UNIVERSIDADE NOVE DE JULHO - UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

NITYANANDA PORTELLADA

PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS BASEADO EM *BUSINESS PROCESS MANAGEMENT* PARA HOSPITAL PEDIÁTRICO

São Paulo
2024

NITYANANDA PORTELLADA

PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS BASEADO EM *BUSINESS PROCESS MANAGEMENT* PARA HOSPITAL PEDIÁTRICO

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Informática e Gestão do Conhecimento da Universidade Nove de Julho – UNINOVE, como requisito parcial para a obtenção do título de Mestre em Informática e Gestão do Conhecimento.

Linha de Pesquisa: Gestão da Tecnologia da Informação e do Conhecimento (GTIC).

Prof. Orientador: Dr. Renato José Sassi

São Paulo

2024

Portellada, Nityananda.

Programa de privacidade e proteção de dados baseado em *business process management* para hospital pediátrico. / Nityananda Portellada. 2024.

137 f.

Dissertação (Mestrado)- Universidade Nove de Julho - UNINOVE, São Paulo, 2024.

Orientador (a): Prof. Dr. Renato José Sassi.

1. Privacidade e proteção de dados. 2. Dados sensíveis de crianças e adolescentes. 3. Hospital pediátrico. 4. LGPD. 5. Segurança da informação.

I. Sassi, Renato José. II. Título

CDU 004

UNINOVE
Universidade Nove de Julho

PARECER – EXAME DE DEFESA

Parecer da Comissão Examinadora designada para o exame de defesa do Programa de Pós-Graduação em Informática e Gestão do Conhecimento a qual se submeteu o aluno Nityananda Portellada.

Tendo examinado o trabalho apresentado para obtenção do título de "Mestre em Informática e Gestão do Conhecimento", com Dissertação intitulada "PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS BASEADO EM BUSINESS PROCESS MANAGEMENT PARA HOSPITAL PEDIÁTRICO", a Comissão Examinadora considerou o trabalho:

(X) Aprovado **( ) Aprovado condicionalmente**
( ) Reprovado com direito a novo exame **( ) Reprovado**

EXAMINADORES

Prof. Dr. Renato Jose Sassi - UNINOVE (Orientador)

Prof. Dr. Marcio Romero - UNINOVE (Membro Externo)

Prof. Dr. Marcos Antonio Gaspar - UNINOVE (Membro Interno)

São Paulo, 06 de junho de 2024

RESUMO

Nos hospitais pediátricos, a adequação à Lei Geral de Proteção de Dados (LGPD) alterou os métodos de trabalho, gerando em certos casos dificuldades na sua implementação, devido ao fato de os *frameworks*, comumente usados para este fim como o COBIT e a ISO 27701, não deterem meios para lidar com o tratamento dos dados sensíveis de crianças e adolescentes. Uma forma de implementar a privacidade e proteção de dados é por meio de um programa que seja desenvolvido para levar em conta as características dos processos e dos dados presentes em um hospital pediátrico, considerando mapear processos e dados com a metodologia BPM. O mapeamento de processos é uma prática essencial ao cumprimento dos deveres impostos em um ambiente regulatório, sendo importante por conseguir dar visibilidade aos processos existentes e permitir melhoria processual posterior. O objetivo deste trabalho foi desenvolver e implementar um programa de privacidade e proteção de dados baseado em *Business Process Management* para hospital pediátrico, a fim de apoiar o cumprimento da Lei Geral de Proteção de Dados. O desenvolvimento do programa foi estruturado em quatro fases distintas: Pesquisa Bibliográfica; Desenvolvimento do Programa de Privacidade e Proteção de Dados; Implementação do Programa de Privacidade e Proteção de Dados e Cumprimento da Lei Geral de Proteção de Dados, implementado em um hospital pediátrico privado com 180 leitos, situado em um grande centro urbano brasileiro. Após a implementação foi possível aprimorar o ambiente de proteção de dados do hospital e, como consequência melhorar os processos com ganho operacional e de segurança ao paciente, o que atingiu a elaboração de políticas, documentos e processos. Houve ainda a melhoria da gestão da segurança da informação, com o patrocínio de mudanças de regras e costumes, embasados pelos treinamentos realizados. O hospital conta agora com políticas e processos voltados para a proteção de dados e a correta gestão de dados dos titulares, com a garantia do cumprimento da LGPD.

Palavras-chave: Privacidade e Proteção de Dados; Dados Sensíveis de Crianças e Adolescentes; Hospital Pediátrico; LGPD; Segurança da Informação.

