CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Título do Artigo: SEGURANÇA DA INFORMAÇÃO: DIRETRIZES PARA PROTEÇÃO DE DADOS E MITIGAÇÃO DE ATAQUES NA ÁREA DA SAÚDE

Autores: Amanda Divino Rossi Rodrigues
amanda.rossi@fatec.sp.gov.br

Julia Bergamim Silva Simião
julia.simiao@fatec.sp.gov.br

Orientador: Prof. Me. Wdson de Oliveira
wdson.oliveira01@fatec.sp.gov.br

Resumo

Este artigo faz uma análise simples e prática sobre como um hospital público lida com Segurança da Informação e com a LGPD. A ideia central foi entender como os dados pessoais são protegidos no dia a dia e identificar pontos fracos que podem colocar informações de pacientes e funcionários em risco. Para isso, foram observadas rotinas internas e analisados processos relacionados ao uso de sistemas, controle de acesso, descarte de documentos, treinamentos e políticas internas. Os resultados mostram que o hospital já tem alguns avanços, como assinaturas digitais, antivírus atualizado e biometria em áreas restritas. Mesmo assim, ainda há muitas falhas importantes, como falta de treinamentos contínuos, inexistência de políticas formais, descarte inadequado de documentos, uso de logins genéricos e pouca conscientização dos colaboradores. Também foram identificados riscos no uso de dispositivos pessoais, no acesso remoto, nas redes Wi-Fi abertas e na ausência de procedimentos claros para tratar incidentes. No geral, a análise indica que o hospital ainda está em uma fase inicial de maturidade em segurança da informação e precisa evoluir para atender às exigências da LGPD e das normas ISO. O estudo reforça a necessidade de investir em capacitação, organização de processos e melhorias técnicas para proteger dados sensíveis e evitar problemas futuros.

Palavras-chave: LGPD; Segurança da Informação; Proteção de Dados; Saúde; Governança.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Abstract

This article presents a practical analysis of how a public hospital handles Information Security and compliance with the Brazilian General Data Protection Law (LGPD). The study aimed to understand how personal data is protected in daily routines and to identify weaknesses that may expose sensitive information from patients and employees. The research was conducted through direct observation and analysis of internal processes related to system usage, access control, document disposal, training, and internal policies. The results show that the hospital has some positive practices, such as the use of digital signatures, updated antivirus solutions, and biometric access in restricted areas. However, several significant gaps remain, including the lack of continuous training, absence of formal policies, improper document disposal, the use of generic logins, and low employee awareness. Additional risks were identified regarding personal devices, remote access, open Wi-Fi networks, and the lack of clear incident response procedures. Overall, the findings indicate that the hospital is still at an early stage of information security maturity and must improve to adequately meet LGPD and ISO standards. The study highlights the need for investments in staff training, structured processes, and technical improvements to strengthen data protection and prevent future incidents.

Keywords: *LGPD; Information Security; Data Protection; Healthcare; Governance.*

Dezembro/2025

1. INTRODUÇÃO

A saúde digital transformou a forma como hospitais e clínicas operam, trouxe inovações como a informatização de prontuários médicos, sistemas de gestão hospitalar e o uso da telemedicina. Esses recursos ampliaram a eficiência dos serviços e facilitaram o atendimento aos pacientes. No entanto, essa evolução também aumentou os riscos de ataques cibernéticos, vazamentos de informações e falhas de proteção de dados sensíveis. Segundo Santos (2018), "a segurança da informação vem sendo primordial, principalmente em empresas, e até mesmo no âmbito doméstico, como forma de proteger dados e informações confidenciais de pessoas ou empresas não autorizadas e mal-intencionadas, que roubam os dados por diversos motivos, seja pelo desafio da quebra de segurança ou pelo roubo de informações privilegiadas, que possam fazer com que uma empresa se destaque mais que a outra, aumentando seus lucros."

Para enfrentar esses desafios, o Brasil criou a Lei Geral de Proteção de Dados (LGPD), inspirada na norma europeia GDPR (Regulamento Geral de Proteção de Dados). De acordo com Melo (2020), o cidadão passa a compreender melhor quem tem acesso aos seus dados, de que forma eles são utilizados e com qual finalidade são tratados.

Silveira (2021) destaca que os ataques cibernéticos representam uma ameaça à segurança da informação no setor da saúde, podendo comprometer a proteção dos dados e a segurança dos pacientes. Ataques de *ransomware*, *phishing* e engenharia social têm se tornado cada vez mais frequentes em hospitais e clínicas. Em 2020, um ataque de *ransomware* no Hospital Universitário de Düsseldorf, na Alemanha levou à interrupção dos serviços médicos (Olhar Digital, 2020).

Além dos ataques externos, a negligência interna também representa uma ameaça. Segundo Leme e Blank (2020), um programa de governança em privacidade deve ser construído de forma transparente, focada na gestão de riscos e adaptada à realidade da organização.

Casos recentes no Brasil comprovam a relevância da proteção de dados pessoais no setor da saúde. Em 2024, o Tribunal de Justiça do Distrito Federal e Territórios condenou um hospital público pelo vazamento de informações médicas de uma paciente, reconhecendo falha na adoção de medidas de segurança e determinando que o hospital pagasse uma indenização por danos morais. Essa decisão evidencia que a ausência de mecanismos eficazes de proteção pode gerar não apenas riscos à privacidade, mas também responsabilização jurídica às instituições (TJDFT, 2024).

