INSTITUTO FEDERAL DE ALAGOAS
***CAMPUS* MACEIÒ**
BACHARELADO EM SISTEMAS DA INFORMAÇÃO

ÍCARO R. F. MOURA
VICTOR A. M. PACCOLA

UMA ANÁLISE DOS DESAFIOS ORGANIZACIONAIS E TÉCNICOS NA ADEQUAÇÃO DA OPERAÇÃO DE UM HOSPITAL PARTICULAR À LEI GERAL DE PROTEÇÃO DE DADOS

MACEIÓ - AL
2025

ÍCARO R. F. MOURA
VICTOR A. M. PACCOLA

UMA ANÁLISE DOS DESAFIOS ORGANIZACIONAIS E TÉCNICOS NA ADEQUAÇÃO DA OPERAÇÃO DE UM HOSPITAL PARTICULAR À LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação Sistemas de Informação do Instituto Federal de Alagoas, campus Maceió, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Tárcio Rodrigues Bezerra

MACEIÓ - AL
2025

FICHA CATALOGRÁFICA

Dados Internacionais de Catalogação na Publicação
Instituto Federal de Alagoas
Campus Maceió
Biblioteca Benevides Monte

005.8
M929a Moura, Ícaro R. F.
Uma análise dos desafios organizacionais e técnicos na adequação da operação de um hospital particular à lei geral de proteção de dados / Ícaro R. F. Moura, Victor A. M. Paccola. - Dados eletrónicos (1 arquivo : 252 KB). - 2025.

Sistema requerido: Adobe Acrobat Reader
Modo de acesso: Internet.
Orientação: Profª. Dr. Tárcio Rodrigues Bezerro.
Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Instituto Federal de Alagoas, Campus Maceió, Maceió, 2025.

1. LGPD. 2. Segurança da Informação. 3. Governança de Dados. 4. Privacidade. I. Paccola, Victor A. M. II. Título.

Bibliotecária Nalva Maria Amaral / CRB-4/989

ÍCARO R. F. MOURA
VICTOR A. M. PACCOLA

UMA ANÁLISE DOS DESAFIOS ORGANIZACIONAIS E TÉCNICOS NA ADEQUAÇÃO DA OPERAÇÃO DE UM HOSPITAL PARTICULAR À LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação Sistemas de Informação do Instituto Federal de Alagoas, campus Maceió, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Aprovada em: 03/06/2025. Conceito Obtido: APROVADO

Orientador:

gov.br Documento assinado digitalmente
TARCIO RODRIGUES BEZERRA
Data: 25/06/2025 22:03:16-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Tárcio Rodrigues Bezerra - IFAL / Campus Maceió

Banca examinadora:

gov.br Documento assinado digitalmente
MONICA XIMENES CARNEIRO DA CUNHA
Data: 26/06/2025 15:39:49-0300
Verifique em https://validar.iti.gov.br

Prof.ª Dr.ª Mônica Ximenes Carneiro da Cunha – IFAL / Campus Maceió

Prof. Dr. Tárcio Rodrigues Bezerra – IFAL / Campus Maceió

gov.br Documento assinado digitalmente
RICARDO RUBENS GOMES NUNES FILHO
Data: 26/06/2025 20:38:22-0300
Verifique em https://validar.iti.gov.br

Prof. Ricardo Rubens Gomes Nunes Filho - IFAL / Campus Maceió

AGRADECIMENTOS

Agradeço à minha família, especialmente aos meus pais, Elaine Paccola e Francis Paccola, pelo apoio constante e por acreditarem em mim em todos os momentos. À minha noiva, Ana Larissa, por seu incentivo e presença firme durante toda a trajetória.

Sou grato ao Prof. Dr. Tárcio Rodrigues Bezerra, meu orientador, pela orientação, paciência e contribuições valiosas ao desenvolvimento desta pesquisa.

Agradeço também aos professores e à coordenação do curso de Bacharelado em Sistemas de Informação, pelo conhecimento compartilhado e pelo apoio à minha formação.

A Deus, e à minha avó Maria Noemia (*in memoriam*), minha eterna inspiração, deixo meu agradecimento mais profundo.

Por fim, agradeço a todos que contribuíram, de alguma forma, para a realização deste trabalho.

Victor Aurelio Melo Paccola

A realização deste Trabalho de Conclusão de Curso representa não apenas o encerramento de uma etapa acadêmica, mas também a concretização de um sonho que só foi possível com o apoio de muitas pessoas especiais.

Agradeço à minha família, em especial à minha mãe Edilene Moura e minha bisa, Deusa Almeida (*in memoriam*) estou aqui realizando o nosso sonho, pelo amor incondicional, pelos valores que me foram ensinados e por estar sempre ao meu lado, torcendo por mim e apoiando minhas decisões.

Aos meus colegas e amigos, que compartilharam comigo os desafios da graduação e me ofereceram apoio nos momentos mais difíceis.

Ao meu orientador, Prof. Dr. Tárcio Rodrigues Bezerra, pela paciência, dedicação e valiosas contribuições durante todo o processo. Seu conhecimento e incentivo foram fundamentais para a construção deste trabalho.

A todos os professores que, ao longo do curso, contribuíram com seus ensinamentos e exemplos, auxiliando na minha formação pessoal e profissional.

E a todos que, direta ou indiretamente, fizeram parte dessa trajetória, deixo aqui minha mais sincera gratidão.

Ícaro Rodolpho de Farias Moura

PACCOLA, Victor A. M.; MOURA, Ícaro R. F. Uma análise dos desafios organizacionais e técnicos na adequação da operação de um hospital particular à Lei Geral de Proteção de Dados. 2025. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal de Alagoas, Campus Maceió, 2025.

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) impõe desafios relevantes para instituições de saúde, sobretudo no tratamento de dados sensíveis de pacientes. Este estudo investiga a adequação de um hospital privado de grande porte à LGPD, com ênfase nos sistemas de informação e nas práticas de segurança da informação, buscando identificar os principais obstáculos técnicos e organizacionais enfrentados durante o processo de conformidade. Para tanto, adota-se o modelo metodológico Goal-Question-Metric (GQM), que permitiu estruturar a análise a partir da definição de objetivos mensuráveis, questões investigativas e métricas associadas. Os resultados revelam lacunas em aspectos como infraestrutura de segurança, gestão de acessos, atualização contratual e treinamento de colaboradores, evidenciando deficiências na governança da privacidade e na implementação de controles internos. Com base nas evidências obtidas por meio de análise documental e validação com profissionais da instituição, são propostas recomendações para o aprimoramento da conformidade normativa, contribuindo para a proteção efetiva dos dados pessoais no ambiente hospitalar.

Palavras-chave: LGPD. Segurança da Informação. Governança de Dados. Privacidade.

PACCOLA, Victor A. M.; MOURA, Ícaro R. F. An analysis of organizational and technical challenges in the adaptation of a private hospital’s operation to the General Data Protection Law. 2025. Undergraduate Thesis (Bachelor’s Degree in Information Systems) – Federal Institute of Alagoas, Maceió Campus, 2025.

ABSTRACT

The Brazilian General Data Protection Law (LGPD) presents significant challenges for healthcare institutions, especially regarding the handling of patients' sensitive data. This study investigates the compliance process of a large private hospital with the LGPD, focusing on information systems and information security practices to identify the main technical and organizational challenges encountered. The research adopts the Goal-Question-Metric (GQM) model, which enabled a structured analysis based on defined objectives, investigative questions, and measurable metrics. The results reveal gaps in areas such as security infrastructure, access management, contract updates, and staff training, indicating weaknesses in data governance and the implementation of internal controls. Based on the evidence gathered through document analysis and validation with institutional professionals, this study proposes recommendations to enhance regulatory compliance and strengthen the protection of personal data in hospital environments.

Key words: LGPD. Information Security. Data Governance. Privacy.

LISTA DE FIGURAS

LISTA DE QUADRO

LISTA DE ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados

CDC – Código de Defesa do Consumidor

CFM – Conselho Federal de Medicina

DPO – Data Protection Officer (Encarregado de Proteção de Dados)

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados da União Europeia)

GQM – Goal-Question-Metric (Objetivo-Pergunta-Métrica)

ISO – International Organization for Standardization (Organização Internacional de Padronização)

IEC – Comissão Eletrotécnica Internacional

LGPD – Lei Geral de Proteção de Dados

NIST – National Institute of Standards and Technology

RBAC – Role-Based Access Control (Controle de Acesso Baseado em Função)

SGSI – Sistema de Gestão de Segurança da Informação

TI – Tecnologia da Informação

CSF – Estrutura de Segurança Cibernética

SUMÁRIO

1. INTRODUÇÃO

A proteção da privacidade de dados é um direito fundamental assegurado a todo cidadão, sendo essencial para garantir que suas informações pessoais sejam resguardadas contra acessos indevidos e violações de segurança. Com o avanço tecnológico e a crescente digitalização dos serviços, a proteção de dados tornou-se uma preocupação central em diversos setores, demandando a implementação de mecanismos legais robustos que regulamentem a coleta, o armazenamento e o tratamento de dados pessoais. No Brasil, esse tema foi formalmente regulamentado com a promulgação da LGPD, instituída pela Lei nº 13.709/2018, que estabelece diretrizes claras para o tratamento de dados pessoais por organizações públicas e privadas, com o objetivo de garantir a segurança, a transparência e o respeito aos direitos dos titulares dos dados (Aragão & Schiocchet, 2020).

No contexto atual, a LGPD desempenha um papel fundamental ao estabelecer diretrizes que asseguram que os dados pessoais fornecidos às organizações sejam tratados de maneira ética e responsável, promovendo maior transparência e governança na relação entre instituições e indivíduos (Doneda, 2019). No setor da saúde, essa legislação introduziu mudanças significativas, exigindo que hospitais e demais estabelecimentos de assistência médica informem claramente os motivos da coleta de dados, bem como os meios e finalidades de seu tratamento, garantindo que os pacientes tenham conhecimento prévio sobre como, quando e por quem essas informações serão utilizadas (Cueva, 2017). Esse requisito é de extrema relevância, pois os dados dos pacientes constituem um dos ativos mais críticos para o funcionamento de sistemas hospitalares, impactando diretamente a prestação de serviços, a continuidade do atendimento e a gestão institucional (Schirmer & Thaines, 2021). Dessa forma, garantir a segurança e a integridade dessas informações não apenas fortalece a conformidade legal, mas também consolida um compromisso ético com a privacidade e a dignidade dos indivíduos.

Isso impõe desafios adicionais para a proteção de dados pessoais, especialmente diante da obrigatoriedade de conformidade com a LGPD. Hospitais e instituições de saúde lidam diariamente com um grande volume de informações sensíveis, incluindo prontuários médicos, resultados de exames laboratoriais, registros de consultas e dados biométricos, o que torna a adequação à legislação um fator essencial para a privacidade e segurança dos pacientes. No entanto, a implementação da LGPD não se restringe apenas à adoção de medidas técnicas e jurídicas, mas exige também mudanças estruturais, culturais e processuais dentro das

organizações, impactando desde a governança da informação até a capacitação contínua dos colaboradores.

Diante desse cenário, emerge o questionamento central desta pesquisa: quais são os principais desafios enfrentados na busca pela conformidade? Para responder a essa questão, a presente pesquisa utilizará o modelo GQM (Goal-Question-Metric) como uma abordagem estruturada para avaliar o nível de conformidade do hospital com a LGPD. A validação dessa estrutura será realizada por meio da coleta de documentos e análise dos dados fornecidos pelos profissionais envolvidos no processo de adequação, possibilitando a identificação de lacunas e oportunidades de melhoria. Assim, espera-se que os achados deste estudo contribuam para o aprimoramento das práticas de governança e segurança da informação nas instituições de saúde, promovendo uma cultura organizacional voltada à proteção da privacidade e à conformidade regulatória.

1.1. OBJETIVO

A objetificação científica em um Trabalho de Conclusão de Curso (TCC) refere-se à formulação clara, específica e mensurável dos objetivos da pesquisa, permitindo que o estudo tenha direcionamento, coerência e validade acadêmica. Ela envolve a definição do objetivo geral, que estabelece a finalidade central da investigação, e dos objetivos específicos, que detalham os passos necessários para alcançar essa meta.

1.1.1. Objetivo Geral

Investigar o processo de implementação da LGPD em um hospital privado de grande porte, analisando os desafios técnicos e organizacionais enfrentados pelos membros da organização na adequação à conformidade regulatória.

1.1.2. Objetivos Específicos

- Identificar e medir a eficácia das práticas de segurança da informação adotadas para garantir a conformidade com a LGPD.
- Analisar o nível de conscientização da organização em relação aos requisitos da LGPD.

- Avaliar os desafios técnicos e organizacionais enfrentados na implementação da LGPD no hospital, a partir da percepção dos membros da organização.
- Compreender os impactos percebidos pela organização após a implantação da LGPD.

1.2. ABORDAGEM DA PESQUISA

A pesquisa adota uma abordagem metodológica mista, combinando métodos qualitativos e quantitativos, com foco na investigação dos desafios técnicos e organizacionais enfrentados na implementação da LGPD em um hospital privado. O estudo busca compreender a experiência da organização a partir do ponto de vista dos seus membros, utilizando o framework Goal-Question-Metrics (GQM) (BASILI et al., 1994) como estrutura analítica. Para isso, foram analisados documentos institucionais, conduzida uma investigação de causas raízes, além da aplicação de questionários de validação que permitirão a coleta e análise de dados quantitativos.

1.3. DELIMITAÇÃO DO ESTUDO

Este estudo se limita à análise da implementação da LGPD em um hospital privado específico, considerando os desafios encontrados durante esse processo. A pesquisa foca na percepção dos membros da organização que participaram ou foram impactados pela implementação, sem realizar uma avaliação formal da conformidade do hospital à legislação. Além disso, a investigação abrange aspectos técnicos e organizacionais, sem se aprofundar em questões jurídicas ou regulatórias externas, mas buscando evidenciar o esforço organizacional interno empreendido nesta jornada.

1.4. JUSTIFICATIVA

A implementação da LGPD representa um grande desafio para instituições de saúde, devido à complexidade do tratamento de dados sensíveis, à necessidade de adequação de processos internos e ao impacto organizacional gerado por essa transformação. No contexto hospitalar, onde o sigilo e a segurança das informações são fundamentais, compreender os desafios enfrentados pode contribuir para uma visão mais clara das dificuldades práticas que surgem nesse processo (Gonçalves & Werner, 2024). Essa realidade se torna ainda mais

crítica em ambientes hospitalares, que lidam com um elevado volume de dados sensíveis, como prontuários médicos, históricos de exames e informações biométricas. A exposição indevida desses dados pode gerar consequências significativas para os pacientes, incluindo riscos de discriminação, fraudes e violações à privacidade.

Este estudo busca compreender os desafios enfrentados pelos hospitais na conformidade com a LGPD, considerando o impacto ético e legal dessas violações, e se justifica pela necessidade de documentar e analisar os desafios da implementação da LGPD do ponto de vista dos membros da organização, gerando conhecimento que pode auxiliar outras instituições em processos semelhantes. A escolha da abordagem do GQM permite estruturar a investigação de maneira objetiva e mensurável, garantindo que os desafios sejam identificados de forma sistemática e alinhada à realidade do hospital.

Além disso, ao registrar as percepções dos envolvidos, a pesquisa poderá contribuir para a compreensão das dificuldades técnicas e organizacionais enfrentadas, promovendo um entendimento mais aprofundado sobre os impactos da LGPD em ambientes hospitalares. Pesquisas anteriores indicam que a adoção de metodologias estruturadas auxilia na adaptação e conformidade com regulamentações de proteção de dados (Botelho & Camargo, 2021).

1.5. ESTRUTURA DO TRABALHO

Este trabalho está organizado em cinco capítulos, conforme descrito a seguir:

O **Capítulo 1** apresenta o contexto da pesquisa, o problema investigado, os objetivos gerais e específicos, a justificativa e a abordagem metodológica adotada.

Já no **Capítulo 2**, é apresentado o Referencial Teórico que fundamenta o estudo, por meio da revisão da literatura sobre a LGPD e sua aplicação no setor hospitalar. Aborda também *frameworks* de governança e segurança da informação, como ISO/IEC 27001, ISO/IEC 27701, NIST Privacy Framework e a metodologia GQM.

O **Capítulo 3** trata da Metodologia, descreve a abordagem utilizada no estudo, baseada na aplicação do modelo GQM para estruturação e avaliação dos desafios da adequação hospitalar à LGPD. São apresentados os métodos de coleta e análise de dados, incluindo a investigação documental, os questionários aplicados e a validação das métricas propostas.

O **Capítulo 4** apresenta Resultados e Discussão. Expõe as principais descobertas da pesquisa, detalhando os desafios enfrentados pelo hospital no processo de conformidade com

a LGPD. São analisados aspectos como segurança da informação, adequação contratual, gestão de consentimento, monitoramento de auditorias e capacitação dos colaboradores.

O **Capítulo 5** (Conclusão) apresenta as considerações finais do estudo, destacando os principais achados frente aos objetivos estabelecidos, limitações da pesquisa e sugestões para trabalhos futuros.

2. REFERENCIAL TEÓRICO

O referencial teórico do estudo abrange três principais eixos: (1) a LGPD e sua aplicação no contexto hospitalar, (2) o framework GQM para estruturação da investigação, e (3) normas e frameworks complementares que orientam a segurança da informação e governança de dados.

2.1. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei nº 13.709/2018, conhecida como LGPD, estabelece diretrizes para o tratamento de dados pessoais no Brasil. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD busca garantir a privacidade e a segurança dos dados, além de estabelecer direitos para os titulares das informações e obrigações para as organizações que realizam o tratamento desses dados.

A LGPD entrou em vigor em setembro de 2020 e trouxe mudanças significativas para empresas e instituições públicas e privadas. Seus princípios fundamentais incluem transparência, necessidade, adequação, segurança e responsabilização. A lei exige que organizações mapeiem e classifiquem os dados que tratam, justifiquem sua coleta com uma base legal, obtenham consentimento quando necessário, e garantam direitos como acesso, retificação e exclusão de dados.

A fiscalização e a aplicação da LGPD no Brasil são conduzidas pela Autoridade Nacional de Proteção de Dados (ANPD), que tem o papel de regulamentar, orientar e aplicar sanções às empresas que descumprem as regras.

2.1.1. A LGPD no Ambiente Hospitalar

A aplicação da LGPD no setor da saúde, especialmente em hospitais, é um desafio complexo, pois envolve o tratamento de dados sensíveis, como informações sobre o estado de

saúde dos pacientes, prontuários médicos, exames laboratoriais e históricos clínicos. Esses dados requerem um nível elevado de segurança, uma vez que sua exposição indevida pode resultar em danos significativos aos titulares, como discriminação, fraudes e violações da privacidade (Gonçalves & Werner, 2024).

No ambiente hospitalar, a LGPD exige a adoção de princípios fundamentais, como transparência, necessidade, adequação e segurança no tratamento de dados. Além disso, é necessário garantir medidas técnicas e administrativas que protejam as informações pessoais contra acessos não autorizados e incidentes de segurança (Gonçalves & Werner, 2024). A conformidade com a Lei também implica a adoção de práticas de governança de privacidade, anonimização de dados sempre que possível e minimização da coleta de informações sensíveis.

O Art. 11 da LGPD estabelece regras específicas para o tratamento desses dados, exigindo maior nível de proteção e limitando seu uso a finalidades legítimas, como a prestação de serviços de saúde e pesquisa científica (Botelho & Camargo, 2021). Segundo Gonçalves & Werner (2024), é imprescindível que hospitais adotem sistemas de informação interoperáveis para garantir segurança e continuidade do atendimento ao paciente, minimizando riscos de exposição indevida dos dados sensíveis. A seguir quadro 1 lista alguns desafios comuns encontrados na literatura em um ambiente hospitalar:

Quadro 1 - Lista de desafios em hospitais

Hospitais enfrentam desafios como:
Mapeamento e controle do fluxo de dados pessoais dos pacientes (Gonçalves & Werner, 2024);
Definição de bases legais para o tratamento dos dados (consentimento, cumprimento de obrigação legal, proteção da vida, entre outros) (Botelho & Camargo, 2021);
Adoção de medidas de segurança para evitar vazamentos e acessos não autorizados (Cetic, 2021);
Treinamento dos profissionais de saúde e administrativos sobre boas práticas de privacidade e proteção de dados (Gonçalves & Werner, 2024);
Adequação de contratos e relações com terceiros (planos de saúde, laboratórios, fornecedores de tecnologia, etc.) (ANAHP, 2019).

Fonte: Elaborado pelos autores.

