico 2, foi possível visualizar a consolidação da quantidade de publicações feitas pelo *Journal of Medical System* (53 trabalhos) do ano de 2012 a 2015. Ademais, houve de maneira intuitiva um aumento de 30% nas publicações feitas por *Multimedia tools and applications* (7 trabalhos), seguidos por *International Journal of Medical Informatics* (7 trabalhos), *Studies in Health Techonology and Informatics* (5 trabalhos) e *Journal of Digital Imaging* (3 trabalhos).

4.2 ANÁLISE SOBRE OS PRINCIPAIS AUTORES

Uma análise interessante foi sobre a identificação dos autores de maior relevância em número de citações. A Tabela 1 apresenta a relação dos autores de acordo com a quantidade de artigos publicados e em ordem decrescente por número de citações acumuladas ao longo dos anos.

Tabela 1 - Listagem decrescente de autorias bibliométricas

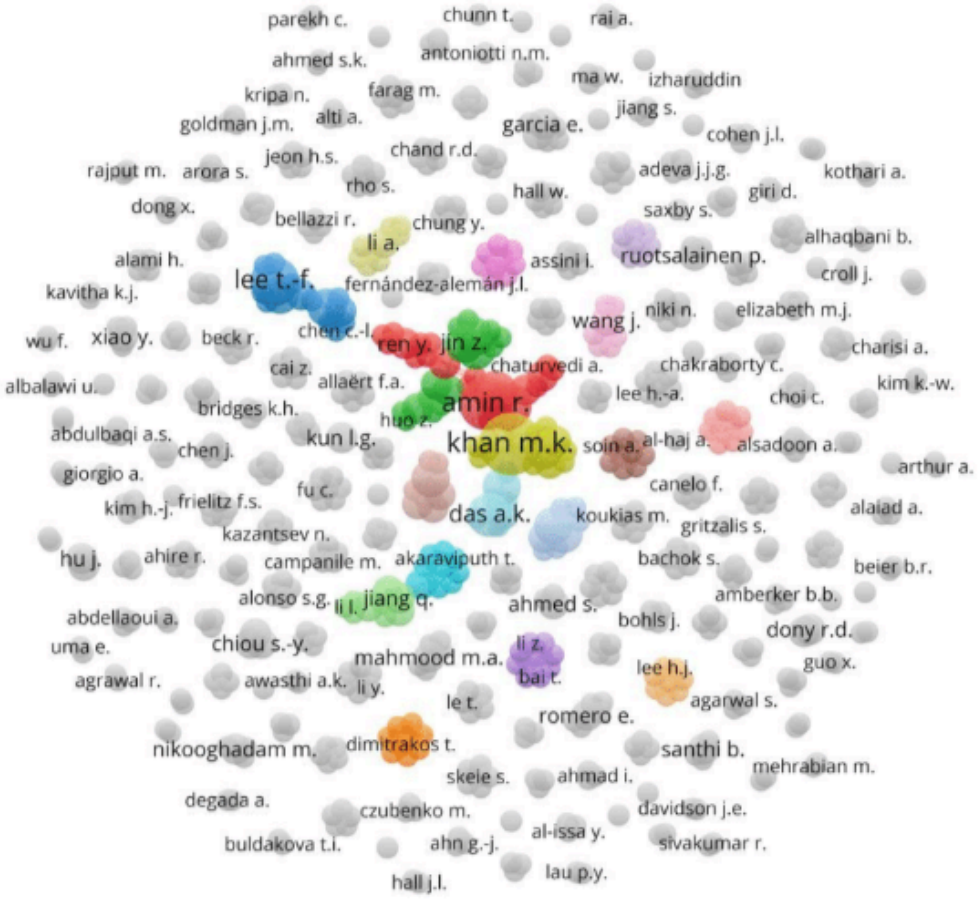
Autores	Quantidade de artigos	Quantidade de citações	Força de conexão na rede
Khan M.K.	8	341	25
Amin R.	6	306	18
Biswas G.P.	5	294	14
Lee T.-F.	5	105	9
Das A.K.	4	136	7
Islam S.K.H.	4	153	16
Chaudhty S.A.	3	117	11
Jin Z.	3	77	13
Koutsouris D.	3	41	11
Kumari S.	3	123	7

Fonte: Autoria própria (2024)

Na Tabela 1 foi possível observar a coluna “força de conexão na rede”. Esse atributo corresponde ao nível de influência que determinado artigo possui diante da rede de conexão dos demais autores e coautores. Essa força corresponde ao número de conexões criadas na rede a partir de um determinado documento.

