GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTES HOSPITALARES, DESAFIOS DA LEI GERAL DA PROTEÇÃO DE DADOS E ESTRATÉGIAS DE MITIGAÇÃO DE RISCOS CIBERNÉTICOS: Uma revisão integrativa

INFORMATION SECURITY MANAGEMENT IN HOSPITAL ENVIRONMENTS, LGPD CHALLENGES, AND CYBER RISK MITIGATION STRATEGIES: An Integrative Review

Ryan Lucas do Carmo Pereira
rlcp@discente.ifpe.edu.br
Koenigsberg Lee Ribeiro de Andrade Lima
koenigsberglee@abreuelima.ifpe.edu.br

RESUMO

A crescente digitalização dos serviços de saúde ampliou o uso de sistemas de informação em ambientes hospitalares, tornando a proteção de dados sensíveis um desafio estratégico para as instituições. Nesse contexto, a Lei Geral de Proteção de Dados estabelece diretrizes para o tratamento de dados pessoais e impacta diretamente a gestão hospitalar. Este estudo teve como objetivo analisar os desafios da gestão da segurança da informação em hospitais, considerando as exigências legais e as estratégias de mitigação de riscos cibernéticos descritas na literatura científica. Trata-se de uma revisão integrativa realizada a partir de estudos publicados nas bases PubMed, Scopus, Web of Science, SciELO e LILACS, selecionados conforme critérios previamente definidos, resultando em uma amostra final de dez estudos. Os resultados evidenciaram que hospitais estão entre os setores mais vulneráveis a ataques cibernéticos, especialmente ransomware, além de apresentarem fragilidades relacionadas ao fator humano, ao uso de sistemas legados e à incorporação de dispositivos médicos conectados. Observou-se ainda que a adequação às exigências legais ocorre de forma desigual, sobretudo em instituições públicas, em razão de limitações estruturais, financeiras e de

governança. Conclui-se que a efetividade da segurança da informação hospitalar depende da integração entre conformidade legal, governança da informação, tecnologia, capacitação profissional e gestão estratégica, sendo a proteção de dados essencial para a continuidade dos serviços de saúde e para a segurança do paciente.

Palavras-chave: Segurança da Informação. Hospitais. LGPD. Riscos Cibernéticos. Gestão Hospitalar.

ABSTRACT

The increasing digitalization of healthcare services has expanded the use of information systems in hospital environments, making the protection of sensitive data a strategic challenge for healthcare institutions. In this context, the General Data Protection Law establishes guidelines for the processing of personal data and directly impacts hospital management. This study aimed to analyze the challenges of information security management in hospitals, considering legal requirements and cyber risk mitigation strategies described in the scientific literature. This is an integrative literature review conducted using studies published in the PubMed, Scopus, Web of Science, SciELO, and LILACS databases, selected according to previously defined criteria, resulting in a final sample of ten studies. The results showed that hospitals are among the sectors most vulnerable to cyberattacks, especially ransomware, and present weaknesses related to human factors, legacy systems, and the incorporation of connected medical devices. It was also observed that compliance with legal requirements occurs unevenly, particularly in public institutions, due to structural, financial, and governance limitations. It is concluded that the effectiveness of hospital information security depends on the integration of legal compliance, information governance, technology, professional training, and strategic management, with data protection being essential for the continuity of healthcare services and patient safety.

Keywords: Information Security. Hospitals. LGPD. Cyber Risks. Hospital Management.

1 INTRODUÇÃO

A transformação digital no setor de saúde intensificou a adoção de prontuários eletrônicos, telessaúde e sistemas baseados em nuvem, criando dependência significativa de tecnologias da informação e ampliando a superfície de ataque das organizações de saúde. Romanov & Varnfield (2025) destacam que, embora essas tecnologias melhorem a qualidade e eficiência dos serviços de saúde, a interconexão crescente entre sistemas clínicos e digitais também eleva os desafios de cibersegurança, expondo infraestruturas e dados sensíveis a ameaças mais sofisticadas. Nesse contexto, conforme destacam Kruse *et al. (*2017, p.2), ‘’Os hospitais permanecem vulneráveis às tendências e ameaças modernas devido à lenta adaptação das suas defesas’’.

Diante desse cenário de crescente digitalização e ampliação da superfície de ataque na assistência à saúde, torna-se evidente a necessidade de marcos regulatórios capazes de orientar e disciplinar o tratamento das informações em saúde. A literatura aponta que a intensificação do uso de tecnologias da informação, quando não acompanhada por estruturas adequadas de governança e segurança, potencializa riscos à privacidade e à proteção de dados sensíveis, exigindo respostas

institucionais e normativas mais robustas (Kruse et al., 2017; Whitman & Mattord, 2018).

No Brasil, o tratamento de dados pessoais passou a ser regulamentado pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD). O texto legal estabelece que sua finalidade é garantir “os direitos fundamentais de liberdade e de privacidade” no tratamento de dados pessoais (Brasil, 2018). Para as instituições de saúde, que lidam diariamente com informações classificadas como dados sensíveis, a LGPD impõe não apenas exigências normativas, mas também obrigações operacionais e organizacionais que afetam o funcionamento institucional. Estudos que abordam os desafios de implementação da LGPD em hospitais públicos mostram que a adaptação à legislação exige revisões de processos internos, governança e estrutura de segurança da informação, o que implica em custos e mudanças administrativas significativas para as organizações de saúde (Gonçalves & Werner, 2025).

Revisões integrativas da literatura destacam ainda que, apesar de avanços na regulação, persistem barreiras na efetivação de práticas que garantam a proteção e o uso responsável de dados em saúde, tais como a insuficiente capacitação profissional, o uso inadequado dos sistemas pelos colaboradores, limitações na infraestrutura tecnológica e falhas na implementação de políticas institucionais de segurança da informação, fatores que impactam a capacidade de adaptação das instituições (Santos et al., 2025). Ademais, análises sobre o princípio de segurança na LGPD sugerem que a adoção de medidas técnicas e administrativas robustas é imprescindível para a garantia da funcionalidade dos sistemas e para a proteção dos titulares de dados, ligando diretamente a conformidade legal à continuidade dos serviços hospitalares (Petry & Hupffer, 2023).

O impacto financeiro decorrente de incidentes cibernéticos em ambientes hospitalares tem se mostrado significativamente elevado. O relatório Cost of a Data Breach 2024, registrou o setor de saúde como o maior custo médio global por violação de dados, permanecendo entre os setores mais dispendiosos na remediação de vazamentos e interrupções. O mesmo documento reforça que a saúde continua apresentando o custo médio mais alto por violação de dados, pelo 13º ano consecutivo o que demonstra a criticidade da segurança da informação nesse contexto (IBM, 2024).

No Brasil, os valores são igualmente expressivos. O relatório aponta que o custo médio de uma violação de dados no país atingiu 6,75 milhões, e instituições de saúde apresentaram custos ainda maiores, chegando a 10,46 milhões por incidente. Esses números revelam que incidentes cibernéticos comprometem não apenas a privacidade, mas também a sustentabilidade operacional e financeira das instituições hospitalares (IBM, 2024).

No contexto técnico da segurança da informação em saúde, a literatura destaca um conjunto multifacetado de ameaças recorrentes que exploram tanto vulnerabilidades humanas quanto tecnológicas. Revisões sistemáticas apontam que a combinação de erro humano, dispositivos conectados à rede e sistemas legados contribui para a incidência de ataques cibernéticos, incluindo ransomware e phishing, em organizações de saúde (Ewoh & Vartiainen, 2024).

A proliferação de dispositivos do tipo Internet of Medical Things (IoMT) amplia a superfície de ataque ao introduzir pontos de vulnerabilidade em dispositivos médicos conectados (Deb et al., 2025). Além disso, relatos apontam que técnicas de

engenharia social e phishing exploram diretamente fragilidades humanas em ambientes clínicos, resultando em acesso não autorizado e compromissos de dados sensíveis (Aldosari, 2025).

É observado que, durante a pandemia de COVID-19, o setor vivenciou um aumento expressivo de ataques, destacando que a rápida mudança para serviços digitais e práticas remotas ampliou significativamente o risco para organizações de saúde. O estudo também reforça que a maioria dos ataques encontra sucesso em falhas humanas e práticas inadequadas de segurança por parte dos colaboradores (He *et al*., 2021).

Para além das questões técnicas, órgãos reguladores brasileiros, como a ANPD, têm emitido guias e recomendações voltadas especificamente ao tratamento de dados sensíveis em saúde, orientando instituições quanto à governança, anonimização, avaliação de riscos e justificativas legais para o processamento dessas informações. Em seu Guia Orientativo, é enfatizado que as políticas de segurança devem integrar aspectos tecnológicos e administrativos, destacando a necessidade de capacitação contínua. (Brasil, 2022).

Diante desse panorama marcado por aumento de ataques, custos elevados, mudanças regulatórias e desafios humanos e tecnológicos, observa-se que muitas instituições hospitalares ainda enfrentam dificuldades na estruturação de estratégias integradas de segurança da informação. A literatura aponta lacunas importantes na área de gestão, indicando que a proteção de dados não deve ser compreendida apenas como responsabilidade da área de TI, mas como um eixo estratégico da governança hospitalar (HE *et al*., 2021).

Nesse contexto, emerge o seguinte problema de pesquisa: como as instituições hospitalares podem mitigar riscos cibernéticos e fortalecer a segurança da informação, garantindo a proteção de dados sensíveis, a continuidade dos serviços assistenciais e a conformidade com a LGPD, sob a perspectiva da gestão hospitalar?

Diante desse cenário, este estudo tem como objetivo analisar as evidências científicas, legais e normativas relacionadas à segurança da informação em ambientes hospitalares, com foco na proteção de dados sensíveis e na mitigação de riscos cibernéticos em conformidade com a LGPD, sob a perspectiva da gestão hospitalar.

Além disso, busca identificar os principais indicadores de ataques cibernéticos em ambientes hospitalares, compreender as exigências da LGPD quanto ao tratamento de dados sensíveis e propor estratégias práticas de mitigação de riscos voltadas ao fator humano, à gestão de terceiros e à continuidade dos serviços. Para alcançar esse propósito, o estudo visa mapear os principais riscos e ameaças cibernéticas que afetam o setor hospitalar, tais como ransomware, phishing, falhas humanas, sistemas legados e vulnerabilidades em dispositivos médicos; identificar fragilidades na governança da segurança da informação; compreender o papel do gestor hospitalar na promoção de uma cultura organizacional orientada à proteção de dados e na tomada de decisões estratégicas; e sistematizar práticas e diretrizes aplicáveis à realidade brasileira, integrando evidências científicas, normas legais e relatórios especializados.

Este artigo encontra-se organizado da seguinte forma: na seção introdutória, são apresentadas a contextualização do tema, o problema de pesquisa e os objetivos do estudo. Em seguida, a seção de desenvolvimento aborda os fundamentos teóricos relacionados à segurança da informação em ambientes hospitalares, às exigências

da LGPD e ao cenário de ameaças cibernéticas no setor da saúde. Posteriormente, é descrito o percurso metodológico adotado na pesquisa. Na sequência, são apresentados e discutidos os principais resultados obtidos a partir da revisão integrativa realizada. Por fim, a última seção reúne as considerações finais do estudo, destacando as contribuições, limitações e recomendações para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste estudo está estruturada em seções que abordam os principais aspectos relacionados à segurança da informação em ambientes hospitalares. Inicialmente, discute-se o contexto da segurança da informação no setor da saúde e os desafios associados à proteção de dados sensíveis. Em seguida, são apresentadas as diretrizes da Lei Geral de Proteção de Dados (LGPD) aplicadas ao contexto hospitalar. Por fim, abordam-se as principais estratégias de gestão e mitigação de riscos cibernéticos nas instituições de saúde. Ewoh e Vartiainen (2024) destacam que as organizações de saúde em todo o mundo enfrentam um número crescente de ciberataques que ameaçam infraestruturas críticas, resultando em violação de sistemas de informações em saúde, exposição de dados sensíveis de pacientes e riscos significativos à continuidade dos serviços clínicos, em grande parte devido à interconectividade dos sistemas digitais, à complexidade dos dispositivos e à crescente dependência de tecnologias da informação no cuidado à saúde. Relatórios recentes indicam que o setor de saúde apresenta, de forma recorrente, os maiores custos médios associados a violações de dados, evidenciando impactos financeiros, operacionais e reputacionais significativos para as instituições (IBM Security, 2024).