A LGPD exige que hospitais desenvolvam políticas de privacidade e governança de dados, estabeleçam processos de resposta a incidentes de segurança e nomeiem um Encarregado de Proteção de Dados (DPO) para garantir a conformidade (Gonçalves & Werner, 2024). Além disso, a anonimização e a pseudo-anonimização de dados, sempre que possível, são ferramentas essenciais para mitigar riscos e garantir a segurança da informação no setor hospitalar (Botelho & Camargo, 2021). A anonimização, ao remover permanentemente qualquer possibilidade de associação dos dados a um indivíduo, isenta essas informações das exigências da LGPD. Já a pseudo-anonimização permite a utilização dos dados de forma controlada, uma vez que os identificadores são armazenados separadamente em ambiente seguro. Dessa forma, hospitais podem utilizar dados para pesquisa e análise sem comprometer a privacidade dos pacientes. No entanto, mesmo com essas técnicas, é essencial adotar medidas adicionais de proteção, como criptografia e controle de acessos, garantindo que as informações permaneçam protegidas contra acessos indevidos e usos inadequados.

2.2. GOAL-QUESTION-METRIC (GQM)

A mensuração estruturada e orientada a objetivos é uma técnica essencial que apoia o entendimento, o controle, a previsão, a avaliação e a melhoria de processos e produtos (Pfhal, 2002). O modelo Goal-Question-Metric (GQM), desenvolvido por Basili, Caldiera e Rombach (1994), é amplamente reconhecido por sua aplicação em iniciativas de melhoria contínua e avaliação de conformidade, especialmente em ambientes que exigem uma abordagem estruturada para análise e mensuração. Sua principal contribuição está na capacidade de alinhar os objetivos organizacionais às práticas de medição, promovendo coerência entre o que se deseja alcançar e o que de fato é observado. A escolha por esse modelo nesta pesquisa justifica-se pela necessidade de transformar dados documentais em informações relevantes e organizadas logicamente, assegurando uma base metodológica clara para a tomada de decisão e interpretação dos resultados, conforme será detalhado na seção de metodologia.

2.3. NORMAS E FRAMEWORKS COMPLEMENTARES

A implementação da LGPD em um ambiente hospitalar não pode ser dissociada de boas práticas e normas já consolidadas na área de segurança da informação e governança de dados. Algumas das principais referências que complementam a análise são:

2.3.1. Regulamentos e Leis Complementares

A governança da privacidade e a segurança da informação no Brasil não se limitam à LGPD, sendo complementadas por outras normativas que garantem a proteção dos dados pessoais e regulamentam seu uso em diferentes contextos. O Código de Defesa do Consumidor (Lei nº 8.078/1990), por exemplo, assegura aos consumidores o direito de acesso e correção de seus dados, reforçando a transparência e a responsabilidade no tratamento dessas informações (BRASIL, 1990). Já o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios para o uso da internet, garantindo privacidade, proteção de dados e segurança digital, sendo um dos principais marcos regulatórios para o tratamento de informações pessoais em ambientes digitais (BRASIL, 2014).

Além dessas leis, normativas específicas, como a Resolução CFM nº 1.821/2007, do Conselho Federal de Medicina, reforçam a importância do sigilo médico e da confidencialidade dos dados de saúde, exigindo que instituições médicas adotem medidas para proteger informações sensíveis dos pacientes (CFM, 2007). A integração dessas legislações à LGPD fortalece a governança de dados e orienta a implementação de boas práticas de segurança e conformidade regulatória, contribuindo para um ambiente mais seguro e confiável no tratamento de informações pessoais.

2.3.1.1. Código de Defesa do Consumidor (Lei nº 8.078/1990)

O Código de Defesa do Consumidor (CDC), instituído pela Lei nº 8.078/1990, representa um marco regulatório essencial para a proteção dos consumidores no Brasil, garantindo direitos fundamentais como transparência, segurança e acesso à informação. Embora sua aplicação seja mais evidente nas relações comerciais, sua interseção com a governança da privacidade e proteção de dados se intensificou com a entrada em vigor da LGPD, especialmente no setor da saúde, onde pacientes figuram como consumidores de serviços médicos (BRASIL, 1990).

No ambiente hospitalar, o CDC assegura que pacientes tenham acesso irrestrito às suas informações de saúde, incluindo prontuários médicos, exames laboratoriais e históricos

clínicos, conforme estabelecido no artigo 43. A regulamentação exige que as instituições de saúde garantam clareza e precisão nos dados armazenados, possibilitando que o titular solicite correções ou exclusão de informações equivocadas. Além disso, a proteção contra práticas abusivas, como compartilhamento não autorizado de dados médicos com operadoras de planos de saúde ou terceiros, reforça a importância da conformidade hospitalar com princípios éticos e legais de segurança da informação.

Dessa forma, o CDC, em conjunto com a LGPD, impõe diretrizes para a transparência na relação entre instituições médicas e pacientes, exigindo que os hospitais justifiquem a coleta, armazenamento e uso de dados sensíveis, garantindo segurança jurídica e minimizando riscos regulatórios e éticos.

2.3.1.2. Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios fundamentais para proteção da privacidade e governança de dados em ambientes digitais, assegurando que informações pessoais não sejam expostas indevidamente por provedores de serviços e plataformas digitais. Sua aplicação no setor da saúde se tornou cada vez mais relevante devido à crescente digitalização dos prontuários médicos, integração de plataformas hospitalares e avanço da telemedicina, exigindo medidas robustas de segurança da informação e proteção contra acessos indevidos (BRASIL, 2014).

No contexto hospitalar, o artigo 7º do Marco Civil da Internet assegura a inviolabilidade das comunicações eletrônicas e a proteção de registros médicos armazenados em ambientes digitais. Isso significa que sistemas de prontuário eletrônico, plataformas de teleconsulta e bases de dados hospitalares devem adotar protocolos de criptografia, controle de acessos e autenticação robusta, impedindo que informações sensíveis sejam interceptadas ou vazadas indevidamente (PINHEIRO; BONNA, 2020).

Além disso, a regulamentação estabelece que hospitais e instituições médicas que utilizam serviços digitais devem garantir que os dados sejam armazenados de forma segura e que o acesso esteja restrito aos profissionais autorizados. O descumprimento dessas diretrizes pode acarretar responsabilidade legal e sanções regulatórias, evidenciando a necessidade de um alinhamento rigoroso entre a infraestrutura digital hospitalar e os princípios da proteção de dados.

2.3.1.3. Resolução CFM nº 1.821/2007 – Sigilo Médico e Proteção de Dados

A Resolução CFM nº 1.821/2007, do Conselho Federal de Medicina (CFM), reforça a necessidade de proteção de dados sensíveis em ambientes médicos, estabelecendo diretrizes sobre sigilo profissional e privacidade das informações de saúde dos pacientes. A regulamentação estabelece que dados médicos são confidenciais e não podem ser divulgados sem autorização expressa do paciente, salvo em casos previstos em lei, o que está diretamente alinhado aos princípios da LGPD (CFM, 2007).

Com a digitalização dos prontuários eletrônicos e o uso crescente de tecnologias de gestão hospitalar, a necessidade de conformidade com essa resolução se tornou ainda mais evidente. A Resolução CFM nº 1.821/2007 determina que instituições de saúde implementem medidas de segurança para impedir acessos indevidos a informações médicas, recomendando práticas como anonimização de dados, restrição de acessos e auditoria contínua dos registros eletrônicos.

Além disso, a resolução destaca a responsabilidade ética e legal dos profissionais de saúde na manipulação de dados médicos, prevendo sanções disciplinares em casos de vazamento ou uso indevido de informações de pacientes. Essa regulamentação, quando integrada às exigências da LGPD e às normas internacionais de segurança da informação, como a ISO/IEC 27701, garante maior proteção da privacidade e governança eficiente dos dados hospitalares (ALVES; MENDONÇA, 2020).

2.3.2. Normas e Frameworks Internacionais para Segurança e Privacidade da Informação

2.3.2.1. ISO/IEC 27001 – Gestão da Segurança da Informação

A ISO/IEC 27001 é a principal norma internacional para gestão da segurança da informação. Ela define requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), incluindo:

- Políticas e controles de segurança para garantir a confidencialidade, integridade e disponibilidade dos dados;
- Gestão de riscos de segurança da informação para identificar e mitigar vulnerabilidades;

- Monitoramento e auditorias regulares para garantir a conformidade e a melhoria contínua.

A conformidade com a ISO/IEC 27001 é um diferencial para hospitais, pois reforça a adoção de práticas robustas para a proteção de dados sensíveis.

2.3.2.2. ISO/IEC 27701 – Gestão da Privacidade da Informação

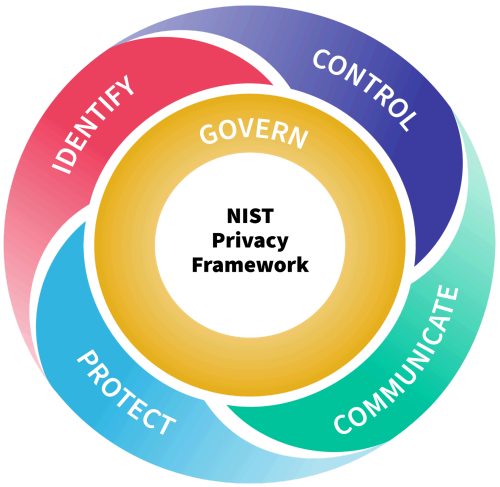
A ISO/IEC 27701 complementa a ISO/IEC 27001, trazendo diretrizes específicas para privacidade e proteção de dados pessoais. Essa norma é altamente relevante para hospitais, pois ajuda a estruturar processos alinhados à LGPD e ao GDPR, incluindo:

- Políticas de governança de privacidade;
- Gestão de consentimento e direitos dos titulares de dados;
- Processos de resposta a incidentes de privacidade.

2.3.2.3. NIST Privacy Framework – Estrutura de Governança da Privacidade

O NIST Privacy Framework, desenvolvido pelo National Institute of Standards and Technology (NIST) dos EUA, é um modelo amplamente adotado para a gestão da privacidade em organizações. Ele fornece um framework de riscos para que instituições identifiquem, avaliem e reduzam impactos na proteção de dados pessoais.
Os pilares do NIST estão representados na imagem abaixo:

Figura 1. Funções da NIST Privacy Framework



Fonte: NIST Privacy Framework

3. METODOLOGIA

3.1. TIPO DE PESQUISA

Esta pesquisa caracteriza-se como um estudo de caso único com abordagem de método misto, de natureza observacional. A estrutura metodológica adotada neste estudo foi parcialmente inspirada na proposta apresentada por Bezerra (2014), especialmente quanto à sistematização de fases, validação empírica e aplicação de métodos observacionais em estudos de caso institucionais. O foco está na análise sistemática de documentos institucionais produzidos por consultores externos contratados por um hospital privado de grande porte, no contexto de sua adequação à LGPD. Em nenhuma etapa houve intervenção direta no processo analisado; a pesquisa se restringe à observação, categorização e interpretação crítica dos registros já existentes.

A abordagem qualitativa esteve presente na leitura crítica e interpretação dos documentos, relatórios, atas, registros e evidências organizacionais que retratam o esforço de conformidade à LGPD. Já a dimensão quantitativa foi incorporada por meio da aplicação da ferramenta GQM, que permite extrair métricas específicas associadas aos desafios e objetivos levantados durante o diagnóstico.

A escolha pelo método misto justificou-se pela complexidade da temática, que envolve aspectos subjetivos — como cultura organizacional, percepção institucional e maturidade em governança de dados — e também indicadores objetivos, como número de treinamentos realizados, níveis de conformidade técnica, ou medidas de segurança implementadas. A análise combinada possibilita uma compreensão mais completa do cenário organizacional e das dificuldades enfrentadas.

Dessa forma, o estudo se estrutura como uma pesquisa aplicada, exploratória e observacional, voltada à compreensão e avaliação crítica de um processo institucional específico, sem que haja qualquer manipulação direta sobre os dados ou os envolvidos.

3.2. PROCEDIMENTOS METODOLÓGICOS

Do ponto de vista metodológico, esta pesquisa adota um método científico de natureza exploratória, observacional e descritiva. É exploratória por buscar aprofundar o conhecimento sobre os desafios enfrentados por uma organização de saúde na implementação da LGPD, tema ainda recente e em constante evolução. É observacional porque não há qualquer

interferência do pesquisador no ambiente ou nos dados analisados; toda a investigação se baseia em registros e documentos previamente produzidos por terceiros. Por fim, é descritiva na medida em que se propõe a caracterizar e interpretar, com base em evidências documentais, o processo de adequação realizado pela organização.

A pesquisa se ancora em uma abordagem sistêmica, reconhecendo que a conformidade com a LGPD não se limita à adoção de ferramentas tecnológicas, mas envolve a interdependência entre pessoas, processos, cultura organizacional, políticas institucionais e infraestrutura de segurança da informação. O olhar sistêmico permite compreender como esses elementos se articulam — ou falham em se articular — no contexto da governança de dados pessoais.

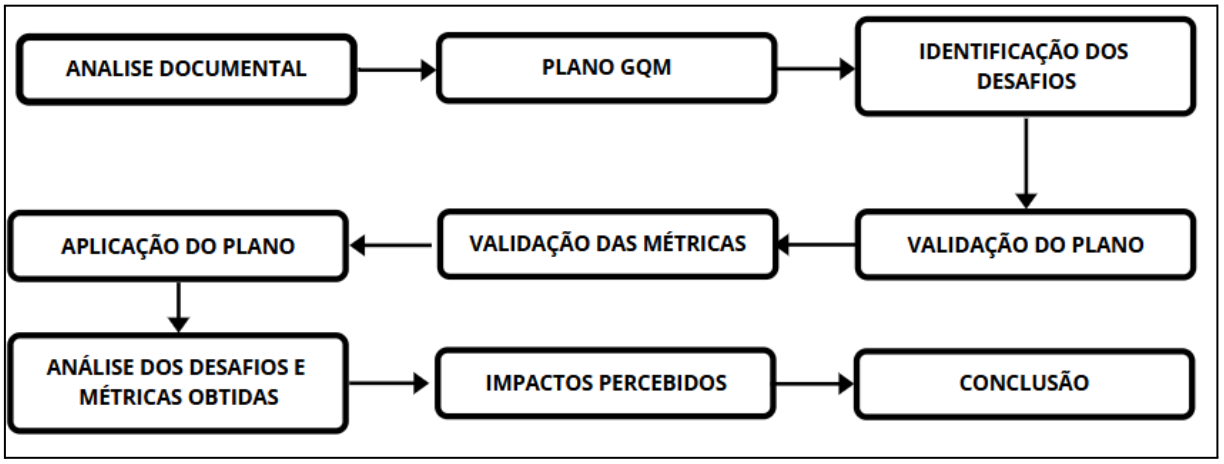
Do ponto de vista epistemológico, a pesquisa adota uma postura pós-positivista, reconhecendo que, embora busque ancorar-se em dados concretos e verificáveis, a realidade organizacional é atravessada por fatores subjetivos, como cultura, valores, percepções e resistências internas. Essa perspectiva permite equilibrar a análise objetiva dos dados com a compreensão contextualizada do comportamento institucional diante da regulação imposta pela LGPD.

Como ferramenta de avaliação, utiliza-se a estrutura GQM – Goal-Question-Metric, que fornece um arcabouço lógico e orientado por objetivos para a formulação das perguntas de pesquisa e para a definição das métricas observáveis. Essa estrutura será aplicada após uma fase inicial de diagnóstico, funcionando como ferramenta analítica para organizar os dados levantados em blocos coerentes e alinhados com os propósitos do estudo. A aplicação do GQM permite não apenas sistematizar a análise, mas também conferir maior objetividade à avaliação do nível de conformidade da organização, à luz das diretrizes da LGPD e das boas práticas em segurança da informação.

3.3. DESENHO DA PESQUISA

A estrutura metodológica desta pesquisa está representada na Figura 2 na qual apresenta o desenho metodológico da pesquisa, detalhando as etapas seguidas na condução do estudo. O desenho da pesquisa foi organizado de forma sequencial e lógica, partindo da análise documental dos registros institucionais até a identificação dos impactos percebidos pela organização em relação à implementação da LGPD.

Figura 2. Desenho da Pesquisa



Fonte: Elaborado pelos autores

Inicialmente, foi realizada uma análise documental com o objetivo de compreender o contexto organizacional, os processos adotados e os registros gerados durante a tentativa de conformidade com a legislação. A partir dessa base, foi desenvolvido um plano estruturado conforme o modelo GQM (Goal-Question-Metric), permitindo a definição de objetivos analíticos, perguntas de investigação e métricas mensuráveis.

Na sequência, o plano GQM foi submetido a uma etapa de validação com membros da organização, a fim de assegurar sua aderência à realidade institucional e aprimorar a coerência dos indicadores propostos. Por fim, foi conduzida uma avaliação dos impactos percebidos, com base em questionário estruturado, permitindo mensurar os efeitos técnicos e organizacionais associados à implementação da LGPD.

3.4. ANÁLISE DOCUMENTAL

A etapa de análise documental será conduzida com o objetivo de examinar registros institucionais relacionados ao processo de adequação do hospital estudado à LGPD. Esta etapa metodológica teve caráter exploratório e descritivo, sendo estruturada de forma não intervencionista, a fim de garantir a integridade dos dados e a fidelidade ao contexto original no qual foram produzidos.

Foram coletados documentos internos previamente elaborados por consultores externos e equipes técnicas da instituição, incluindo atas de reuniões, relatórios técnicos, políticas internas, planos de ação, registros de treinamentos, inventários de dados e sistemas,

bem como demais materiais institucionais que contenham evidências das ações vinculadas ao processo de conformidade com a LGPD.

A seleção documental foi orientada por critérios de pertinência e relevância, priorizando registros que contenham informações diretamente relacionadas aos aspectos técnicos e organizacionais da implementação. Tais documentos foram analisados criticamente, com o intuito de identificar lacunas, inconsistências e oportunidades de melhoria nos procedimentos adotados pela instituição.

Além disso, foi verificada a existência de estruturas metodológicas prévias, como a adoção de roteiros operacionais ou roadmaps, que possam indicar o planejamento interno conduzido durante a adequação. Estes elementos servirão de insumo para a posterior construção do plano de mensuração baseado na abordagem GQM, garantindo que os objetivos analíticos e métricas propostos estejam fundamentados em evidências empíricas documentadas.

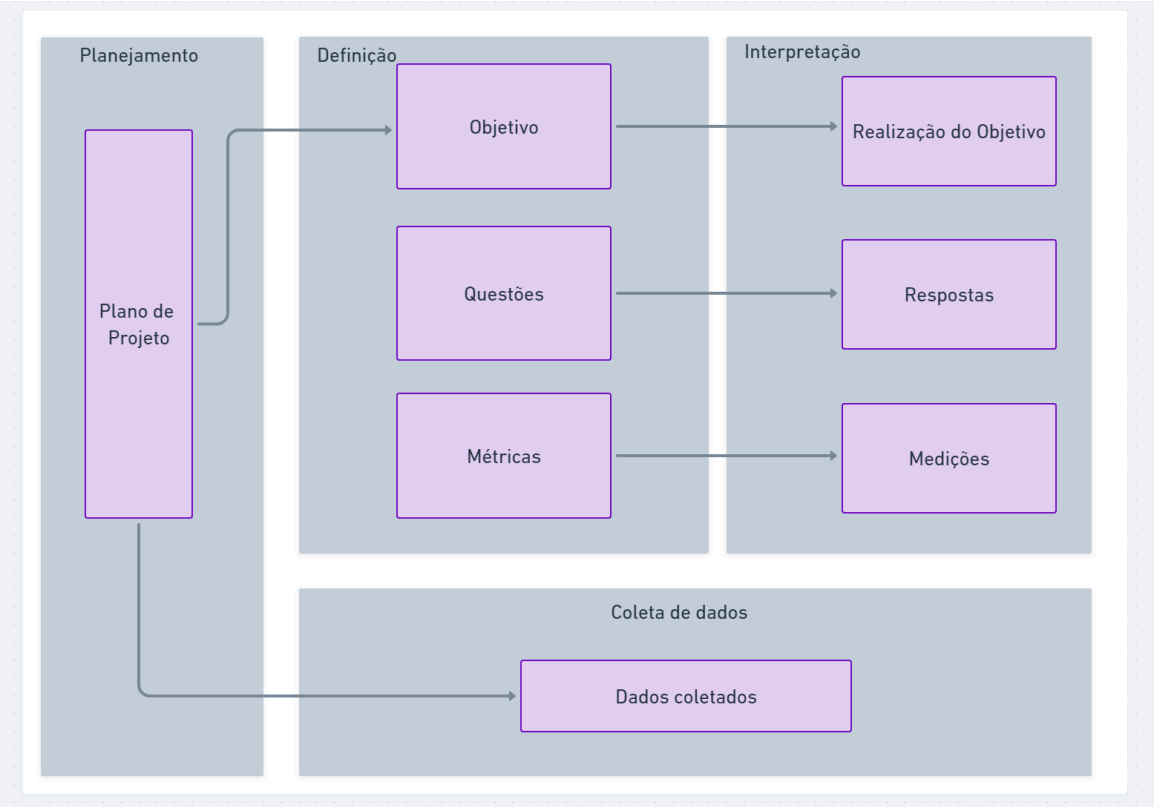
Dessa forma, a análise documental desempenhou papel fundamental na delimitação dos desafios institucionais enfrentados, subsidiando a formulação dos objetivos da pesquisa, a definição das métricas observáveis e a organização lógica do modelo metodológico adotado.