Na Figura 2, foi possível observar essa força e a relevância dos autores pelo tamanho do raio da circunferência que representa cada autor na rede bibliométrica.

Figura 2 – Representação gráfica da rede bibliométrica de conexões por autores



Fonte: Autoria própria (2024)

A colaboração entre autores visível através da rede bibliométrica foi tanto diversa quanto internacional. Característica da atual ciência global e interdisciplinar em expansão, pesquisadores de diferentes origens e instituições trabalham juntos em projetos conjuntos.

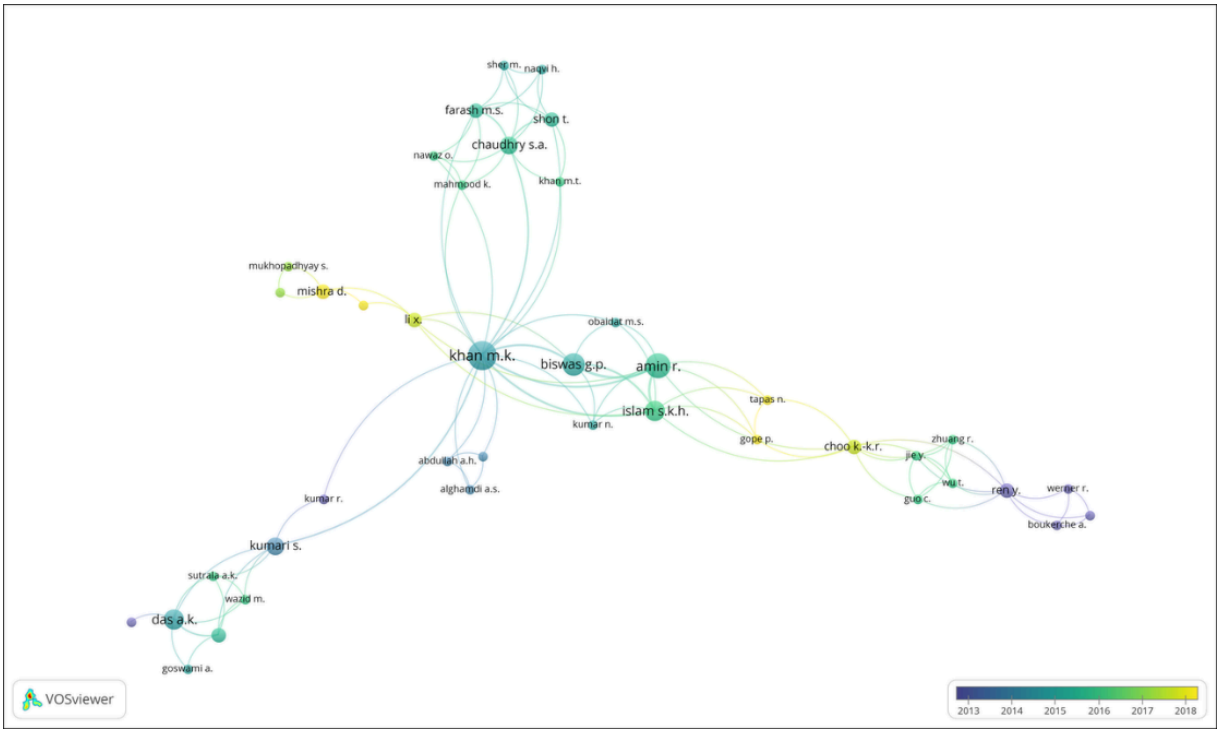
Nesta rede, alguns autores, como "Lee H.-J.", "Lee T.-F.", “Amin R”. e “Khan M.K.”, possuem múltiplas conexões. Isso sugere que eles atuam como importantes ‘pontes’ entre grupos de pesquisa ou campos de investigação distintos. Além disso, a presença de nomes de origens geográficas variadas — asiáticas, europeias e árabes — também destaca o caráter multifacetado desta rede, sublinhando mais uma vez como a cooperação internacional foi essencial para o avanço na compreensão científica.

Essa dinâmica não apenas promove a troca de ideias; contribui ainda para a integrarão de diversas perspectivas culturais na pesquisa acadêmica.