Estudos científicos também destacam que a rápida digitalização dos serviços de saúde, aliada à presença de sistemas legados, falhas humanas e carência de políticas institucionais robustas, amplia substancialmente a superfície de ataque dos hospitais (HE *et al*., 2021., Kruse *et al*., 2017).

Nesse contexto, a LGPD surge como um marco regulatório fundamental ao impor exigências específicas para o tratamento de dados sensíveis em saúde, demandando das organizações hospitalares não apenas adequação legal, mas também o fortalecimento da governança da informação e da atuação estratégica do gestor hospitalar. Assim, a segurança da informação passa a ser compreendida como um elemento multidimensional, que integra tecnologia, processos organizacionais e fatores humanos, servindo de base para a análise teórica desenvolvida nas subseções a seguir. (ANPD, 2022; Brasil, 2018)

2.1 Segurança da Informação e LGPD na Saúde

A segurança da informação constitui um elemento essencial para o funcionamento adequado das instituições hospitalares, uma vez que estas lidam diariamente com grandes volumes de dados sensíveis, críticos para a continuidade do cuidado e para a tomada de decisões clínicas. Fundamentada nos princípios da confidencialidade, integridade e disponibilidade, conforme estabelecido pelas normas ISO/IEC 27001 e ISO/IEC 27002, a segurança da informação busca assegurar que os dados estejam acessíveis apenas a pessoas autorizadas, permaneçam íntegros ao longo do tempo e disponíveis sempre que necessários para a assistência à saúde. No contexto hospitalar, a violação desses princípios pode resultar não apenas em prejuízos financeiros e legais, mas também em riscos diretos à segurança do paciente,

afetando diagnósticos, tratamentos e a continuidade dos serviços (ISO/IEC, 2022).

Estudos recentes indicam que o setor de saúde apresenta características que o tornam especialmente vulnerável a incidentes de segurança da informação, como a heterogeneidade dos sistemas, a integração de tecnologias antigas com soluções digitais modernas e a necessidade de acesso rápido às informações clínicas por diferentes profissionais. Segundo Kruse *et al*., (2017), hospitais frequentemente operam com sistemas legados que não foram projetados para atender aos padrões atuais de segurança, o que amplia as possibilidades de exploração por agentes maliciosos. Além disso, pesquisas apontam que a pressão assistencial, a sobrecarga de trabalho e a multiplicidade de usuários aumentam a probabilidade de falhas humanas, consideradas um dos principais vetores de incidentes de segurança em ambientes hospitalares (HE *et al*., 2021; Mitnick; Simon, 2002).

Nesse cenário, a LGPD representa um marco regulatório fundamental para a reorganização das práticas de segurança da informação na saúde. A legislação classifica dados referentes à saúde como dados pessoais sensíveis, exigindo salvaguardas técnicas e administrativas mais rigorosas para seu tratamento. A LGPD introduz princípios como finalidade, necessidade, adequação e segurança, que demandam das instituições hospitalares maior controle sobre o ciclo de vida dos dados, desde a coleta até o descarte (Brasil, 2018).

Conforme Doneda (2019), a proteção de dados em saúde envolve uma complexa articulação entre direitos fundamentais, ética profissional e interesses coletivos, o que exige uma abordagem organizacional estruturada. Dados empíricos reforçam a relevância dessas exigências legais. O relatório Cost of a Data Breach Report (2024) aponta que o setor de saúde mantém, pelo 13º ano consecutivo, o maior custo médio global por violação de dados, refletindo despesas relacionadas à interrupção de serviços, recuperação de sistemas, sanções regulatórias e danos reputacionais (IBM Security, 2024). No contexto brasileiro, os impactos são igualmente expressivos, com custos médios por incidente superiores aos de outros setores, o que evidencia a vulnerabilidade das instituições de saúde e a necessidade de investimentos contínuos em segurança da informação (Brasil, 2018).

A Autoridade Nacional de Proteção de Dados (ANPD) também destaca que a conformidade com a LGPD no setor da saúde não se restringe à adoção de ferramentas tecnológicas, mas requer a implementação de políticas institucionais, definição clara de responsabilidades e capacitação contínua dos colaboradores. Em seus guias orientativos, a ANPD enfatiza a importância da governança de dados, da minimização das informações tratadas e do controle rigoroso de acessos, especialmente em ambientes hospitalares, onde múltiplos profissionais necessitam acessar prontuários e sistemas clínicos simultaneamente. Onde a ausência dessas práticas compromete a efetividade da proteção de dados e expõe as instituições a riscos legais e operacionais. (ANPD, 2022).

Dessa forma, a literatura evidencia que a segurança da informação em ambientes hospitalares deve ser compreendida como um processo contínuo e estratégico, integrado à gestão organizacional e às exigências legais, como as previstas na LGPD. Estudos demonstram que a adoção de uma abordagem sistêmica, que articula tecnologia, processos e pessoas, é essencial para fortalecer a resiliência institucional, uma vez que ataques cibernéticos e violações de dados não se restringem a falhas pontuais, mas refletem a falta de governança e preparo

organizacional (Ewoh & Vartiainen, 2024).

Nesse contexto, a atuação do gestor hospitalar torna-se central, pois a liderança institucional influencia diretamente a cultura de segurança, a alocação de recursos, a definição de políticas formais e a implementação de controles técnicos e organizacionais capazes de proteger dados sensíveis sem comprometer a qualidade da assistência prestada (Whitman & Mattord, 2018; Sêmola, 2014). Segundo Santos *et al*. (2025), estratégias efetivas de segurança da informação abrem caminho para práticas sustentáveis que contribuem simultaneamente para a conformidade legal, a continuidade dos serviços de saúde e a proteção da privacidade dos pacientes.

2.2 Cenário de Ameaças no Setor de Saúde

A intensificação da digitalização dos serviços de saúde, impulsionada pela adoção de prontuários eletrônicos, sistemas integrados de gestão hospitalar, telessaúde e dispositivos médicos conectados, ampliou significativamente a superfície de ataque das instituições hospitalares. Esse cenário tem colocado o setor da saúde entre os principais alvos de agentes maliciosos em escala global, em virtude do alto valor dos dados clínicos no mercado ilícito e da criticidade dos serviços prestados. Estudos indicam que ataques cibernéticos a hospitais tendem a gerar impactos mais severos do que em outros setores, pois comprometem diretamente a continuidade assistencial, a segurança do paciente e a confiança da sociedade nas instituições de saúde (HE *et al*., 2021; Kruse *et al*., 2017).

Dados recentes reforçam a gravidade desse cenário. Relatórios internacionais apontam que o setor de saúde permanece, de forma recorrente, entre os mais atacados por crimes cibernéticos, especialmente por ataques de ransomware e campanhas de phishing direcionadas a profissionais da área. O *Cost of a Data Breach Report 2024* indica que as organizações de saúde apresentam os maiores custos médios por violação de dados, refletindo não apenas despesas técnicas de recuperação, mas também perdas operacionais, paralisação de serviços e impactos regulatórios. No contexto brasileiro, o mesmo relatório demonstra que instituições de saúde registram custos superiores à média internacional, o que evidencia fragilidades estruturais e a necessidade de estratégias preventivas mais eficazes (Brasil, 2024; IBM Security, 2024).

Entre as ameaças mais recorrentes, destaca-se o ransomware, considerado atualmente o principal risco cibernético para hospitais. Esse tipo de ataque explora a dependência crítica de sistemas digitais para criptografar dados e interromper operações, exigindo pagamentos de resgate para a restauração dos serviços. A literatura aponta que hospitais são alvos preferenciais desse tipo de ataque devido à urgência do atendimento e à menor tolerância a interrupções prolongadas, o que aumenta a probabilidade de pagamento do resgate (HE *et al*., 2021).

Casos amplamente divulgados demonstram que ataques de ransomware podem resultar no cancelamento de cirurgias, atrasos em diagnósticos e no comprometimento de serviços essenciais, gerando riscos diretos à segurança do paciente. Uma análise abrangente de 374 ataques de ransomware a instituições de saúde nos Estados Unidos, ocorridos entre 2016 e 2021, constatou que 44,4% dos ataques causaram interrupções no atendimento, incluindo desativação de sistemas eletrônicos de saúde (41,7%), cancelamentos ou atrasos em cuidados agendados (10,2%) e desvio de ambulâncias (4,3%), além de prolongadas paralisações

operacionais que podem impactar a continuidade do cuidado clínico e o fluxo de atendimento ao paciente (Neprash *et al*., 2022).

Outra ameaça relevante no cenário hospitalar refere-se à engenharia social e ao phishing, que exploram vulnerabilidades humanas em ambientes de alta pressão e múltiplas demandas. Pesquisas indicam que grande parte dos incidentes de segurança tem origem em falhas humanas, como abertura de e-mails maliciosos, uso de senhas fracas e compartilhamento inadequado de informações sensíveis (Mitnick & Simon, 2002).

Em ambientes hospitalares, a dependência de sistemas digitais para o registro, acesso e gestão de informações clínicas sensíveis torna os processos assistenciais particularmente suscetíveis a incidentes de segurança da informação. Estudos empíricos indicam que ataques cibernéticos, como o ransomware, comprometem o funcionamento rotineiro dos hospitais, afetam a tomada de decisão clínica e colocam em risco a continuidade do cuidado, evidenciando a criticidade da proteção da informação nesse contexto (SINGER et al., 2024).

A literatura mostra que falhas humanas continuam a ser um dos principais fatores contribuintes para incidentes de segurança, muitas vezes desencadeadas por comportamentos inseguros, desconhecimento de práticas adequadas ou respostas inadequadas a tentativas de ataque (Ewoh & Vartiainen, 2024; Aldosari, 2025). Nesse contexto, programas contínuos de conscientização e treinamento em segurança da informação são essenciais não apenas para reforçar boas práticas, mas também para reduzir a probabilidade de incidentes e aprimorar o preparo dos profissionais frente a ameaças emergentes, sempre trabalhar com o letramento digital e capacitação nessa área com os colaboradores, promovendo uma cultura organizacional de proteção e resiliência (Mitnick & Simon, 2002).

Além das ameaças externas, a literatura destaca vulnerabilidades internas relacionadas à infraestrutura tecnológica das instituições de saúde. Sistemas legados, dispositivos médicos conectados sem atualizações regulares e a ausência de segmentação adequada de redes aumentam significativamente o risco de exploração por agentes maliciosos, pois ampliam a superfície de ataque e dificultam a implementação de controles de segurança eficazes. Revisões sistemáticas de cibersegurança em saúde mostram que muitos hospitais dependem de equipamentos e softwares antigos, sem suporte de fabricantes, o que cria pontos de entrada exploráveis por malware e outras ameaças cibernéticas (Ewoh & Vartiainen, 2024).