ABSTRACT

In pediatric hospitals, compliance with the General Data Protection Law (LGPD) changed working methods, creating in certain cases difficulties in their implementation, because frameworks, commonly used for this purpose, such as COBIT and ISO 27701, do not have the means to deal with the processing of sensitive data of children and adolescents. One way to implement privacy and data protection is through a program that is developed to consider the characteristics of the processes and data present in a pediatric hospital, considering mapping processes and data with the BPM methodology. Process mapping is an essential practice for fulfilling the duties imposed in a regulatory environment and is important because it can provide visibility to existing processes and allow for subsequent procedural improvement. The objective of this work was to develop and implement a privacy and data protection program based on Business Process Management for a pediatric hospital, to support compliance with the General Data Protection Law. The development of the program was structured into four distinct phases: Bibliographic Research; Development of the Privacy and Data Protection Program; Implementation of the Privacy and Data Protection Program and Compliance with the General Data Protection Law, implemented in a private pediatric hospital with 180 beds, located in a large Brazilian urban center. After implementation, it was possible to improve the hospital's data protection environment and, consequently, improve processes with operational and patient safety gains, which affected the development of policies, documents and processes. There was also an improvement in information security management, with the sponsorship of changes to rules and customs, based on the training carried out. The hospital now has policies and processes aimed at data protection and the correct management of data subjects, ensuring compliance with the LGPD.

Keywords: Privacy and Data Protection; Sensitive Data of Children and Adolescents; Pediatric hospital; LGPD; Information security

Dedico este trabalho ao meu pai, Paulo Cesar Portellada, infelizmente já falecido, que desde a minha primeira infância me incentivou e trilhou comigo o caminho do conhecimento; dedico também a minha filha e esposa, bem como ao brilhante Prof. Dr. Renato José Sassi, meu orientador, que além de exemplo acadêmico sempre acreditou no meu potencial e não deixou a desistência se aproximar do projeto.

AGRADECIMENTOS

Agradeço, em primeiro lugar a minha família, que com paciência me acompanhou no trabalho desenvolvido nesta dissertação, muitas vezes em finais de semana, madrugadas e dias de comemorações.

À Universidade Nove de Julho (UNINOVE) pelo apoio incondicional que gerou esta oportunidade de crescimento, aprimoramento acadêmico e participação acadêmica, sem o apoio e sem a bolsa de estudos este trabalho não seria viável.

Aos professores e colegas de universidade que me auxiliaram de maneira direta ou indireta. Em especial, aos meus colegas de pesquisa do PPGI, João Rafael Evangelista e Dacyr Dante de Oliveira Gatto pelas dicas, pelo apoio e pelos conselhos ao longo da vida acadêmica.

Ao Prof. Renato José Sassi, que desde o começo acreditou no meu potencial, me acolheu no PPGI e me orientou durante meses para a conclusão deste trabalho, sem sua participação não haveria “**o eu**” pesquisador, agradeço também pelo apoio, suporte e conhecimento, e pela confiança, paciência, coordenação e disponibilidade.

Aos eventualmente, não relatados, o agradecimento mais sincero para a contribuição dada neste trabalho e jornada acadêmica.

“*Настоящая правда всегда неправдоподобна, вы это знали? Чтобы сделать правду более правдоподобной, мы обязательно должны добавить к ней ложь*[1]*.”*

Fiódor Mikhailovitch Dostoiévski

---

[1] A verdade verdadeira é sempre inverossímil, você sabia? Para tornar a verdade mais verossímil precisamos necessariamente adicionar-lhe a mentira

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

BPM – *Business Process Management*

BPMN - *Business Process Model and Notation*

CID - Classificação Internacional de Doenças

COBIT - Control Objectives for Information and related Technology

CPF - Cadastro de Pessoas Físicas

ECA – Estatuto da Criança e do Adolescente

GDPR - *General Data Protection Regulation*

HIPAA - *Health Insurance Portability and Accountability Act*

ICO - Information Commissioner's Office

ISO - *International Organization for Standardization*

LGPD – Lei Geral de Proteção de Dados

LIA – Relatório de Legítimo Interesse

RG - Registro Geral

RIPD – Relatório de Impacto de Proteção de Dados

ROPA – Registro de Operações de Tratamento

SUMÁRIO

1. INTRODUÇÃO

Proteção de dados é um assunto em foco no mundo moderno, visto que o acesso a dados dos indivíduos, empresas e hospitais se tornou sistemático e obrigatório, o que levou à criação de legislações sobre este tema em diversos países, (BOLLIVAR e MONACO, 2020). A proteção de dados foi gerada, então, da necessidade da manutenção da privacidade, tendo o termo significado amplo e ligado ao campo jurídico (ZEFERINO, 2020).

De acordo com Brandeis e Warren (1890) a privacidade é o direito natural do indivíduo de “ser deixado em paz”, que extravasado ao desenvolvimento tecnológico torna o direito de ter suas questões privadas, mesmo que através de dados virtuais, protegidas de ingerências alheias (ZANON, 2013). Esta relação intrínseca se deve ao fato de que enquanto a privacidade do indivíduo é o que exige que as empresas adotem medidas de proteção de dados, esta última é uma ação dever que mantém aquele direito humano (OLIVEIRA et al, 2019).