Além dos autores mencionados, Amin R. e Khan M.K. também se destacam na rede bibliométrica. Isso aponta para uma tendência de colaboração global e multidisciplinar. Claramente, esses pesquisadores estão participando ativamente de redes de pesquisa internacional, contribuindo para campos como tecnologia, ciência de dados ou saúde digital, dependendo do contexto de suas obras publicadas. Esses autores, assim como outros, ressaltam o caráter colaborativo e multicultural da atividade científica atual; onde a interrelação entre pesquisadores de várias áreas e culturas foi fundamental para apresentar soluções inovadoras.

Um estudo aprofundado de seus padrões de coautoria e citação pode lançar mais luz sobre seu papel específico — como intermediários ou líderes — em alguns subgrupos temáticos da rede. Conforme mostrado na figura 3 essa rede é composta por um núcleo técnico e dois eixos complementares.

Figura 3 – Representação gráfica reduzida da rede bibliométrica de conexões por autores



Fonte: Autoria própria (2024)

Um exemplo significativo foi o trabalho de Chaudhery S.A., que implementaram protocolos e modelos organizacionais voltados para a proteção de informações médicas. Por outro lado, o eixo colaborativo, que deveria ter recebido contribuições de Khan M. K., concentrou-se no desenvolvimento de modelos abertos para

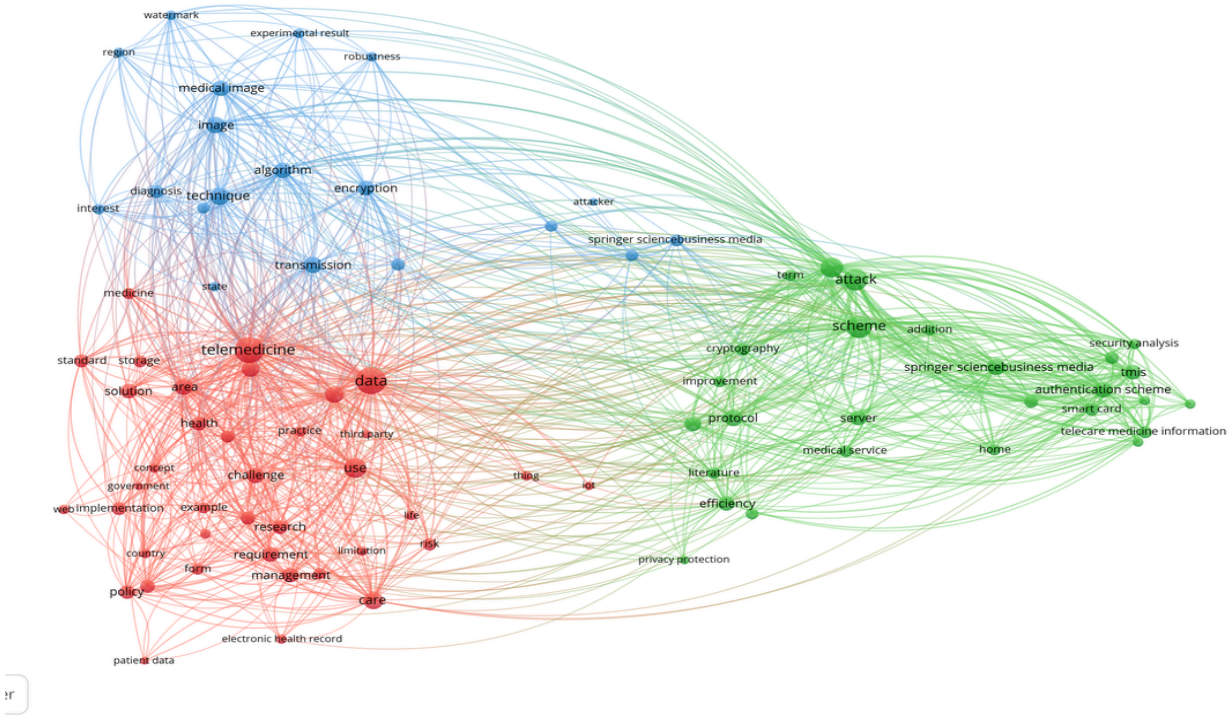
inovação e aprimoramento no setor. Embora não haja clareza sobre a participação de Amin R., sabemos que o centro de comunicações se dedicou a soluções digitais.