Estudos sobre a Internet das Coisas (IoMT) também evidenciam que dispositivos médicos conectados frequentemente carecem de mecanismos de atualização automática e proteções robustas, tornando-os alvos fáceis para ataques que podem comprometer funcionalidades críticas, como sistemas de monitoramento e administração de medicamentos (Deb *et al*., 2025).

Anderson (2020) ressalta que muitos equipamentos médicos não foram projetados com requisitos mínimos de segurança e permanecem em operação por longos períodos sem suporte adequado, criando pontos críticos de exposição. Esses fatores evidenciam que o cenário de ameaças no setor de saúde é multifacetado e exige uma abordagem integrada, que considere aspectos tecnológicos, humanos e organizacionais.

Nesse sentido, Whitman e Mattord (2018) destacam que a efetividade da segurança da informação depende do alinhamento entre liderança, processos organizacionais e cultura institucional, reforçando que a atuação do gestor hospitalar é determinante para a mitigação de riscos em ambientes críticos como o hospitalar.

2.3 O Papel do Gestor na Segurança da Informação

A segurança da informação em ambientes hospitalares não deve ser tratada exclusivamente como uma função técnica do setor de tecnologia da informação, mas como um componente estratégico da gestão organizacional. A efetividade das práticas de segurança depende do comprometimento da alta gestão, responsável por estabelecer políticas institucionais, definir prioridades, alocar recursos e fomentar uma cultura organizacional orientada à proteção da informação e dos dados sensíveis (ISO/IEC 27001, 2022). Whitman e Mattord (2018) destacam que a liderança exerce papel central na criação de ambientes organizacionais seguros, uma vez que decisões gerenciais influenciam diretamente o comportamento dos colaboradores e a maturidade dos controles de segurança.

De acordo com Sêmola (2014), no contexto hospitalar, o gestor assume responsabilidades ampliadas, pois lida com informações altamente sensíveis e com serviços essenciais à vida humana. Onde é indicado que instituições que contam com estruturas formais de governança da segurança da informação, como comitês multidisciplinares, definição clara de papéis e processos decisórios documentados, apresentam maior capacidade de prevenção e resposta a incidentes cibernéticos. A atuação do gestor hospitalar inclui, portanto, a integração entre áreas assistenciais, administrativas e tecnológicas, garantindo que a segurança da informação esteja alinhada aos objetivos estratégicos da instituição e à qualidade do atendimento prestado.

A LGPD reforça ainda mais o papel estratégico do gestor ao estabelecer obrigações relacionadas à governança e à responsabilização das organizações pelo tratamento de dados pessoais. A legislação introduz conceitos como prestação de contas, que exige das instituições a demonstração de medidas eficazes de segurança e conformidade. Nesse sentido, cabe ao gestor hospitalar assegurar a implementação de políticas internas, a designação de responsáveis pelo tratamento de dados, como o encarregado de dados (DPO), e a supervisão das práticas adotadas por colaboradores e terceiros. A ausência dessa atuação gerencial pode resultar em sanções administrativas, danos reputacionais e impactos financeiros significativos (Brasil, 2018; Brasil, 2022).

Outro aspecto relevante do papel do gestor está relacionado à gestão do fator humano, reconhecido pela literatura como um dos principais pontos de vulnerabilidade em segurança da informação. Pesquisas indicam que falhas humanas continuam sendo responsáveis por grande parte dos incidentes de segurança, especialmente em ambientes complexos e de alta pressão, como os hospitais. Nesse contexto, o gestor hospitalar deve promover programas contínuos de capacitação, campanhas de conscientização e treinamentos específicos, capazes de sensibilizar os profissionais de saúde quanto à importância da proteção de dados e ao uso seguro dos sistemas de informação. (Mitnick; Simon, 2002).

Além disso, o gestor hospitalar desempenha papel fundamental na gestão de riscos e na tomada de decisões estratégicas relacionadas à segurança da informação,

onde a literatura aponta que a identificação, avaliação e priorização de riscos cibernéticos devem fazer parte do planejamento institucional, permitindo a adoção de medidas preventivas e corretivas adequadas à realidade organizacional. Essa abordagem possibilita que a segurança da informação seja incorporada aos processos decisórios, contribuindo para a sustentabilidade da instituição e para a continuidade dos serviços assistenciais mesmo diante de incidentes (Sêmola, 2014).

Por fim, destaca-se que o gestor hospitalar também é responsável por assegurar a integração da segurança da informação aos planos de continuidade de negócios e de resposta a incidentes. Normas internacionais, como a ISO 22301, enfatizam que organizações críticas devem manter capacidade de operar em níveis aceitáveis durante eventos disruptivos, o que, no ambiente hospitalar, significa garantir a continuidade do cuidado ao paciente mesmo em situações de falhas sistêmicas ou ataques cibernéticos. Assim, a atuação do gestor na segurança da informação transcende a prevenção de incidentes, abrangendo também a resiliência organizacional e a proteção da assistência à saúde. (ISO, 2019).

2.4 Estratégias de Mitigação e Boas Práticas

Diante do aumento expressivo de incidentes cibernéticos no setor de saúde, a literatura evidencia que estratégias de mitigação devem ser baseadas em dados concretos e integradas à gestão hospitalar. Estudos empíricos apontam que organizações que adotam abordagens preventivas estruturadas incluindo prevenção tecnológica, capacitação de pessoal e políticas institucionais conseguem reduzir vulnerabilidades e fortalecer a resiliência organizacional, minimizando impactos de incidentes de segurança da informação (Rahim *et al*., 2024).

De acordo com o *Cost of a Data Breach Report 2024*, instituições que possuem estratégias maduras de segurança, com políticas definidas e planos de resposta, apresentam redução média de até 35% nos custos totais de uma violação de dados quando comparadas àquelas sem tais práticas, esses dados demonstram que a mitigação de riscos não é apenas uma exigência legal, mas também uma decisão estratégica de gestão. (IBM Security, 2024).

No que se refere ao fator humano, dados empíricos apontam que esse continua sendo um dos principais vetores de incidentes cibernéticos. Estudos indicam que aproximadamente 74% das violações de dados envolvem algum tipo de falha humana, como engenharia social, uso inadequado de credenciais ou erros operacionais (IBM Security, 2024). Em ambientes hospitalares, esse percentual torna-se ainda mais crítico devido à sobrecarga de trabalho e à necessidade de acesso rápido às informações clínicas. Pesquisas demonstram que programas contínuos de treinamento e conscientização podem reduzir em até 45% a taxa de sucesso de ataques de phishing, reforçando a importância de investimentos sistemáticos em capacitação de profissionais de saúde (HE *et al*., 2021).

Outra estratégia amplamente respaldada por dados refere-se à implementação de políticas institucionais formais de segurança da informação. Estudos comparativos apontam que organizações de saúde que possuem políticas documentadas de controle de acesso, uso de sistemas e classificação da informação apresentam níveis significativamente mais elevados de maturidade em segurança, além de menor incidência de incidentes reportados (Sêmola, 2014). A Autoridade Nacional de Proteção de Dados destaca que a ausência dessas políticas dificulta a comprovação

de conformidade com a LGPD e amplia o risco de sanções administrativas, que podem chegar a até 2% do faturamento da organização, limitadas a 50 milhões por infração (ANPD, 2022; Brasil, 2018).

A adoção de checklists operacionais e rotinas de monitoramento contínuo também é sustentada por evidências empíricas. Segundo Whitman e Mattord (2018), a utilização sistemática de checklists reduz falhas operacionais recorrentes e contribui para a padronização de processos críticos de segurança. Relatórios indicam que hospitais que realizam verificações periódicas de atualização de sistemas, testes de backup e revisão de acessos conseguem reduzir em até 27% o tempo médio de detecção de incidentes, fator considerado decisivo para a minimização de impactos (IBM Security, 2024). Esses dados reforçam a importância de instrumentos simples; porém eficazes, no contexto da gestão hospitalar.

No âmbito da resposta a incidentes, dados demonstram que instituições que possuem planos formais e testados apresentam desempenho significativamente superior durante crises cibernéticas. O *Cost of a Data Breach Report 2024* aponta que organizações com planos de resposta a incidentes testados regularmente reduzem, em média, 54 dias no tempo de contenção de uma violação de dados. Em hospitais, essa redução é particularmente relevante, pois impacta diretamente a continuidade assistencial e a segurança do paciente. Normas internacionais, como a ISO 22301, reforçam que a capacidade de resposta rápida e organizada é essencial para manter operações críticas durante eventos disruptivos (ISO, 2019).

Por fim, os dados analisados indicam que estratégias de mitigação devem estar integradas aos planos de continuidade de negócios das instituições hospitalares. Relatórios internacionais mostram que organizações que realizam testes periódicos de seus planos de contingência apresentam maior resiliência operacional e menor probabilidade de paralisação total dos serviços durante incidentes cibernéticos (IBM Security, 2024). A literatura destaca que a segurança da informação deve ser tratada como um processo contínuo, sujeito a revisões e aprimoramentos constantes, acompanhando a evolução das ameaças e das tecnologias utilizadas na saúde. Dessa forma, a adoção de estratégias baseadas em dados fortalece a governança hospitalar, assegura a conformidade com a LGPD e contribui para a sustentabilidade institucional. (Sêmola, 2014; Whitman; Mattord, 2018).

2.5 Consolidação Fundamentação Teórica

A análise da literatura científica, normativa e legal evidencia que a segurança da informação em ambientes hospitalares constitui um desafio crescente, impulsionado pela intensificação da digitalização dos serviços de saúde e pelo aumento expressivo de ameaças cibernéticas direcionadas ao setor. Os dados apresentados ao longo da fundamentação teórica demonstram que instituições de saúde figuram, de forma recorrente, entre as mais impactadas por incidentes de segurança, tanto em termos financeiros quanto operacionais, registrando os maiores custos médios por violação de dados quando comparadas a outros setores econômicos, esse cenário reforça que a proteção da informação em saúde não se limita à preservação da privacidade, mas envolve diretamente a continuidade assistencial e a segurança do paciente. (IBM Security, 2024).

Os estudos analisados também indicam que a vulnerabilidade do setor hospitalar decorre de múltiplos fatores interdependentes, como a presença de

sistemas legados, a utilização de dispositivos médicos conectados sem atualizações adequadas e a predominância do fator humano como vetor de incidentes. Evidências empíricas apontam que falhas humanas estão associadas a grande parte das violações de dados, especialmente em contextos organizacionais caracterizados por alta pressão e complexidade operacional, como os hospitais. Esses achados reforçam a necessidade de abordagens integradas que considerem não apenas aspectos tecnológicos, mas também organizacionais e comportamentais. (Mitnick; Simon, 2002; HE *et al*., 2021).

No âmbito regulatório, a LGPD emerge como um elemento estruturante da governança da informação em saúde, ao impor obrigações específicas para o tratamento de dados sensíveis e exigir das instituições a adoção de medidas técnicas e administrativas capazes de demonstrar conformidade. A literatura evidencia que a adequação à LGPD ultrapassa o cumprimento formal da legislação, demandando o fortalecimento da governança, a definição clara de responsabilidades e a atuação estratégica da gestão hospitalar na condução das práticas de segurança. A ausência dessas estruturas amplia o risco de sanções administrativas e de danos reputacionais, além de comprometer a sustentabilidade institucional (ANPD, 2022; Brasil, 2018).

Os dados apresentados também demonstram que a adoção de estratégias de mitigação baseadas em evidências contribui de forma significativa para a redução de impactos decorrentes de incidentes cibernéticos. Instituições que implementam políticas formais, treinamentos contínuos, checklists operacionais e planos de resposta a incidentes testados apresentam melhor desempenho na detecção, contenção e recuperação de eventos de segurança, reduzindo custos, tempo de indisponibilidade e prejuízos assistenciais, mostrando a importância de tratar a segurança da informação como um processo contínuo e integrado à gestão hospitalar (Whitman; Mattord, 2018; IBM Security, 2024).