3.5. FRAMEWORK: GOAL-QUESTION-METRIC (GQM)

Para organizar e sistematizar a análise dos dados documentais, esta pesquisa adota como ferramenta metodológica o modelo Goal-Question-Metric (GQM), originalmente proposto por Basili, Caldiera e Rombach (1994). Trata-se de uma abordagem sistemática, orientada por objetivos, que transforma intenções analíticas em perguntas investigativas e, posteriormente, em métricas observáveis e mensuráveis. A utilização do GQM nesta etapa metodológica garante um nível mais elevado de objetividade, mesmo em um contexto predominantemente qualitativo e observacional.

A mensuração estruturada e orientada a objetivos é uma técnica essencial para o entendimento, controle, avaliação e melhoria de processos e produtos. O GQM oferece uma estrutura lógica e hierárquica baseada em três níveis de abstração como podemos ver na figura 3 a seguir:

Figura 3 – O método GQM.



Fonte: Adaptado de Van Solinger e Berghout (1999).

Nível conceitual (Objetivo): Define-se o propósito da medição, especificando o objeto de estudo, o foco de qualidade, o ponto de vista adotado e o ambiente no qual o processo ocorre.

Nível operacional (Questão): Formula-se um conjunto de perguntas que desdobram o objetivo em aspectos específicos e investigáveis, guiando a interpretação dos dados.

Nível quantitativo (Métrica): São definidas as métricas que permitirão responder de forma objetiva às perguntas estabelecidas, associando indicadores claros e mensuráveis aos elementos observados.

A aplicação do GQM não estrutura a pesquisa como um todo, mas será empregada como instrumento metodológico complementar, a partir dos desafios técnicos e organizacionais identificados na fase de diagnóstico documental. Com isso, o GQM assume um papel essencial na transição entre a coleta dos dados brutos e a construção de blocos interpretativos organizados logicamente.

A aplicação da ferramenta será realizada em quatro etapas:

1. Planejamento: Delimitação do escopo de análise, com base nas áreas mais críticas à conformidade com a LGPD identificadas durante o diagnóstico. Nessa fase, também são definidos os objetivos de medição da pesquisa.

2. Definição: A partir dos objetivos definidos, são formuladas perguntas específicas que orientam a coleta de dados. Cada pergunta é acompanhada por uma ou mais métricas observáveis, extraídas diretamente dos documentos analisados.

3. Coleta de dados: Os dados são extraídos dos registros documentais previamente disponibilizados, tais como relatórios de conformidade, atas de reuniões, registros de treinamentos, planos de ação, entre outros. A coleta ocorre de forma não-intervencionista e com base nas métricas definidas.

4. Interpretação: Os dados coletados são analisados com base nos objetivos previamente definidos, permitindo avaliar a eficácia das ações de adequação à LGPD, identificar lacunas e apontar níveis de maturidade nos diferentes eixos da conformidade — processos, pessoas, tecnologia e governança.

O uso do GQM nesta pesquisa garante um nível mais elevado de sistematização e objetividade, mesmo em um contexto predominantemente qualitativo e observacional. Além disso, permite que os resultados obtidos possam ser apresentados de forma clara, mensurável e alinhada às boas práticas em segurança da informação e privacidade de dados.

3.6. PLANO GQM

O plano GQM nesta pesquisa foi organizado em quatro fases principais: planejamento, definição, coleta de dados e interpretação. No planejamento, foi definido o escopo do estudo, caracterizando o contexto do hospital e identificando os principais fatores críticos de sucesso relacionados à adequação à LGPD. Essa etapa resultou em um plano geral que orientará a análise.

Na fase de definição, foi elaborado um plano GQM, contendo os objetivos de medição, as perguntas associadas e as métricas necessárias. Para isso, foram utilizadas técnicas como análise documental e, se necessário, entrevistas estruturadas com profissionais envolvidos no projeto. O objetivo foi descrever com clareza o que será avaliado, considerando o ponto de vista dos membros da organização e o ambiente hospitalar. Em seguida, foram formuladas as questões que representam os principais desafios enfrentados e, a partir delas,

definidas as métricas que permitirão avaliar os aspectos técnicos e organizacionais da implementação.

A fase de coleta de dados foi realizada com base nos documentos fornecidos pela empresa de TI responsável pela implementação da LGPD. Foram utilizados instrumentos como relatórios técnicos, políticas internas, registros de auditoria e formulários institucionais para reunir as informações relevantes. Esses dados foram organizados conforme as métricas definidas no plano GQM.

Por fim, na fase de interpretação, os dados coletados foram analisados de forma a responder às perguntas formuladas e verificar se os objetivos foram atendidos. Essa interpretação será feita à luz da LGPD, das boas práticas de segurança da informação e dos principais frameworks normativos, como a ISO/IEC 27001 e 27701, permitindo uma avaliação crítica e sistemática do processo de adequação realizado pelo hospital.

3.7. VALIDAÇÃO DO PLANO GQM

Antes da aplicação definitiva do plano GQM, foi realizada uma etapa de validação com profissionais da organização que participaram ou acompanharam o processo de adequação à LGPD. O objetivo é garantir que os objetivos analíticos, perguntas estruturadas e métricas definidas no plano estejam adequadamente alinhados à realidade institucional e representem de forma fidedigna os desafios enfrentados.

A validação foi conduzida por meio da aplicação de um questionário estruturado, elaborado com base nas dimensões do GQM. O instrumento foi aplicado de forma digital, por meio de plataforma online (como SurveyMonkey ou Google Forms), garantindo agilidade, rastreabilidade e facilidade de acesso aos respondentes.

O questionário teve como finalidade:

- Obter a validação semântica e conceitual dos objetivos, perguntas e métricas previstas;
- Confirmar se os indicadores sugeridos são mensuráveis a partir dos documentos disponíveis;
- Permitir ajustes no plano GQM, caso alguma métrica se revele inadequada, incoerente ou inaplicável à prática da instituição.

A amostra de participantes foi compostas por profissionais que atuaram diretamente nas etapas do roadmap da LGPD, incluindo representantes das áreas de Tecnologia da Informação, Jurídico, Compliance, Recursos Humanos, Segurança da Informação, Comitê LGPD e consultoria externa, conforme a distribuição de responsabilidades apresentada anteriormente.

A escolha dos participantes foi do tipo intencional não probabilística, com base no critério de expertise e envolvimento com as atividades analisadas, o que permitirá capturar múltiplas percepções sobre a estrutura proposta sem comprometer a profundidade da análise.
As respostas obtidas foram analisadas de forma descritiva, com foco em identificar possíveis inconsistências, lacunas ou melhorias na estrutura do plano. Eventuais ajustes serão incorporados antes do início da coleta definitiva de dados e da interpretação com base no GQM.

3.8. IMPACTOS PERCEBIDOS

Nesta seção foram apresentados os impactos percebidos pela organização após a implantação da LGPD, que serão obtidos por meio de um questionário avaliativo aplicado aos colaboradores da instituição, bem como o processo metodológico a ser adotado para validação desta percepção.

3.8.1. Processo Metodológico dos impactos

A percepção dos impactos decorrentes da implantação da LGPD foi avaliada utilizando um questionário estruturado, disponibilizado aos colaboradores da instituição por meio da plataforma Google Forms. O questionário foi elaborado com base nos objetivos e desafios previamente definidos na aplicação do modelo Goal-Question-Metric (GQM), contemplando aspectos organizacionais e técnicos relacionados à adequação à LGPD.

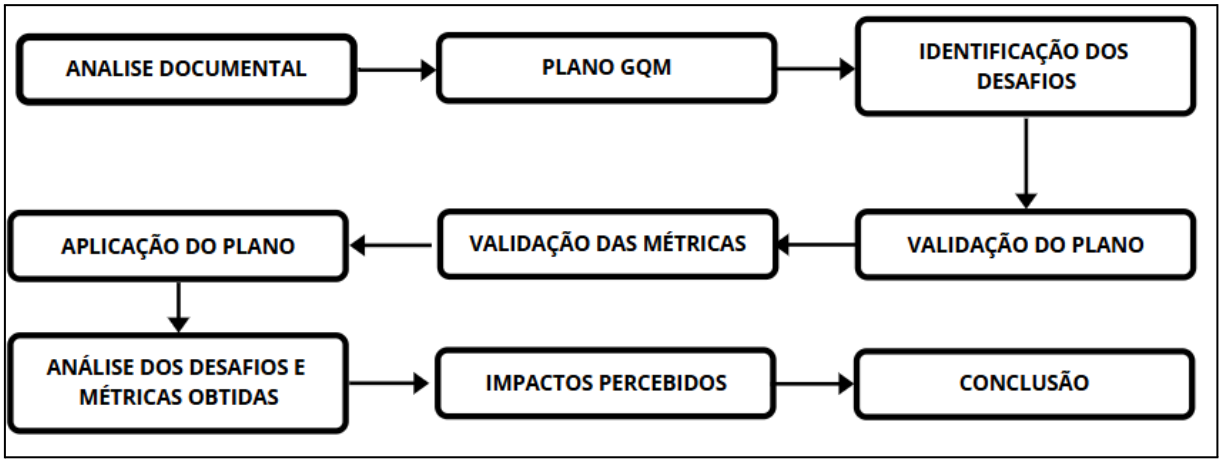
O instrumento avaliativo foi dividido em duas seções principais: impactos organizacionais e impactos técnicos. Cada seção contém afirmações específicas nas quais os respondentes indicaram seu grau de concordância por meio de uma escala Likert de cinco pontos, variando entre "Discordo totalmente" e "Concordo totalmente".
A coleta de dados foi realizada de maneira anônima e confidencial, permitindo que os colaboradores expressassem suas percepções sem restrições. As respostas foram tabuladas e

analisadas quantitativamente para identificar o grau de impacto percebido em cada área abordada pelo questionário.

4. RESULTADOS OBTIDOS

Este capítulo apresenta os resultados obtidos a partir da execução das etapas metodológicas previstas no desenho da pesquisa, conforme representado na Figura 4. O percurso foi estruturado de forma sequencial e lógica, com base no modelo GQM, visando garantir a coerência entre os objetivos analíticos, os dados coletados e as interpretações realizadas.

Figura 4. Estrutura dos resultados obtidos



Fonte: Elaborado pelos autores

A primeira etapa consistiu na análise documental de registros institucionais produzidos durante o processo de adequação à LGPD. Essa etapa serviu como base para a elaboração do plano GQM, o qual sistematizou os objetivos de medição, as perguntas de investigação e as métricas correspondentes. Em seguida, com base nos documentos analisados, foram identificados os desafios técnicos e organizacionais enfrentados pela instituição.

Após a definição dos desafios, o plano foi submetido à validação por profissionais da organização, assegurando a aderência dos elementos propostos à realidade institucional. Com o plano validado, procedeu-se à validação das métricas, por meio de questionário específico, a fim de confirmar sua clareza, relevância e viabilidade de mensuração.

Com o plano integralmente validado, realizou-se a aplicação do modelo GQM, utilizando os dados extraídos da documentação para alimentar as métricas propostas. A partir

dessa aplicação, foi possível realizar uma análise detalhada dos desafios identificados e dos valores obtidos, permitindo uma avaliação crítica sobre o grau de conformidade do hospital com os requisitos da LGPD.

Posteriormente, foi conduzida uma etapa dedicada à mensuração dos impactos percebidos, a partir da aplicação de um instrumento avaliativo junto aos colaboradores. Essa fase teve como objetivo capturar a percepção institucional sobre os efeitos da implementação da LGPD, tanto em aspectos organizacionais quanto técnicos.

Por fim, os achados foram sistematizados e discutidos com base nas evidências documentais, nas métricas quantitativas e nas percepções coletadas, servindo de base para as conclusões e recomendações apresentadas ao final do trabalho.

4.1. ANÁLISE DOCUMENTAL

A primeira etapa dos resultados desta pesquisa foi a análise documental, conduzida a partir da documentação institucional disponibilizada por um dos profissionais diretamente envolvidos na implementação da LGPD no hospital estudado. Esses documentos foram solicitados e obtidos com o intuito inicial de compreender o processo de adequação à legislação e identificar maneiras eficazes de demonstrar o estado atual da conformidade.

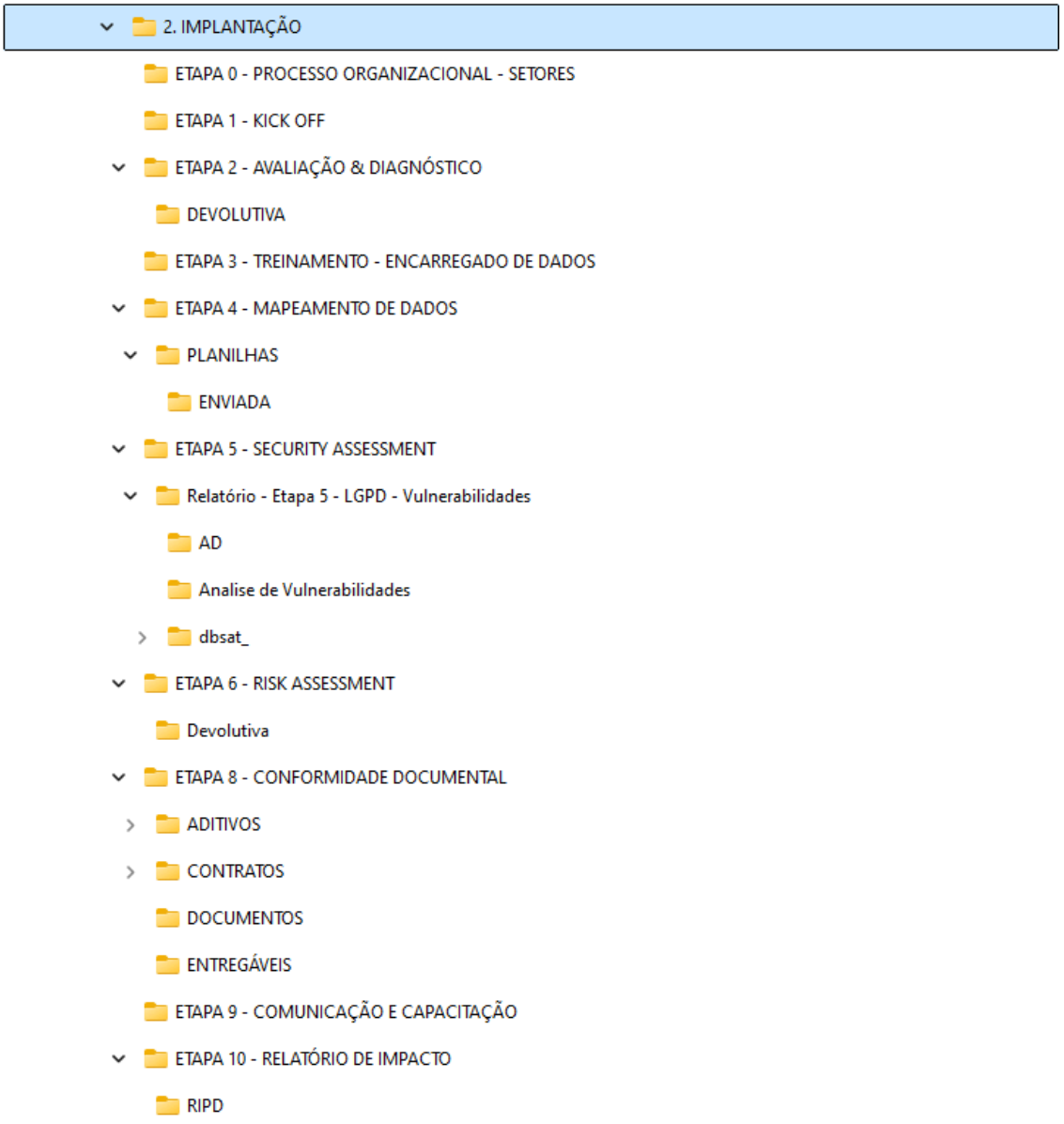
Ao analisar a documentação recebida — que incluía relatórios técnicos produzidos por consultores externos, atas de reuniões, planos de ação, inventários de dados e sistemas, registros operacionais e materiais de capacitação — constatou-se que o projeto de implementação estava incompleto, caracterizado por diversas ações parcialmente executadas e com múltiplas pendências. Esses fatores levaram à identificação inicial de um cenário complexo e fragmentado, com "pontas soltas" e dificuldades significativas na gestão operacional e técnica da proteção de dados.

Diante dessa constatação, optou-se por focar na identificação das dificuldades enfrentadas pela instituição durante o processo de adequação regulatória, estruturando essa análise em torno dos desafios evidenciados pela documentação. Para isso, buscou-se um modelo que permitisse uma análise quantitativa mais robusta e organizada desse cenário complexo. A escolha recaiu sobre o modelo GQM, reconhecido pela sua eficácia na tradução de objetivos qualitativos em métricas observáveis e quantitativas.

Durante o aprofundamento da análise documental, observou-se que os consultores responsáveis pela implementação estruturaram suas ações por meio de um roadmap organizacional dividido em dez etapas. Essas etapas, identificadas após sucessivas leituras

críticas dos documentos, forneciam uma estrutura clara e lógica do fluxo operacional pretendido pelos consultores para alcançar a conformidade com a LGPD. Desta forma, decidiu-se utilizar esse roadmap como eixo condutor da análise conforme ilustrado na Figura 5.

Figura 5 – Estrutura da Documentação Analisada



Fonte: Documentação da consultoria.

As dez etapas identificadas foram:

- Etapa 1 – Kick Off: Reunião inicial e definição de escopo.
- Etapa 2 – Avaliação e Diagnóstico: Avaliação inicial da conformidade e esforço necessário.
- Etapa 3 – Instrução do Encarregado de Dados (DPO): Capacitação do encarregado e equipe jurídica.
- Etapa 4 – Mapeamento de Dados: Identificação e classificação dos dados pessoais.
- Etapa 5 – Security Assessment: Avaliação técnica da segurança da informação.
- Etapa 6 – Risk Assessment: Avaliação e tratamento dos riscos identificados.
- Etapa 7 – Política de Proteção de Dados: Formulação e validação de diretrizes internas.
- Etapa 8 – Conformidade Documental: Revisão e adequação de documentos internos e contratos.
- Etapa 9 – Comunicação e Capacitação: Programas de treinamento e conscientização dos colaboradores.
- Etapa 10 – Conclusão: Consolidação do processo e recomendações para monitoramento contínuo.

Essas etapas não só orientaram a análise documental, como também possibilitaram uma compreensão detalhada dos processos organizacionais e das limitações operacionais encontradas pelos consultores e pelas equipes internas ao longo do projeto. Dessa forma, a análise documental não apenas forneceu um panorama inicial essencial para compreender as circunstâncias do projeto, mas também fundamentou toda a construção e aplicação subsequente do modelo GQM, garantindo coerência e consistência metodológica nos resultados apresentados nas próximas seções deste capítulo.

4.2. CONSTRUÇÃO DO PLANO GQM

Após a conclusão da análise documental, foi necessário estruturar uma abordagem metodológica para traduzir os desafios observados em indicadores mensuráveis, permitindo uma avaliação quantitativa precisa do cenário identificado. Para isso, optou-se pela utilização do modelo GQM, originalmente proposto por Basili et al. (1994), em virtude de sua eficácia na sistematização e mensuração clara de aspectos qualitativos em ambientes complexos.

Inicialmente, foi estabelecido o objetivo geral da medição, seguindo rigorosamente o formato GQM, exibido no quadro 2:

Quadro 2 – Objetivo da Medição

Objetivo	Descrição
Investigar	A adequação dos processos de TI e Segurança da Informação à LGPD
Com o objetivo de	Identificar e avaliar as principais dificuldades técnicas e organizacionais enfrentadas na implementação
Com relação a	Maturidade e eficácia da conformidade legal
No ponto de vista de	Membros da organização
No contexto de	Um hospital de grande porte em processo de conformidade regulatória

Fonte: Elaborado pelos autores

A partir desse objetivo central, definiu-se uma pergunta principal norteadora para estruturar e direcionar a análise, mostrada no quadro 3:

Quadro 3 – Pergunta Principal

Código	Questão
O1.Q1	Quais são os principais desafios técnicos e organizacionais enfrentados pelo hospital durante o processo de implementação da LGPD, conforme identificados na documentação institucional analisada?