Mais do que atender às exigências da LGPD, proteger dados na área da saúde significa garantir a privacidade, a dignidade e a segurança dos pacientes. O vazamento de informações médicas pode expor fragilidades pessoais, abrir portas para chantagens e fraudes. Nesse sentido, este estudo se justifica pela necessidade de propor estratégias que fortaleçam a proteção de dados e ajudem as instituições de saúde a se tornarem mais resilientes frente às ameaças digitais.

O objetivo deste estudo é analisar os desafios da implementação da Lei Geral de Proteção de Dados (LGPD) em um hospital público de médio porte, com foco na mitigação de ataques e na proteção de dados sensíveis. Os objetivos específicos deste artigo incluem: identificar os principais riscos e vulnerabilidades na proteção de dados, avaliar as fragilidades estruturais e humanas, comparar as práticas atuais do hospital com as exigências da lei e com as normas ISO 27001/27799, e, por fim, apresentar recomendações para mitigar ataques cibernéticos, e aprimorar a proteção de dados.

2. REFERENCIAL TEÓRICO

A segurança da informação na saúde envolve aspectos tecnológicos, jurídicos e organizacionais. O referencial teórico apresenta esses elementos para compreender como a proteção de dados se aplica a ambientes hospitalares.

2.1 Segurança da Informação na Área da Saúde

A segurança da informação é o conjunto de práticas e medidas destinadas a preservar a confidencialidade, integridade e disponibilidade dos dados, princípios conhecidos como os três pilares fundamentais da área. A confidencialidade garante que apenas pessoas autorizadas tenham acesso às informações; a integridade assegura que os dados permaneçam exatos e não sejam alterados indevidamente; e a disponibilidade garante que as informações estejam acessíveis sempre que necessário para a continuidade das atividades (ISO/IEC 27002, 2022).

No setor da saúde, essa proteção tem caráter ainda mais crítico, pois envolve dados de pacientes, como prontuários médicos, diagnósticos, históricos clínicos e exames, que são classificados pela LGPD como dados sensíveis, e exigem tratamento diferenciado. Esses dados, se expostos, podem afetar não só a privacidade dos pacientes, mas também o atendimento e prejudicar a confiança no hospital.

De acordo com Passo (2022), a proteção de informações médicas deve ser tratada como prioridade estratégica dentro das organizações de saúde, pois falhas nesse campo podem gerar implicações éticas, jurídicas e financeiras.

Essa preocupação se torna ainda mais urgente diante das particularidades do setor da saúde, considerado altamente vulnerável devido ao uso crescente de sistemas integrados, telemedicina e dispositivos conectados (IoT hospitalar), que ampliam os pontos de risco (LEME; BLANK, 2020). Nesse cenário, as ameaças não vêm apenas de ataques externos, como *ransomware e phishing*, mas também falhas internas, como senhas fracas, uso compartilhado de acessos e a ausência de uma cultura organizacional voltada à proteção de dados.

2.2 LGPD e Dados Sensíveis na Saúde

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, foi decretada para proteger os direitos fundamentais e a

privacidade das pessoas. Inspirada no regulamento europeu GDPR, essa legislação estabelece regras para a coleta, tratamento, armazenamento e compartilhamento de dados, visando garantir maior transparência e proteção aos titulares (MELO, 2020).

No setor da saúde, a LGPD assume papel central, pois os dados médicos se enquadram na categoria de dados sensíveis. Conforme o artigo 5º, inciso II da lei, são considerados sensíveis aqueles relacionados à saúde, vida sexual, origem racial ou étnica, convicção religiosa, opinião política, entre outros (BRASIL, 2018). Segundo Sousa (2024), o tratamento dessas informações deve seguir regras mais rígidas, como a obtenção de consentimento explícito do paciente e a aplicação de medidas de segurança proporcionais ao risco envolvido.

Segundo a Lei nº 13.709/2018, o tratamento de dados sensíveis só pode ocorrer em situações específicas:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> (…)
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
> (BRASIL, 2018).

De acordo com a LGPD: “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018, art. 46).

Conforme destaca Neves (2025), a implementação da LGPD, em setembro de 2020, trouxe avanços importantes, mas ainda há desafios: levantamento da Associação Brasileira de Empresas para Proteção de Dados mostrou que apenas 36% das instituições declararam estar totalmente em conformidade com a legislação. Esse cenário evidencia a urgência de fortalecer

políticas de segurança no setor, não apenas para cumprir exigências legais, mas para garantir a continuidade dos serviços e a confiança dos pacientes.

2.3 Normas e Boas Práticas

Para proteger os dados na área da saúde, é essencial seguir normas e boas práticas. De acordo com Silveira (2021), a governança de dados em hospitais deve unir diretrizes técnicas, administrativas e jurídicas, garantindo que todo o ciclo das informações, desde a coleta até o descarte, seja feito com segurança. As principais recomendações incluem implementar controles de acesso por perfil, realizar auditorias internas regularmente e criar comitês de governança digital.

Leme e Blank (2020) enfatizam que a conformidade com os marcos regulatórios, como a LGPD, deve ser complementada pela adoção de *frameworks* de segurança reconhecidos internacionalmente, como a ISO/IEC 27001, que define diretrizes para sistemas de gestão de segurança da informação, e a ISO/IEC 27799, que é especificamente voltada ao setor da saúde. Para que os hospitais possam se alinhar com processos tecnológicos à proteção jurídica e ética dos pacientes, essas normas se tornam um guia prático.