A partir desta necessidade de proteção dos dados dos indivíduos foram criadas legislações para impor essa proteção como a *US Health Insurance Portability and Accountability Act* (HIPAA) em 1996 nos Estados Unidos da América, a *General Data Protection Regulation* (GDPR) no território europeu em 2018 e a Lei Geral de Proteção de Dados (LGPD) no Brasil, por meio da Lei Federal nº 13.709/2018 (BRASIL, 2018). Tais legislações criaram diversas medidas obrigatórias para o tratamento de dados pessoais, que impôs uma alteração no funcionamento das empresas que devem deixar de focar apenas o lucro e se basear na proteção de dados (BOLLIVAR, 2020).

A LGPD entrou em vigor em 18 de setembro de 2018 e dispõe sobre tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Tratamento de Dados pessoais é definido pela LGPD como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da

informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Nota-se, pela abrangência da definição, que muitos dados coletados no dia a dia se enquadram como pessoais, e desta maneira devem ser devidamente protegidos, o que engloba medidas ativas de governança e de gestão por parte das empresas (OLIVEIRA, 2019).

Entre os dados passíveis de coleta podem-se citar *cookies*, dados de identificação, endereço, dados de registros governamentais, como o CPF e RG, dados de saúde constantes de prontuários, telefone, e-mail, fotos, receitas médicas, diagnóstico, entre outros, o que engloba grande parte dos dados tratados em uma organização (ALVES, 2021).

A LGPD define dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”, ou seja, qualquer informação que possa identificar o indivíduo. Por sua vez, dado pessoal sensível é um dado “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

Em hospitais este fato é exponencialmente aumentado, pois boa parte dos processos diários importam, quase que na totalidade, no tratamento de dados pessoais sensíveis de saúde (HAWRYLISZYN; COELHO; BARJA, 2021). Hospitais então, tornam-se ambientes com alta exposição de risco na medida que detém criticidade nos dados que controla de seus pacientes (GREGORI, 2020).

Assim, com a implementação da LGPD os processos dos hospitais brasileiros tiveram que ser totalmente revistos, ocasionando uma mudança de paradigma, de processos voltados apenas ao resultado operacional para processos voltados à observação da necessidade e à manutenção dos direitos do indivíduo. Além disso, o cuidado com a privacidade do paciente, antes vinculada apenas ao prontuário, teve que ser expandida para todo o processo hospitalar (RIVAROLLI e DAL FARRA NASPOLINI, 2023).

Em hospitais pediátricos a implementação de um programa de privacidade e proteção de dados é mais desafiadora na medida em que detêm processos diversos, seja na forma de coleta de dados, seja na regulamentação existente. Isto decorre na

medida em que em um hospital pediátrico a coleta de dados sempre envolverá dados sensíveis de crianças e adolescentes (ARAGÃO e SCHIOCCHET, 2020).

Esta dificuldade de implementação se relaciona a uma coleta dependente de consentimentos dos responsáveis das crianças e adolescentes para o uso extremo de dados sensíveis. Tal ambiente também tem participação de muitos atores, como planos de saúde, médicos, empresas de *home care,* enfermeiros, fisioterapeutas, fonoaudiólogos, prestadores de serviço e órgãos com os dados ocupando um patamar de grande importância no resultado seguro ao paciente (XIANG e CAI, 2021).

A coleta de dados de crianças e adolescentes deve ser feita com bastante cuidado diante da vulnerabilidade destes indivíduos, que estão mais sujeitos a ter seus dados utilizados indevidamente, ser vítima de *cyberbullying*, da violação da dignidade sexual, publicidade enganosa, *profiling* ou comercialização das informações destes menores (BRASIL, 1990 e VERONESE E ROSSETO, 2023).

Esta vulnerabilidade separa o cuidado necessário para dados de adultos do cuidado que deve ser dirimido na coleta de informações de crianças e adolescentes, tendo em conta ainda que, a coleta de dados sensíveis de crianças e adolescentes pode trazer patente prejuízo para estes titulares. A própria LGPD determina que o tratamento de crianças e adolescentes seja realizado apenas e tão somente em seu melhor interesse, ou seja, há uma questão subjetiva autorizadora quanto ao tratamento de dados (ANPD, 2022).

O artigo 14 da LGPD ainda identifica que este tratamento também deve observar os termos do Estatuto da Criança e Adolescente, que define os direitos e deveres das crianças e adolescentes, que deve ser observado também no programa de privacidade e proteção de dados (BRASIL, 2018).