Fonte: Elaborado pelos autores

A partir dessa pergunta, foi realizada uma análise detalhada dos documentos coletados na etapa anterior (seção 4.1 – Análise Documental), visando identificar claramente os desafios enfrentados pela organização. Esses desafios foram organizados em categorias, correspondendo às etapas críticas evidenciadas no roadmap de implementação institucional, totalizando oito desafios principais listados no quadro 4:

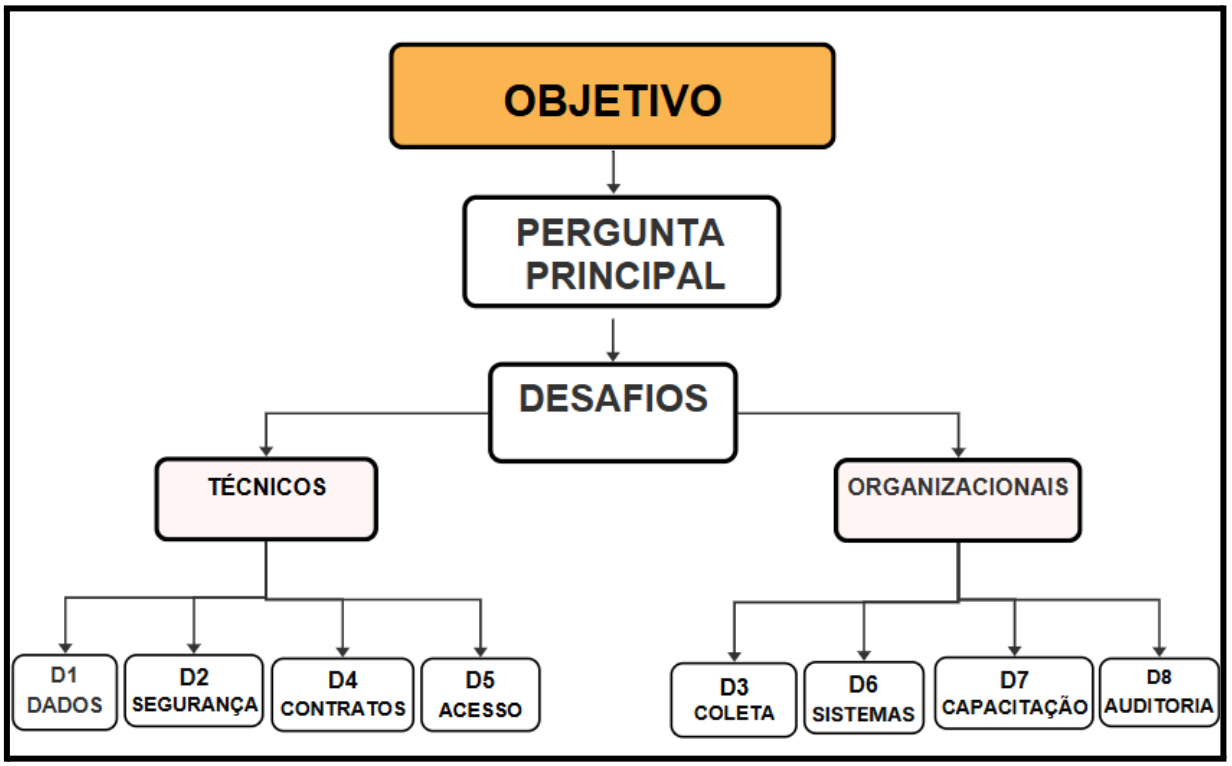
Quadro 4 – Desafios Relacionados à Implementação da LGPD

#	Desafio
D1	Identificar todos os dados pessoais tratados pelo hospital e classificá-los conforme a sensibilidade e finalidade do uso
D2	Avaliar a segurança dos sistemas existentes para identificar vulnerabilidades que possam comprometer a proteção de dados pessoais.
D3	Avaliar se os processos de coleta de dados, incluindo consentimento, estão sendo conduzidos de forma adequada e conforme as exigências da LGPD.
D4	Analisar e Monitorar se os contratos com prestadores de serviços e parceiros estão em conformidade com os requisitos da LGPD.
D5	Estabelecer e implementar controles de acesso e segurança adequados para proteger os dados pessoais dos pacientes e colaboradores.
D6	Avaliar a adequação dos sistemas às políticas de privacidade e segurança de dados conforme a LGPD.
D7	Garantir que todos os colaboradores recebam treinamentos contínuos sobre as práticas de conformidade com a LGPD.
D8	Estabelecer um processo de monitoramento contínuo e auditoria das operações relacionadas à privacidade e proteção de dados pessoais.

Fonte: Elaborado pelos autores

Para cada um dos desafios definidos, foram estabelecidas métricas quantitativas específicas, permitindo uma avaliação objetiva e direta do cenário atual encontrado no hospital. Essas métricas foram extraídas diretamente dos documentos institucionais analisados, garantindo coerência e fundamentação documental para cada indicador escolhido. Dessa forma, o plano GQM final ficou organizado em uma estrutura hierárquica clara e objetiva como visto na figura 6:

Figura 6 – Plano GQM



Fonte: Elaborado pelos autores

A estrutura detalhada, contendo a relação completa das perguntas secundárias para cada desafio e respectivas métricas quantitativas, encontra-se documentada em quadros específicos apresentados nos apêndices desta pesquisa. Cabe ressaltar que, antes da aplicação definitiva, este plano GQM foi submetido a uma etapa formal de validação junto aos membros diretamente envolvidos na implementação da LGPD, conforme detalhado na seção seguinte (4.3 – Validação do Plano GQM). Tal validação teve o objetivo de garantir que os desafios e métricas identificados refletissem precisamente o contexto real da instituição.

Deste modo, o processo de construção do plano GQM permitiu transformar uma realidade complexa, inicialmente observada em documentação dispersa e incompleta, em uma estrutura analítica clara e quantificável, contribuindo para uma avaliação objetiva e rigorosa do nível de adequação da instituição às exigências da LGPD.

4.3. VALIDAÇÃO DO PLANO

Após a construção do plano GQM, foi realizada a validação dos desafios técnicos e organizacionais identificados no hospital estudado. Esta etapa visou garantir que os desafios

levantados representassem com precisão as principais dificuldades enfrentadas no processo de adequação à LGPD. A pesquisa foi conduzida por meio da aplicação de questionários estruturados a dois profissionais selecionados por sua atuação direta no projeto. Os questionários, enviados eletronicamente, abordavam a validação dos desafios em três dimensões:

- Avaliação Quantitativa: Para cada desafio identificado, os participantes atribuíram uma nota de 1 a 10, indicando o grau de representatividade do desafio em relação à realidade vivida.
- Análise Qualitativa: Questões abertas permitiram aos participantes comentarem sobre a clareza, a relevância e eventuais ajustes necessários nos desafios listados.
- Identificação de lacunas: Solicitou-se aos participantes que indicassem outros desafios não contemplados, caso identificasse alguma omissão relevante.

A análise dos resultados demonstrou alta aderência dos desafios à experiência prática dos profissionais. Especialmente, os desafios relacionados à segurança dos sistemas, à conformidade documental e à capacitação dos colaboradores foram apontados como plenamente representativos. Em contraste, aspectos ligados ao monitoramento contínuo e à auditoria interna foram reconhecidos como relevantes, mas ainda pouco estruturados no contexto institucional.

4.4. RESULTADOS DA APLICAÇÃO DO PLANO GQM

A aplicação do modelo GQM estruturou a análise dos documentos e das evidências coletadas ao longo da pesquisa. O plano foi desenvolvido com base na definição de um objetivo central, que foi desdobrado em perguntas analíticas e, posteriormente, em métricas mensuráveis, permitindo uma avaliação sistemática da conformidade do hospital com a LGPD. Para mensurar cada um desses desafios, foi definido um conjunto de métricas associadas, descritas no Quadro 5 a seguir:

Quadro 5 – Métricas para cada Desafio

ID	Métrica
D1.M1	Quantidade de processos internos com dados pessoais identificados e classificados
D1.M2	Percentual de processos internos com dados pessoais classificados como sensíveis
D2.M1	Número de vulnerabilidades identificadas
D2.M2	Percentual de vulnerabilidades alta ou crítica
D2.M3	Número de riscos mapeados
D2.M4	Percentual de riscos elevados e críticos
D3.M1	Percentual de dados coletados com base legal estabelecida
D3.M2	Percentual de consentimentos documentados
D4.M1	Percentual de contratos revisados quanto à LGPD
D4.M2	Percentual de contratos com cláusulas de conformidade em vigor
D4.M3	Taxa de atualização de contratos com terceiros
D5.M1	Percentual de implementação dos controles de acesso segundo a ISO/27001
D5.M2	Porcentagem de riscos com nível de controle classificado como 'Existente'
D6.M1	Quantidade de sistemas a serem avaliados
D6.M2	Quantidade de controles de segurança implementados
D7.M1	Percentual de colaboradores que completam treinamentos contínuos
D8.M1	Número de auditorias internas realizadas

Fonte: Elaborado pelos autores

Essa estrutura GQM validada proporcionou um modelo robusto de análise que será detalhado nas próximas seções, onde cada desafio será analisado individualmente à luz das métricas observadas.

4.5. VALIDAÇÃO DAS MÉTRICAS

Após a validação dos desafios, procedeu-se à etapa de validação das métricas associadas, com o objetivo de confirmar sua pertinência, clareza e viabilidade prática de mensuração.

Esta etapa utilizou uma estratégia de validação cruzada com três questionários distintos, voltados a diferentes aspectos do plano GQM:

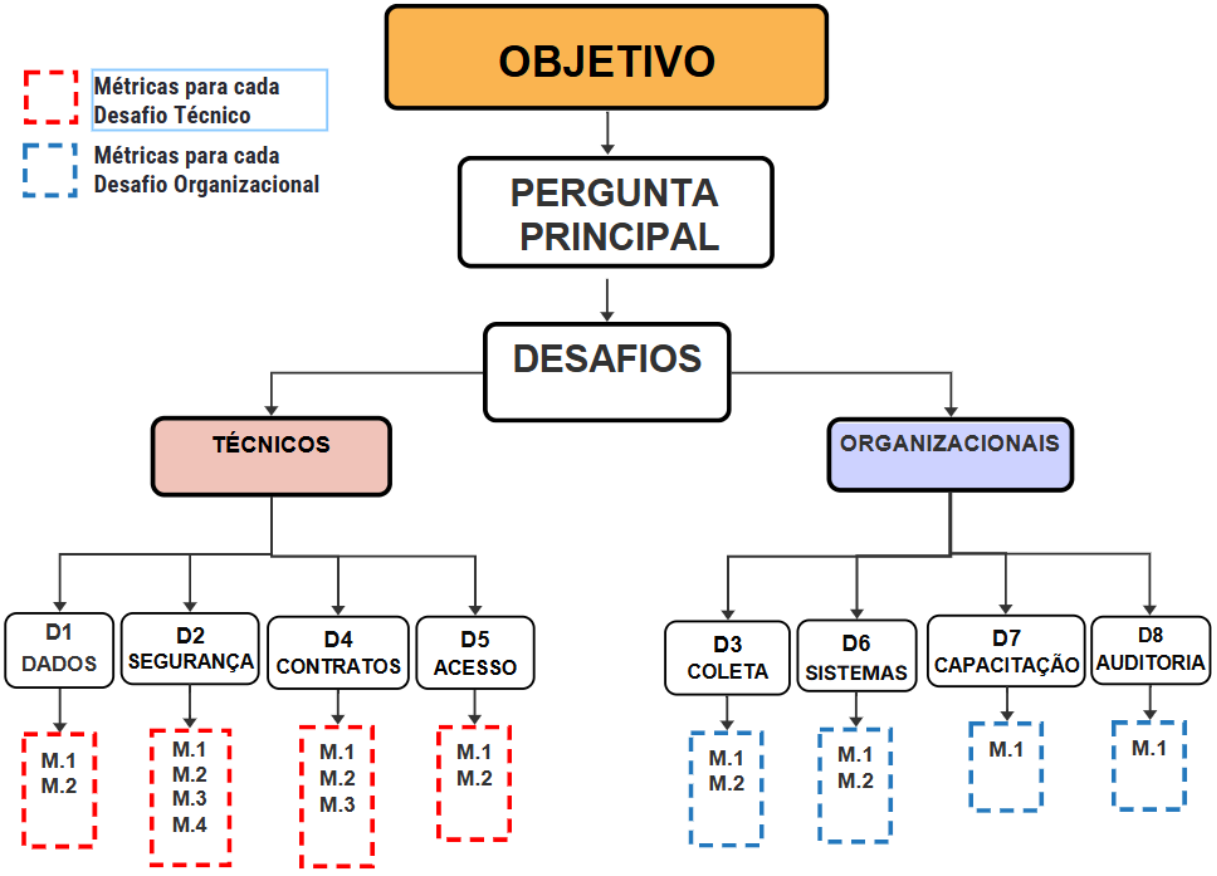
- Questionário 1: Validação dos desafios (já abordado na seção 4.3);
- Questionário 2: Investigação de causas-raiz para as dificuldades enfrentadas, com perguntas abertas;
- Questionário 3: Avaliação específica das métricas, com enfoque na análise de coerência, relevância e aplicabilidade.

As métricas propostas foram apresentadas em conjunto com seus respectivos desafios. Os profissionais participantes realizaram a avaliação:

- Quantitativamente, atribuindo notas de 1 a 10 para indicar a adequação de cada métrica;
- Qualitativamente, fornecendo sugestões de reformulação ou complementação das métricas propostas.

Para apoiar a visualização da estrutura validada, apresenta-se o diagrama consolidado do plano GQM na figura 7:

Figura 7 – Plano GQM Validado



Fonte: Elaboração Própria

A análise das respostas indicou que métricas relacionadas à segurança dos sistemas, conformidade documental e capacitação de colaboradores apresentaram alta aderência. Em contrapartida, métricas voltadas ao monitoramento contínuo e auditorias internas exigiram ajustes para melhor representar a realidade operacional da instituição.

Com base nos resultados obtidos, foram realizados refinamentos pontuais na formulação de algumas métricas, garantindo sua clareza e sua aplicabilidade ao ambiente estudado.

4.6. ANÁLISE DOS DESAFIOS IDENTIFICADOS E MÉTRICAS OBTIDAS

A seguir, apresenta-se o Quadro 6, que resume os desafios enfrentados na implementação da LGPD, e a Tabela 1, que apresenta os resultados obtidos com base nas métricas estabelecidas.

Quadro 6 – Classificação dos Desafios da Implementação

ID	Classificação	Descrição
D1	Técnico	Identificar todos os dados pessoais tratados pelo hospital e classificá-los conforme a sensibilidade e finalidade do uso.
D2	Técnico	Avaliar a segurança dos sistemas existentes para identificar vulnerabilidades que possam comprometer a proteção de dados pessoais.
D3	Organizacional	Avaliar se os processos de coleta de dados, incluindo consentimento, estão sendo conduzidos de forma adequada e conforme as exigências da LGPD.
D4	Técnico	Analisar e Monitorar se os contratos com prestadores de serviços e parceiros estão em conformidade com os requisitos da LGPD.
D5	Técnico	Estabelecer e implementar controles de acesso e segurança adequados para proteger os dados pessoais dos pacientes e colaboradores.
D6	Organizacional	Avaliar a adequação dos sistemas às políticas de privacidade e segurança de dados conforme a LGPD.
D7	Organizacional	Garantir que todos os colaboradores recebam treinamentos contínuos sobre as práticas de conformidade com a LGPD.
D8	Organizacional	Estabelecer um processo de monitoramento contínuo e auditoria das operações relacionadas à privacidade e proteção de dados pessoais.

Fonte: Elaborado pelos autores

Tabela 1 – Resultados das Métricas Obtidas

ID	Métrica	Resultado
D1.M1	Quantidade de processos internos com dados pessoais identificados e classificados	853 processos identificados
D1.M2	Percentual de processos com dados pessoais classificados como sensíveis	77,63% dos processos classificados como sensíveis
D2.M1	Número de vulnerabilidades identificadas	211 vulnerabilidades
D2.M2	Percentual de vulnerabilidades alta ou crítica	50,7% das vulnerabilidades são altas ou críticas

D2.M3	Número de riscos mapeados	80 riscos identificados
D2.M4	Percentual de riscos elevados e críticos	73,75% dos riscos classificados como elevados ou críticos
D3.M1	Percentual de dados coletados com base legal estabelecida	28,72% dos processos possuem base legal estabelecida
D3.M2	Percentual de consentimentos documentados	0% dos processos têm consentimento documentado
D4.M1	Percentual de contratos revisados quanto à LGPD	62,63% dos contratos revisados para atender à LGPD
D4.M2	Percentual de contratos com cláusulas de conformidade em vigor	0% dos contratos possuem cláusulas de conformidade em vigor
D4.M3	Taxa de atualização de contratos com terceiros	0% dos contratos foram formalmente atualizados
D5.M1	Percentual de implementação dos controles de acesso segundo a ISO/27001	85% dos sistemas críticos possuem controles de acesso implementados
D5.M2	Porcentagem de riscos com nível de controle classificado como 'Existente'	46,25% dos riscos possuem nível de controle classificado como 'Existente'
D6.M1	Quantidade de sistemas a serem avaliados	24 sistemas identificados para avaliação
D6.M2	Quantidade de controles de segurança implementados	10 controles de segurança implementados
D7.M1	Percentual de colaboradores que completam treinamentos contínuos	0% dos colaboradores completaram treinamentos contínuos
D8.M1	Número de auditorias internas realizadas	0 auditorias internas realizadas até o momento

Fonte: Elaborado pelos autores

A seguir, detalha-se a análise individual de cada um dos desafios e seus respectivos resultados.

4.6.1. Desafio 1 – Identificação e Classificação dos Dados Pessoais

A primeira fase consistiu na coleta de dados, realizada por meio da utilização de planilhas preenchidas pelos representantes de 80 setores do hospital. Cada setor descreveu minuciosamente os processos que envolvem o tratamento de dados pessoais, garantindo a integração com os requisitos legais da LGPD e permitindo um levantamento adequado das informações coletadas. Posteriormente, a segunda fase envolveu a classificação dos dados identificados. Esses foram categorizados em dados pessoais comuns e dados pessoais sensíveis, utilizando critérios como titularidade (paciente, colaborador ou fornecedor), finalidade do uso (assistencial, administrativo ou financeiro), base legal aplicável (consentimento, obrigação legal, execução de contrato ou proteção da vida) e periodicidade de backup e armazenamento (tempo de retenção e ciclo de revisão). A terceira fase compreendeu a organização sistemática desses dados, garantindo que fossem documentados de maneira clara e objetiva.

O mapeamento realizado seguiu os princípios estabelecidos no artigo 6º da LGPD, que trata dos fundamentos para o tratamento de dados pessoais, assegurando que apenas os dados essenciais fossem identificados e documentados (princípio da necessidade), respeitando os critérios normativos para coleta e armazenamento (princípio da adequação) e promovendo a conscientização dos setores sobre suas responsabilidades no tratamento dos dados pessoais (princípio da transparência). Para os dados sensíveis, foram aplicadas diretrizes específicas previstas no artigo 11º da LGPD, que trata das hipóteses legais para o tratamento de dados pessoais sensíveis, em razão do maior impacto em caso de uso inadequado. Entre os dados considerados sensíveis estavam informações de saúde e biometria utilizada para controle de acesso e identificação de pacientes e colaboradores.

Os resultados obtidos evidenciaram a importância desse processo para a segurança da informação no ambiente hospitalar. A análise quantitativa demonstrou que foram identificados e classificados 853 processos internos que lidam com dados pessoais, distribuídos entre os setores de Tecnologia da Informação, Recursos Humanos, Assistenciais e Administrativos. Para a validação dessas informações, consolidaram-se os dados via planilhas setoriais e realizou-se uma revisão qualitativa considerando finalidade, sensibilidade e base legal. O resultado dessa análise indicou que 77,63% dos processos analisados envolviam dados sensíveis, sendo os setores mais críticos a Tecnologia da Informação, em razão dos logs de acesso e biometria; Recursos Humanos, devido aos dados de saúde e biometria dos colaboradores; e Atendimento ao Paciente, que trata de históricos médicos e diagnósticos.

A partir desses resultados, concluiu-se que o hospital possui um alto volume de dados sensíveis, o que exige medidas de segurança reforçadas. Além disso, o mapeamento de todos os processos permitiu uma visão abrangente do fluxo de dados, contribuindo para a implementação de ações corretivas. A criação de um comitê multidisciplinar foi essencial para validar as informações e garantir conformidade com a LGPD.