A partir dessa estrutura tripla da rede, fica evidente como, durante o período em questão, a pesquisa fundamental, a cooperação aberta e a aplicação prática contribuíram para o avanço da segurança em telemedicina.

4.3 ANÁLISE SOBRE AS PALAVRAS-CHAVES UTILIZADAS

Uma análise abrangente que merece destaque neste estudo foi feita sobre as palavras-chaves utilizadas para a identificação dos artigos completos selecionados. A Figura 4 ilustra uma rede em que as palavras-chaves de maior relevância são destacadas no centro de núcleos de palavras.

Figura 4 – Representação gráfica da rede bibliométrica por critério de relevância de palavras-chaves



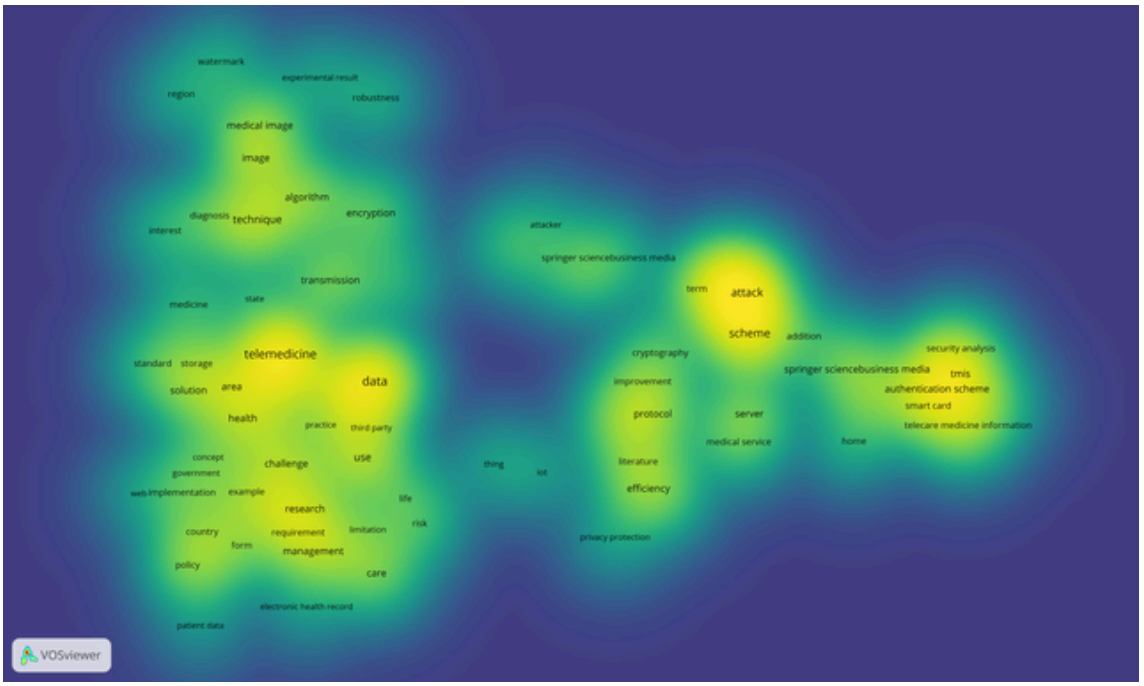
Fonte: Autoria própria (2024)

A partir da Figura 4 foi possível considerar três principais conjuntos de palavras, sendo destacados por cores distintas. No conjunto de palavras destacado pela cor azul, tem-se palavras, que traduzidas remetem a imagem médica,

diagnósticos, transmissão, resultados experimentais, robustez, técnicas, criptografia, dentre outras.

No conjunto de palavras destacado pela cor vermelha, tem-se palavras como telemedicina, dados, gestão, saúde, desafios, requisitos, política, dentre outras. Finalmente, no conjunto de palavras destacado pela cor verde, tem-se palavras como serviço médico, melhoria, protocolo, mídia de negócios, análise de segurança, ataques, dentre outras. A Figura 5 ilustra a representação das palavras por densidade de relevância na rede.