Dessa forma, a síntese da fundamentação teórica demonstra que a segurança da informação em hospitais deve ser compreendida como uma responsabilidade multidimensional, que articula tecnologia, processos organizacionais, pessoas e governança, não se limitando a respostas reativas a incidentes isolados, mas demandando ações contínuas e estratégicas. Evidências empíricas recentes mostram que ataques cibernéticos, como os de ransomware que vêm crescendo em frequência e sofisticação, causam interrupções nos sistemas eletrônicos de saúde, cancelamento de atendimentos e deslocamentos de ambulâncias, impactando diretamente a continuidade assistencial e potencialmente a segurança dos pacientes, o que reforça a necessidade de uma abordagem integrada de segurança organizacional (Neprash *et al*., 2022).

A dimensão organizacional da segurança da informação também está associada ao aumento da exposição de dados sensíveis (como registros eletrônicos de saúde) e à complexidade de gestão desses ativos, que cresce à medida que mais dispositivos conectados compõem o ecossistema hospitalar (Ewoh; Vartiainen, 2024; Dzamesi; Elsayed, 2025). Nesse contexto, a atuação do gestor hospitalar destaca-se como elemento central para a efetividade das práticas de segurança, pois é por meio da liderança, da tomada de decisão estratégica, do desenvolvimento de políticas institucionais e do alinhamento entre áreas assistenciais, administrativas e tecnológicas que se torna possível mitigar riscos cibernéticos, atender às exigências

legais como as impostas pela LGPD e garantir a continuidade do cuidado em ambientes de saúde cada vez mais digitalizados. Essa base teórica sustenta a análise metodológica e a discussão dos resultados apresentados nas seções seguintes deste estudo.

3 METODOLOGIA

O presente estudo adota o método de revisão integrativa da literatura, cuja finalidade é reunir, analisar e sintetizar o conhecimento científico previamente produzido acerca do tema investigado, permitindo a identificação de evidências relevantes e a ampliação da compreensão teórica sobre o objeto de estudo. Esse método possibilita a avaliação crítica e a integração de diferentes achados científicos, contribuindo para o desenvolvimento e aprofundamento da temática analisada (Mendes; Silveira; Galvão, 2010).

A escolha desse método justifica-se pela necessidade de consolidar produções científicas, legais e institucionais relacionadas à segurança da informação em ambientes hospitalares, considerando os riscos cibernéticos, as exigências da Lei Geral de Proteção de Dados (LGPD) e o papel da gestão hospitalar na mitigação desses riscos. Além disso, a revisão integrativa é amplamente empregada nas áreas da saúde e da gestão por permitir a incorporação de múltiplas perspectivas teóricas e metodológicas, aspecto particularmente relevante diante da natureza multidimensional do fenômeno investigado.

A condução metodológica do estudo seguiu as seis etapas da revisão integrativa propostas por Mendes, Silveira e Galvão (2010), assegurando rigor científico, transparência e reprodutibilidade ao processo de pesquisa. Inicialmente, realizou-se a elaboração da questão norteadora do estudo, definindo o foco da investigação sobre segurança da informação em ambientes hospitalares. Em seguida, procedeu-se à amostragem por meio da busca sistemática de estudos primários nas bases de dados selecionadas, utilizando descritores controlados e termos alternativos relacionados ao tema. Na terceira etapa, foi realizada a extração dos dados dos estudos incluídos, contemplando informações relevantes para a caracterização das produções científicas. Posteriormente, realizou-se a avaliação crítica dos estudos primários, considerando critérios metodológicos e a relevância para o objetivo da pesquisa. Na quinta etapa, desenvolveu-se a análise e síntese dos resultados, permitindo a integração das evidências encontradas e a identificação dos principais achados sobre riscos cibernéticos, proteção de dados sensíveis e conformidade com a legislação vigente. Por fim, procedeu-se à apresentação do trabalho final, organizando os achados de forma sistemática e estruturada.

3.1 ETAPA 1: Elaboração da questão de pesquisa

Na primeira etapa, definiu-se como tema central a gestão da segurança da informação em ambientes hospitalares, diante do aumento de incidentes cibernéticos e da necessidade de adequação às exigências legais da LGPD. A partir dessa delimitação temática, formulou-se a seguinte questão de pesquisa:

Quais evidências científicas existem sobre estratégias de gestão da segurança da informação adotadas por hospitais para mitigar riscos cibernéticos, atender às exigências da LGPD e garantir a continuidade dos serviços de saúde?

Essa questão orientou todo o processo de busca, seleção, análise e síntese dos estudos incluídos na revisão.

3.2 ETAPA 2: Amostragem ou busca na literatura dos estudos primários

A segunda etapa consistiu na definição da estratégia de busca e na identificação dos estudos nas bases de dados selecionadas, bem como no estabelecimento dos critérios de inclusão e exclusão. A busca foi realizada em bases de dados reconhecidas pela relevância científica nas áreas da saúde, gestão e tecnologia da informação, sendo elas: PubMed, Scopus, Web of Science e LILACS.

Para a estratégia de busca, foram utilizados descritores controlados e termos alternativos relacionados ao tema do estudo. Como descritores exatos, destacam-se: segurança da informação, hospitais e dados sensíveis. Como termos alternativos ou complementares, foram utilizados: cibersegurança, LGPD, gestão hospitalar, riscos cibernéticos, ransomware e continuidade dos serviços, com o objetivo de ampliar a sensibilidade da busca e identificar estudos relevantes sobre segurança da informação em ambientes hospitalares. Os termos foram combinados

por meio dos operadores booleanos AND e OR, nos idiomas português e inglês. O recorte temporal estabelecido compreendeu o período de 2010 a 2025, considerando a intensificação da digitalização dos serviços de saúde e a consolidação do marco regulatório brasileiro de proteção de dados, especialmente a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que estabeleceu diretrizes para o tratamento e a proteção de dados pessoais no Brasil, incluindo dados sensíveis relacionados à saúde.

Os critérios de inclusão para seleção dos artigos foram: artigos científicos disponíveis na íntegra, publicações nos idiomas português e inglês, estudos publicados entre 2010 e 2025, pesquisas que abordassem segurança da informação, proteção de dados, cibersegurança ou gestão de riscos em ambientes hospitalares, documentos normativos, legislações e relatórios técnicos relevantes para o contexto da saúde. Como critérios de exclusão concontram-se os estudos duplicados, publicações fora do recorte temporal, artigos sem relação com o ambiente hospitalar e trabalhos com abordagem estritamente técnica, sem análise organizacional ou gerencial.

A utilização da estratégia de busca construída resultou na identificação inicial de 126 estudos (Quadro 1), distribuídos da seguinte forma: PubMed (38), Scopus (32), Web of Science (24), SciELO (18) e LILACS (14). Todos os registros foram importados para a plataforma Rayyan onde se organizou uma planilha eletrônica para controle, identificação de duplicatas e apoio à triagem inicial.

Quadro 01: Bases de dados, estratégias de busca e resultado de artigos encontrados. Abreu e Lima, Pernambuco, 2025.

FONTES DE INFORMAÇÃO	ESTRATÉGIA DE BUSCA	RESULTADOS
PubMed	("information security" OR cybersecurity) AND (hospitals OR "healthcare organizations") AND ("data protection" OR "sensitive data")	38

Scopus	("information security" OR cybersecurity OR "cyber risks") AND ("hospital management" OR hospitals) AND (LGPD OR "data protection law")	32
Web of Science	("cybersecurity" AND hospitals) AND ("information governance" OR "risk management")	24
SciELO	("segurança da informação" OR cibersegurança) AND (hospitais OR "gestão hospitalar") AND (LGPD)	18
LILACS	("segurança da informação" AND saúde) AND (hospitais) AND ("proteção de dados")	14

Fonte: Elaborado pelo autor (2025).

O processo de análise dos dados ocorreu inicialmente por meio de leitura textual exploratória, com o objetivo de aprofundar a compreensão dos conteúdos selecionados e identificar os principais núcleos de sentido presentes nos estudos analisados. Essa etapa possibilitou o reconhecimento e a delimitação de enunciados relevantes relacionados à segurança da informação em ambientes hospitalares, à proteção de dados sensíveis e à conformidade com a LGPD.

A partir dessa leitura, os enunciados identificados foram organizados e agrupados de forma sistemática, permitindo o agrupamento por afinidade das informações e a produção de textos analíticos que integraram descrição e interpretação dos achados. A análise fundamentou-se na construção de um sistema de categorias, aplicado ao corpus da pesquisa, entendido como o conjunto de estudos científicos e documentos normativos selecionados, os quais expressam diferentes perspectivas teóricas e contextuais sobre o fenômeno investigado, conforme proposto por Moraes (2003).

Posteriormente às buscas, procedeu-se à seleção dos estudos primários, em consonância com a questão de pesquisa e os critérios de inclusão e exclusão previamente definidos. Todos os registros foram importados para a plataforma Rayyan, utilizada para o gerenciamento das referências e identificação de duplicatas.

Nessa etapa, foram identificados e removidos 34 registros duplicados, resultando em 92 estudos únicos para a fase de triagem. Em seguida, realizou-se a leitura e análise dos títulos e resumos, o que resultou na exclusão de 51 estudos por não apresentarem aderência à temática da segurança da informação, da proteção de dados pessoais ou da gestão de riscos cibernéticos em ambientes hospitalares.

Assim, 41 estudos foram selecionados para a etapa de leitura do texto completo. Após a análise na íntegra, 31 publicações foram excluídas por não atenderem plenamente aos critérios de inclusão, seja por não contemplarem o

contexto hospitalar, por abordarem a temática de forma superficial ou por não responderem diretamente à questão de pesquisa.

Dessa forma, a amostra final foi constituída por dez estudos, os quais atenderam integralmente aos critérios metodológicos estabelecidos e apresentaram contribuições relevantes para a compreensão dos desafios relacionados à segurança da informação, à conformidade com a Lei Geral de Proteção de Dados e às estratégias de mitigação de riscos cibernéticos em ambientes hospitalares. O processo de seleção dos estudos é apresentado no **Quadro 02** e na **Figura 01**.

Durante a análise dos títulos e resumos, observou-se que os estudos excluídos concentravam-se, majoritariamente, em temáticas não alinhadas ao escopo desta revisão, tais como pesquisas voltadas exclusivamente à segurança da informação em setores não relacionados à saúde, estudos de caráter estritamente técnico sem interface com a gestão hospitalar, investigações focadas em proteção de dados fora do contexto organizacional e publicações que não abordavam aspectos legais ou normativos, como a LGPD.

Na etapa de leitura do texto completo, os 10 estudos selecionados atenderam aos critérios de inclusão propostos na metodologia deste trabalho, sendo considerados adequados para compor a amostra final, uma vez que responderam de forma consistente à questão norteadora desta revisão integrativa.

Quadro 02: Processo de seleção. Abreu e Lima, Pernambuco, 2025.

Fontes de informação	Artigos encontrados	Artigos selecionados
PubMed	38	3
Scopus	32	3
Web of Science	24	2
SciELO	18	1
LILACS	14	1
TOTAL	**126**	**10**

Fonte: Elaborado pelo autor (2025).