A gestão de mídias e o descarte seguro de documentos físicos são partes importantes da segurança da informação. Tanto a LGPD quanto normas como a ISO/IEC 27001 recomendam que documentos com dados pessoais sensíveis sejam destruídos completamente, por meio de fragmentação, trituração, incineração ou outro descarte controlado. Quando isso não é feito da forma correta, prontuários, relatórios e dados clínicos podem acabar expostos, criando riscos éticos, legais e até operacionais.

Entre as recomendações das normas ISO/IEC 27001 e 27002, o controle A.9 é um dos principais. Ele exige mecanismos de controle de acesso, como o bloqueio automático quando a sessão fica inativa. Isso evita que pessoas não autorizadas usem o sistema caso alguém deixe o computador desbloqueado, o

que é muito importante em ambientes de saúde, onde circula muita gente o tempo todo.

Além disso, Costa (2022) sugere que os resultados da pesquisa TIC Saúde demonstram avanços no uso da telessaúde, mas apontam fragilidades em relação às boas práticas de segurança. Isso nos mostra que, mesmo diante dos avanços tecnológicos, a falta de um protocolo consolidado ainda expõe os hospitais à riscos que podem ser mitigados apenas com políticas de conscientização e treinamento periódico e contínuo de profissionais.

2.4 A Crescente de Ataques Cibernéticos em Hospitais

Devido ao alto valor dos dados médicos no mercado ilegal, o setor da saúde se tornou um grande e frequente alvo de ataques cibernéticos nos últimos anos. Holts, Marin e Vedolin (2024) destacam que os hackers exploram tanto as falhas técnicas como a falta de preparo para a resposta de incidentes, ameaçando diretamente o andamento dos atendimentos médicos.

Existem casos concretos que demonstram a gravidade do problema, um exemplo é o ataque de *ransomware* à um hospital em Düsseldorf, na Alemanha, comprometeu os seus sistemas e resultou na morte de uma paciente que precisou ser transferida para outra unidade (OLHAR DIGITAL, 2020). No Brasil, a situação também é preocupante: uma reportagem do jornal O Estado de S. Paulo apontou que os hackers já conseguem até mesmo manipular resultados de exames, o que apresenta riscos direto à saúde dos pacientes (BASETTE, 2025).

Através desse cenário podemos notar a necessidade de uma abordagem mais rigorosa de segurança cibernética, considerando que os hospitais não estão lidando apenas com informações sigilosas, mas com serviços críticos e vidas humanas. Neves (2025) nos alerta, que a proteção das informações dos pacientes ainda é um desafio cotidiano, principalmente pela falta de infraestrutura tecnológica suficiente e a falta de um plano de resposta a incidentes bem estruturados.

2.5 Tecnologias Emergentes e a Proteção de Dados em Saúde

Embora o setor da saúde esteja avançando no uso de tecnologias como Internet das Coisas (IoT), telessaúde e computação em nuvem, a instituição analisada ainda não utiliza esses recursos de forma estruturada. Por isso, esta seção traz apenas um panorama conceitual, para contextualizar tendências tecnológicas que influenciam a privacidade e a segurança, mesmo que elas não façam parte do ambiente estudado.

Com a chegada da era digital, aumentaram os riscos relacionados à segurança da informação no setor da saúde, especialmente com a adoção de sistemas eletrônicos de saúde e o uso expandido de tecnologias conectadas. A IoT e a telessaúde, embora relevantes como tendência nacional, não foram observadas na instituição, mas representam riscos importantes para organizações que fazem uso desses recursos (LEME; BLANK, 2020).

De acordo com Passo (2022), as instituições precisam equilibrar inovação e segurança, adotando tecnologias de proteção, como criptografia avançada, autenticação multifatorial e monitoramento em tempo real. A autora ainda ressalta que a proteção de dados pessoais na saúde deve ser tratada como parte de estratégia para inovação, e não como uma barreira para a transformação digital.

Costa (2022) evidencia, no estudo TIC Saúde, que, apesar do avanço significativo da telessaúde no Brasil, ainda existem grandes falhas na forma de armazenamento e transferências dos dados sensíveis, principalmente em sistemas de armazenamento em nuvem sem uma diretriz de segurança adequada.

Silveira (2021) complementa que a governança digital precisa acompanhar essas mudanças, implementando estruturas que envolvam compliance regulatório, investimento em tecnologia e treinamento dos profissionais de saúde. Isso porque, a proteção competente dos dados depende não somente dos recursos tecnológicos, mas também da conscientização de

cada organização para que a privacidade e confiança do paciente sejam valorizadas.

2.6 Estratégias de Mitigação de Ataques

A grande incidência de ataques cibernéticos em instituições da saúde, torna obrigatória a expansão de estratégias de mitigação que incorporem tecnologias, processos e pessoas. Segundo Silveira (2021), a primeira linha de defesa é a implementação de uma política de segurança da informação estruturada, com protocolos de prevenção, detecção e resposta a incidentes. Então para evitar perdas irreversíveis em casos de *ransomware*, esses critérios devem incluir monitoramento contínuo, backups regulares, controles de acessos e segmentação de redes.