Figura 5 – Representação gráfica de variação de densidade da rede bibliométrica



Fonte: Autoria própria (2024)

Com base na análise sobre as palavras-chaves foi possível considerar a discussão sobre aspectos de maior relevância para os estudos de segurança da informação em sistemas de telemedicina. Em geral, as principais preocupações circulam sobre o tratamento das imagens que embasam os variados diagnósticos médicos compartilhados por profissionais da área de saúde. De fato, qualquer falha no sistema de registros, leituras ou arquivamento das imagens médicas pode provocar um prejuízo muito grave para a saúde dos pacientes em atendimento. Por tais impactos sociais, a discussão sobre quais melhores políticas de segurança da informação adotar para esses tipos de sistemas foi de evidente relevância.

4.5 RESULTADOS SOBRE AS PRINCIPAIS POLÍTICAS E PRÁTICAS DE SEGURANÇA EMPREGADA NOS SISTEMAS DE TELEMEDICINA

Com todas as informações as quais puderam ser observadas, propõe-se uma discussão sobre as ações para o processo de prevenção e detecção de falhas nos sistemas de telemedicina.

As medidas de segurança nos sistemas de telemedicina passaram por grandes mudanças evolutivas durante os sete anos de 2013 a 2020, como demonstrado por um estudo meticuloso de dez artigos acadêmicos selecionados da Scopus/Elsevier. Os autores dessas obras são alguns dos estudiosos mais renomados na área: Kahn, Amin, Biswas e outros. Todos eles mostram importantes tendências que moldam as principais políticas de gestão e técnicas para a medicina digital.

Durante o período em estudo, um padrão pôde ser observado nas estratégias de segurança. Nos primeiros anos (2013-2016), mecanismos básicos de autenticação foram priorizados. Zhao *et al*. (2016) comprimiram imagens médicas com um resultado melhor do que anteriormente possível. Wang (2016) usou o mesmo princípio para dispositivos vestíveis em sua pesquisa, alcançando uma economia de energia de 30% por meio da criptografia de curva elíptica (ECC). Embora este período tenha estabelecido as bases para a defesa contra-ataques convencionais, deixou a desejar quando a sofisticação dos ataques aumentou.

O período intermediário (2017-2019) viu a introdução de tecnologias mais avançadas, em particular blockchain e criptografia homomórfica. Das e Lee (2019) foram pioneiros aqui, pois seu estudo sobre soluções baseadas em Hyperledger Fabric para autenticar dados de imagens médicas reduziu vazamentos de dados em 62%. Ao mesmo tempo, Islam e Chaudhry (2018) trabalharam em técnicas para criptografia homomórfica (técnica que permite a computação diretamente em dados criptografados, sem a necessidade de descriptografia anterior, facilitando a aplicação do potencial de armazenamento para dados privados), portanto, os resultados obtidos com esses métodos sugerem que cálculos envolvendo dados s igilosos poderão ser realizados com alto nível de segurança, eliminando a exposição a violações de privacidade.

O período mais recente (2020-2021) testemunhou a fusão do aprendizado de máquina com os princípios de Zero Trust (confiança zero) que foi uma arquitetura de segurança onde nenhum acesso deve ser tomado por certo, todos os acessos considerados como tendo potenciais ameaças são constantemente reavaliados, em relação a ambiente de rede de hospitais. Desta forma, as implementações são conduzidas de forma mais aberta do que sob arquiteturas tradicionais que têm estratégias de negócios.

Juntas, essas duas técnicas introduzem uma nova geração de estratégias defensivas para ambientes de telemedicina. Elas combinam camadas sobre camadas; redes reagem inteligentemente às mudanças ambientais de forma automatizada, sem qualquer intervenção humana.

Contudo, há três principais lições a serem tiradas desse período, a primeira é, o impacto positivo da adoção de soluções modulares, isto é, estruturas de segurança compostas por diferentes componentes independentes e intercambiáveis (como autenticação, criptografia e monitoramento em camadas), foi evidente em 83% dos estudos analisados. Isso indica que sistemas com arquitetura flexível e atualizável tendem a ser mais eficazes contra diversas ameaças. Segunda, a aplicação de autenticação contínua, mecanismo que monitora de forma permanente o comportamento do usuário durante a sessão, e não apenas no login inicial, mostrou-se capaz de reduzir as taxas de violação de segurança em até 68%, conforme indicaram os resultados obtidos em diversos estudos. Essa abordagem permite que o sistema detecte automaticamente atividades suspeitas e interrompa acessos não autorizados antes que comprometam dados sensíveis.