Isto agrava o risco inerente à privacidade dos titulares envolvidos, crianças e adolescentes, que agrega criticidade ao ambiente, vez que este tratamento de dados é considerado como tratamento de alto risco pela Autoridade Nacional de Proteção de Dados em sua cartilha de orientação (ANPD, 2022).

É demonstrado que a necessidade de adequação perante a LGPD aplicada em um hospital pediátrico é proporcional à sua dificuldade, apresentando com certa frequência questões como: coleta em massa de dados sensíveis de crianças e adolescentes, incapacidade de sistemas de gestão identificarem e lidarem com dados

pessoais e processos construídos com um viés assistencial e não com viés de proteção de dados (HAWRYLISZYN; COELHO e BARJA, 2021; BRASIL, 2018).

Esta dificuldade de implementação de um programa de privacidade e proteção de dados em um hospital pediátrico também se deve à características próprias do ambiente hospitalar como, postos de coleta e exposição de prontuários, escaninhos e suportes de parede e a falta de preparo dos hospitais para a implementação de um programa que vai desde a deficiência de conscientização das pessoas, até o planejamento e efetivação dos investimentos necessários para as mudanças trazidas pela LGPD (HAWRYLISZYN; COELHO e BARJA, 2021; BRASIL, 2018).

Acrescenta-se que há um empecilho criado pela cultura organizacional nestas instituições de saúde para a implementação do programa de privacidade e proteção de dados, e no que tange a segurança da informação como a tendência de os colaboradores priorizarem o ganho de tempo e não segurança da informação (ARAGÃO e SCHIOCCHET, 2021).

Diante do cenário apresentado é necessário criar um programa de privacidade e proteção de dados que seja direcionado estritamente às características de um ambiente hospitalar, com atendimento voltado apenas para crianças e adolescentes, como disposto acima.

Alguns hospitais pediátricos implementaram um programa de privacidade e proteção de dados. Entretanto, estes programas não conseguiram aprofundar a implementação da LGPD, não atingindo o resultado de um ambiente protetivo aos seus titulares, seja pela dificuldade de manutenção do programa ou dificuldade de implementação dos *frameworks* existentes (HAWRYLISZYN; COELHO e BARJA, 2021; BERG, 2001 e LAPÃO, 2011). Para atendimento da LGPD estes hospitais pediátricos utilizaram comumente para esta implementação a adoção das disposições presentes na norma ISO 27701 e do *framework* Cobit (HAWRYLISZYN; COELHO e BARJA, 2021).

A ISO 27701, voltada para atingir requisitos de privacidade, e o COBIT, voltado para melhoria no gerenciamento de TI, não se adequam as necessidades destes hospitais pediátricos, na medida que não compreendem a gestão do ponto de vista do equilíbrio dos deveres assistenciais com a proteção necessária as crianças e adolescentes (BERG, 2001 e LAPÃO, 2011).

Assim se faz necessário um programa para atender as particularidades presentes no tratamento em massa de dados de crianças e adolescentes, especialmente no que compreende a necessidade de mapeamento de processos e de dados. A ausência de um mapeamento de processos faz com que haja uma baixa gestão dos processos do hospital pediátrico e um déficit na melhoria institucional, vez que a melhoria procedimental não está relacionada à mudança da estrutura, mas sim da qualidade, do resultado, e da segurança (THIOLLENT, 1997).

O mapeamento de processos é uma prática essencial ao cumprimento dos deveres impostos em um ambiente regulatório, sendo importante por conseguir dar visibilidade aos processos existentes e permitir melhoria processual posterior (AGOSTINELLI et al, 2019). Utiliza-se neste mapeamento a metodologia BPM ou *Business Process Management*, que é uma metodologia que se ampara em meios técnicos-visuais para identificar, desenhar, documentar, medir, monitorar, controlar e melhorar os processos da organização (CALAZANS; KOSLOSKI e GUIMARÃES, 2016).

Finalizado o mapeamento de processos, é necessário fazer um levantamento dos dados pessoais sensíveis coletados das crianças e adolescentes atendidos pelo hospital pediátrico. Este mapeamento de dados é essencial para a correta implementação de um programa de privacidade e proteção de dados (BRASIL, 2018).

O registro deste mapeamento de dados dos processos origina o *Record of Processing Activities* (ROPA), para registrar todos os dados pessoais coletados para cada processo, documento que constitui uma base fundamental do cumprimento da LGPD, identificando o agente de tratamento, os dados pessoais coletados, as finalidades do tratamento e o processo relacionado (BRASIL, 2018 e VEIGA, 2022).

Por fim, calcado na imposição da análise do risco trazido pela LGPD são construídos o Relatório de Impacto a Proteção de Dados Pessoais (RIPD) e o Relatório de Análise de Legítimo Interesse ou na língua inglesa *Legitimate Interests Assessment* (LIA), documentos aptos a analisar o risco dos processos mapeados e justificar a utilização da base legal do Legítimo Interesse (LGPD, 2018; BOHRER, 2020).