De acordo com Holts, Marin e Vedolin (2024), os hospitais precisam adotar uma postura proativa, implementando sistemas de gestão de vulnerabilidades e planos de contingência capazes de reduzir o impacto de ataques. Sem essas medidas, pode haver o comprometimento do atendimento médico e, dessa forma, colocar vidas em risco como aconteceu no hospital na Alemanha, conforme citado anteriormente, onde uma paciente faleceu devido à paralisação dos sistemas hospitalares por causa de um ataque de *ransomware* (OLHAR DIGITAL, 2020).

Para Leme e Blank (2020), a mitigação dos riscos cibernéticos deve ser tratada integralmente à governança corporativa, associando os requisitos técnicos e deveres legais estabelecidas pela LGPD. Incluindo a indicação de encarregados de proteção de dados (DPO – *Data Protection Officer*) – que é responsável em cuidar da conformidade e ser o contato entre a instituição, os funcionários e os titulares dos dados – a realização de avaliações de impacto à proteção de dados (DPIA – *Data Protection Impact Assessment)* e a definição de diretrizes para a notificação de incidentes à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

Além dessas medidas técnicas, a conscientização e treinamento dos profissionais da saúde é indicada como um dos alicerces mais efetivos. Basette (2025) aponta que as falhas humanas, como cliques em links infectados ou uso de senhas fracas, ainda refletem uma das principais formas de entrada para os hackers. Sendo assim, é essencial que haja programas de capacitação regularmente e simulações de ataques (*phishing tests*) para que a cultura de segurança dentro das organizações seja consolidada.

Enfim, Neves (2025) ressalta que a mitigação de ataques cibernéticos na área da saúde deve ser encarada como um processo dinâmico e permanente, baseado em análise de riscos e melhoria contínua. Então para garantir a resiliência operacional e a proteção dos dados sensíveis de pacientes, é necessário haver um equilíbrio entre tecnologia, políticas internas e responsabilidade ética.

3. METODOLOGIA

Este estudo caracterizou-se como uma pesquisa exploratória e descritiva, de abordagem qualitativa, desenvolvida por meio de um estudo de caso. Essa escolha se justifica pela necessidade de compreender, em profundidade, o contexto de uma instituição de saúde real, identificando vulnerabilidades e propondo estratégias de mitigação de riscos relacionadas à segurança da informação e à adequação à LGPD.

A pesquisa foi realizada em um hospital público de médio porte que realiza atendimentos ambulatoriais, internações e procedimentos de média complexidade. A escolha da instituição se deve à sua relevância regional e ao uso de sistemas informatizados para gestão de prontuários eletrônicos, exames laboratoriais e radiologia, além da possibilidade de atividades médicas remotas, fatores que ampliam os desafios de segurança digital.

A coleta de dados ocorreu por meio da observação direta das rotinas de acesso físico e lógico às dependências e sistemas do hospital, do diálogo informal com colaboradores, da análise documental de normas internas, fluxos

de acesso e políticas de backup, e da vivência profissional da pesquisadora, que possibilitou identificar na prática pontos de vulnerabilidade e comportamentos de risco no tratamento das informações.

Os dados obtidos foram analisados de forma qualitativa e comparados às boas práticas recomendadas pelas normas ISO/IEC 27001 e ISO/IEC 27799, bem como aos requisitos da Lei nº 13.709/2018 (LGPD). A análise permitiu identificar falhas e propor melhorias alinhadas à legislação vigente e às diretrizes internacionais de segurança da informação.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Durante a observação do ambiente hospitalar, foram identificadas situações que demonstram avanços importantes na adequação à LGPD, mas também fragilidades importantes na rotina de segurança da informação.

A análise a seguir foi organizada para comparar o que foi observado na prática com o que a LGPD exige e com os controles recomendados pelas normas ISO/IEC 27001, 27002 e 27799. Por isso, cada ponto analisado no hospital, como acesso à informação, descarte de documentos, tecnologia, políticas internas e governança, é discutido com base nessas normas, mostrando onde a instituição está alinhada e onde ainda precisa melhorar em relação às boas práticas de segurança da informação.

4.1 Conscientização e Treinamentos sobre Segurança da Informação

Ao iniciar suas atividades, cada colaborador assina o Termo de Responsabilidade de Uso de Recursos da Tecnologia da Informação e Comunicação, pelo qual toma conhecimento sobre o uso adequado dos recursos tecnológicos do hospital, como e-mail e acesso à rede interna. Porém, a aplicação desse termo ainda é muito formal e superficial. A maioria dos colaboradores relata que apenas assinou o documento, sem receber orientações

sobre o conteúdo, os riscos envolvidos ou as consequências do descumprimento das normas.

Antes da entrada em vigor da Lei Geral de Proteção de Dados (LGPD), em 2020, os colaboradores participaram de um treinamento online obrigatório sobre o tema, realizado em 2019. Mas o conteúdo foi só introdutório e não continuou nos anos seguintes, o que diminui sua eficácia. A falta de treinamentos regulares contraria o controle 7.2 da ISO/IEC 27001, que estabelece que todos os colaboradores devem ser instruídos e conscientizados sobre segurança da informação de forma periódica.

Atualmente, observa-se que nem todos os novos colaboradores recebem informações claras sobre a LGPD. Alguns relatam ter recebido apenas um impresso com instruções para acessar o curso online, sem acompanhamento ou explicações, enquanto outros informam não ter recebido qualquer tipo de treinamento. Essa inconsistência no processo de integração reforça a ausência de uma política estruturada de conscientização e evidencia a fragilidade da instituição quanto à formação de uma cultura organizacional voltada à proteção de dados.