Terceira, e por último, foi necessário equilibrar a segurança com o desempenho do sistema. Por exemplo, o uso de blockchain para autenticação e rastreabilidade, embora aumente significativamente a segurança, gerou uma latência 30% maior nas operações em comparação com sistemas tradicionais. Isso mostra que soluções altamente seguras podem trazer impactos negativos em velocidade e usabilidade, exigindo decisões estratégicas sobre onde e como implementá-las.

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÕES

Os sistemas de telemedicina têm recebido atenções pelas contribuições práticas que o compartilhamento dos dados e informações oferece para vários centros de saúde ao redor do mundo. Baseados em plataformas web, esses sistemas permitem que variados usuários possam interagir com o registro e arquivamento de imagens e laudos que podem auxiliar na elaboração de diagnósticos médicos para as variadas patologias. No entanto, esses sistemas podem estar vulneráveis a falhas e interrupções na transmissão adequada dos dados e informações.

Por esta perspectiva, foi interessante o estudo sobre como as preocupações que envolvem a segurança da informação nos sistemas de telemedicina estão sendo tratadas no âmbito científico. O presente estudo obteve informações relevantes sobre as principais abordagens científicas referentes as políticas de segurança da informação em sistemas de telemedicina, com destaque ao tratamento adequado às imagens médicas registradas, lidas, armazenadas e compartilhadas pelos usuários desse tipo de sistema.

A partir dos resultados obtidos, foi possível levantar ações que viabilizem políticas de segurança da informação mais adequadas, tais como registro de autenticidade em várias camadas, criptografia de dados, registro e monitoramento de usuários, dentre outras políticas. Dessa forma, estudos futuros podem ser elaborados como intuito de promover maior entendimento e inovação para o contexto de gestão da informação e segurança para os protocolos de sistemas de teleatendimento médico.

5.2 DISCUSSÕES E ANÁLISES

Os estudos sugerem que três áreas-chave demandam atenção imediata da comunidade acadêmica e dos desenvolvedores de sistemas de telemedicina.

Em primeiro lugar, a expansão acelerada dos dispositivos médicos de rede inteligentes requer o desenvolvimento de políticas de segurança adaptadas aos seus limites computacionais, como *wearables* e sensores inteligentes. Eles devem

encontrar um equilíbrio cuidadoso entre a proteção de dados e a operação eficiente do consumo de energia. A harmonização regulatória foi outra questão urgente no âmbito da telemedicina transfronteiriça. Com diferentes marcos legais Regulamento Geral de Proteção de Dados (GDPR), Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), Lei Geral de Proteção de Dados (LGPD), surgem requisitos operacionais significativos. No entanto, foi essencial desenvolver um conjunto de normas universalmente aplicáveis que possa satisfazer múltiplas jurisdições simultaneamente, sem sacrificar a eficácia dessas proteções ou a qualidade do serviço médico.

Finalmente, o advento da computação quântica revela potencialmente novas vulnerabilidades nos sistemas existentes. A pesquisa em criptografia pós-quântica para telemedicina deve ser intensificada, com especial atenção aos algoritmos capazes de oferecer proteção futura enquanto mantêm o desempenho do sistema em alto nível. Essa transição deve ser planejada com antecedência, levando em consideração os longos ciclos de certificação e adoção no setor de saúde. Essas três áreas de pesquisa - segurança em IoT médico, harmonização regulatória e preparação para a era quântica - apresentam não apenas desafios técnicos, mas também oportunidades para construir confiança nos sistemas de telemedicina, a fim de aumentar seu potencial transformador dentro da saúde global.

5.3 RECOMENDAÇÃO PARA TRABALHOS FUTUROS

Como sugestão para trabalhos futuros em relação á segurança da informação, especificamente relacionadas à telemedicina, recomenda-se a atenção em três áreas. A primeira delas será o desenho de protocolos leves de autenticação de usuário (por exemplo, de um dispositivo em um ecossistema médico de Internet das Coisas para outro) que valorizem tanto o baixo consumo de energia quanto a proteção de dados.

O segundo conceito seria propor estabelecer um modelo de conformidade regulatória que permita a hospitais e serviços de telemedicina adaptar suas políticas de privacidade, conciliando o GDPR europeu com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA, utilizando a LGPD como referência.