4.6.2. Desafio 2 – Avaliação da Segurança dos Sistemas

A avaliação da segurança dos sistemas hospitalares representou uma etapa central no processo de adequação à LGPD, especialmente no que diz respeito à proteção de dados pessoais contra acessos não autorizados e violações de segurança. Para essa análise, foram utilizados documentos técnicos produzidos por uma empresa terceirizada especializada, contratada pela instituição hospitalar com a finalidade de realizar um diagnóstico aprofundado da infraestrutura de TI e segurança da informação.

A metodologia aplicada pela consultoria foi dividida em duas etapas principais, cujos resultados foram posteriormente analisados nesta pesquisa sob a perspectiva do plano GQM. A primeira etapa, denominada Security Assessment, consistiu em uma inspeção detalhada dos sistemas utilizados pelo hospital, incluindo servidores, redes, estações de trabalho e dispositivos de armazenamento. Foram identificadas vulnerabilidades internas e externas, categorizadas por nível de severidade: baixa, média, alta e crítica.

Na sequência, foi conduzido o Risk Assessment, com apoio de workshops e auditorias técnicas, com o objetivo de mapear os riscos associados às vulnerabilidades identificadas. Os riscos foram classificados com base em dois eixos principais: impacto potencial e probabilidade de exploração, alinhando-se aos parâmetros estabelecidos pela ISO 31000 para gestão de riscos e aos padrões do NIST para categorização de ameaças e definição de níveis de segurança.

A análise seguiu os princípios do artigo 6º da LGPD, que destaca a importância da adoção de medidas preventivas e de segurança no tratamento de dados pessoais. Também se observou a correspondência entre a abordagem aplicada e as boas práticas definidas pelas normas ISO/IEC 27001 e 27701.

Os resultados documentados indicaram a identificação de 211 vulnerabilidades, das quais 159 (75,3%) eram internas e 52 (24,7%) externas. Do total, 107 vulnerabilidades (50,7%) foram classificadas como altas ou críticas, revelando a existência de pontos sensíveis na infraestrutura hospitalar. A análise de riscos indicou a existência de 80 riscos

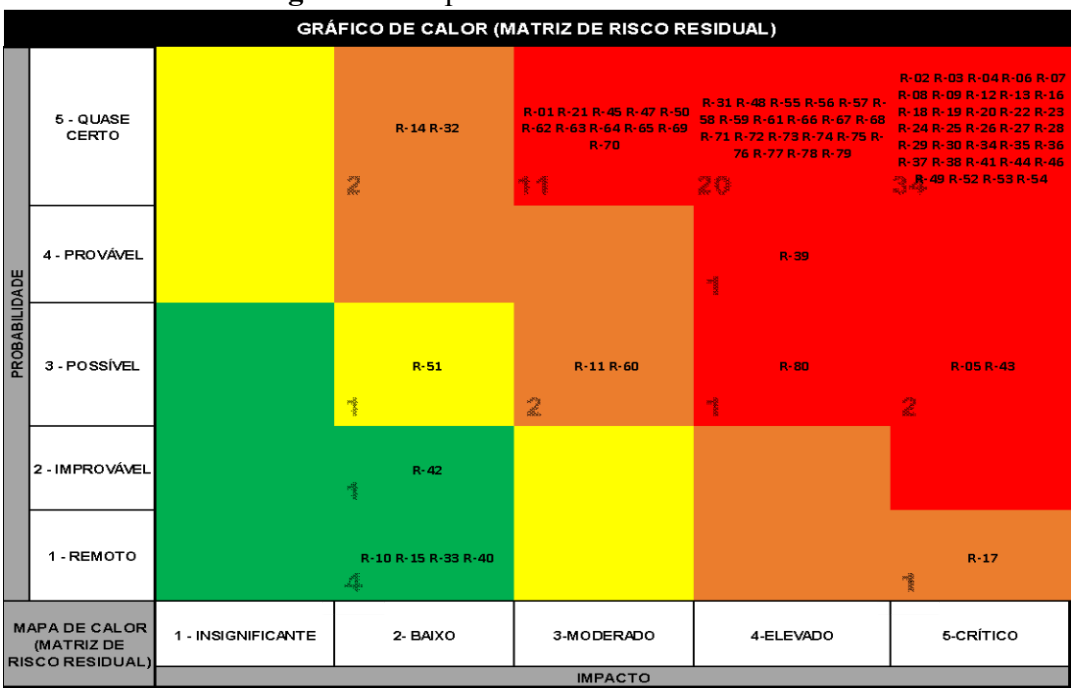
documentados, sendo 73,75% considerados elevados ou críticos, segundo os critérios técnicos utilizados.

As métricas aplicadas, conforme o plano GQM, foram:

- D2.M1 – Número de vulnerabilidades identificadas: 211
- D2.M2 – Percentual de vulnerabilidades altas ou críticas: 50,7%
- D2.M3 – Número de riscos mapeados: 80
- D2.M4 – Percentual de riscos classificados como elevados ou críticos: 73,75%

A Figura 8 ilustra a distribuição dos desafios identificados ao longo da implementação, por meio de um mapa de calor que evidencia os pontos críticos, permitindo uma visualização gráfica da relação entre impacto e probabilidade de ocorrência das ameaças identificadas.

Figura 8 - Mapa de Calor: Matriz de Risco



Fonte: Documentos da implementação do Hospital

A análise desses documentos evidenciou que a organização possui fragilidades relevantes em sua segurança de sistemas, exigindo a priorização de ações corretivas. Entre as recomendações descritas no material analisado, destacam-se: a correção imediata de vulnerabilidades críticas, o fortalecimento de controles de segurança para sistemas internos e externos, a implementação de auditorias contínuas e a criação de um plano de resposta a incidentes, em conformidade com a ISO 27001 e a LGPD.

A identificação dessas fragilidades, ainda que realizada por terceiros, representa um marco relevante na estratégia institucional de proteção de dados, pois evidencia a importância da gestão proativa de riscos como base para a governança de segurança da informação no ambiente hospitalar.

4.6.3. Desafio 3 – Conformidade dos Processos de Coleta de Dados com a LGPD

A conformidade dos processos de coleta de dados com os princípios e exigências da LGPD é um fator determinante para a segurança jurídica das instituições hospitalares. Neste desafio, analisaram-se documentos técnicos produzidos no contexto do processo de adequação institucional, com o objetivo de avaliar se os processos de coleta estavam devidamente

amparados por bases legais e acompanhados de registros formais de consentimento, conforme previsto na legislação.

A análise documental foi conduzida sobre materiais fornecidos por consultores externos contratados pelo hospital. Entre os documentos observados, destacam-se relatórios de adequação documental, inventários de processos e registros contratuais, que evidenciaram o grau de conformidade dos fluxos de coleta com os requisitos do artigo 7º da LGPD, que define as hipóteses legais para o tratamento de dados pessoais.

Foram utilizadas duas métricas, definidas previamente no plano GQM validado:

- D3.M1 – Percentual de dados coletados com base legal documentada
- D3.M2 – Percentual de consentimentos formalmente registrados

A primeira métrica (D3.M1) foi aplicada sobre o universo de 853 processos internos, identificados como relacionados à coleta de dados pessoais. Desses, apenas 245 apresentaram documentação que explicitava a base legal utilizada, como consentimento, obrigação legal, execução de contrato, proteção da vida ou legítimo interesse. O resultado representa um índice de 28,72% de conformidade documental com as exigências legais.

$$Percentual\ de\ Dados\ com\ Base\ legal\ = \frac{245}{853} \times 100\ =\ 28,72\%$$

A segunda métrica (D3.M2) foi aplicada a um subconjunto de 608 processos, previamente classificados como demandantes de consentimento expresso por parte dos titulares dos dados. A análise revelou que nenhum desses processos possuía registros formais de consentimento arquivados ou vinculados documentalmente aos fluxos de tratamento, caracterizando um risco elevado de não conformidade com a LGPD.

Os métodos utilizados para essa avaliação incluíram a categorização dos processos conforme a hipótese legal prevista, a análise de contratos e formulários utilizados na coleta, e a verificação da existência de registros digitais de aceite. A ausência de formalização do consentimento nos processos identificados levanta preocupações jurídicas significativas e evidencia a fragilidade dos mecanismos institucionais de governança da privacidade. Com base nos achados documentais, os relatórios técnicos analisados recomendaram medidas corretivas urgentes, entre as quais se destacam:

- Auditoria interna dos processos identificados, com foco na formalização retroativa dos registros de consentimento;
- Implementação de soluções tecnológicas para o gerenciamento de consentimentos, incluindo módulos de aceite eletrônico, rastreamento e integração com os sistemas de informação hospitalar;
- Revisão e atualização de contratos, formulários e fluxos administrativos, com inserção obrigatória de cláusulas de consentimento explícito;
- Capacitação dos colaboradores, com treinamentos periódicos voltados à importância da coleta legal e documentada dos dados;
- Criação de um plano de conformidade setorializado, garantindo que todas as áreas do hospital passem a operar em alinhamento com a LGPD.

A análise revelou que a organização apresenta lacunas relevantes nos controles sobre a legalidade da coleta de dados pessoais, com impacto direto sobre sua segurança jurídica. A ausência de registros formais de consentimento nos 608 processos analisados representa um risco significativo de responsabilização civil, administrativa ou regulatória. A implementação das medidas propostas é essencial para mitigar esses riscos e assegurar a conformidade institucional com a legislação vigente.

4.6.4. Desafio 4 – Conformidade dos Contratos com a LGPD

A conformidade dos contratos institucionais com as exigências da LGPD representa um eixo estratégico na governança de dados de qualquer organização. No caso da instituição hospitalar analisada, a adequação contratual às diretrizes da LGPD configura-se como um aspecto essencial para garantir a segurança jurídica das relações mantidas com terceiros, especialmente com prestadores de serviços que lidam com dados pessoais sensíveis.

A análise deste desafio foi conduzida a partir da documentação produzida por consultores externos, responsáveis por revisar e auditar os contratos vigentes no hospital. A avaliação considerou aspectos como: existência de cláusulas de proteção de dados, presença de termos específicos de responsabilidade, previsão de medidas de segurança compatíveis com a legislação e mecanismos de atualização contratual.

Foram aplicados três métricas, conforme definido no plano GQM:

- D4.M1 – Percentual de contratos revisados quanto à conformidade com a LGPD

- D4.M2 – Percentual de contratos com cláusulas de conformidade formalizadas
- D4.M3 – Taxa de atualização de contratos com terceiros

A primeira métrica (D4.M1) foi aplicada sobre um universo de 479 contratos considerados relevantes para a conformidade com a LGPD, dos quais 300 passaram por algum processo de revisão formal, resultando em um índice de 62,63% de conformidade contratual mínima.

A segunda métrica (D4.M2) buscou identificar a presença de cláusulas formais de proteção de dados nos contratos revisados. A análise documental indicou que nenhum dos contratos continha cláusulas específicas relacionadas à LGPD, resultando em um índice de 0% de conformidade com essa exigência legal.

A terceira métrica (D4.M3) avaliou a atualização contratual de documentos celebrados com terceiros com foco na inclusão de exigências legais de privacidade. A análise evidenciou que nenhum contrato havia sido atualizado formalmente com essa finalidade até o momento da revisão documental.

A ausência de cláusulas formais de proteção de dados em contratos institucionais foi classificada nos relatórios técnicos como um risco crítico à conformidade jurídica, em razão da possibilidade de responsabilização solidária da organização em caso de incidentes envolvendo dados tratados por terceiros. Além disso, a ausência dessas cláusulas compromete a responsabilização contratual de prestadores de serviço e fragiliza a estrutura de governança de dados da instituição.

Embora os documentos revisados tenham apontado a necessidade de ações corretivas específicas como a revisão de contratos pendentes, a criação de modelos padronizados de cláusulas contratuais e a implementação de rotinas periódicas de atualização, convém destacar que este material possui caráter sigiloso. Sua divulgação integral poderia expor vulnerabilidades contratuais que ainda estão em processo de tratamento pela organização. Assim, a descrição detalhada das recomendações é limitada neste trabalho, preservando-se a confidencialidade das informações estratégicas e respeitando-se os limites éticos da pesquisa documental.

Ainda que a revisão de parte dos contratos represente um avanço, o fato de nenhum contrato conter cláusulas de conformidade com a LGPD representa uma falha crítica que deve ser endereçada com prioridade. A partir da análise documental, ficou evidente que a adequação contratual é um pilar ainda incipiente na estratégia de privacidade institucional, mas de extrema importância para mitigar riscos legais e operacionais futuros.

4.6.5. Desafio 5 – Implementação de Controles de Acesso e Segurança

A implementação de controles de acesso e segurança é um dos pilares para a proteção de dados pessoais em ambientes hospitalares, especialmente diante da complexidade de sistemas e do alto volume de informações sensíveis. Neste desafio, a análise documental teve como foco avaliar o grau de conformidade dos sistemas institucionais com os princípios da LGPD e os requisitos da norma ISO/IEC 27001, com base nos dados produzidos por consultoria técnica contratada pelo hospital.

O levantamento foi baseado em evidências documentais extraídas dos Relatórios de Diagnóstico ISO/27001 e das versões 1.0 e 2.0 do Security Assessment, elaborados pela empresa de consultoria contratada. A avaliação considerou dois aspectos principais: o grau de implementação dos controles nos sistemas críticos e o nível de controle associado aos riscos identificados durante a análise de segurança da informação.
As métricas utilizadas, conforme o plano GQM, foram:

- D5.M1 – Percentual de implementação dos controles de acesso segundo a ISO/27001.
- D5.M2 – Porcentagem de riscos com nível de controle classificado como ‘Existente’.

A primeira métrica (D5.M1) foi aplicada à análise de 20 sistemas críticos das áreas de TI, Recursos Humanos e assistência. O relatório técnico indicou que 85% desses sistemas já contavam com a implementação dos principais controles exigidos, incluindo:

- Controle de acesso baseado em funções (RBAC);
- Registro e monitoramento de atividades por meio de logs de auditoria;
- Revisão periódica das permissões atribuídas aos usuários.
- Resultado de D5.M1: 85% de conformidade nos sistemas críticos auditados.

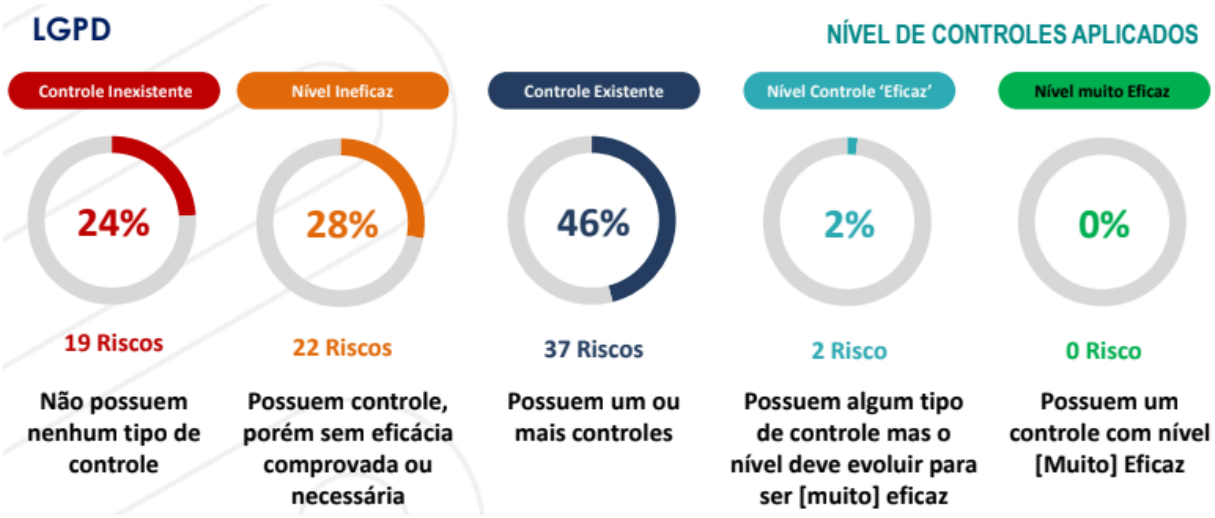
A segunda métrica (D5.M2) referiu-se à proporção de riscos identificados que apresentavam pelo menos algum tipo de controle implementado. Entre os 80 riscos mapeados, a classificação documental revelou:

- 19 riscos (24%) sem controle implementado (classificação: inexistente);

- 22 riscos (28%) com controles ineficazes ou não comprovados;
- 37 riscos (46%) com controle existente, porém não auditado;
- 2 riscos (2%) com controle classificado como eficaz;
- 0 riscos (0%) com controle muito eficaz.

A Figura 4 ilustra visualmente esses níveis de controle, conforme categorização presente no relatório técnico.

Figura 9. Nível de Controles Aplicados



Fonte: Implementação da empresa contratada - LGPD - Apresentação - Risk Assessment v1.2

A análise da métrica D5.M2 indica que 46,25% dos riscos identificados possuíam algum nível de controle documentado, embora muitos ainda não tenham sido testados quanto à sua eficácia real.

Apesar dos avanços observados na implementação de controles de acesso, os dados documentais revelaram fragilidades críticas. 15% dos sistemas analisados ainda não possuíam mecanismos adequados de controle, o que compromete a rastreabilidade e a limitação de acesso a dados sensíveis. Além disso, 53,75% dos riscos identificados não estavam cobertos por controles eficazes, o que amplia a exposição da instituição a incidentes de segurança e sanções regulatórias.

Diante desse cenário, os relatórios técnicos recomendaram uma série de medidas corretivas:

- Correção das deficiências nos sistemas críticos ainda não conformes, com implementação de RBAC e ativação de mecanismos de auditoria;
- Testes de eficácia nos 37 riscos com controles existentes, a fim de verificar sua capacidade real de mitigação;
- Estabelecimento de auditorias contínuas, conforme os padrões da ISO/IEC 27001, para validação periódica dos controles;
- Revisão recorrente das permissões de acesso, garantindo alinhamento com as funções e responsabilidades dos colaboradores.

A análise documental evidenciou que, embora haja esforços estruturais para a implementação de controles, a ausência de verificação sistemática e auditoria dos mecanismos existentes representa um ponto crítico. O fortalecimento da cultura de segurança da informação, aliado à adoção de mecanismos de controle contínuo, será essencial para garantir a integridade, disponibilidade e confidencialidade dos dados pessoais tratados pela instituição.

4.6.6. Desafio 6 – Avaliação da Adequação dos Sistemas às Políticas de Privacidade e Segurança de Dados

A conformidade dos sistemas de informação com as políticas de privacidade e segurança de dados é um fator essencial para a governança da informação em ambientes hospitalares, especialmente diante das exigências impostas pela LGPD. Neste desafio, foi realizada uma análise observacional com base em documentação interna da área de TI da instituição, a fim de verificar se os sistemas utilizados no tratamento de dados pessoais e sensíveis estavam alinhados aos critérios estabelecidos pela LGPD.

Foram identificados, por meio de inventários e relatórios técnicos, vinte e quatro sistemas que exigiam avaliação de conformidade, incluindo softwares de gestão clínica e administrativa, plataformas de segurança e soluções de armazenamento. Entre os principais sistemas avaliados, destacam-se o MV Soul, utilizado para a gestão de prontuários eletrônicos e dados financeiros; o Sistema Rastro, voltado para o rastreamento de instrumentais cirúrgicos; o SAP Business One, aplicado à gestão empresarial; e o Kaspersky Endpoint, responsável pela proteção de endpoints e servidores. A seleção desses sistemas se deu com base na sua relevância para o tratamento direto de dados pessoais, conforme levantamento prévio feito pela equipe técnica da instituição.

A verificação da conformidade desses sistemas levou em consideração critérios como local de armazenagem, mecanismos de segurança, periodicidade de backup, permissões de acesso, existência de logs de transações e práticas de descarte de dados desnecessários, além das políticas de compartilhamento com terceiros. Esses critérios foram aplicados com base nos requisitos da LGPD, cruzando-os com as recomendações das normas ISO/IEC 27001 e 27701.

A aplicação das métricas D6.M1 e D6.M2, previstas no plano GQM, possibilitou quantificar a aderência da instituição às exigências legais. A primeira métrica registrou a existência de 24 sistemas a serem avaliados quanto à sua conformidade. A segunda identificou que apenas 10 desses sistemas apresentavam controles de segurança implementados de forma documentada e consistente, totalizando 41,66% de conformidade no universo analisado.

Os resultados indicaram que, embora haja iniciativas institucionais voltadas à segurança da informação, a aplicação dos controles avaliados se mostrou parcial e, em muitos casos, fragmentada. Houve inconsistência na documentação de logs de auditoria, ausência de rotinas sistemáticas para descarte de dados desnecessários e falhas na formalização de políticas sobre o compartilhamento de dados com terceiros. A integração entre os sistemas e a existência de critérios uniformes para retenção, rastreamento e proteção de dados também se revelaram pontos frágeis na estrutura atual.