Ainda que muitos colaboradores conheçam superficialmente o conceito de LGPD, boa parte não entende sua importância prática e o impacto da lei na rotina hospitalar. Não há campanhas visuais, comunicados internos ou canais de comunicação específicos sobre o tema, o que reforça a percepção de que a proteção de dados ainda é tratada como um assunto técnico e restrito à equipe de TI.

A Tabela 1 mostra, de forma resumida, como era a rotina do hospital antes da LGPD e como ela ficou depois. Essa comparação ajuda a visualizar o que realmente mudou e o que ainda continua frágil no dia a dia, principalmente quando falamos de segurança da informação e proteção de dados.

Tabela 1: Comparativo Antes e Depois da LGPD

Aspecto	*Antes da LGPD*	*Depois da LGPD*
Compartilhamento de dados de pacientes	Frequente	Restrito
Treinamentos sobre proteção de dados	Baixa	Raros
Controle de identidade	Superficial	Reforçado
Conscientização geral	Baixa	Moderada

Fonte: Autores (2025)

4.2 Práticas de Acesso e Controle da Informação

Em relação ao acesso físico, o hospital mantém controle apenas em duas portarias principais: a de entrada de funcionários, com catracas biométricas e crachás temporários para visitantes e prestadores de serviço, e a internação de pacientes. Nas demais portarias, como os setores de exames, ambulatórios, o acesso é praticamente livre, não há controle de quem entra ou sai da instituição, e os demais acessos internos são totalmente acessíveis, o que representa uma vulnerabilidade considerável à segurança física das informações e dos equipamentos.

Nos sistemas internos, também foram identificadas fragilidades importantes. Não há bloqueio automático de tela nos computadores, o que permite que qualquer pessoa acesse informações quando o usuário se ausenta. Além disso, não existe política de troca periódica de senhas, e muitos setores utilizam logins genéricos compartilhados, com combinações simples como “nome-setor123” como senha. Essa prática viola diretamente o controle A.9.2 da ISO/IEC 27002, que determina que o acesso a sistemas deve ser individualizado, rastreável e concedido conforme o perfil de cada usuário.

Por outro lado, o sistema de gestão hospitalar, na parte dos prontuários eletrônicos, que reúne dados clínicos sensíveis, é mais seguro: cada profissional tem seu próprio login, e os da área assistencial (como médicos, enfermeiros, fisioterapeutas e nutricionistas) utilizam assinatura digital com cartão, garantindo a integridade e autenticidade dos registros no prontuário médico.

Foram identificadas práticas de envio de documentos e dados de pacientes por e-mail e WhatsApp, principalmente para confirmar consultas ou exames. Embora essas ações sejam feitas com boa intenção e para dar mais agilidade, elas trazem riscos de exposição indevida, já que nem sempre é possível garantir que o destinatário seja realmente autorizado a receber essas informações. Essa prática também descumpre o art. 46 da LGPD, que determina a adoção de medidas de segurança capazes de evitar o compartilhamento indevido de informações.

O atendimento telefônico segue o mesmo padrão: as informações são repassadas após confirmação de nome, data de nascimento e nome da mãe. No entanto, esse processo não assegura a identidade real do interlocutor, mantendo vulnerável o princípio da confidencialidade.

Outro ponto identificado foi a falta de orientações formais sobre o uso de redes sociais pelos funcionários. Em um ambiente hospitalar, postar fotos, comentários ou registros internos pode, sem querer, expor pacientes ou informações sensíveis.

4.3 Gestão de Documentos e Infraestrutura Tecnológica

Em relação ao armazenamento físico das informações, existe um setor destinado à guarda de prontuários e documentos originais, o que mostra uma preocupação com a organização e integridade dos registros. Porém, cópias duplicadas ou impressões incorretas nos setores muitas vezes são reaproveitadas como rascunho e nem sempre descartadas de forma segura.

Embora o hospital possua uma fragmentadora de papel, não há orientação expressa sobre o seu uso. Na prática, grande parte dos papéis com dados de pacientes é descartada em lixo comum, expondo informações pessoais e clínicas. Essa prática contraria diretamente o que determina o artigo 46 da LGPD,e a ISO/IEC 27799, que traz regras específicas para proteger registros clínicos. A norma exige cuidados rigorosos no armazenamento, transporte e descarte de documentos médicos, incluindo a destruição completa de materiais

que não podem ser arquivados. Jogar documentos no lixo comum, reutilizar informações sensíveis como rascunho e não orientar sobre o uso da fragmentadora são violações diretas dessas regras e aumentam muito o risco de expor dados clínicos.

A instituição utiliza antivírus atualizado e sistemas operacionais licenciados, o que representa um ponto positivo no aspecto técnico da segurança da informação. Além disso, conta com firewall ativo, responsável por bloquear o acesso a diversos sites externos considerados não seguros. Porém, o bloqueio não é total, permitindo ainda o acesso a algumas páginas que podem representar risco à rede interna.

O hospital oferece uma rede Wi-Fi aberta para visitantes, acessada por meio de login com e-mail pessoal (como Gmail, Outlook ou Facebook), sem outra forma de autenticação. Embora seja prática, essa configuração pode trazer vulnerabilidades, pois não há isolamento total entre essa rede e os sistemas internos. Existem também redes restritas, protegidas por senha, usadas apenas pela diretoria e por alguns colaboradores em atividades administrativas. No entanto, não há uma política formal para gestão, controle ou registro desses acessos, o que dificulta o monitoramento e aumenta o risco de uso indevido.