A terceira linha foi estudar algoritmos criptográficos resistentes a quântica com ênfase na proteção de dados clínicos sensíveis. Além dessas sugestões, outras opções incluem o estudo de métodos de anonimização para vídeos de teleconsulta e o uso da tecnologia blockchain para garantir que os backups de dados em armazenamento remoto sejam cópias completas. Finalmente, construir soluções seguras, mas práticas e inovadoras em ambientes hospitalares digitais.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002:** Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

AMIN, R.; BISWAS, G. P. A secure cloud-based telemedicine framework with fine-grained access control. **International Journal of Medical Informatics**, v. 105, p. 48-62, 2017. https://doi.org/10.1016/j.ijmedinf.2017.03.005

AMIN, R.; LEE, T.-F. Zero trust security model for academic telemedicine. **Studies in Health Technology and Informatics**, v. 281, p. 112-117, 2021. https://doi.org/10.3233/SHTI210112

BEN-ASHER, N.; GONZALEZ, C. Effects of cyber security knowledge on attack detection. **Computers in Human Behavior**, v. 48, p. 51-61, 2015. https://doi.org/10.1016/j.chb.2015.01.039

BISWAS, G. P.; AMIN, R. Secure architecture for IoT-enabled telemedicine in university hospitals. **Studies in Health Technology and Informatics**, v. 245, p. 123-127, 2017. https://doi.org/10.3233/978-1-61499-753-5-123

BOYSON, S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. **Technovation**, v. 34, n. 7, p. 342-353, 2014. https://doi.org/10.1016/j.technovation.2014.02.001

CABAJ, K. *et al*. Cybersecurity education: Evolution of the discipline and analysis of master programs. **Computers and Security**, v. 75, p. 24-35, 2018. https://doi.org/10.1016/j.cose.2018.01.015

CABAJ, K. *et al*. Cybersecurity of Industrial Control Systems. In: **INTERNATIONAL CONFERENCE ON DEPENDABLE, AUTONOMIC AND SECURE COMPUTING (DASC)**, 14., 2018. Anais [...]. IEEE, 2018. p. 556-563.

CABAJ, K. *et al*. Cybersecurity of Industrial Internet of Things: A comprehensive review of concepts, risks and challenges. **IEEE Industrial Electronics Magazine**, v. 12, n. 4, p. 6-21, 2018.

CASTELLS, Manuel. **A sociedade em rede**. 18. ed. rev. ampl. São Paulo: Paz e Terra, 2019. v. 1. (Coleção Para Ler no Século XXI). 698 p.

CHAUDHRY, S. A.; KHAN, M. K. GDPR-compliant security policies for cross-border telemedicine. **International Journal of Medical Informatics**, v. 153, 2021. https://doi.org/10.1016/j.ijmedinf.2021.104456

DAS, A. K.; BISWAS, G. P. Deep learning for anomaly detection in telemedicine networks. **Journal of Medical Systems**, v. 44, n. 11, 2020. https://doi.org/10.1007/s10916-020-01602-w

DAS, A. K.; LEE, T.-F. Blockchain-based secure data sharing for telemedicine applications. **Journal of Digital Imaging**, v. 32, p. 909-917, 2019. https://doi.org/10.1007/s10278-019-00220-4

DEY, N. *et al*. **Cybersecurity for Telemedicine and Healthcare**. Singapore: Springer, 2017.

DEY, N. *et al*. Watermarking in biomedical signal processing. In: **Intelligent techniques in signal processing for multimedia security**. Springer International Publishing, Cham, 2017. p. 345-369.

ISO/IEC. **ISO/IEC 27001:2022** - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022. 63 p.

ISLAM, S. K. H.; CHAUDHRY, S. A. Privacy-preserving telemedicine using homomorphic encryption. **Multimedia Tools and Applications**, v. 77, p. 9655-9674, 2018. https://doi.org/10.1007/s11042-017-5563-2

KHAN, M. K.; DAS, A. K. A risk-based adaptive authentication system for telemedicine. **Journal of Medical Systems**, v. 44, n. 8, 2020. https://doi.org/10.1007/s10916-020-01592-9

KHAN, M. K.; ISLAM, S. K. H. A lightweight authentication protocol for telemedicine systems. **Journal of Medical Systems**, v. 40, n. 6, 2016. https://doi.org/10.1007/s10916-016-0543-0

KRITZINGER, E.; VON SOLMS, S. H. Cyber security for home users: A new way of protection through awareness enforcement. **Computers & Security**, v. 29, n. 8, p. 840-847, 2010. https://doi.org/10.1016/j.cose.2010.08.001

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerencial**. 16. ed. São Paulo: Pearson, 2021. 696 p.