Diante desse cenário, os relatórios técnicos analisados sugeriram medidas de padronização dos controles técnicos, com destaque para a necessidade de documentação formal das políticas de segurança já aplicadas e a implantação de mecanismos de auditoria contínua. A priorização dos sistemas que tratam dados sensíveis, como os utilizados nas áreas assistenciais, foi apontada como etapa fundamental para reduzir os riscos de não conformidade.

A análise deste desafio permitiu não apenas mensurar o nível atual de adequação dos sistemas à LGPD, mas também evidenciar os principais pontos de atenção que devem ser enfrentados para garantir um ambiente tecnológico mais seguro e juridicamente alinhado às obrigações legais de proteção de dados pessoais.

4.6.7. Desafío 7 – Treinamento Contínuo dos Colaboradores sobre à LGPD

A capacitação contínua dos colaboradores sobre as diretrizes da LGPD constitui um dos pilares da governança organizacional no tratamento de dados pessoais. No hospital analisado, a ausência de treinamentos formais estruturados foi identificada como uma fragilidade relevante durante o processo de avaliação da conformidade com a LGPD. A análise deste desafio baseou-se na métrica D7.M1, que mensura o percentual de colaboradores que completaram treinamentos contínuos sobre proteção de dados.

Os dados observados foram obtidos a partir de relatórios internos e documentos de diagnóstico fornecidos no contexto da consultoria contratada para implementar a LGPD na instituição. A amostra analisada compreendeu um total de 333 colaboradores, distribuídos entre setores assistenciais, administrativos, jurídicos e técnicos. Os documentos analisados indicaram que, até o momento da avaliação, nenhum colaborador havia concluído treinamentos contínuos sobre a LGPD, resultando em 0% de aderência à métrica estipulada.

Esse dado revela a inexistência de um programa estruturado de capacitação periódica, o que representa um risco crítico para a conformidade institucional. A ausência de treinamentos compromete não apenas a compreensão dos colaboradores sobre suas responsabilidades legais no tratamento de dados pessoais e sensíveis, como também aumenta a vulnerabilidade da organização diante de falhas operacionais, incidentes de segurança e descumprimento regulatório. Além disso, essa lacuna dificulta a comprovação de conformidade em auditorias externas e compromete a credibilidade institucional frente a órgãos fiscalizadores.

A análise documental sugere que o hospital ainda não desenvolveu um calendário fixo de formações periódicas, tampouco implantou registros formais de participação dos colaboradores em ações educativas sobre a LGPD. Essa carência compromete a construção de uma cultura organizacional orientada à privacidade e à segurança da informação.

Como recomendação, os documentos analisados destacaram a importância da criação de um programa de capacitação contínua, com treinamentos presenciais e online que sejam adaptáveis às rotinas e necessidades dos diferentes setores. A segmentação dos conteúdos, conforme o perfil funcional, também foi recomendada: profissionais da área de Tecnologia da Informação devem receber formação sobre segurança da informação e gestão de acessos; o setor de Recursos Humanos deve ser instruído quanto à proteção de dados dos colaboradores; e a equipe assistencial deve ser orientada sobre o tratamento ético e seguro dos dados de pacientes.

Outras sugestões incluíram a criação de mecanismos formais de registro, monitoramento e certificação dos treinamentos realizados, a manutenção de um histórico institucional de capacitação, e a promoção de campanhas de conscientização com o uso de ferramentas comunicacionais internas, como newsletters, cartazes, intranet e ações interativas. Tais iniciativas visam não apenas cumprir exigências legais, mas também fortalecer a compreensão organizacional sobre o papel de cada colaborador na proteção dos dados tratados pela instituição.

Dessa forma, a ausência de um programa de treinamento contínuo representa não apenas um indicador de não conformidade, mas também um ponto estratégico de melhoria. O investimento em capacitação se apresenta como uma condição indispensável para reduzir riscos operacionais e assegurar que os princípios da LGPD estejam incorporados ao cotidiano dos processos institucionais.

4.6.8. Desafio 8 – Monitoramento e Auditoria Contínuos da Conformidade com a LGPD

A ausência de um processo estruturado de auditoria interna foi identificada como uma das principais fragilidades na condução da conformidade com a LGPD no ambiente hospitalar. A análise deste desafio foi conduzida com base na métrica D8.M1, prevista no plano GQM, que mensura a quantidade de auditorias internas realizadas com o objetivo de verificar a efetividade das ações de adequação à LGPD.

Segundo os documentos institucionais analisados, incluindo relatórios de conformidade e documentos de planejamento, nenhuma auditoria interna havia sido conduzida até o momento da avaliação. Essa constatação indicou que, apesar das iniciativas de mapeamento, diagnóstico e implementação de controles, o hospital ainda não havia estruturado um ciclo de monitoramento contínuo e independente para avaliar a eficácia das ações adotadas.

A inexistência de auditorias representa uma limitação importante na governança da privacidade e segurança da informação. Sem um processo formal de verificação periódica, torna-se inviável identificar falhas persistentes, avaliar o nível de maturidade institucional em relação à LGPD e comprovar, de forma sistemática, a conformidade perante órgãos reguladores. Além disso, a falta de auditorias compromete a capacidade da instituição de responder adequadamente a incidentes de segurança e de implementar ações corretivas com base em evidências.

A documentação observada justificou essa lacuna com base na priorização da fase inicial de adequação, que concentrou esforços na identificação de vulnerabilidades, implementação de controles e revisão de políticas. No entanto, essa justificativa não anula a necessidade de estabelecer mecanismos de verificação recorrentes, especialmente em contextos sensíveis como o hospitalar, onde o volume e a criticidade dos dados tratados exigem rigor operacional contínuo.

Como recomendação, os documentos técnicos analisados sugeriram a criação de um plano formal de auditoria, com cronograma definido — anual ou semestral — conforme a complexidade e maturidade dos processos internos. Indicadores-chave de conformidade, como a efetividade dos controles de acesso, a aderência aos princípios da LGPD e a existência de registros documentais de consentimento, foram indicados como critérios prioritários para orientar a execução dessas auditorias.

Também foi apontada a necessidade de capacitação de equipes internas para atuar como auditores de conformidade, garantindo independência e competência técnica no processo. Em casos onde a equipe interna não possui maturidade suficiente, recomendou-se a contratação de auditores externos especializados, assegurando imparcialidade e aderência às melhores práticas.

Além disso, os relatórios propuseram a adoção de ferramentas tecnológicas de monitoramento contínuo, como painel de controle (dashboards), softwares de auditoria e sistemas de alerta para não conformidades. Essas soluções, combinadas com um processo bem definido de tratamento das não conformidades identificadas, com prazos e responsáveis formalmente estabelecidos, seriam fundamentais para consolidar a governança da LGPD no hospital.

Em síntese, a análise da métrica D8.M1 revelou que a inexistência de auditorias internas até o momento constitui um fator crítico de risco, mas também uma oportunidade estratégica para a instituição desenvolver uma estrutura sólida de monitoramento contínuo. A implementação das medidas sugeridas permitirá ao hospital aprimorar seus mecanismos de controle, fortalecer sua segurança jurídica e garantir maior transparência e responsabilidade no tratamento dos dados pessoais.

4.7. IMPACTOS PERCEBIDOS

A adequação às normativas de proteção de dados pessoais, especialmente no contexto hospitalar, gerou impactos significativos na estrutura organizacional e técnica da instituição, conforme identificado na percepção dos colaboradores através do questionário avaliativo aplicado.

4.7.1. Impactos Organizacionais

Segundo os respondentes, a organização demonstrou avanços no estabelecimento de políticas claras para gestão e proteção de dados pessoais, refletindo um aumento perceptível na transparência das práticas relacionadas ao tratamento de dados sensíveis. Entretanto, apesar desses avanços, os colaboradores indicaram que a cultura institucional ainda não está plenamente consolidada no que diz respeito à conscientização sobre privacidade e proteção de dados. A capacitação dos colaboradores, embora reconhecida como uma iniciativa importante, não foi considerada suficientemente abrangente ou contínua, destacando uma área que necessita de melhorias adicionais.

Além disso, foi percebido uma manutenção da imagem institucional, assim como um aumento moderado na confiança dos pacientes e parceiros após a implementação das medidas alinhadas à LGPD. Contudo, a eficiência operacional relacionada à reestruturação dos processos internos apresentou resultados variados, apontando para a necessidade de maior clareza e padronização dos procedimentos operacionais e das responsabilidades setoriais.

4.7.2. Impactos Técnicos

No âmbito técnico, os respondentes reconheceram avanços relevantes na segurança digital, principalmente pela implementação de controles de acesso mais rigorosos, coerentes com metodologias reconhecidas como RBAC e uso sistemático de logs de auditoria. Essas medidas foram percebidas como eficazes na mitigação dos riscos de acessos não autorizados e no fortalecimento da segurança da informação.

Por outro lado, a percepção dos colaboradores revelou uma fragilidade na área de monitoramento contínuo e auditoria. A falta de um ciclo estruturado e sistemático de auditorias internas foi apontada como uma limitação significativa, impactando negativamente a capacidade da instituição em validar a eficácia das medidas implementadas e em detectar em tempo hábil as inconformidades.

Esses resultados indicam uma percepção mista em relação aos impactos técnicos, sugerindo que embora tenham ocorrido avanços notáveis, ainda existem lacunas críticas que precisam ser endereçadas para garantir uma conformidade robusta e sustentável com as normativas da LGPD.

4.8. AMEAÇAS À VALIDADE

A validade dos resultados de uma pesquisa está diretamente relacionada à consistência dos procedimentos metodológicos adotados e à capacidade dos instrumentos utilizados de representar com fidelidade o fenômeno investigado. No contexto deste estudo, foram identificadas algumas ameaças à validade que merecem destaque, sobretudo em razão das características do estudo de caso e da abordagem observacional adotada.

Uma das principais ameaças refere-se à limitação amostral na etapa de validação do plano GQM e de suas métricas. A aplicação dos questionários foi realizada com um número reduzido de respondentes, restrito a dois profissionais envolvidos diretamente no processo de adequação à LGPD. Essa limitação compromete a validade externa, na medida em que reduz a possibilidade de generalização dos achados para outros contextos organizacionais, além de limitar a diversidade de perspectivas avaliativas sobre os desafios enfrentados.

Outra ameaça relevante diz respeito à ausência de participação da alta gestão da organização. A governança da privacidade e da segurança da informação, especialmente em ambientes hospitalares, requer envolvimento institucional em níveis estratégicos. A ausência de representantes da direção institucional ou de setores como Recursos Humanos e Jurídico na validação das métricas e desafios identificados pode ter restringido a compreensão global do processo de adequação à LGPD, afetando a validade do construto.

Adicionalmente, a dependência exclusiva de registros documentais e percepções internas para a formulação do plano GQM constitui uma limitação metodológica. Embora a análise documental tenha sido sistemática e os instrumentos de coleta devidamente estruturados, a ausência de auditorias externas ou de triangulação com fontes independentes limita a validade interna, dificultando a confirmação objetiva de algumas das inferências realizadas.

Por fim, ressalta-se a possibilidade de viés de confirmação durante a análise das métricas. Como os dados foram extraídos de documentos produzidos pelos próprios agentes responsáveis pela implementação da LGPD, existe o risco de supervalorização de ações positivas ou subnotificação de falhas, o que pode afetar a neutralidade da interpretação.

Apesar dessas ameaças, foram adotadas estratégias de mitigação, como a aplicação de questionários estruturados, a utilização de escalas de avaliação quantitativas e a validação cruzada das métricas com base em critérios objetivos. Ainda assim, recomenda-se cautela na extrapolação dos resultados e reforça-se a importância de futuras pesquisas com amostras ampliadas e envolvimento mais amplo dos setores institucionais.

5. CONCLUSÕES

A implementação da LGPD em instituições hospitalares impõe desafios significativos que transcendem o aspecto técnico, exigindo reestruturações culturais, operacionais e estratégicas. O presente trabalho teve como objetivo investigar os principais desafios enfrentados por um hospital particular de grande porte durante o processo de adequação à LGPD, com base em uma abordagem metodológica estruturada pelo modelo GQM. Por meio da análise documental, construção e validação de um plano de métricas, e aplicação de instrumentos avaliativos, foi possível obter uma visão ampla e sistemática da maturidade da instituição quanto à conformidade regulatória.

Os resultados apontaram a existência de lacunas relevantes nos processos internos, sobretudo no que se refere à gestão da segurança da informação, ao controle de acessos, à capacitação de colaboradores e à formalização contratual com terceiros. Embora ações pontuais tenham sido identificadas, o cenário evidenciou um processo de adequação ainda em andamento, com limitações operacionais e organizacionais que comprometem a plena aderência à legislação vigente.

A utilização do modelo GQM demonstrou-se eficaz na sistematização dos dados e na transformação de objetivos qualitativos em indicadores mensuráveis, permitindo uma análise mais objetiva do cenário institucional. A aplicação do modelo, acompanhada de validações com profissionais da organização, proporcionou insights importantes sobre os pontos críticos da conformidade com a LGPD, além de oferecer subsídios para o aprimoramento das práticas de governança e proteção de dados pessoais.

Entretanto, algumas limitações metodológicas devem ser reconhecidas. A principal refere-se à baixa participação de setores estratégicos, como a alta gestão institucional, o que impacta na abrangência das percepções obtidas. Além disso, a limitação do número de participantes na validação das métricas restringe a generalização dos resultados e a robustez estatística das análises. Ainda assim, os dados levantados foram suficientes para cumprir os objetivos da pesquisa e gerar recomendações aplicáveis ao contexto estudado.

Como contribuição prática, o trabalho oferece um modelo replicável de diagnóstico e avaliação da conformidade com a LGPD, que pode ser adaptado a outras instituições do setor de saúde. Espera-se que os achados aqui sistematizados possam auxiliar na promoção de uma cultura organizacional mais consciente e proativa em relação à privacidade e proteção de dados, fomentando decisões baseadas em evidências e alinhadas às exigências legais.

Como proposta para futuras pesquisas, sugere-se explorar a relação entre a maturidade organizacional das instituições de saúde e os critérios de fiscalização adotados pela ANPD, investigando como diferentes níveis de governança impactam na percepção de conformidade e nos resultados das auditorias regulatórias. Tal aprofundamento poderá contribuir para o desenvolvimento de políticas públicas mais eficazes e orientadas à realidade das organizações de saúde brasileiras.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *Revista Eletrônica de Comunicação, Informação & Inovação em Saúde*, Rio de Janeiro, v. 14, n. 3, 2020. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012. Acesso em: 5 mar. 2025.

ANAHP – ASSOCIAÇÃO NACIONAL DE HOSPITAIS PRIVADOS. *Observatório Anahp 2019*. São Paulo: ANAHP, 2019. Disponível em: https://www.anahp.com.br/wp-content/uploads/2022/12/OBS2019-WEB-v4.pdf. Acesso em: 27 fev. 2025.

BEZERRA, Tárcio Rodrigues. Capturando a dinâmica de gestão da terceirização de tecnologia da informação para o apoio a decisões: um estudo de caso em organizações públicas. 2014. 235 f. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Campina Grande, Campina Grande, 2014. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/154. Acesso em: 27 fev. 2025.

BOTELHO, M. C.; CAMARGO, E. P. do A. A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista de Direito Sanitário*, São Paulo, v. 21, p. e0021, dez. 2021. Acesso em: 5 mar. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 abr. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 mar. 2024.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e criar a Autoridade Nacional de Proteção de Dados. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 21 mar. 2024.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821, de 11 de julho de 2007. Define regras para guarda, manuseio e confidencialidade dos prontuários médicos. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-cfm-no-1-821-de-11-de-julho-de-2007. Acesso em: 27 fev. 2025.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 13, p. 59-67, out./dez. 2017. Disponível em: https://www.trf1.jus.br/trf1/conteudo/files/BibliografiaProteodeDados2.ed.final.pdf. Acesso em: 27 fev. 2025.

DONEDA, D.; LIMA BARRETO, M.; ARAÚJO ALMEIDA, B. de. Uso e proteção de dados pessoais na pesquisa científica. *Revista de Direito Público*, Brasília, v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3895. Acesso em: 5 mar. 2025.

GONÇALVES, C. G. 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, out. 2024.

ISO. *ISO/IEC 27001:2022 - Information security management systems*. Disponível em: https://www.iso.org/standard/27001. Acesso em: 5 fev. 2025.

ISO. *ISO/IEC 27701:2019 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. Disponível em: https://www.iso.org/standard/71670.html. Acesso em: 5 fev. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST Privacy Framework: a tool for improving privacy through enterprise risk management*. Gaithersburg, MD, 2020.

PFHAL, D.; RUHE, G. IMMoS: a methodology for integrated measurement, modelling and simulation. *Software Process: Improvement and Practice*, v. 7, n. 3-4, p. 189–210, set. 2002.

PINHEIRO, V. S.; BONNA, A. P. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 21, n. 3, p. 365–394, 2020. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555. Acesso em: 5 mar. 2025.

SCHIRMER, D.; THAINES, A. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à Associação dos Contabilistas do Vale do Paranhana/RS. [S.l.: s.n.], [2021?]. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956/1235. Acesso em: 5 mar. 2025.

SOLINGEN, D. M. (Rini) van; BERGHOUT, E. W. *The Goal/Question/Metric Method: a practical guide for quality improvement of software development*. New York: McGraw-Hill, 1999. Disponível em: https://research.tue.nl/en/publications/the-goalquestionmetric-method-a-practical-guide-for-quality-impro. Acesso em: 5 fev. 2025.

VASILI, V.; CALDIERA, G.; ROMBACH, H. D. The Goal Question Metric Approach. 1994. Disponível em: https://www.cs.toronto.edu/~sme/CSC444F/handouts/GQM-paper.pdf. Acesso em: 5 fev. 2025.

GLOSSÁRIO

Dados pessoais: Qualquer informação relacionada a pessoa natural identificada ou identificável.

Dados sensíveis: Dados sobre origem racial, convicção religiosa, opinião política, saúde, vida sexual, entre outros.

Titular dos dados: Pessoa natural a quem se referem os dados pessoais.

Tratamento de dados: Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, uso, acesso etc.

Controlador: Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa que realiza o tratamento de dados em nome do controlador.

Encarregado (DPO): Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados.

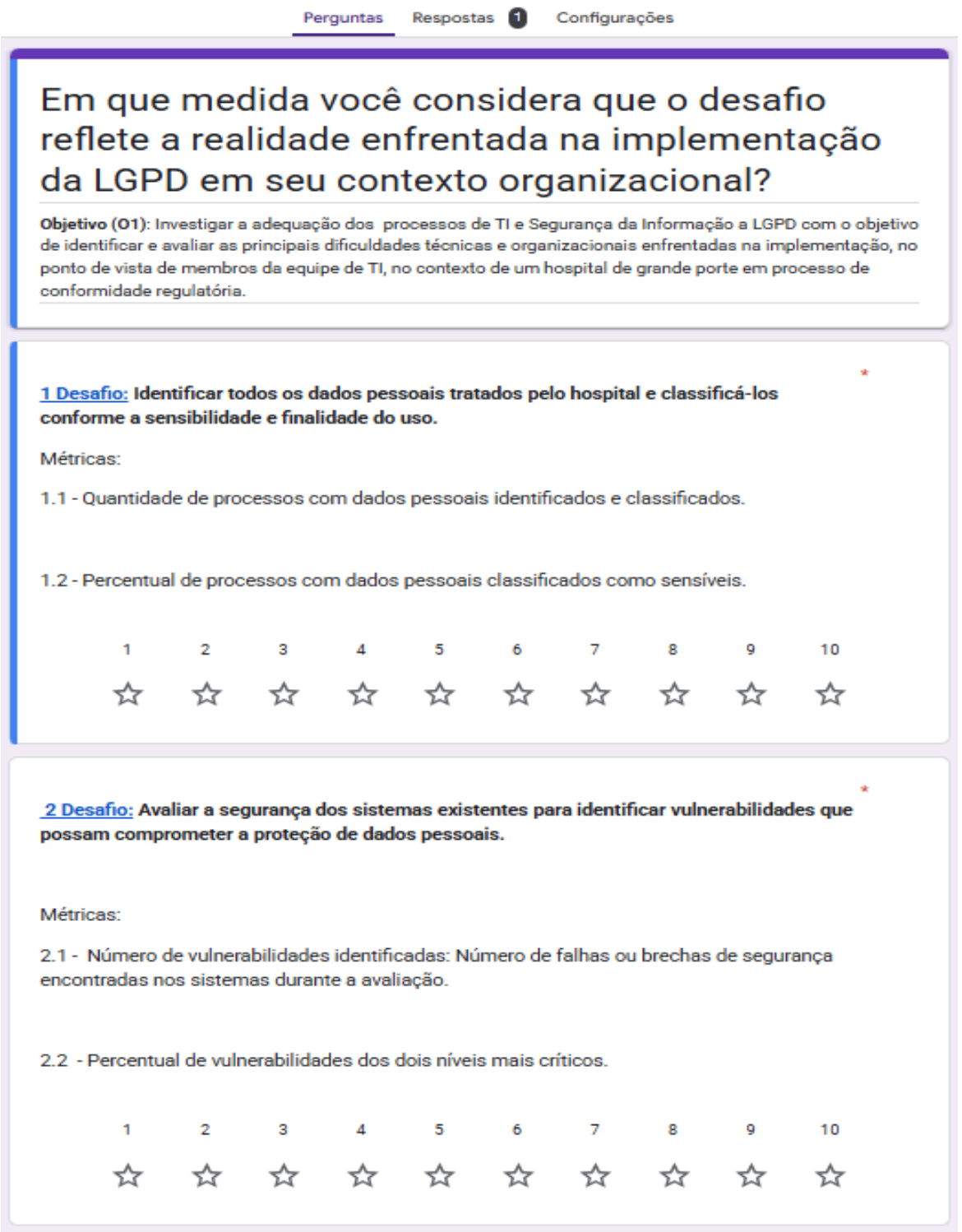
Anonimização: Processo no qual os dados não podem ser relacionados a um titular.