Outro ponto importante é o acesso remoto concedido a médicos que realizam laudos de exames fora do ambiente hospitalar. Esses profissionais utilizam notebooks pessoais, configurados pela equipe de TI para permitir o acesso remoto seguro aos sistemas necessários. Embora o procedimento facilite o trabalho e garanta agilidade nos atendimentos, ele também aumenta a exposição a riscos, já que os dispositivos não são corporativos, podendo conter softwares não monitorados ou vulneráveis.

Além disso, há um médico terceirizado responsável pelos laudos de eletroencefalograma. Nesse caso, o processo acontece totalmente fora da rede hospitalar: o exame é anexado em uma plataforma online mantida pelo próprio profissional, que emite o laudo e o disponibiliza na mesma plataforma, para depois serem baixados e incluídos no prontuário eletrônico do paciente. Apesar de agilizar o trabalho, essa prática exige cuidado com a segurança na

transmissão dos dados, controle de acesso, uso de criptografia e conformidade com a LGPD.

Mesmo com esses mecanismos, ainda não existe uma política formal para atualização dos sistemas (como patches de segurança) nem uma separação bem definida entre as redes administrativas e assistenciais, o que pode facilitar a propagação de ataques. Também há equipamentos antigos em uso, embora esteja em andamento um processo gradual de substituição. A modernização tecnológica e o controle dos acessos, tanto locais quanto remotos, são essenciais para manter a confidencialidade, integridade e disponibilidade das informações, princípios básicos da segurança da informação.

4.4 Políticas Internas, Governança e Conformidade com a LGPD

A instituição não tem uma política de privacidade disponível ao público, seja no site ou em locais físicos. Além disso, não existe um termo de consentimento para a coleta ou uso de dados sensíveis, como fotos, gravações ou exames, como pede o art. 11 da LGPD. Essa falta de formalização mostra que a instituição ainda não cumpre totalmente o que a lei exige.

Em caso de incidentes, não existe um procedimento formal de resposta, nem definição de responsabilidades para comunicação ou contenção. Falta também a designação de um Encarregado de Proteção de Dados (DPO), função obrigatória prevista pela legislação. A inexistência de papéis formalmente definidos na gestão da privacidade contraria as diretrizes de governança recomendadas pela ISO/IEC 27799, que reforça a necessidade de atribuição clara de responsabilidades e monitoramento contínuo.

Além da ausência de um encarregado formal (DPO), verificou-se que a instituição não realiza Relatórios de Impacto à Proteção de Dados (DPIA) para avaliar riscos associados ao tratamento de dados sensíveis, conforme orienta a LGPD. Também não existe um procedimento estruturado para comunicação de incidentes à ANPD e aos titulares, o que demonstra que os requisitos de

transparência e mitigação previstos na legislação não estão plenamente atendidos.

Por fim, não existem políticas internas nem auditorias periódicas voltadas à segurança da informação, o que impede a instituição de avaliar seus avanços e identificar fragilidades com base em dados concretos. Essa ausência também demonstra que o hospital não possui um SGSI (Sistema de Gestão de Segurança da Informação), como previsto pela ISO/IEC 27001.

Os principais pilares da segurança da informação, confidencialidade, integridade e disponibilidade, são atendidos apenas parcialmente:

- A confidencialidade é comprometida pelo compartilhamento indevido de informações e ausência de bloqueio automático de tela;
- A integridade é ameaçada pela falta de rastreabilidade em logins genéricos e descarte incorreto de papéis;
- A disponibilidade depende de equipamentos antigos e backups irregulares, o que pode afetar o funcionamento em casos de falha técnica.

Mesmo assim, os avanços, como o uso de assinaturas digitais e o controle de acesso por biometria em algumas áreas, mostram que a instituição está em processo de amadurecimento e que o primeiro passo, que é reconhecer a importância da segurança da informação, já foi dado.

Para deixar mais claro onde estão os principais pontos de vulnerabilidade, a Tabela 2 apresenta um resumo dos riscos identificados, com a descrição de cada fragilidade e o impacto que ela pode gerar no hospital.

Tabela 2: Resumo das fragilidades identificadas

Tipo de Risco	Descrição	Impacto Potencial
Acesso não autorizado	Logins genéricos e senhas simples	Vazamento de informações e alteração indevida de dados
Falta de conscientização	Treinamento desatualizado e pontual	Erros humanos e descumprimento da LGPD
Falhas físicas	Livre circulação em áreas restritas	Risco à confidencialidade de documentos

Descarte inadequado	Impressões com dados sensíveis descartadas incorretamente	Exposição de informações pessoais
Falta de política formal	Ausência de DPO e de plano de contingência	Falhas na resposta a incidentes

Fonte: Autores (2025)

A falta de políticas formais, planos de resposta a incidentes e definição clara de responsabilidades coloca a instituição em risco de repetir situações que já foram reconhecidas pela Justiça como falhas graves de proteção de dados. Um exemplo é o caso citado na introdução, em que o TJDFT condenou um hospital público pelo vazamento de informações médicas causado pela falta de controles mínimos de segurança e governança. Do mesmo modo, percebe-se que a ausência de medidas estruturadas de prevenção, registro e resposta pode gerar responsabilização e prejuízos aos pacientes, mostrando que as fragilidades identificadas no hospital analisado não são apenas possibilidades teóricas, mas problemas que já ocorreram na realidade do sistema de saúde brasileiro