O **Quadro 03** apresenta a síntese dos principais achados, conforme descrito a seguir:

Quadro 03: Instrumento de coleta de dados 1: Apresentação da síntese dos artigos incluídos na Revisão Integrativa: Identificação do estudo, autores, fontes de informação e periódicos. Abreu e Lima/PE, 2025

Nº	Identificação do estudo	Autores	Fontes de informação	Periódicos
1	Cybersecurity in healthcare: a systematic review of modern threats and trends	Kruse et al.	PubMed	Technology and Health Care

2	Health care cybersecurity challenges and solutions under the climate of COVID-19: a scoping review	He et al.	PubMed	Journal of Medical Internet Research
3	Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021	Neprash et al.	Web of Science	JAMA Health Forum
4	Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review	Ewoh & Vartiainen	Scopus	Journal of Medical Internet Research
5	Cybersecurity in healthcare: new threat to patient safety	Aldosari	Scopus	Cureus
6	LGPD e serviços de saúde pública: desafios da implementação da Lei Geral de Proteção de Dados em hospitais públicos	Gonçalves & Werner	SciELO	Revista do CAAP
7	Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023	Santos et al.	SciELO	Physis

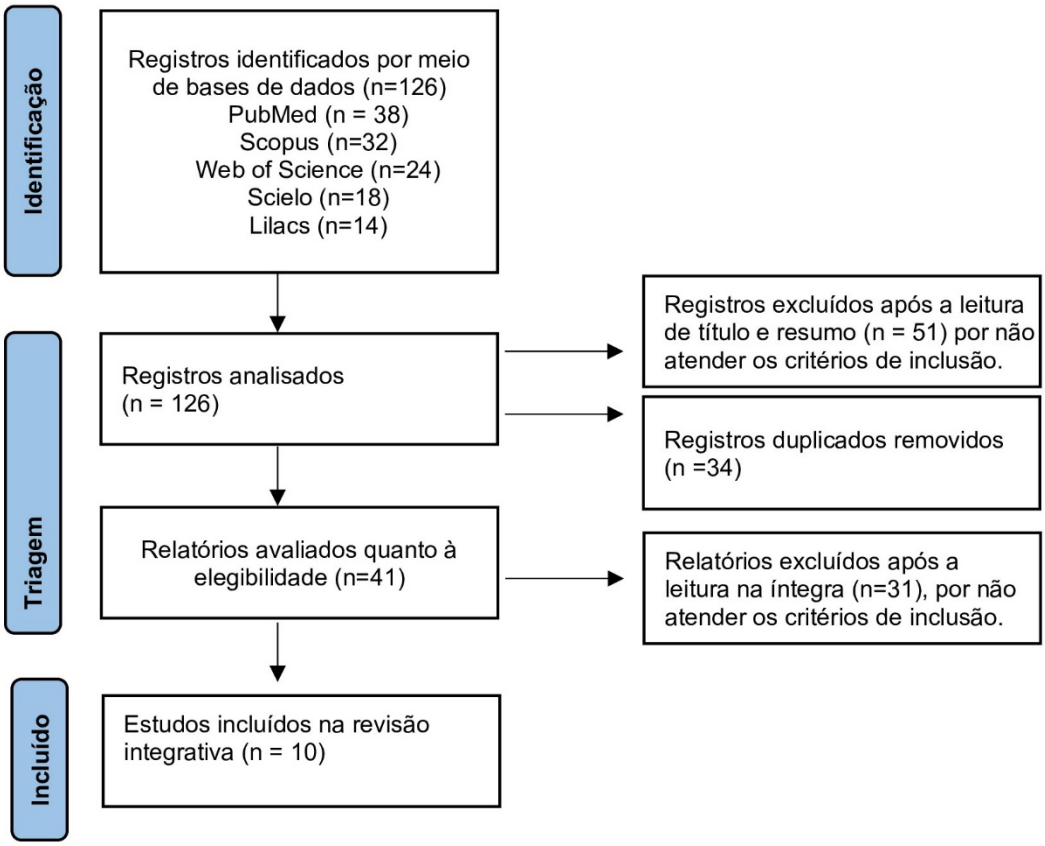
8	O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD	Petry & Hupffer	LILACS	Revista CNJ
9	Securing the Internet of Medical Things (IoMT): real-world attack taxonomy and practical security measures	Deb et al.	Web of Science	arXiv
10	A review on the security vulnerabilities of the IoMT against malware attacks and DDoS	Dzamesi & Elsayed	Scopus	arXiv

Fonte: Elaborado pelo autor (2025).

Após a aplicação das estratégias de busca e dos critérios de seleção previamente definidos, obteve-se uma amostra final composta por 10 estudos, considerados relevantes para a análise da segurança da informação em ambientes hospitalares no contexto da proteção de dados sensíveis e da conformidade com a Lei Geral de Proteção de Dados. A caracterização dos estudos selecionados é apresentada no **Quadro 2**, que sintetiza informações como autores, ano de publicação, objetivos e principais contribuições das pesquisas analisadas. Para a composição da amostra, foram adotados como critérios de inclusão estudos publicados dentro do recorte temporal estabelecido, disponíveis na íntegra e que abordassem aspectos relacionados à segurança da informação, proteção de dados sensíveis, riscos cibernéticos ou à aplicação da legislação de proteção de dados no contexto da saúde e da gestão hospitalar. Foram excluídos estudos duplicados, publicações que não apresentavam relação direta com o tema da pesquisa, documentos incompletos e trabalhos que não abordavam especificamente a segurança da informação ou a proteção de dados em ambientes de saúde. O processo de identificação, seleção e inclusão dos estudos foi conduzido de forma sistemática, seguindo as recomendações do PRISMA – Preferred Reporting Items for Systematic Reviews and Meta-Analyses, com o objetivo de assegurar transparência, rastreabilidade e rigor metodológico na condução da revisão integrativa, sendo o fluxo dessas etapas apresentado na figura correspondente ao fluxograma do método. A **Figura 1** apresentada a seguir mostra o fluxograma PRISMA, que descreve as etapas de identificação dos registros nas bases de dados, remoção de duplicatas, triagem por título e resumo, avaliação dos textos completos

e definição final dos estudos incluídos na análise. Esse procedimento possibilitou a organização do processo de seleção dos estudos e a justificativa das exclusões realizadas em cada etapa, contribuindo para a confiabilidade e a reprodutibilidade dos resultados obtidos.

Figura 1: Fluxograma do processo de seleção dos estudos incluídos na revisão integrativa.



Fonte: PRISMA (2020), adaptado pelo autor (2025).

3.3 ETAPA 3: Extração dos dados dos estudos selecionados.

Após a seleção dos estudos que atenderam aos critérios de inclusão, procedeu-se à definição das informações a serem extraídas dos 10 estudos que compuseram a amostra final desta revisão integrativa. Essa etapa teve como objetivo sistematizar os dados relevantes para responder à questão norteadora da pesquisa e subsidiar a análise crítica dos achados.

Para a organização, análise e posterior síntese das informações, foram elaborados pelo próprio autor dois instrumentos de coleta de dados, estruturados de forma a contemplar os aspectos descritivos dos estudos selecionados. O **Instrumento 01** contemplou a identificação dos estudos, incluindo autores, fonte de informação, periódico e ano de publicação, conforme apresentado no **Quadro 03**, deste trabalho. O **Quadro 06** abrangeu informações relacionadas aos objetivos, ao método adotado, à amostra ou objeto de estudo, aos principais resultados e à categoria temática atribuída a cada estudo.

Após a seleção dos estudos, procedeu-se à organização do corpus de

análise, composto pelos artigos incluídos na revisão. Inicialmente, foi realizada a leitura flutuante dos textos na íntegra, com o objetivo de identificar aspectos recorrentes relacionados à segurança da informação em ambientes hospitalares. Em seguida, aplicou-se a análise temática de conteúdo, realizada de forma sistemática por meio da codificação dos trechos relevantes, agrupamento por similaridade de sentido e identificação de padrões de convergência entre os estudos.

ETAPA 4: Avaliação dos estudos primários

Realizou-se uma análise crítica e sistemática dos estudos selecionados, considerando os aspectos metodológicos, os objetivos propostos e a convergência ou divergência dos resultados apresentados. Essa avaliação foi conduzida de forma minuciosa, buscando compreender possíveis diferenças ou resultados conflitantes entre os estudos, à luz das abordagens metodológicas adotadas e do contexto em que foram desenvolvidos.

A análise dos estudos permitiu identificar padrões, lacunas e complementaridades entre os achados relacionados à segurança da informação, à proteção de dados pessoais e à gestão de riscos cibernéticos em ambientes hospitalares. A avaliação detalhada dos estudos e a síntese crítica dos resultados encontram-se apresentadas na **seção 04** deste trabalho.

3.4 ETAPA 5: Análise e síntese dos resultados

A análise e a interpretação dos resultados foram conduzidas à luz da literatura científica selecionada, conforme orientam Minayo (2010), ao destacar que a pesquisa qualitativa busca compreender fenômenos complexos a partir da interpretação crítica dos dados e de seus significados no contexto em que se inserem. Nesse sentido, procedeu-se à discussão dos principais achados desta revisão integrativa, considerando os referenciais teóricos e normativos que fundamentam a segurança da informação e a proteção de dados pessoais na assistência à saúde.

A avaliação crítica dos estudos permitiu identificar convergências, divergências e lacunas de conhecimento, conforme preconizado por Whittemore e Knafl (2005) e Mendes, Silveira e Galvão (2008), que ressaltam que a revisão integrativa possibilita a comparação de diferentes abordagens metodológicas e perspectivas teóricas, favorecendo uma compreensão ampliada do estado do conhecimento sobre determinado fenômeno. Dessa forma, os resultados foram organizados a partir da análise comparativa dos estudos incluídos, considerando as temáticas investigadas e sua relação com o objeto de pesquisa proposto.

Esse processo analítico possibilitou compreender o panorama atual da produção científica acerca da segurança da informação em ambientes hospitalares, evidenciando não apenas os avanços relacionados à adoção de tecnologias digitais na saúde, mas também os impactos organizacionais, assistenciais e legais decorrentes da exposição a riscos cibernéticos e do tratamento inadequado de dados sensíveis. Conforme destaca Sêmola (2014), tais impactos extrapolam o âmbito técnico, atingindo dimensões estratégicas da gestão hospitalar e exigindo abordagens integradas de governança e gestão de riscos.

A revisão integrativa evidenciou, ainda, que, embora haja crescimento no número de publicações sobre cibersegurança em saúde, persistem lacunas relevantes, especialmente no que se refere à integração entre aspectos técnicos, organizacionais e regulatórios, bem como à efetiva implementação de políticas de segurança da informação alinhadas à Lei Geral de Proteção de Dados Pessoais

(LGPD) no contexto hospitalar. Observa-se, também, a necessidade de maior aprofundamento em estudos que abordem a capacitação contínua dos profissionais de saúde e gestores hospitalares quanto às boas práticas de segurança da informação, aspecto considerado essencial para a efetividade das medidas de proteção (Minayo, 2010; Sêmola, 2014).

Apesar dos avanços identificados, os estudos analisados demonstram que a segurança da informação em ambientes hospitalares permanece como um desafio complexo e multifatorial, exigindo investimentos contínuos em governança, gestão de riscos, conscientização dos profissionais e adoção de normas e frameworks reconhecidos, como os sistemas de gestão da segurança da informação. Nesse contexto, reforça-se a importância do fortalecimento do papel da gestão hospitalar na promoção de uma cultura organizacional voltada à proteção de dados e à continuidade dos serviços de saúde, contribuindo diretamente para a segurança do paciente e para a confiabilidade das informações utilizadas na assistência.

O **Quadro 04** a seguir sintetiza as convergências, divergências e lacunas de conhecimento identificadas entre os autores analisados, oferecendo uma visão integrada dos principais achados da literatura e subsidiando a compreensão crítica dos resultados desta revisão integrativa.