Pseudoanonimização: Processo no qual os dados são dissociados do titular, mas podem ser Reidentificados com informações adicionais.

Segurança da informação: Conjunto de práticas para proteger dados contra acessos não autorizados e vazamentos.

APÊNDICE

Apêndice A – Formulários de Validação dos desafios



3 Desafio: Avaliar se os processos de coleta de dados, incluindo consentimento, estão sendo conduzidos de forma adequada e conforme as exigências da LGPD.

Métricas:

3.1 - Percentual de dados coletados com a base legal estabelecida para a coleta.

3.2 - Percentual de consentimentos documentados em relação ao total de dados pessoais coletados.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

*

4 Desafio: Analisar se os contratos com prestadores de serviços e parceiros estão em conformidade com os requisitos da LGPD.

Métricas:

4.1 - Percentual de contratos revisados quanto à LGPD: Percentual de contratos que foram revisados para atender às exigências da LGPD em relação ao total de contratos com terceiros.

4 Desafio: Monitorar e garantir que todos os contratos com prestadores de serviços estejam sempre em conformidade com a LGPD.

Métricas:

4.1 - Percentual de contratos com cláusulas de conformidade em vigor: Percentual de contratos com cláusulas específicas de proteção de dados que estão em conformidade com a LGPD.

4.2 - Taxa de atualização de contratos com terceiros: Percentual de contratos que foram atualizados para atender às exigências da LGPD após a implantação das melhorias.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

5 Desafio: Estabelecer e implementar controles de acesso e segurança adequados para proteger os dados pessoais dos pacientes e colaboradores. *

Métricas:

5.1 - Percentual de implementação dos controles de acesso segundo a ISO/27001

5.2 - Taxa de incidentes de segurança registrados: Número de incidentes de segurança relacionados ao acesso não autorizado aos dados pessoais durante o processo de implantação.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

6 Desafio: Avaliar a adequação dos sistemas às políticas de privacidade e segurança de dados conforme a LGPD. *

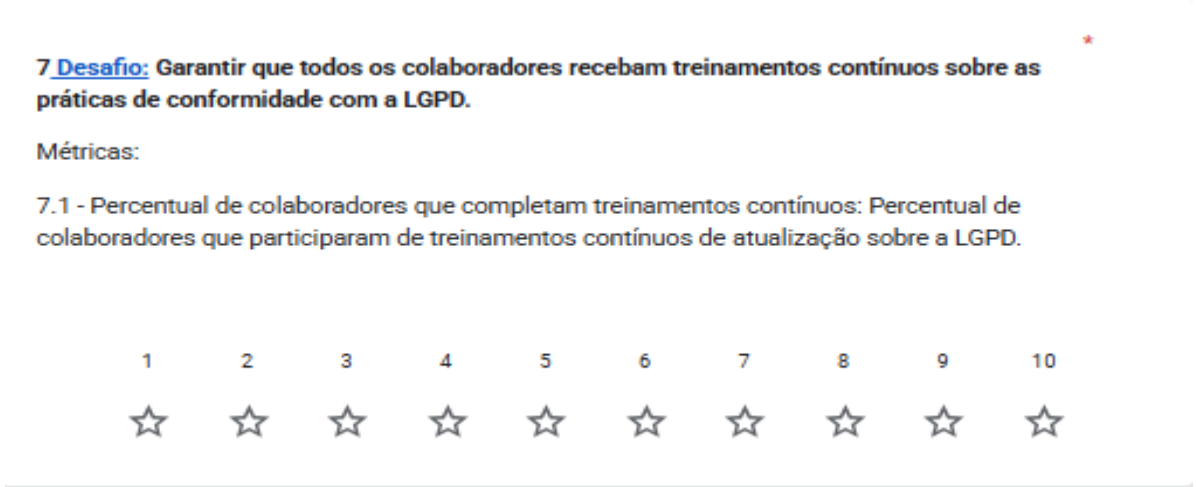
Métricas:

6.1 - Quantidade de sistemas a serem avaliados.

6.2 - Quantidade de controles de segurança.

1 2 3 4 5 6 7 8 9 10

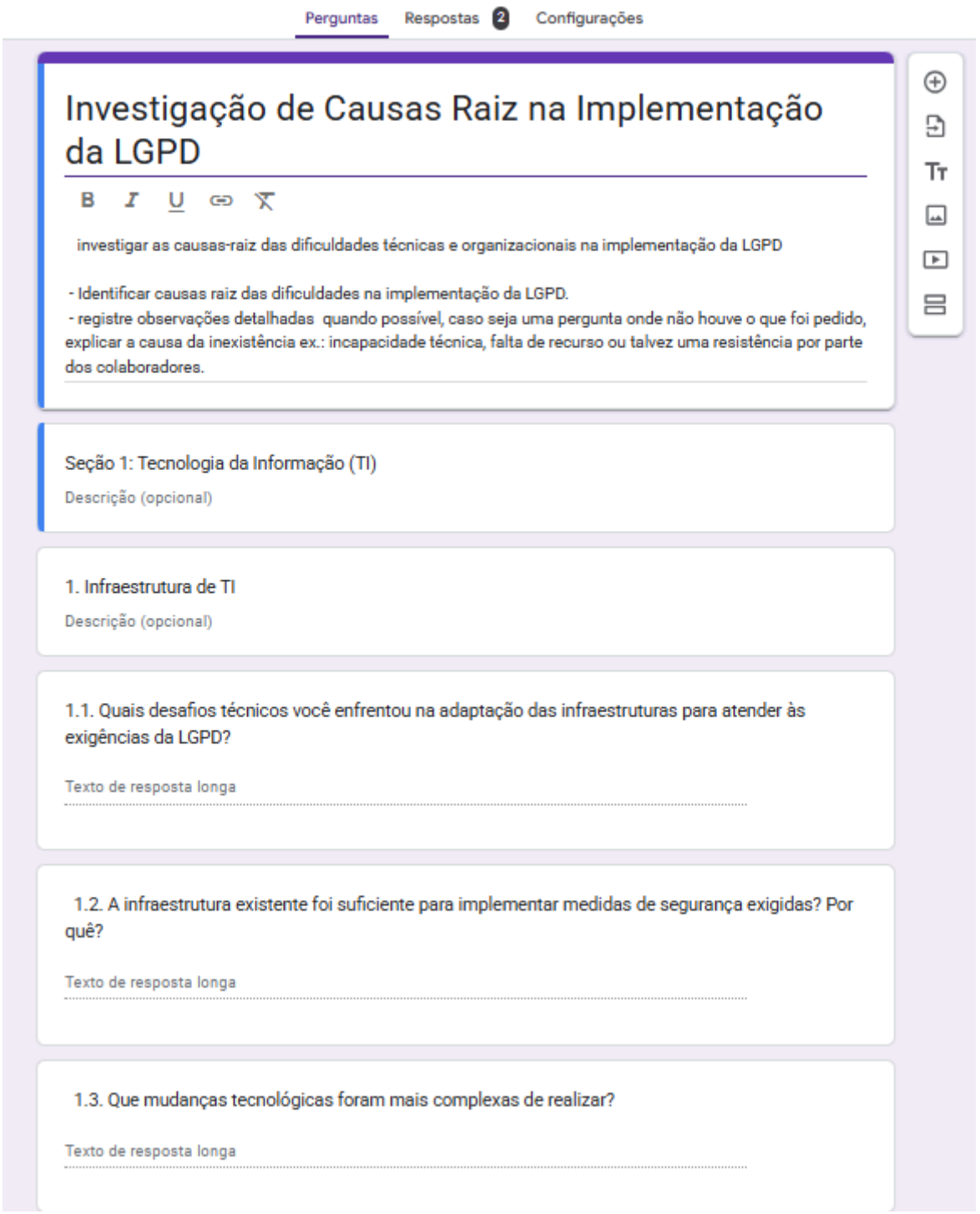
☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆



Resposta do Entrevistado

Desafio	Descrição Resumida	Nota (1 a 10)
Desafio 1	Identificação e classificação de dados pessoais	10
Desafio 2	Avaliação da segurança dos sistemas	10
Desafio 3	Conformidade dos processos de coleta de dados	5
Desafio 4	Conformidade dos contratos com a LGPD	9
Desafio 5	Implementação de controles de acesso e segurança	8
Desafio 6	Adequação dos sistemas às políticas de privacidade e segurança	10
Desafio 7	Treinamento contínuo dos colaboradores	8
Desafio 8	Monitoramento e auditoria contínuos	7

Apêndice B – Formulários de Causas-Raízes



2. Gestão de Dados e Sistemas

Descrição (opcional)

2.1. Quais problemas ocorreram na integração de sistemas para gestão de dados pessoais?

Texto de resposta longa

2.2. Houve dificuldades na classificação ou localização de dados pessoais? Explique.

Texto de resposta longa

2.3. Como a equipe lidou com o consentimento e a gestão de acessos?

Texto de resposta longa

3. Segurança da Informação

Descrição (opcional)

3.1. Quais barreiras foram encontradas na implementação de controles de segurança recomendados?

Texto de resposta longa

3.2. A equipe de TI recebeu treinamento suficiente para lidar com essas mudanças?

Texto de resposta longa

3.3. Os incidentes de segurança estão sendo monitorados adequadamente? Quais melhorias são necessárias

Texto de resposta longa

Seção 2: Gestão Organizacional

Descrição (opcional)

1. Governança e Cultura Organizacional

Descrição (opcional)

1.1. Houve resistência interna à implementação da LGPD? Por parte de quais áreas?

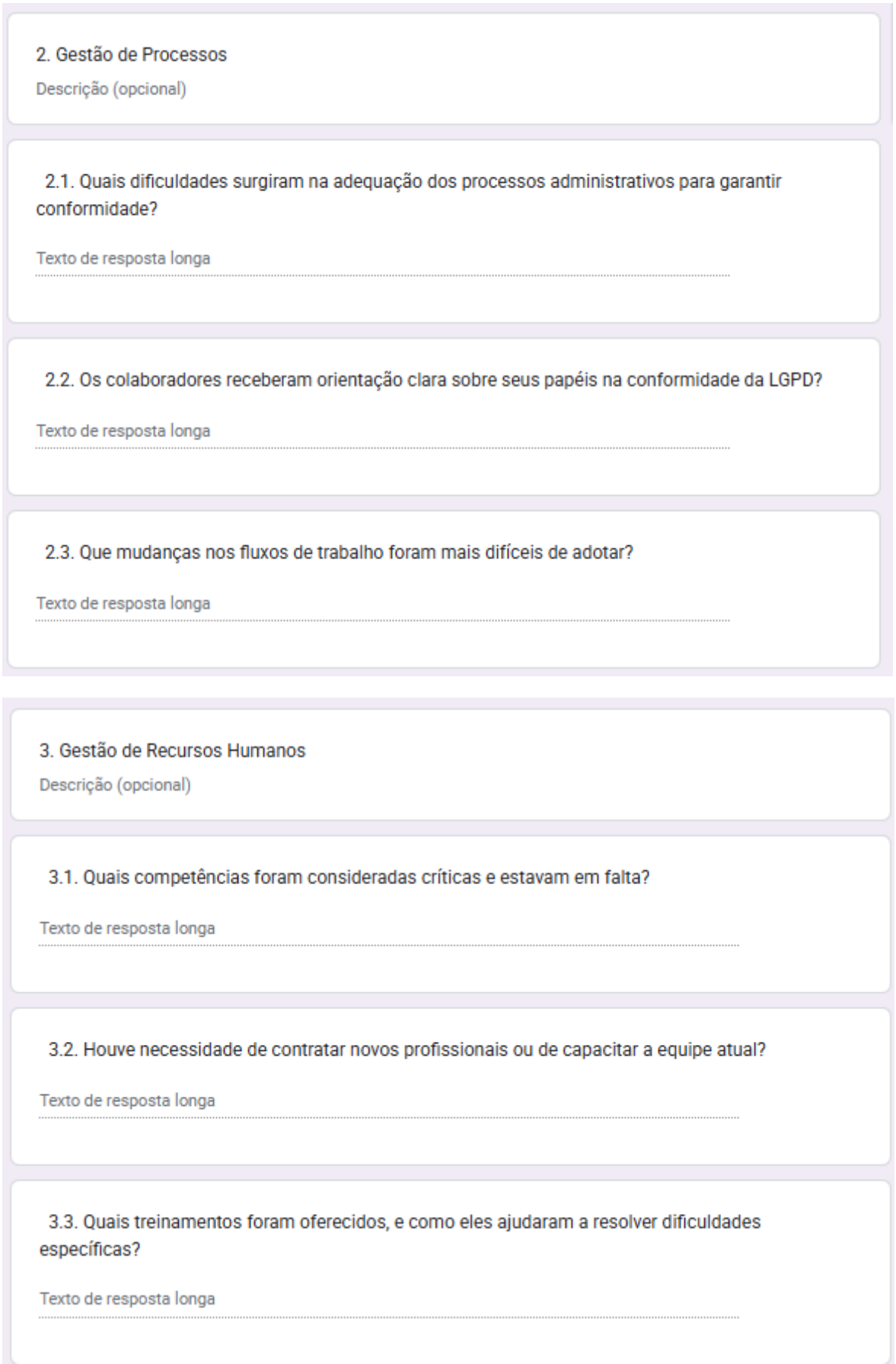
Texto de resposta longa

1.2. As políticas organizacionais foram revisadas para incorporar as diretrizes da LGPD? Explique como.

Texto de resposta longa

1.3. Quais práticas de governança foram mais difíceis de implementar?

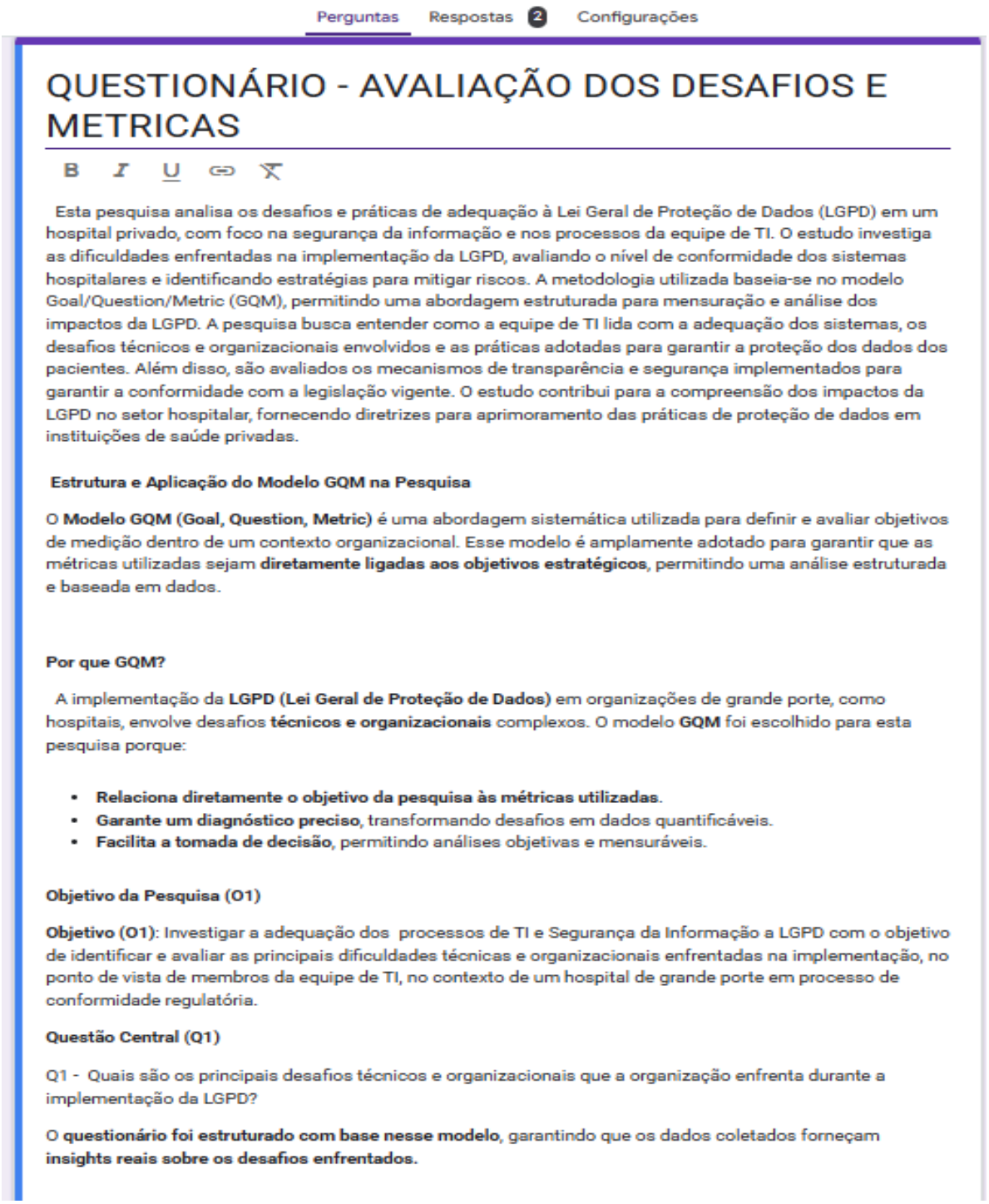
Texto de resposta longa



Resposta dos entrevistados.

Seção	Pergunta	Entrevistado 1	Entrevistado 2
TI - Infraestrutura	1.1	Não muito, porque tinha um pouco de familiaridade com a infraestrutura passada	Exigiu uma revisão e padronização de rotinas...
TI - Infraestrutura	1.2	Algumas medidas sim, exemplo: política de senha, restrição de acesso etc...	Tivemos os recursos e sistemas para a implantação...
TI - Infraestrutura	1.3	Gerenciamento de Vulnerabilidades e Autenticação de duplo fator	Padronizar todos os processos que envolviam perfis de acesso...
TI - Gestão de Dados e Sistemas	2.1	Problemas de operacionalidades, os colaboradores resistindo às mudanças	Não houve integração dos sistemas...
TI - Gestão de Dados e Sistemas	2.2	Um pouco, pois os colaboradores não estavam familiarizados com o processo de mapeamento	Sim, exigiu que todos os setores contribuíssem...
TI - Gestão de Dados e Sistemas	2.3	Lidou bem, pois já existiam políticas	Tivemos o apoio da Direção do hospital...
TI - Segurança da Informação	3.1	Problemas financeiros	Realizar a análise de riscos... interoperabilidade entre os sistemas
TI - Segurança da Informação	3.2	Algumas mudanças sim	Sim, foram realizados treinamentos...
TI - Segurança da Informação	3.3	Melhorias: Ter um painel centralizado para gestão de riscos	Foi criado um fluxo sobre vazamento de dados...
Governança e Cultura Organizacional	1.1	Por partes de todas as áreas	Todas as áreas tiveram resistência...
Governança e Cultura Organizacional	1.2	Sim, a consultoria analisou as políticas	Sim, inclusive criamos algumas políticas internamente...
Governança e Cultura Organizacional	1.3	Implementação da Unidade de GRC	Implementação da Unidade de GRC, criação do comitê de privacidade...
Gestão de Processos	2.1	Dificuldade na anonimização dos dados sensíveis	
Gestão de Processos	2.2	Receberam, via videoconferências	Comunicado nos meios de comunicação da instituição
Gestão de Processos	2.3	Revisão e adaptação de processos de coleta e armazenamento	
Gestão de RH	3.1	Gestão de Vulnerabilidades	Não tínhamos setor de segurança da informação
Gestão de RH	3.2	Não	Capacitação de membro da equipe de redes e infraestrutura
Gestão de RH	3.3	Consultoria realizou treinamentos para TI	Cursos de segurança cibernética, ISO 27001 e 27002

Apêndice C – Formulários de Validação dos Desafios e Métricas



Perguntas Respostas 2 Configurações

QUESTIONÁRIO - AVALIAÇÃO DOS DESAFIOS E METRICAS

Esta pesquisa analisa os desafios e práticas de adequação à Lei Geral de Proteção de Dados (LGPD) em um hospital privado, com foco na segurança da informação e nos processos da equipe de TI. O estudo investiga as dificuldades enfrentadas na implementação da LGPD, avaliando o nível de conformidade dos sistemas hospitalares e identificando estratégias para mitigar riscos. A metodologia utilizada baseia-se no modelo Goal/Question/Metric (GQM), permitindo uma abordagem estruturada para mensuração e análise dos impactos da LGPD. A pesquisa busca entender como a equipe de TI lida com a adequação dos sistemas, os desafios técnicos e organizacionais envolvidos e as práticas adotadas para garantir a proteção dos dados dos pacientes. Além disso, são avaliados os mecanismos de transparência e segurança implementados para garantir a conformidade com a legislação vigente. O estudo contribui para a compreensão dos impactos da LGPD no setor hospitalar, fornecendo diretrizes para aprimoramento das práticas de proteção de dados em instituições de saúde privadas.