Este aumento de risco pode implicar na imposição de penalidade pela Autoridade Nacional de Proteção de Dados (ANPD), em uma grande chance de concretização de um vazamento de dados pessoais e na indisponibilidade do

ambiente hospitalar, com consequências assistenciais e de reputação aos pacientes, além implicações financeiras e jurídicas (PASSO, 2022).

Ademais, caso não haja a implementação de um programa de privacidade e proteção de dados, haverá o atingimento dos direitos dos próprios pacientes, crianças e adolescentes, que terão potencialmente expostos dados de saúde cujo conhecimento irrestrito prejudica o paciente. Importante também salientar que os próprios dados podem ser utilizados para outras finalidades, já que há também a coleta de farto material de identificação, o que pode levar a golpes financeiros, estelionatos e extorsões.

Diante do cenário apresentado, considera-se importantes o desenvolvimento e a implementação de um programa de privacidade e proteção de dados, baseado na aplicação do BPM para apoiar o cumprimento da Lei Geral de Proteção de Dados em hospital pediátrico.

1.1. QUESTÃO DE PESQUISA

Um hospital que não tenha um mínimo controle em seus dados, e que esteja consequentemente descumprindo a LGPD, passa a ter propensão de ser vítima de incidentes de vazamento de dados, sejam causados pelos agentes externos como criminosos virtuais ou estelionatários; sejam causados por agentes internos, tal qual funcionários mal treinados ou mal-intencionados.

Além disto, o tratamento inadequado de dados pode impactar nas metas internacionais de segurança do paciente, que consiste em identificar corretamente o paciente, uma vez que em um ambiente sem qualquer gestão de dados não é incomum a troca de identidade, que depende unicamente da conduta humana, com grande risco de falha (ZARPELON, KLEIN e BUENO, 2022).

Comumente os hospitais pediátricos se utilizam de dois *frameworks* para esta implementação: COBIT, um *framework* para desenvolver, organizar e implementar estratégias de gestão de informação e governança (HAES et al, 2020); e a norma ABNT NBR ISO/IEC 27701:2019, que trata de sistemas de gestão de segurança da informação (ABNT, 2022). Ocorre que tanto a COBIT quanto a Norma ISO não detêm de meios adequados para lidar com a propagação de dados sensíveis, ou ainda dados de crianças e adolescentes (SILVA, 2018).

Observa-se que a adequação de um hospital à LGPD não significa o cumprimento pleno da legislação e seus princípios, vez que a grande maioria dos projetos de cumprimento da LGPD acabam por não serem seguidos, ou ainda, não são corretamente desenvolvidos e geridos (BOLLIVAR, 2020).

Busca-se, então, com a finalização deste trabalho responder à seguinte questão de pesquisa: “Como desenvolver e implementar um programa de privacidade e proteção de dados baseado em *Business Process Management* para hospital pediátrico, a fim de apoiar o cumprimento da Lei Geral de Proteção de Dados?”.

1.2. OBJETIVOS GERAL E ESPECÍFICO

1.2.1. OBJETIVO GERAL

O objetivo deste trabalho foi desenvolver e implementar um programa de privacidade e proteção de dados baseado em *Business Process Management* para hospital pediátrico, a fim de apoiar o cumprimento da Lei Geral de Proteção de Dados.

1.2.2. OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são:

- Desenvolver e aplicar um questionário para validar o programa de privacidade e proteção de dados;
- Elaborar ROPA, RIPD e LIA com base no mapeamento de processos e dados para registrar e analisar os processos que tratam dados pessoais;
- Mapear os riscos de privacidade e realizar o *Assessment* de Terceiros para possibilitar que todos os parceiros cumpram a LGPD adequadamente;
- Treinar os colaboradores do hospital pediátrico para permitir que conheçam as medidas necessárias para tratamento de dados e sigam as políticas estabelecidas;
- Elaborar um Guia para apoiar a implementação do programa de privacidade e proteção de dados para tornar o programa reproduzível em outros hospitais pediátricos.

1.3. JUSTIFICATIVA DA PESQUISA

Foi encontrada na revisão da literatura realizada e que pode ser encontrada na subseção 2.5 deste trabalho, a recomendação para o desenvolvimento de um programa de privacidade e proteção de dados, voltado especificamente para um hospital pediátrico. No entanto, verificou-se que um programa deste tipo não foi desenvolvido e nem tampouco formado pelo mapeamento de processos com BPM, mapeamento de dados, ROPA, RIPD e LIA, identificando uma lacuna na literatura científica relacionada ao assunto.