Quadro 04 – Convergências, divergências e lacunas do conhecimento entre os autores selecionados

Eixo de análise	**Convergências entre os autores**	**Divergências identificadas**	**Lacunas do conhecimento**
Segurança da informação em saúde	Os autores convergem ao reconhecer que o setor da saúde apresenta elevada vulnerabilidade a incidentes cibernéticos, em razão da sensibilidade dos dados, da criticidade dos serviços e da crescente dependência de sistemas digitais.	Alguns autores enfatizam mais os aspectos técnicos das ameaças, enquanto outros priorizam dimensões organizacionais, regulatórias e gerenciais da segurança da informação.	Escassez de estudos empíricos que integrem, de forma sistemática, dimensões técnicas, organizacionais e regulatórias no contexto hospitalar.

Governança e papel da gestão	Há consenso de que a segurança da informação não é apenas uma responsabilidade técnica, mas um elemento estratégico que depende do comprometimento da alta gestão e de estruturas formais de governança.	Parte da literatura aborda a governança de forma normativa ou conceitual, enquanto outros estudos discutem sua aplicação prática em contextos específicos.	Falta de investigações que avaliem a efetividade real das estruturas de governança da segurança da informação em hospitais brasileiros.
Gestão de riscos cibernéticos	Os autores concordam que a identificação, avaliação e mitigação de riscos cibernéticos devem integrar o planejamento institucional para garantir continuidade dos serviços e segurança do paciente.	Divergem quanto ao nível de maturidade das práticas de gestão de riscos, variando entre recomendações gerais e modelos mais estruturados.	Necessidade de estudos quantitativos que mensurem o impacto da gestão de riscos na redução de incidentes e prejuízos operacionais em hospitais.
Aspectos técnicos e sistemas legados	Reconhecimento comum de que sistemas legados e dispositivos médicos antigos representam pontos críticos de vulnerabilidade à segurança da informação.	Alguns estudos tratam os sistemas legados como problema central, enquanto outros os analisam como parte de um conjunto mais amplo de riscos organizacionais.	Carência de pesquisas aplicadas sobre estratégias viáveis de modernização tecnológica e mitigação de riscos em ambientes hospitalares com restrições orçamentárias.

Capacitação e fator humano	Convergência quanto à importância da conscientização e capacitação contínua dos profissionais de saúde e gestores para a efetividade das práticas de segurança da informação.	Diferentes níveis de aprofundamento são observados quanto às metodologias de capacitação e avaliação de sua eficácia.	Escassez de estudos que avaliem, de forma sistemática, os efeitos da capacitação em segurança da informação na redução de incidentes causados por falhas humanas.
Regulamentação e LGPD	Os autores reconhecem a relevância dos marcos regulatórios, especialmente da LGPD, como indutores de práticas de segurança e proteção de dados em saúde.	Parte da literatura foca na análise normativa, enquanto outros estudos discutem desafios práticos de implementação nos serviços de saúde.	Poucos estudos analisam a implementação efetiva da LGPD em hospitais e seus impactos organizacionais e assistenciais.

Fonte: Elaborado pelo autor (2025).

3.5 ETAPA 6: Apresentação do trabalho final

Como etapa final desta revisão integrativa, procedeu-se à síntese do conhecimento produzido, a partir da análise crítica e integrada das evidências disponíveis nos estudos selecionados. Essa síntese teve como finalidade organizar e sistematizar os principais achados relacionados à segurança da informação, à proteção de dados pessoais e à gestão de riscos cibernéticos em ambientes hospitalares.

Com o objetivo de sistematizar e organizar os achados desta revisão integrativa, foram elaborados quadros de síntese que reúnem as principais informações extraídas dos estudos selecionados. Esses quadros possibilitam uma visão comparativa dos artigos incluídos, favorecendo a compreensão das características metodológicas, dos objetivos, dos resultados e das categorias temáticas emergentes.

Os resultados obtidos foram consolidados de forma descritiva e, permitindo a integração das evidências e a identificação dos principais desafios, impactos e estratégias de mitigação abordados na literatura. A apresentação dos achados foi realizada por meio de quadros síntese para caracterização dos estudos incluídos, categorização temática dos conteúdos analisados e descrição interpretativa dos resultados, além da utilização de figura ilustrativa do fluxo de seleção dos estudos. A síntese do conhecimento resultante deste processo é apresentada na seção de Resultados, na qual os achados são discutidos à luz do referencial teórico e do objetivo proposto para o estudo.

4 RESULTADOS E ANÁLISE

Os resultados desta revisão integrativa foram obtidos a partir da análise aprofundada dos 10 estudos selecionados na amostra final, os quais atenderam integralmente aos critérios metodológicos definidos. A leitura permitiu identificar padrões recorrentes, convergências temáticas e lacunas relevantes relacionadas à gestão da segurança da informação em ambientes hospitalares, aos desafios impostos pela Lei Geral de Proteção de Dados (LGPD) e às estratégias de mitigação de riscos cibernéticos.

De modo geral, os estudos analisados evidenciam que a segurança da informação em hospitais é um fenômeno multidimensional, influenciado por fatores legais, tecnológicos, organizacionais e humanos. Observou-se que, embora haja consenso quanto à relevância da proteção de dados sensíveis na saúde, persistem dificuldades significativas na implementação prática de medidas integradas de segurança, especialmente sob a perspectiva da gestão hospitalar.

Esse processo permitiu a construção de núcleos temáticos interpretativos, que subsidiaram a síntese e a organização dos resultados da revisão integrativa.

As categorias temáticas identificadas foram:

Quadro 05: Categorias e números de identificação. Abreu e Lima, Pernambuco 2025.

Número de identificação	Categoria
I	Exigências da LGPD e governança da informação
II	Principais riscos e ameaças cibernéticas em hospitais
III	Vulnerabilidades associadas ao fator humano e a sistemas legados
IV	Papel do gestor hospitalar na segurança da informação
V	Estratégias de mitigação e continuidade dos serviços de saúde

Fonte: Elaborado pelo autor (2025).

Esses núcleos temáticos permitiram uma análise integrada dos estudos selecionados, contribuindo para a compreensão dos desafios enfrentados pelos ambientes hospitalares no contexto da segurança da informação e da proteção de dados pessoais, bem como das estratégias adotadas para a mitigação dos riscos cibernéticos.

Com o objetivo de sistematizar e organizar os achados desta revisão integrativa, foram elaborados quadros de síntese que reúnem as principais informações extraídas dos estudos selecionados. Esses quadros possibilitam uma visão comparativa dos artigos incluídos, favorecendo a compreensão das características metodológicas, dos objetivos, dos resultados e das categorias temáticas emergentes.

O **Quadro 06** a seguir apresenta a caracterização geral dos estudos onde os artigos trazem as categorias de análise pré-definidas., construídas com base na recorrência temática e na convergência dos achados dos estudos incluídos. Essas categorias permitem compreender, de forma sistematizada, como a literatura aborda

os principais aspectos relacionados à segurança da informação em ambientes hospitalares, evidenciando desafios, riscos e estratégias de enfrentamento no contexto da transformação digital e da proteção de dados. A organização dos resultados por categorias possibilita uma leitura integrada dos achados, favorecendo a identificação de padrões e tendências nos estudos analisados e contribuindo para a compreensão do fenômeno investigado.

Quadro 06: Síntese dos estudos incluídos na revisão integrativa: Objetivos, métodos, amostra estudada, principais resultados, categorias e autores. Abreu e Lima/PE, 2025.

Nº	Objetivos	Métodos	Amostra estudada	Principais resultados	Categoria	Autores
1	Analisar ameaças cibernéticas em saúde	Revisão sistemática	Hospitais	Identifica ransomware e falhas humanas como principais ameaças	II	Kruse et al.
2	Investigar impactos da COVID-19 na cibersegurança	Scoping review	Organizações de saúde	Aumento expressivo de ataques durante a pandemia	II	He et al.
3	Avaliar efeitos do ransomware em hospitais	Estudo longitudinal	Hospitais dos EUA	Interrupção de serviços e riscos ao paciente	II	Neprash et al.
4	Identificar vulnerabilidades sociotécnicas	Revisão sistemática	Sistemas de saúde	Fator humano e sistemas legados como principais riscos	III	Ewoh & Vartiainen
5	Analisar riscos à segurança do paciente	Revisão narrativa	Instituições de saúde	Ataques cibernéticos afetam diretamente o cuidado	II	Aldosari
6	Analisar desafios da LGPD em hospitais públicos	Estudo qualitativo	Hospitais públicos	Dificuldades na governança e adequação legal	I	Gonçalves & Werner

7	Investigar abordagens regulatórias em saúde	Revisão integrativa	Estudos regulatórios	Necessidade de integração entre lei e gestão	I	Santos et al.
8	Analisar o princípio da segurança na LGPD	Análise documental	Legislação e jurisprudência	Segurança como eixo central da conformidade	I	Petry & Hupffer
9	Analisar riscos na IoMT	Revisão técnica	Dispositivos médicos	IoMT amplia a superfície de ataque	III	Deb et al.
10	Identificar vulnerabilidades da IoMT	Revisão sistemática	Sistemas IoMT	Dispositivos médicos carecem de proteção	III	Dzamesi & Elsayed

Fonte: Elaborado pelo autor (2025).

4.1 Exigências da LGPD e Governança da Informação

Os estudos incluídos demonstram convergência ao apontar a LGPD como um elemento central na reestruturação da governança da informação em ambientes hospitalares, conforme evidenciado nos estudos E1, E3, E5 e E8, que ressaltam a necessidade de adequação institucional às exigências legais, implementação de políticas de segurança da informação e definição de responsabilidades no tratamento de dados sensíveis. A legislação é descrita como um marco regulatório que impõe às instituições de saúde a necessidade de revisar processos internos, estabelecer políticas formais de segurança da informação e fortalecer mecanismos de controle e responsabilização.

Os resultados indicam que hospitais que apresentam estruturas incipientes de governança da informação enfrentam maiores dificuldades na adequação à LGPD, especialmente no que se refere à gestão do ciclo de vida dos dados, ao controle de acessos e à definição de bases legais para o tratamento de informações sensíveis. Em contrapartida, instituições que adotam modelos formais de governança, com definição clara de responsabilidades e documentação de processos, demonstram maior capacidade de demonstrar conformidade legal.

Os estudos também evidenciam que a atuação da ANPD, por meio de guias e orientações, contribui para a padronização das práticas, porém a aplicação dessas diretrizes ainda ocorre de forma heterogênea entre as instituições. Foram identificadas dificuldades relacionadas à interpretação dos dispositivos legais, à limitação de recursos financeiros e à carência de profissionais especializados em proteção de dados no contexto hospitalar.

4.2 Principais Riscos e Ameaças Cibernéticas em Hospitais

A análise dos estudos revela que os hospitais figuram entre os setores mais expostos a ataques cibernéticos, com destaque para o ransomware como a ameaça de maior impacto operacional e assistencial. Os resultados indicam que ataques dessa natureza estão frequentemente associados à indisponibilidade de sistemas

críticos, paralisação de serviços e necessidade de adoção de medidas emergenciais para manutenção do atendimento.

Além do ransomware, os estudos apontam que ataques de phishing e engenharia social são amplamente utilizados como vetores iniciais de comprometimento dos sistemas hospitalares. Essas ameaças exploram fragilidades humanas e organizacionais, especialmente em ambientes caracterizados por alta rotatividade de profissionais, múltiplos níveis de acesso e sobrecarga de trabalho.

Os resultados também demonstram que a ampliação do uso de tecnologias digitais, como prontuários eletrônicos, plataformas de telessaúde e sistemas integrados, contribui para o aumento da superfície de ataque. A dependência crescente desses sistemas torna os hospitais menos tolerantes a falhas e mais suscetíveis a impactos severos em caso de incidentes de segurança.