Estrutura e Aplicação do Modelo GQM na Pesquisa

O **Modelo GQM (Goal, Question, Metric)** é uma abordagem sistemática utilizada para definir e avaliar objetivos de medição dentro de um contexto organizacional. Esse modelo é amplamente adotado para garantir que as métricas utilizadas sejam **diretamente ligadas aos objetivos estratégicos**, permitindo uma análise estruturada e baseada em dados.

Por que GQM?

A implementação da **LGPD (Lei Geral de Proteção de Dados)** em organizações de grande porte, como hospitais, envolve desafios **técnicos e organizacionais** complexos. O modelo **GQM** foi escolhido para esta pesquisa porque:

- **Relaciona diretamente o objetivo da pesquisa às métricas utilizadas**.
- **Garante um diagnóstico preciso**, transformando desafios em dados quantificáveis.
- **Facilita a tomada de decisão**, permitindo análises objetivas e mensuráveis.

Objetivo da Pesquisa (O1)

Objetivo (O1): Investigar a adequação dos processos de TI e Segurança da Informação a LGPD com o objetivo de identificar e avaliar as principais dificuldades técnicas e organizacionais enfrentadas na implementação, no ponto de vista de membros da equipe de TI, no contexto de um hospital de grande porte em processo de conformidade regulatória.

Questão Central (Q1)

Q1 - Quais são os principais desafios técnicos e organizacionais que a organização enfrenta durante a implementação da LGPD?

O **questionário foi estruturado com base nesse modelo**, garantindo que os dados coletados forneçam **insights reais sobre os desafios enfrentados.**

1 Desafio: Identificar todos os dados pessoais tratados pelo hospital e classificá-los conforme a sensibilidade e finalidade do uso.

*A conformidade com a LGPD exige que as organizações realizem um **mapeamento detalhado** dos dados pessoais tratados internamente. Esse processo envolve **identificar quais dados são coletados, sua finalidade, base legal e nível de sensibilidade**. No contexto hospitalar, isso é ainda mais crítico, pois a maioria das informações são **dados sensíveis**, como históricos médicos, biometria e registros clínicos, exigindo maior proteção.*

Métricas:

1.1 - Quantidade de processos com dados pessoais identificados e classificados.

1.2 - Percentual de processos com dados pessoais classificados como sensíveis.

*Durante a implementação da LGPD no hospital, **853 processos organizacionais foram mapeados**, e **77,63% desses processos lidam com dados sensíveis**. Essa categorização permitiu alinhar os processos às exigências legais e definir estratégias para mitigação de riscos.*

Q 1.1 Você considera que identificar todos os dados pessoais tratados pelo hospital e classificá-los conforme a sensibilidade e finalidade do uso foi realmente um desafio? *

Escala de Avaliação (0 a 10):
0 = Não foi um desafio significativo
5 = Foi um desafio moderado, mas controlável
10 = Foi um grande desafio, com dificuldades significativas

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 1.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
0 = Não está de acordo.
5 = Razoável.
10 = Sim, concordo plenamente com os resultados da métrica.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 1.3 - Caso tenha avaliado com 5 o menos, explique o porquê.

Sua resposta

2 Desafio: Avaliar a segurança dos sistemas existentes para identificar vulnerabilidades que possam comprometer a proteção de dados pessoais.

A segurança dos sistemas hospitalares é essencial para a proteção dos dados pessoais e a conformidade com a LGPD. Durante a implementação, foram identificadas 211 vulnerabilidades, sendo 50,7% classificadas como altas ou críticas, exigindo atenção prioritária.

Além disso, a análise de riscos apontou 80 riscos no total, dos quais 73,75% foram categorizados como elevados ou críticos, representando eventos com grande impacto na operação do hospital. Esse levantamento foi essencial para priorizar ações corretivas e garantir que os sistemas e processos estejam alinhados às diretrizes de segurança da informação.

Segue abaixo as métricas com os dados obtidos.

2.1 - Número de Vulnerabilidades Identificadas:

Foram identificadas **211 vulnerabilidades** por meio do **Relatório de Security Assessment (Etapa 5)**.Essas vulnerabilidades foram detectadas por **ferramentas de análise automatizada** e **testes manuais realizados pela equipe de segurança.159 eram vulnerabilidades internas** (dentro dos sistemas do hospital) e **52 externas** (exposição a ameaças externas).

2.2 - Percentual de Vulnerabilidades Altas ou Críticas:

No total, **107 vulnerabilidades** foram classificadas como **Altas (63) ou Críticas (44)**.Isso representa **50,7%** das vulnerabilidades, indicando que metade delas exigia ação imediata.

2.3 - Número de Riscos Identificados:

A análise de riscos foi realizada na **Etapa 6 - Relatório de Risk Assessment v1.2**, onde foram mapeados **80 riscos** relacionados à segurança e privacidade dos dados. Os riscos foram identificados por meio de **entrevistas com equipes técnicas, auditorias internas e avaliação de conformidade com normas como a ISO 31000 e ISO 27001**.

2.4 - Percentual de Riscos Elevados e Críticos:

Dos **80 riscos identificados, 22 foram classificados como elevados e 37 como críticos.** O percentual de riscos altos e críticos chegou a **73,75%**, reforçando a necessidade de correções urgentes para mitigar impactos financeiros, operacionais e regulatórios.

Q 2.1 - Em sua opinião, **avaliar a segurança dos sistemas existentes para identificar vulnerabilidades que possam comprometer a proteção de dados pessoais** foi um desafio relevante durante a implementação da LGPD? *

📌 ***Escala de Avaliação (0 a 10):***
🔴 ***0** = Não foi um desafio significativo*
🟠 ***5** = Foi um desafio moderado, mas controlável*
🟢 ***10** = Foi um grande desafio, com dificuldades significativas*

1	2	3	4	5	6	7	8	9	10
☆	☆	☆	☆	☆	☆	☆	☆	☆	☆

Q 2.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
- ***0** = Não está de acordo.*
- ***5** = Razoável.*
- ***10** = Sim, concordo plenamente com os resultados da métrica.*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 2.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Texto de resposta longa

3 Desafio: Avaliar se os processos de coleta de dados, incluindo consentimento, estão sendo conduzidos de forma adequada e conforme as exigências da LGPD.

Durante a implementação da LGPD, foi analisada a conformidade da coleta de dados pessoais no hospital. O levantamento indicou que, dos **853 processos mapeados**, apenas **28,72%** possuem uma base legal documentada para justificar a coleta de dados pessoais. Além disso, nos **608 processos que exigiriam consentimento formal**, **nenhum registro foi encontrado**, evidenciando um risco de não conformidade com a legislação. Esses dados foram obtidos a partir do **Mapeamento de Dados (Etapa 4)** e do **Relatório de Adequação Documental (Etapa 8)**.

As métricas foram validadas a partir do **Mapeamento de Dados (Etapa 4)** e do **Relatório de Adequação Documental (Etapa 8)**, que analisaram os processos do hospital que tratam dados pessoais e verificaram a conformidade com a LGPD.

3.1 - Percentual de Dados Coletados com Base Legal

Dos **853 processos mapeados**, **245** possuem uma base legal documentada, representando **28,72%** de conformidade. A validação foi feita por meio da análise documental dos processos e categorização conforme os critérios da LGPD.

3.2 - Percentual de Consentimentos Documentados

Dos **608 processos** que exigiam consentimento, **nenhum foi encontrado documentado**, resultando em **0% de conformidade**. A verificação foi feita através da análise de registros e documentos internos, evidenciando a falta de um controle estruturado para a coleta formal de consentimentos.

Q 3.1 - Com base nessa análise, você considera que avaliar se os processos de coleta de dados, incluindo consentimento, estão sendo conduzidos de forma adequada e conforme as exigências da LGPD foi um desafio relevante na implementação? *

Escala de Avaliação (0 a 10):
0 = Não foi um desafio significativo
5 = Foi um desafio moderado, mas controlável
10 = Foi um grande desafio, com dificuldades significativas

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 3.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
0 = Não está de acordo.
5 = Razoável.
10 = Sim, concordo plenamente com os resultados da métrica.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 3.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Sua resposta

4 Desafio: : Analisar e Monitorar se os contratos com prestadores de serviços e parceiros estão em conformidade com os requisitos da LGPD

A adequação dos contratos à LGPD é essencial para assegurar que as relações com terceiros estejam protegidas por cláusulas que garantam a segurança e o correto tratamento dos dados pessoais. Durante o processo de conformidade, foi conduzida uma revisão documental dos contratos existentes para verificar se atendiam às exigências legais e se possuíam cláusulas específicas para proteção de dados.

Resultados das Métricas

4.1 Percentual de contratos revisados quanto à LGPD

Dos **479 contratos identificados**, **300 passaram por revisão**, representando **62,63%** do total. Isso demonstra um avanço na adequação, mas ainda há **37,37% de contratos pendentes**, indicando a necessidade de continuidade no processo de revisão.

4.1 Percentual de contratos com cláusulas de conformidade em vigor

Não foram encontradas evidências documentais de contratos já formalizados com cláusulas específicas para proteção de dados, resultando em **0% de contratos com cláusulas adequadas**. Isso sugere que, apesar das revisões realizadas, ainda não houve uma implementação prática e padronizada dessas cláusulas.

4.3 Taxa de atualização de contratos com terceiros

A atualização formal dos contratos também não foi registrada, mantendo o índice de **0%**. Isso reforça a necessidade de estabelecer prazos e ações concretas para garantir a inserção de cláusulas de proteção de dados nos contratos ativos.

Os resultados indicam que a revisão contratual está em andamento, mas a implementação de ajustes práticos ainda não ocorreu. O principal desafio agora é garantir que os contratos revisados sejam de fato atualizados e formalizados para alcançar plena conformidade com a LGPD.

Descrição (opcional)

Q 4.1 Diante desses resultados, você considera que **Analisar e Monitorar se os contratos com prestadores de serviços e parceiros estão em conformidade com os requisitos da LGPD** foi um **desafio**? *

Escala de Avaliação (0 a 10):
0 = Não foi um desafio significativo
5 = Foi um desafio moderado, mas controlável
10 = Foi um grande desafio, com dificuldades significativas

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 4.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
0 = Não está de acordo.
5 = Razoável.
10 = Sim, concordo plenamente com os resultados da métrica.

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 4.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Texto de resposta longa

5º Desafio: Estabelecer e Implementar Controles de Acesso e Segurança para Proteger os Dados Pessoais dos Pacientes e Colaboradores

A segurança dos dados pessoais no ambiente hospitalar depende da implementação eficaz de controles de acesso que garantam que apenas usuários autorizados possam visualizar ou manipular informações sensíveis. Para avaliar esse processo, foram analisados os sistemas críticos e a eficácia dos controles de segurança existentes, conforme os padrões da **ISO/27001** e as diretrizes da **LGPD**.

Resultados das Métricas

5.1 Percentual de Implementação dos Controles de Acesso Segundo a ISO/27001

Dos **20 sistemas críticos avaliados**, **17 apresentaram controles de acesso implementados** de acordo com a ISO/27001, totalizando **85% de conformidade.** Os critérios de avaliação incluíram o uso de **acesso baseado em funções (RBAC), monitoramento de logs e revisões periódicas de credenciais. Ainda** há **15% dos sistemas pendentes de adequação**, exigindo ajustes para atingir plena conformidade.

5.2 Porcentagem de Riscos com Nível de Controle Classificado como "Existente"

Entre os **80 riscos identificados**, **37 apresentaram algum nível de controle já implementado**, resultando em **46,25%** de riscos classificados como "Existente". Esses controles, embora estejam presentes, **não foram validados quanto à sua eficácia**, exigindo testes e ajustes para garantir proteção adequada aos dados sensíveis.

Os dados indicam um **bom avanço na implementação de controles de acesso e mitigação de riscos**, mas também revelam a necessidade de **aperfeiçoamento contínuo** para aumentar a maturidade da segurança da informação no hospital.

Descrição (opcional)

Q 5.1 Com base nos desafios enfrentados para implementar controles de acesso e segurança * nos sistemas críticos do hospital, você considera que **Estabelecer e Implementar Controles de Acesso e Segurança para Proteger os Dados Pessoais dos Pacientes e Colaboradores** foi um **desafio**?

📌 ***Escala de Avaliação (0 a 10):***
🔴 ***0** = Não foi um desafio significativo*
🟠 ***5** = Foi um desafio moderado, mas controlável*
🟢 ***10** = Foi um grande desafio, com dificuldades significativas*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 5.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
🔴 ***0** = Não está de acordo.*
🟠 ***5** = Razoável.*
🟢 ***10** = Sim, concordo plenamente com os resultados da métrica.*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 5.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Texto de resposta longa

6° Desafio: Avaliar a Adequação dos Sistemas às Políticas de Privacidade e Segurança de Dados Conforme a LGPD

A adequação dos sistemas de TI às políticas de **privacidade e segurança de dados** é um elemento essencial para garantir a conformidade com a **LGPD** e minimizar riscos associados ao tratamento de dados pessoais e sensíveis. Essa análise envolve a **identificação dos sistemas em uso** e a **avaliação dos controles de segurança implementados**, permitindo identificar falhas e promover melhorias para elevar o nível de proteção.

Resultados das Métricas

Quantidade de Sistemas Avaliados (Métrica 6.1)
Foram analisados **25 sistemas** utilizados em diferentes áreas do hospital, incluindo **ERP, gestão de prontuários, segurança de rede e armazenamento de dados**.Cada sistema foi avaliado quanto à **sua conformidade com as diretrizes da LGPD**, considerando sua estrutura de segurança e privacidade.

Quantidade de Controles de Segurança Avaliados (Métrica 6.2)
Para garantir um monitoramento abrangente, foram analisados **20 critérios de segurança aplicados aos sistemas**, como **logs de transações, permissões de acesso, backup, criptografia, controle de compartilhamento de dados e políticas de retenção. Essa** análise permitiu verificar **o nível de maturidade da segurança dos sistemas**, identificando pontos de vulnerabilidade e oportunidades para aprimoramento.

Os resultados destacam que, embora um número significativo de sistemas já possua controles estabelecidos, **a adequação completa ainda requer ajustes e revisões contínuas** para garantir conformidade plena com a LGPD.

Q 6.1 Com base no processo de avaliação e adequação dos sistemas às **políticas de privacidade e segurança de dados conforme a LGPD**, você considera que **esse processo foi um desafio**? *

📌 ***Escala de Avaliação (0 a 10):***
🔴 ***0** = Não foi um desafio significativo*
🟠 ***5** = Foi um desafio moderado, mas controlável*
🟢 ***10** = Foi um grande desafio, com dificuldades significativas*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 6.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
🔴 ***0** = Não está de acordo.*
🟠 ***5** = Razoável.*
🟢 ***10** = Sim, concordo plenamente com os resultados da métrica.*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 6.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Sua resposta

7° Desafio: Garantir que todos os colaboradores recebam treinamentos contínuos sobre as práticas de conformidade com a LGPD

A capacitação contínua dos colaboradores é um fator essencial para garantir o cumprimento das exigências da **LGPD**, reduzindo riscos operacionais e assegurando que as **políticas de privacidade e proteção de dados** sejam corretamente aplicadas no dia a dia. Durante a **fase de diagnóstico**, foram identificadas **deficiências na conscientização e treinamento** dos profissionais, especialmente em setores que lidam com dados sensíveis, como **TI e Recursos Humanos**.
Resultados da Métrica Percentual de Colaboradores que Completaram Treinamentos Contínuos (Métrica 7.1)Número total de colaboradores: 333.**Número de colaboradores que completaram treinamentos contínuos:** 0.**Percentual obtido: 0%**.

A análise demonstrou que, até o momento, **não há evidências da implementação formal de um programa estruturado de treinamentos contínuos** sobre a LGPD. As ações realizadas foram pontuais e restritas às fases iniciais do diagnóstico, sem a continuidade necessária para consolidar boas práticas organizacionais.

A ausência de capacitação recorrente representa um desafio na construção de uma **cultura organizacional de proteção de dados**, evidenciando a necessidade urgente de estruturar um **plano de treinamentos periódicos**, segmentado por áreas e com certificação da participação dos colaboradores.

Q 7.1 É desafiador **Garantir que todos os colaboradores recebam treinamentos contínuos sobre as práticas de conformidade com a LGPD** mesmo que **não exista evidências da implementação formal de um programa estruturado de treinamentos contínuos?** *

📌 ***Escala de Avaliação (0 a 10):***
🔴 ***0** = Não foi um desafio significativo*
🟠 ***5** = Foi um desafio moderado, mas controlável*
🟢 ***10** = Foi um grande desafio, com dificuldades significativas*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 7.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
🔴 ***0** = Não está de acordo.*
🟠 ***5** = Razoável.*
🟢 ***10** = Sim, concordo plenamente com os resultados da métrica.*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 7.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Sua resposta

8° Desafio: Estabelecer um Processo de Monitoramento Contínuo e Auditoria das Operações Relacionadas à Privacidade e Proteção de Dados Pessoais

O monitoramento contínuo e a auditoria interna são fundamentais para garantir que a conformidade com a **LGPD** seja mantida a longo prazo. Auditorias permitem identificar falhas, avaliar a eficácia dos controles implementados e corrigir eventuais lacunas nos processos de proteção de dados.
Resultados da MétricaNúmero de Auditorias Internas Realizadas (Métrica 8.1)Número total de auditorias realizadas: 0.Justificativa: Até o momento, as auditorias ainda não foram implementadas formalmente, pois a organização se concentrou na adequação inicial dos processos e sistemas.

A ausência de auditorias formais reflete o estágio inicial da conformidade com a LGPD. Para que as melhorias implementadas sejam sustentáveis, é essencial que um plano estruturado de auditoria e monitoramento seja estabelecido.

Q 8.1 Tendo em vista que **a organização ainda não realizou auditorias internas formais para verificar a conformidade com a LGPD**, você considera que **a ausência desse monitoramento representou um desafio significativo na implementação da conformidade regulatória**? *

📌 ***Escala de Avaliação (0 a 10):***
🔴 ***0** = Não foi um desafio significativo*
🟠 ***5** = Foi um desafio moderado, mas controlável*
🟢 ***10** = Foi um grande desafio, com dificuldades significativas*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 8.2 - Você considera que os resultados apresentados, no seu ponto de vista, estão de acordo com a métrica? *

Escala de Avaliação (0 a 10):
🔴 ***0** = Não está de acordo.*
🟠 ***5** = Razoável.*
🟢 ***10** = Sim, concordo plenamente com os resultados da métrica.*

1 2 3 4 5 6 7 8 9 10

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Q 8.3 - Caso tenha avaliado com 5 o menor, explique o porquê.

Sua resposta

Resposta dos entrevistados.

Desafio	Entrevistado	Q1 – Foi um desafio?	Q2 – Métrica condizente?	Q3 – Justificativa (se Q1 ou Q2 ≤ 5)
Desafio 1	Entrevistado 1	10	10	
	Entrevistado 2	10	9	
Desafio 2	Entrevistado 1	9	9	
	Entrevistado 2	10	10	
Desafio 3	Entrevistado 1	10	9	
	Entrevistado 2	10	10	
Desafio 4	Entrevistado 1	10	9	
	Entrevistado 2	9	10	
Desafio 5	Entrevistado 1	10	9	
	Entrevistado 2	10	10	
Desafio 6	Entrevistado 1	10	9	
	Entrevistado 2	10	10	
Desafio 7	Entrevistado 1	10	9	
	Entrevistado 2	9	10	
Desafio 8	Entrevistado 1	7	7	
	Entrevistado 2	10	10	