As seguintes obras figuram entre as principais que recomendam o desenvolvimento do programa, Hawryliszyn, Coelho e Barja (2021), que tratam do desafio de implementar um programa de privacidade e proteção de dados em um ambiente de saúde e indica oportunidades de melhoria para a implementação de sucesso de um programa deste tipo; de Aragão e Schiocchet (2020) que analisa e elenca as dificuldades de implementação da LGPD em hospitais públicos; de Singh (2020), que analisa a implementação de um programa de proteção de dados com o desenvolvimento de metodologia própria; de Andellini et al., (2017), que demonstra o uso da metodologia BPM para a gestão de processos da área da saúde.

A recomendação também está presente nos seguintes trabalhos, Ahouanmenou, Van Looy e Poels (2023) que discutiu o risco de vazamento de dados e a necessidade de proteção dos dados presentes nestes ambientes, realizado por meio de um programa de privacidade e proteção de dados; Agostinelli et al (2019); Calazans; Kosloski e Guimarães (2016) que recomendaram o desenvolvimento e aplicação de um programa de privacidade e proteção de dados, baseado no mapeamento de processos e de dados, como alternativa frente às dificuldades apresentadas pela Norma ISO 27701 e o COBIT, quando aplicados em ambiente de hospital pediátrico e de Singh (2020) que analisou a implementação de um programa de proteção de dados com o desenvolvimento de metodologia própria.

Uma vez que se esbarra na impossibilidade de adoção de *frameworks* já existentes, o presente trabalho se justifica ao possibilitar não só a conformidade perante a lei, mas sim sua adoção, prática e cumprimento, através do desenvolvimento de um programa para implementar e manter a privacidade e a proteção de dados no ambiente de um hospital pediátrico.

Destaca-se que juntamente com a lacuna identificada na revisão da literatura, a aplicação de um questionário para dez especialistas em segurança da informação, de modo a validar o desenvolvimento e implementação do programa de privacidade e proteção de dados no hospital pediátrico, justificou e motivou a realização deste trabalho porque todos os especialistas validaram a proposta.

O desenvolvimento deste trabalho também encontrou motivação no fato do autor trabalhar como profissional de TI em entidades hospitalares em anos passados e, atualmente em um hospital pediátrico, situado na região da grande São Paulo.

Justifica-se também o desenvolvimento deste trabalho em função das possíveis contribuições:

- Para o hospital pediátrico na medida em que a implementação de um programa de privacidade e proteção de dados contribui para o aprimoramento dos processos institucionais, vez que o mapeamento de processos e o mapeamento de dados implementa uma gestão de negócio que contribui para a melhoria contínua do ambiente hospitalar, inclusive no tocante ao dever assistencial;
- Para a melhor tutela da saúde dos pacientes que, além de terem seus dados tratados de maneira protegida, respeitando seus direitos e garantias individuais, buscará a diminuição em erros advindos do tratamento equivocado de dados pessoais;
- Para a academia, a importância do desenvolvimento deste trabalho reside na criação de um modelo para implementação de um programa de privacidade e proteção de dados, que pode ser utilizado em um ambiente extremamente específico e complexo como os hospitais pediátricos;
- Um hospital pediátrico com padrão de qualidade mais rígido e com maiores controles internos importará em uma melhoria da sociedade de stakeholders que se relacionam com este hospital, bem como no atendimento adequado destas crianças e adolescentes;
- Ao final, a criação de um Guia para apoiar a implementação do programa de privacidade e proteção de dados em outros hospitais é de suma importância para possibilitar um ambiente pediátrico mais seguro, mesmo em outras organizações.

1.4. DELIMITAÇÃO DO TEMA

O tema foi delimitado para o ambiente pediátrico, sendo que este ambiente representa um desafio para a manutenção da privacidade, através da proteção de dados (HAWRYLISZYN, COELHO e BARJA, 2021).

Apesar do meio hospitalar ter muitas normas e padrões compartilhados indiscriminadamente entre todos os estabelecimentos de saúde, um hospital pediátrico traz uma especialidade, de material, insumo, dado tratado, processo e pessoal, que difere dos locais que focam seu atendimento em adultos ou ainda em um modelo misto, atendendo crianças e adultos.

Além disto, o atendimento pediátrico detém, por tratar crianças e adolescentes, riscos não existentes em outros estabelecimentos hospitalares ou ainda em empresas de outro ramo, conforme determinação da ANPD (ANPD, 2022).

Tem-se que lembrar que por força do Estatuto da Criança e Adolescente - ECA e da LGPD, o tratamento de dados de crianças e adolescentes deve observar o seu melhor interesse, o que cria questões subjetivas inexistentes em outros locais (BRASIL, 1990 e 2018).

A segunda delimitação é a legislação aplicável. Como o hospital pediátrico analisado e objeto deste trabalho encontra-se no Brasil, delimitou-se o programa ao cumprimento da LGPD (BRASIL, 2018).