Os resultados também permitem retomar os objetivos específicos do estudo. Sobre a comparação das práticas do hospital com as normas ISO/IEC 27001, 27002 e 27799, percebeu-se que várias rotinas, como uso de logins genéricos, falta de bloqueio automático de tela, descarte incorreto de documentos e ausência de políticas formais, não atendem aos controles dessas normas, especialmente nos pontos de gestão de acesso, proteção de mídias, governança e segurança de dados de saúde. Quanto à análise das fragilidades humanas e estruturais, ficou evidente a falta de treinamentos, o uso inseguro de e-mail e WhatsApp, a circulação livre em áreas restritas e o uso de tecnologias desatualizadas, mostrando que os problemas envolvem tanto aspectos técnicos quanto comportamentais. Por fim, no objetivo de identificar estratégias de mitigação para ataques como *ransomware* e *phishing*, as vulnerabilidades encontradas mostram que ações como criar uma política de senhas, segmentar redes, formalizar um plano de resposta a incidentes e oferecer treinamentos

contínuos são medidas fundamentais, e urgentes, diante das falhas identificadas.

4.5 Sugestões de Melhoria e Limitações da Pesquisa

Com base nas observações feitas e na comparação com as normas ISO/IEC 27001, ISO/IEC 27002 e com os princípios da Lei nº 13.709/2018 (LGPD), foi possível identificar pontos importantes que podem ser melhorados para fortalecer a segurança da informação na instituição analisada.

Entre as principais melhorias sugeridas, estão:

- Criar uma Política de Segurança da Informação (PSI) clara, que mostre as responsabilidades de cada um e as regras de uso dos recursos tecnológicos.
- Fazer um plano de gestão de senhas, com troca obrigatória de tempos em tempos, bloqueio automático de tela e senhas com um nível mínimo de segurança.
- Promover treinamentos contínuos sobre LGPD e segurança digital, tanto para quem está chegando quanto para quem já trabalha na instituição, fortalecendo a cultura de proteção de dados.
- Nomear um Encarregado de Proteção de Dados (DPO), como pede a LGPD, como determina a LGPD.
- Adotar regras seguras para o descarte de informações, tanto físicas quanto digitais, orientando sobre o uso da fragmentadora e proibindo o reaproveitamento de documentos sensíveis, em conformidade com a ISO 27799.
- Criar um plano de resposta a incidentes, definindo o que fazer, quem avisar e como agir em caso de falhas de segurança, como previsto na ISO 27001.
- Melhorar o controle físico de acesso, ampliando o uso de catracas e registros de entrada em todas as portarias e áreas restritas.

- Atualizar a infraestrutura tecnológica, trocando equipamentos antigos, atualizando sistemas com frequência e separando melhor as redes dos setores administrativos e assistenciais, seguindo controles da ISO 27002.
- Desenvolver campanhas internas de conscientização, com cartazes e comunicações simples que lembrem boas práticas de segurança e privacidade.

Essas medidas podem ser colocadas em prática aos poucos, de acordo com os recursos e as prioridades da instituição, mas são passos importantes para construir uma cultura de segurança da informação forte e constante.

Sobre as limitações da pesquisa, é importante destacar que o estudo foi feito com base na observação e experiência da pesquisadora em apenas uma instituição pública de saúde, o que limita a possibilidade de aplicar os resultados a outros contextos. Além disso, não foram usados questionários ou entrevistas formais, o que restringe a análise quantitativa sobre a percepção dos colaboradores.

Mesmo assim, os resultados trazem uma visão real das práticas e dos desafios do dia a dia hospitalar, ajudando a gerar reflexões práticas e a abrir caminho para novas pesquisas sobre a aplicação da LGPD e da segurança da informação na área da saúde pública.

5. CONSIDERAÇÕES FINAIS

O principal objetivo deste trabalho foi analisar os desafios de aplicar a Lei Geral de Proteção de Dados (LGPD) em um hospital público de médio porte, observando como a segurança da informação é colocada em prática e o que ainda precisa melhorar. Com as observações e análises feitas, deu para perceber que, mesmo com algumas medidas básicas já em uso, ainda há muitas fragilidades que precisam ser corrigidas.

No caso da instituição estudada, também ficou claro que essas fragilidades técnicas e organizacionais não afetam só a parte prática, mas

também a parte ética, porque a falta de segurança coloca em risco a privacidade e a autonomia dos pacientes. Ou seja, melhorar a proteção dos dados não é só cumprir a LGPD, mas garantir um cuidado mais ético e confiável.

De modo geral, os resultados mostraram que o hospital tem boa intenção em proteger os dados dos pacientes, mas ainda falta uma estrutura mais organizada para isso. A falta de políticas formais, de treinamentos regulares e de um responsável pela proteção de dados deixa a instituição vulnerável e faz com que ela não atenda completamente às exigências da LGPD. Mesmo assim, foram observados alguns avanços, como o uso de assinaturas digitais e o controle por biometria em certas áreas, o que indica um progresso positivo nesse caminho.