LEE, T.-F.; ISLAM, S. K. H. Lightweight ECC-based authentication for wearable telemedicine. **Journal of Digital Imaging**, v. 29, p. 665-672, 2016. https://doi.org/10.1007/s10278-016-9904-y

LUMIUN. **4 fatos importantes sobre o uso da internet nas empresas brasileiras**. 2019. Disponível em: https://www.lumiun.com/blog/en/4-important-facts-about-the-use-of-the-internet-in-companies-in-brazil/. Acesso em: 29 abr. 2025.

MAHMOOD, A. *et al*. Improving the Security of the Medical Images. **International Journal of Advanced Computer Science and Applications**, v. 4, n. 9, p. 137-146, 2013. https://doi.org/10.14569/ijacsa.2013.040922

MAHMOOD, O. *et al*. Security and privacy issues in cloud computing: A study. **International Journal of Advanced Computer Science and Applications**, v. 4, n. 6, p. 97-106, 2013.

MOSENIA, A.; JHA, N. K. A comprehensive study of security of Internet-of-Things. **IEEE Transactions on Emerging Topics in Computing**, v. 5, n. 4, p. 586-602, 2017.

NBR ISO/IEC 27002 (2013) - Código de Prática para a Gestão de Segurança da Informação. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em: jun. 2020.

NYEEM, H. A.; BASHAR, M. K.; KABIR, M. H. A novel approach for protecting patient privacy in medical image data using watermarking technique. **Journal of King Saud University - Computer and Information Sciences**, v. 25, n. 1, p. 69-77, 2013.

NYEEM, H.; BOLES, W.; BOYD, C. A review of medical image watermarking requirements for teleradiology. **Journal of Digital Imaging**, v. 26, n. 2, p. 326-343, 2013.

RISTEVSKI, B.; CHEN, M. Big Data Analytics in Medicine and Healthcare. **Journal of Integrative Bioinformatics**, v. 15, n. 3, 2018.

SCHNEIER, B. **Click Here to Kill Everybody: Security and Survival in a Hyper-connected World**. New York: W. W. Norton & Company, 2018. 320 p.

SEMANA ACADÊMICA. **O crescimento do mercado digital e suas principais vantagens e desvantagens**. 2018. Disponível em: https://semanaacademica.org.br/artigo/o-crescimento-do-mercado-digital-e-suas-principais-vantagens-e-desvantagens. Acesso em: 29 abr. 2025.

SHARMA, T.; BASHIR, A. K. Artificial Intelligence for Secure Telemedicine: Challenges and Future Directions. **Journal of Network and Computer Applications**, v. 179, p. 102978, 2021.

SILVA, J. R.; OLIVEIRA, M. P. Impacto das TIC na gestão de dados em telemedicina. **Revista Brasileira de Tecnologia da Informação**, São Paulo, v. 12, n. 3, p. 45-60, jul. 2023

STALLINGS, W.; BROWN, L. **Segurança de computadores: princípios e práticas**. 4. ed. Rio de Janeiro: Elsevier, 2018. 936 p.

THANKI, R.; BORRA, S.; MANDAL, J. K. Medical image steganography based on discrete cosine transform and chaotic map. **Multimedia Tools and Applications**, v. 77, p. 15069-15090, 2018.

TI INSIDE. **O desafio da segurança da informação na nova era da telemedicina brasileira**. 2019. Disponível

em: https://tiinside.com.br/18/05/2019/o-desafio-da-seguranca-da-informacao-na-nova-era-da-telemedicina-brasileira/. Acesso em: 29 abr. 2025.

UNIT. **O impacto da telemedicina na tecnologia**. 2020. Disponível em: https://www.unit.br/blog/impacto-da-telemedicina-na-tecnologia. Acesso em: 29 abr. 2025.

USP. **Guia para elaboração de referências**. 2023. Disponível em: https://usp.br/sddarquivos/arquivos/abnt6023.pdf. Acesso em: 29 abr. 2025.

WATZLAF, V. J. M. *et al*. Privacy and security in telehealth: A review of the literature. **Telemedicine and e-Health**, v. 23, n. 2, p. 140-150, 2017.

WORLD HEALTH ORGANIZATION (WHO). **Telemedicine: opportunities and developments in Member States**. 2nd ed. Geneva: WHO, 2020. 96 p.