4.3 Vulnerabilidades Associadas ao Fator Humano e a Sistemas Legados

Os estudos analisados apontam, de forma recorrente, o fator humano como uma das principais vulnerabilidades na segurança da informação hospitalar. Falhas relacionadas ao comportamento dos usuários, como compartilhamento inadequado de credenciais, uso de senhas fracas e baixa percepção de risco, foram associadas à ocorrência de incidentes de segurança em diferentes contextos hospitalares.

Os resultados indicam que a ausência de programas contínuos de capacitação e conscientização em segurança da informação contribui para a manutenção de práticas inseguras, especialmente entre profissionais de saúde que priorizam a agilidade no atendimento em detrimento dos controles de segurança. Essa realidade é agravada pela complexidade dos ambientes hospitalares, nos quais múltiplos profissionais necessitam acessar sistemas clínicos simultaneamente.

Outra vulnerabilidade amplamente destacada refere-se ao uso de sistemas legados e dispositivos médicos conectados sem atualizações regulares. Os estudos mostram que muitos hospitais operam com tecnologias antigas, incompatíveis com padrões atuais de segurança, o que dificulta a aplicação de controles eficazes, como criptografia, autenticação forte e monitoramento contínuo. A incorporação de dispositivos da Internet das Coisas Médicas (IoMT) amplia ainda mais esse cenário de risco, ao introduzir novos pontos de vulnerabilidade na infraestrutura hospitalar.

4.4 Papel do Gestor Hospitalar na Segurança da Informação

Os resultados evidenciam que a atuação do gestor hospitalar é um fator determinante para a efetividade das práticas de segurança da informação. Os estudos analisados indicam que instituições com maior envolvimento da alta gestão apresentam níveis mais elevados de maturidade em segurança, refletidos na existência de políticas institucionais, investimentos em infraestrutura e programas de capacitação.

Observou-se que a ausência de uma postura ativa da gestão resulta em abordagens fragmentadas, nas quais a segurança da informação é tratada como uma responsabilidade exclusiva da área de tecnologia da informação. Em contrapartida, os estudos destacam que gestores que incorporam a segurança da informação como um eixo estratégico da governança hospitalar contribuem para a integração entre áreas assistenciais, administrativas e tecnológicas.

Os resultados também apontam que a liderança exerce influência direta na cultura organizacional, impactando o comportamento dos colaboradores e a adesão

às políticas de segurança. Dessa forma, o gestor hospitalar é identificado como um agente central na promoção de práticas seguras, na definição de prioridades institucionais e na garantia da conformidade com a LGPD.

4.5 Estratégias de Mitigação de Riscos Cibernéticos e Continuidade dos Serviços de Saúde

Os estudos analisados demonstram que estratégias estruturadas de mitigação de riscos cibernéticos estão associadas à redução dos impactos financeiros, operacionais e assistenciais decorrentes de incidentes de segurança. A implementação de políticas formais, planos de resposta a incidentes e mecanismos de monitoramento contínuo foi identificada como uma prática recorrente entre instituições mais resilientes.

Os resultados indicam que programas contínuos de treinamento e conscientização dos profissionais de saúde contribuem para a redução da incidência de ataques baseados em engenharia social, fortalecendo a cultura organizacional de proteção de dados. Além disso, a adoção de checklists operacionais, testes regulares de backup e revisão periódica de acessos mostrou-se relevante para a detecção precoce de incidentes.

Outro achado relevante refere-se à integração da segurança da informação aos planos de continuidade dos serviços de saúde. Os estudos evidenciam que hospitais que realizam testes periódicos de seus planos de contingência apresentam maior capacidade de manter a assistência ao paciente durante eventos cibernéticos disruptivos, reduzindo o tempo de indisponibilidade dos sistemas e os riscos à segurança do cuidado.

De forma geral, os resultados desta revisão integrativa indicam que a segurança da informação em ambientes hospitalares permanece como um desafio complexo, marcado pela coexistência de avanços tecnológicos e fragilidades organizacionais. Embora haja crescente produção científica sobre o tema, os estudos revelam que a efetividade das estratégias de mitigação depende da integração entre governança, tecnologia, fator humano e atuação da gestão hospitalar. Os achados reforçam que a proteção de dados sensíveis em saúde não se limita à conformidade legal com a LGPD, mas envolve a garantia da continuidade dos serviços, a segurança do paciente e a sustentabilidade institucional. Esses resultados subsidiam a discussão apresentada na seção seguinte, na qual os achados são analisados à luz da literatura científica e do referencial teórico adotado.

A análise dos resultados desta revisão integrativa permite compreender como a literatura científica tem abordado a gestão da segurança da informação em ambientes hospitalares, especialmente diante dos desafios impostos pela Lei Geral de Proteção de Dados (LGPD) e do crescimento dos riscos cibernéticos no setor da saúde. Os achados evidenciam convergência entre os estudos quanto à relevância do tema, ao mesmo tempo em que revelam lacunas importantes relacionadas à governança, à atuação gerencial e à integração entre aspectos legais, técnicos e humanos.

De forma geral, os estudos analisados indicam que os ambientes hospitalares apresentam elevada complexidade organizacional e tecnológica, o que amplia a exposição a ameaças cibernéticas e dificulta a implementação de estratégias de segurança da informação eficazes. Essa complexidade é reforçada pela crescente digitalização dos serviços de saúde, pela adoção de prontuários eletrônicos e pela

incorporação de dispositivos conectados, fatores que, embora tragam benefícios assistenciais, ampliam a superfície de ataque e os riscos associados à proteção de dados sensíveis.

4.6 LGPD e Governança da Segurança da Informação em Hospitais

Os resultados demonstram que a LGPD tem sido reconhecida como um marco regulatório fundamental para a proteção de dados pessoais na área da saúde, conforme evidenciado nos estudos de Gonçalves e Werner, Santos et al. e Petry e Hupffer. Esses autores destacam que a legislação impõe às instituições hospitalares a necessidade de revisar processos, formalizar políticas e adotar mecanismos de controle capazes de assegurar a confidencialidade, a integridade e a disponibilidade das informações.

Entretanto, a discussão dos achados revela que a adequação à LGPD ainda ocorre de forma desigual, especialmente no contexto dos hospitais públicos. As dificuldades identificadas incluem limitações orçamentárias, ausência de estruturas formais de governança da informação e carência de profissionais especializados em proteção de dados. Esses fatores corroboram a percepção de que a conformidade legal não depende apenas do conhecimento normativo, mas da capacidade institucional de implementar práticas contínuas de gestão da segurança da informação.

Além disso, os estudos apontam que a governança da informação em hospitais ainda é frequentemente fragmentada, com responsabilidades pouco definidas e dependência excessiva das áreas de tecnologia da informação. Tal cenário dificulta a internalização da LGPD como um elemento estratégico da gestão hospitalar, reduzindo sua efetividade enquanto instrumento de proteção de dados e de fortalecimento institucional.

4.7 Riscos e Ameaças Cibernéticas no Setor da Saúde

A análise comparativa dos estudos internacionais, especialmente os de Kruse *et al*., He *et al*., Neprash *et al*. e Aldosari, evidencia que os hospitais figuram entre os principais alvos de ataques cibernéticos, com destaque para o ransomware como a ameaça mais recorrente e impactante. Os autores convergem ao apontar que esse tipo de ataque compromete a disponibilidade de sistemas críticos, podendo resultar na interrupção de serviços assistenciais e em riscos diretos à segurança do paciente.

A pandemia da COVID-19 é identificada como um fator agravante desse cenário, uma vez que acelerou a digitalização dos serviços de saúde e ampliou a dependência de sistemas informatizados, muitas vezes sem o fortalecimento proporcional das medidas de segurança. Esse achado reforça a vulnerabilidade estrutural dos hospitais frente a ataques cibernéticos e evidencia a necessidade de estratégias preventivas mais robustas.

Os estudos também destacam que ataques baseados em engenharia social e phishing exploram fragilidades humanas e organizacionais, sendo frequentemente utilizados como porta de entrada para comprometer sistemas hospitalares. Essa constatação indica que a segurança da informação não pode ser tratada exclusivamente sob a perspectiva tecnológica, exigindo abordagens integradas que considerem o comportamento humano e a cultura organizacional.

4.8 Vulnerabilidades Sociotécnicas e Sistemas Legados

Os achados relacionados às vulnerabilidades sociotécnicas, discutidos principalmente por Ewoh e Vartiainen, Deb et al. e Dzamesi e Elsayed, evidenciam

que o uso de sistemas legados e dispositivos médicos conectados representa um desafio significativo para a segurança da informação em hospitais. Esses sistemas, muitas vezes incompatíveis com padrões atuais de segurança, dificultam a aplicação de controles como autenticação forte, criptografia e monitoramento contínuo.

A crescente adoção da Internet das Coisas Médicas (IoMT) amplia ainda mais esse cenário de risco, ao introduzir novos dispositivos conectados que nem sempre são projetados com foco na segurança da informação. A discussão dos estudos aponta que essas vulnerabilidades técnicas, quando combinadas com falhas humanas, potencializam os riscos cibernéticos e aumentam a probabilidade de incidentes de grande impacto.

Nesse sentido, a literatura analisada reforça a necessidade de abordagens sociotécnicas, que integrem soluções tecnológicas com estratégias de gestão, capacitação e revisão de processos. A ausência dessa integração tende a comprometer a efetividade das medidas de segurança adotadas, mesmo quando investimentos em tecnologia são realizados.

4.9 Atuação do Gestor Hospitalar e Cultura Organizacional

Embora nem todos os estudos tenham como foco central a atuação do gestor hospitalar, os resultados evidenciam que a liderança institucional exerce papel decisivo na efetividade da segurança da informação. A discussão dos achados indica que hospitais com maior envolvimento da alta gestão apresentam níveis mais elevados de maturidade em segurança, refletidos na existência de políticas formais, investimentos contínuos e programas de conscientização.

A literatura analisada sugere que a segurança da informação ainda é frequentemente percebida como uma responsabilidade exclusiva da área de tecnologia da informação, o que limita sua integração às estratégias organizacionais. Esse entendimento reduz o potencial de construção de uma cultura organizacional voltada à proteção de dados e à conformidade com a LGPD.

Dessa forma, a discussão reforça que o gestor hospitalar deve atuar como agente estratégico, promovendo a integração entre áreas assistenciais, administrativas e tecnológicas, além de incentivar comportamentos seguros e alinhar a segurança da informação aos objetivos institucionais e à continuidade dos serviços de saúde.

4.10 Estratégias de Mitigação e Continuidade dos Serviços

Os estudos analisados convergem ao apontar que estratégias estruturadas de mitigação de riscos cibernéticos contribuem significativamente para a redução dos impactos de incidentes de segurança em ambientes hospitalares. A discussão dos achados evidencia que a adoção de políticas formais, planos de resposta a incidentes, testes regulares de backup e programas contínuos de capacitação são práticas associadas a maior resiliência organizacional.

Além disso, a literatura destaca a importância da integração entre segurança da informação e planos de continuidade dos serviços de saúde. Hospitais que realizam testes periódicos de seus planos de contingência demonstram maior capacidade de manter a assistência ao paciente durante eventos cibernéticos disruptivos, reduzindo riscos assistenciais e operacionais.

Esses achados reforçam que a segurança da informação deve ser compreendida como um componente essencial da gestão hospitalar e da segurança do paciente, indo além da mera conformidade legal e assumindo papel estratégico na

sustentabilidade institucional.