Como contribuição, este trabalho mostra a importância de enxergar a segurança da informação como uma prioridade nos hospitais, não só por causa da lei, mas porque é uma forma de cuidar do paciente e garantir que o serviço continue funcionando bem. Coisas simples, como treinar as equipes, revisar senhas e melhorar o controle de acesso, já fazem muita diferença no dia a dia.

Na prática, os resultados podem ajudar gestores, profissionais e equipes técnicas que queiram melhorar a proteção dos dados em hospitais públicos. A experiência mostra que, mais do que ter tecnologia, é preciso ter consciência e participação de todos, desde quem trabalha na recepção até a direção.

Como sugestão para trabalhos futuros, seria interessante fazer novas pesquisas em outras instituições de saúde, tanto públicas quanto privadas, para comparar diferentes níveis de segurança da informação. Também vale aplicar questionários e entrevistas com os colaboradores, para entender melhor o que eles pensam e quais são as maiores dificuldades em relação à LGPD.

Por fim, este estudo mostrou que garantir a segurança dos dados na saúde é um processo contínuo. É algo que depende tanto de tecnologia quanto de pessoas, e só se torna efetivo quando há compromisso coletivo em proteger as informações e respeitar a privacidade de cada paciente.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27000:2021 — Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — Fundamentos e vocabulário. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022 — Segurança da informação, cibersegurança e proteção da privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2019 — Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação. Rio de Janeiro: ABNT, 2019.

Ataque de ransomware em hospital leva paciente à morte na Alemanha. Olhar Digital, 18 set. 2020. Disponível em: https://olhardigital.com.br/2020/09/18/seguranca/ataque-de-ransomware-em-hospital-leva-paciente-a-morte-na-alemanha/. Acesso em: 30 mar. 2025.

BASETTE, F. Ataques cibernéticos à área da saúde crescem; hackers podem alterar até resultados de exames. O Estado de S. Paulo, 30 de mar. 2025 Disponível em: https://www.estadao.com.br/saude/ataques-ciberneticos-a-area-da-saude-crescem-hackers-podem-alterar-ate-resultados-de-exames/. Acesso em: 30 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 set. 2025.

COSTA, Paola. TIC Saúde 2022 aponta avanços na telessaúde, mas segurança de dados ainda deixa a desejar. Futuro da Saúde, 2022. Disponível em: https://futurodasaude.com.br/tic-saude-2022/. Acesso em: 30 set. 2025.

HOLTS, L.; MARIN, I; VEDOLIN, L. Ataques cibernéticos: quando os hackers ameaçam o sistema de saúde. Futuro da saúde, 30 abr. 2024. Disponível em: https://futurodasaude.com.br/ataque-cibernetico/. Acesso em: 30 mar. 2025.

Justiça mantém condenação por vazamento de dados pessoais de paciente. TJDFT, 02 set. 2024. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2024/agosto/justica-mantem-condenacao-por-vazamento-de-dados-pessoais-de-paciente. Acesso em: 25 ago. 2025.

LEME RS, BLANK M. Lei Geral de Proteção de Dados e Segurança da Informação na Área da Saúde. Cadernos Ibero-Americanos de Direito Sanitário. 2020 jul./set.; 9(3): 210-224. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690/. Acesso em: 15 abr. 2025.

MELO, Daniel Ayres de. Privacidade e Proteção de Dados Pessoais em uma Operadora de Plano de Saúde e Suas Unidades Hospitalares. 2020. 56 f. Monografia (Especialização) - Curso de Direito, Departamento de Ciências Jurídicas, Universidade Federal da Paraíba, Santa Rita, 2020.00 de caso no Hospital Unimed Americana. 2018. 19 f. TCC (Graduação) - Curso de Segurança da Informação, Faculdade de Tecnologia de Americana (Fatec Americana), Americana, 2018. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/21263/. Acesso em: 15 abr. 2025.

NEVES, Inon. Proteger informações do paciente ainda é desafio para o setor de Saúde. Saúde Digital News, 24 fev. 2025. Disponível em: https://saudedigitalnews.com.br/24/02/2025/proteger-informacoes-do-paciente-ainda-e-desafio-para-o-setor-de-saude/. Acesso em: 01 set. 2025.

PASSO, Maria Zilá Leal Bezerra. Porque a área da saúde precisa se preocupar com a proteção de dados pessoais. Revista Jurídica Luso-Brasileira, Ano 8 (2022), N.º 2, p. 1301-1317, 2022. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/2/2022_02_1301_1317.pdf. Acesso em: 30 set. 2025.

SILVEIRA, Suzana Aparecida. Segurança a Informação e Proteção de Dados Pessoais*:* estudo de caso e proposta de governança para serviços de saúde. 2021. 211 f. Dissertação (Mestrado) - Curso de Inovação Tecnológica, Departamento de Ciência e Tecnologia, Universidade Federal de São Paulo, São José dos Campos, 2021. Disponível em: https://repositorio.unifesp.br/handle/11600/60909/. Acesso em: 15 abr. 2025

SOUSA, V. L. de; OLIVEIRA, R. de M. e. Os impactos da lei geral de proteção de dados (LGPD) no sistema de saúde brasileiro. Revista JRG de Estudos Acadêmicos, Brasil, São Paulo, v. 7, n. 14, p. e141129, 2024. DOI: 10.55892/jrg.v7i14.1129. Disponível em: https://mail.revistajrg.com/index.php/jrg/article/view/1129. Acesso em: 16 set. 2025.