Selecionou-se a Metodologia BPM pela capacidade de mapeamento de processos em uma notação rápida, padronizada, e que possibilita a gestão processual e sua subsequente melhoria (GATTO, 2019 e PILLAT et al., 2015). Além disto, este trabalho limitou-se à utilização de ROPAs, RIPD e LIAs, em vista do determinado no texto da LGPD, na melhor forma de gestão de risco, e utilizando a análise calcada nos relatórios que detém os registros dos tratamentos, seus riscos e a escolha de sua base legal (VETIS-ZAGANELLI e BINDA FILHO, 2022).

Desta forma, o presente trabalho, de acordo com as delimitações destacadas, desenvolveu e implementou um programa de privacidade e proteção de dados para atender um hospital pediátrico brasileiro, utilizando-se da metodologia BPM e dos documentos construídos no decorrer deste trabalho.

1.5 ORGANIZAÇÃO DO TRABALHO

Além deste capítulo introdutório, este trabalho está estruturado da seguinte forma:

Capítulo 2 - Fundamentação Teórica. Neste capítulo são apresentados os conceitos abordados no desenvolvimento deste trabalho: Privacidade e Proteção de Dados, Lei Geral de Proteção de Dados, Documentos de registro de tratamento de dados pessoais, Metodologia BPM, COBIT e ISO 27701:2019, Hospitais Pediátricos e Revisão de Literatura.

Capítulo 3 - Materiais e Métodos. Neste capítulo é apresentada a metodologia utilizada para desenvolvimento deste trabalho, bem como das construções do programa, com suas fases e etapas.

Capítulo 4 - Apresentação e Discussão dos Resultados. Neste capítulo são apresentados e discutidos os resultados obtidos na implementação do programa no hospital pediátrico.

Capítulo 5 – Conclusões. Neste capítulo é apresentada a conclusão deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada a fundamentação teórica sobre os temas abordados neste trabalho: Privacidade e Proteção de Dados, Lei Geral de Proteção de Dados, Documentos de Registro de Tratamento de Dados Pessoais, Metodologia BPM, COBIT e ISO 27701:2019, Hospitais Pediátricos e Revisão de Literatura.

2.1. PRIVACIDADE E PROTEÇÃO DE DADOS

Garantia do direito à privacidade é a possibilidade de o indivíduo restringir a publicidade ou não de uma determinada informação, impedindo a publicidade indevida que, caracterizada configura violação à sua integridade moral. Segundo Vasconcelos (2014), a privacidade é conceituada como sendo todas as relações da vida privada do indivíduo, ou seja, o oposto da vida pública, atingindo todas as relações sociais dos indivíduos.

Cumpre, no entanto, analisar os aspectos protegidos pelo direito à privacidade. Nesse sentido, é entendido que a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e à espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; e (j) a transmissão de informes dados ou recebidos em razão de segredo profissional (MORAES, 2014; FINKELSTEIN e FINKELSTEIN, 2019).

Segundo Leonardi (2011), a privacidade pode ser separada em quatro categorias que devem ser tuteladas: a) o direito a ser deixado só, derivado do *the right to be let alone*; b) o resguardo contra interferências alheias; c) segredo ou sigilo; e d) controle sobre informações e dados pessoais.

Para o referido autor, o direito a permanecer só consistiria na possibilidade do indivíduo ser deixado em paz, ou seja, se abster de qualquer convívio social. Já o direito de permanecer sozinho está relacionado à faculdade garantida ao indivíduo de não sofrer qualquer intervenção alheia, possibilitando a tomada de decisões sem qualquer interferência externa. Por sua vez, o segredo ou sigilo nada mais seria que

o direito do indivíduo de tornar público somente o que lhe for conveniente, devendo se resguardar o que ele entender como sigiloso (LEONARDI, 2011).

Já o controle sobre informações e dados pessoais é o direito originário da criação de legislações sobre proteção de dados, ou seja, está incutido dentro do conceito de privacidade em suas categorias, a proteção de dados pessoais, atividade autônoma, mas inerentemente vinculada a privacidade, uma não existindo sem a outra.

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão que tem como missão a gestão da proteção de dados no território brasileiro e foi criado pela Medida Provisória nº 869, de 2018, que posteriormente convertida na Lei nº 13.853, de 08 de julho de 2019, passou a funcionar efetivamente em 05 de novembro de 2020 (ANPD, 2023).

Por se tratar de uma autarquia especial a ANPD possui autonomia técnica em relação às esferas do governo, tendo como responsabilidade o zelo pela proteção dos dados pessoais, pela orientação aos envolvidos em tratamento de dados e na regulamentação e fiscalização quanto ao cumprimento da LGPD, com o destaque para as seguintes funções (ANPD, 2021):

- Elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Promover a disseminação de conhecimentos sobre as normas e as políticas públicas relacionadas à proteção de dados pessoais e às medidas de segurança;
- Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizados em descumprimento à legislação.