A discussão dos resultados evidencia que a gestão da segurança da informação em ambientes hospitalares permanece como um desafio complexo e multifacetado, marcado pela necessidade de integração entre aspectos legais, tecnológicos, organizacionais e humanos. Embora a literatura reconheça a importância da LGPD e das estratégias de mitigação de riscos cibernéticos, os estudos revelam lacunas significativas na governança da informação e na atuação gerencial, especialmente no contexto dos hospitais públicos.

Os achados reforçam que a efetividade da segurança da informação depende da adoção de uma abordagem sistêmica, capaz de alinhar conformidade legal, investimentos tecnológicos, capacitação dos profissionais e liderança institucional. Essa compreensão fundamenta as considerações finais apresentadas na seção seguinte, nas quais são sintetizadas as principais contribuições do estudo e apontadas recomendações para a prática e para pesquisas futuras.

5 CONSIDERAÇÕES FINAIS

Os ambientes hospitalares apresentam elevada vulnerabilidade a incidentes de segurança da informação, em razão da crescente digitalização dos serviços de saúde, da adoção de sistemas legados e da incorporação de dispositivos conectados, como os da Internet das Coisas Médicas (IoMT). Ataques cibernéticos, especialmente o ransomware, destacam-se como ameaças recorrentes, com impactos diretos na continuidade dos serviços e na segurança do paciente.

No que se refere à LGPD, os achados demonstram que a legislação representa um avanço significativo na proteção de dados pessoais em saúde, ao estabelecer princípios, direitos e responsabilidades para o tratamento de informações sensíveis. Entretanto, a revisão integrativa revelou que a adequação à LGPD ainda constitui um desafio para muitas instituições hospitalares, sobretudo no setor público, devido a limitações estruturais, financeiras e à ausência de modelos consolidados de governança da informação.

A análise também destacou o papel central do fator humano na segurança da informação hospitalar. A falta de programas contínuos de capacitação e conscientização contribui para a ocorrência de falhas operacionais e para a exploração de vulnerabilidades por meio de ataques de engenharia social. Esses achados reforçam a necessidade de compreender a segurança da informação como um fenômeno sociotécnico, que exige a integração entre soluções tecnológicas, processos organizacionais e comportamento humano.

Outro aspecto relevante identificado diz respeito à atuação do gestor hospitalar. Os estudos analisados indicam que o envolvimento da alta gestão é determinante para o nível de maturidade das práticas de segurança da informação, influenciando a alocação de recursos, a definição de prioridades institucionais e a construção de uma cultura organizacional voltada à proteção de dados e à conformidade legal. Nesse sentido, a segurança da informação deve ser incorporada como um eixo estratégico da gestão hospitalar, e não restrita às áreas técnicas.

Como contribuições, este estudo sistematiza evidências científicas recentes sobre a gestão da segurança da informação em hospitais, oferecendo subsídios para gestores, profissionais de saúde e formuladores de políticas públicas na tomada de decisão e no aprimoramento das práticas institucionais. Além disso, reforça a importância da integração entre LGPD, governança da informação e continuidade dos serviços de saúde, destacando a segurança da informação como elemento essencial

para a qualidade do cuidado e a sustentabilidade organizacional.

Quanto às limitações, destaca-se que esta pesquisa se baseou exclusivamente em estudos disponíveis nas bases de dados selecionadas e no recorte temporal definido, o que pode ter restringido a inclusão de outras produções relevantes. Ademais, por se tratar de uma revisão integrativa, os resultados refletem as evidências disponíveis na literatura, não permitindo generalizações empíricas sobre contextos específicos.

Por fim, sugere-se que pesquisas futuras aprofundem a análise empírica da implementação da LGPD em hospitais brasileiros, bem como avaliem o impacto das estratégias de mitigação de riscos cibernéticos na segurança do paciente e na continuidade dos serviços de saúde. Estudos de natureza aplicada e comparativa podem contribuir para o desenvolvimento de modelos de governança mais eficazes e adequados à realidade do setor hospitalar.

REFERÊNCIAS

ALDOSARI, B. **Cybersecurity in healthcare: new threat to patient safety**. Cureus, v. 17, n. 1, 2025. Disponível em: https://www.proquest.com/docview/3225670167?fromopenview=true&pq-origsite=gscholar&sourcetype=Scholarly%20Journals Acesso em: 25 de dezembro de 2025.

ANDERSON, Ross. **Security engineering: a guide to building dependable distributed systems**. 3. ed. Hoboken: Wiley, 2020. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=eo4Otm_TcW8C&oi=fnd&pg=PT14&dq=Ross.+Security+engineering:+a+guide+to+building+dependable+distributed+systems&ots=gDJOCOcza8&sig=PbRKdu8zLkjzuFMH-_1auv7bge4&redir_esc=y#v=onepage&q=Ross.%20Security%20engineering%3A%20a%20guide%20to%20building%20dependable%20distributed%20systems&f=false Acesso em: 25 de dezembro de 2025.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para tratamento de dados pessoais sensíveis.** Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-tratamento-de-dados-pessoais-para-fins-academicos-e-para-a-realizacao-de-estudos-e-pesquisas?. Acesso em: 18 de novembro de 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 15 de outubro de 2025.

DEB, S. et al. **Securing the Internet of Medical Things (IoMT): real-world attack taxonomy and practical security measures.** Preprint, 2025. Disponível em: https://arxiv.org/abs/2507.19609 Acesso em: 22 de novembro de 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** Rio de Janeiro: Forense, 2019.

DZAMESI, Lily; ELSAYED, Nelly. **A review on the security vulnerabilities of the IoMT against malware attacks and DDoS.** *arXiv*, 13 jan. 2025. Disponível

em: https://arxiv.org/abs/2501.07703. Acesso em: 15 de outubro de 2025.

EWOH, P.; VARTIAINEN, T. **Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review.** Journal of Medical Internet Research, v. 26, 2024. Disponível em: https://www.jmir.org/2024/1/e46904/ Acesso em: 22 de novembro de 2025.

GONÇALVES, C. M.; WERNER, E. M. **LGPD e serviços de saúde pública: desafios da implementação da Lei Geral de Proteção de Dados em hospitais públicos.**
Revista do CAAP, v. 29, n. 1, p. 1–24, 2025. Disponível em: https://periodicos.ufmg.br/index.php/caap/article/view/52340 Acesso em: 25 de novembro de 2025.

HE, Y.; ZHANG, Y.; XING, B.; ZHAO, Y. **Health care cybersecurity challenges and solutions under the climate of COVID-19: a scoping review.** Journal of Medical Internet Research, Toronto, v. 23, n. 4, e21747, 2021. DOI: 10.2196/21747.
Disponível em: https://www.jmir.org/2021/4/e21747/ Acesso em: 02 de dezembro de 2025.

IBM SECURITY. **Cost of a Data Breach Report 2024.** Armonk: IBM Corporation, 2024. Disponível em: www.ibm.com/security/data-breach Acesso em: 02 de dezembro de 2025.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022. Disponivel em: https://intranetcomunix.com/wp-content/uploads/2024/07/ABNT_ISO_27001.pdf Acesso em: 03 de dezembro de 2025.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements. Geneva: ISO, 2019. Disponivel em: https://www-iso.org.translate.goog/standard/75106.html?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc Acesso em: 03 de dezembro de 2025.

KRUSE, C. S. et al. **Cybersecurity in healthcare: a systematic review of modern threats and trends.** Technology and Health Care, Amsterdam, v. 25, n. 1, p. 1–10, 2017. DOI: 10.3233/THC-161263. Disponível em: https://journals.sagepub.com/doi/abs/10.3233/THC-161263 Acesso em: 22 de novembro de 2025.

MENDES, K. D. S.; SILVEIRA, R. C. C. P.; GALVÃO, C. M. **Revisão integrativa: método de pesquisa para a incorporação de evidências na saúde e na enfermagem.** Texto & Contexto – Enfermagem, Florianópolis, v. 17, n. 4, p. 758–764, 2010.
Disponível em: https://www.scielo.br/j/tce/a/XzFkq6tjWs4wHNqNjKJLkXQ/?format=html&lang=pt Acesso em: 17 de novembro de 2025.

MITNICK, Kevin D.; SIMON, William L. T**he art of deception: controlling the human element of security.** New York: John Wiley & Sons, 2002. Disponível em: https://books.google.com.br/books?id=rmvDDwAAQBAJ. Acesso em: 1 de dezembro de 2025.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento: pesquisa qualitativa em saúde.** 12. ed. São Paulo: Hucitec, 2010.

NEPRASH, H. T. et al**. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021.** JAMA Health **Forum**, v. 3, n. 12, e224873, 2022. Disponível em: https://jamanetwork.com/journals/jama-health- forum/fullarticle/2799961 Acesso em: 25 de novembro de 2025.

PAGE, M. J.; McKENZIE, J. E.; BOSSUYT, P. M.; BOUTRON, I.; HOFFMANN, T. C.; MULROW, C. D.; SHAMSEER, L.; TETZLAFF, J. M.; AKL, E. A.; BRENNAN, S. E.; et al. **The PRISMA 2020 statement: an updated guideline for reporting systematic reviews.** *BMJ*, London, v. 372, n. 71, p. 1–9, 2021. DOI: 10.1136/bmj.n71. Disponível em: https://www.bmj.com/content/372/bmj.n71. Acesso em: 25 de novembro de 2025.

PETRY, G. C.; HUPFFER, H. M. **O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD.** Revista CNJ, v. 7, n. 1, p. 85–98, 2023. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/article/view/445 Acesso em: 01 de dezembro de 2025.

RAHIM, Md Jawadur; IBN RAHIM, Muhammad Ihsan; AFROZ, Ahlina; AKINOLA, Omolola. ***Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies*.** Journal of Artificial Intelligence General Science (JAIGS), v. 6, n. 1, p. 438–462, 2024. Disponível em: https://newjaigs.org/index.php/JAIGS/article/view/268. Acesso em: 10 de janeiro de 2026.

RAYYAN. **Rayyan: ferramenta para triagem de estudos em revisões sistemáticas.** Disponível em: https://www.rayyan.ai. Acesso em: 29 de dezembro de 2025.

ROMANOV, Samuel; VARNFIELD, Marlien. **Vital Protection in Digital Healthcare**. 15 Jan. 2025. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2025/volume-1/vital-protection-in-digital-healthcare. Acesso em: 10 de janeiro de 2026.

SANTOS, W. G. et al. **Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023.** Physis, v. 35, n. 1, e350113, 2025.
Disponível em: https://www.scielosp.org/article/physis/2025.v35n1/e350113/ Acesso em: 02 de novembro de 2025.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva.** 3. ed. Rio de Janeiro: Elsevier, 2014.

SINGER, Sara J.; PFAFF, Hannah; SCHULMAN, Kevin A.; et al. **Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals.** Annals of Emergency Medicine, v. 83, n. 1, p. 46–56, 2024. Disponível em:https://www.sciencedirect.com/science/article/pii/S0196064423003529. Acesso em: 10 de janeiro 2026.

WHITMAN, M. E.; MATTORD, H. J. **Principles of information security.** 6. ed. Boston: Cengage Learning, 2018. Disponível em: http://ndl.ethernet.edu.et/bitstream/123456789/89363/1/Principles%20of%20Information%20Security%20by%20Whitman%2C%20Michael%20Mattord%2C%20Herbert%20.pdf Acesso em: 29 de novembro de 2025.

WHITTEMORE, Robin; KNAFL, Kathleen. **The integrative review: updated methodology**. Journal of Advanced Nursing, v. 52, n. 5, p. 546–553, 2005. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1365-2648.2005.03621.x. Acesso em: 25 de dezembro de 2025.