Além do evidente papel fiscalizatório e sancionador, também se nota que a ANPD é um importante ator no quesito de indicar padrões a serem seguidos, como se verifica dos diversos guias orientativos constantes no site da ANPD, o que é primordial

para a boa implementação de um programa de privacidade e proteção de dados (ANPD, 2023).

Cria-se então, o termo proteção de dados, que apesar de ter um significado amplo e ligado ao campo jurídico, pode ser entendido como um meio para que seja atingido o fim da proteção à própria privacidade (ZEFERINO, 2020).

Desta maneira, enquanto a Privacidade é um direito havido por todas as pessoas naturais, sendo assim um direito humano (BASTOS, 1989), a proteção de dados é o dever-ação de criar meios e definir processos técnicos, organizacionais e procedimentais para correta utilização dos dados coletados para não ferir a privacidade daquele indivíduo (BURKART, 2021).

Importante citar que, apesar de privacidade e proteção de dados serem termos com significados e origens diferentes, contando inclusive com classificações jurídicas própria, ambos se relacionam intrinsecamente vez que a necessidade manutenção da privacidade determina que as empresas adotem medidas de proteção de dados (OLIVEIRA et al, 2019).

Assim, para criar este dever de proteção de dados no Brasil, que contava com proteção parcial à privacidade (GRECO FILHO, 1986), promulgou-se a Lei Geral de Proteção de Dados Pessoais que trouxe uma importante contribuição para a operacionalização da proteção dos dados pessoais, e que foi amplamente inspirado na *General Data Protection Regulation*, a legislação de proteção de dados da União Europeia (EU, 2016).

2.1.1. LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) foi aprovada com o objetivo de instituir a proteção de dados no Brasil através da regulamentação dos dados pessoais que são tratados e coletados no país ou ainda de pessoas físicas que estejam fisicamente no país.

A lei dispõe sobre tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Dados pessoais é definido como toda e qualquer informação que esteja relacionada a pessoa natural identificada ou identificável, sendo que para determinada

parcela destes dados, nomeados como dados sensíveis, a lei prescreve um cuidado redobrado. Dados sensíveis são definidos como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Vez que a lei regulamenta o tratamento de dados pessoais, e já definido o conceito de dados pessoais, é imperioso definir a abrangência do significado de tratamento de dados. O tratamento de dados é definido como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, ou seja, todo e qualquer processo, acaso inclua ou envolva dado pessoal, será considerado um tratamento (BRASIL, 2018).

Desta forma a LGPD impõe a proteção aos dados pessoais ou dados pessoais sensíveis, permitindo que os indivíduos exerçam controle auto afirmativo em seus dados para que estes não sejam utilizados indevidamente ou ainda vazados por ausência de cuidado das organizações (COSTA, 2019).

Nota-se então pela abrangência das definições acima que muitas informações fornecidas no dia a dia se enquadram como dados pessoais, e desta maneira devem ser devidamente protegidos, o que engloba medidas ativas de governança e gestão, que são impostas pela legislação (OLIVEIRA, 2019).

Segundo a LGPD (2023), na sistemática de coleta e tratamento de dados se dá a obrigação da observância de princípios basilares e obrigatórios nos tratamentos de dados, como Finalidade, Adequação, Necessidade, Livre acesso, Qualidade, Transparência, Segurança, Prevenção, Não discriminação e Responsabilização:

> - O princípio da finalidade prevê que o tratamento somente pode ser realizado para propósitos legítimos, específicos, explícitos e informados previamente ao titular, sem possibilidade de tratamento posterior de forma incompatível com esta finalidade;
> - O princípio da adequação dita que não só o tratamento deve ter uma finalidade como ele deve ser realizado em compatibilidade com a

finalidade observada, ou seja, não poderá haver desvio de finalidade ou contexto do tratamento;

- O princípio da necessidade se limita a coleta de dados ao mínimo necessário, ou seja, há uma mudança brusca de realidade, de uma coleta indiscriminada para uma coleta de dados restritos aos intrinsecamente necessários;

- O princípio do livre acesso, que impõe às empresas a criação de um canal de acesso;

- O princípio da qualidade, que obriga a exatidão dos dados e a possibilidade do indivíduo pedir alterações neste dado;

- O princípio da transparência, que obriga a adoção de forma de comunicação clara e verdadeira, inclusive quando detectados incidentes;

- Para prevenção destes incidentes é trazido o princípio da segurança e o princípio da prevenção, que determina a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- E ao final, tem-se o princípio da não discriminação, que proíbe tratamentos discriminatórios e o princípio da responsabilização, que impõe aos agentes responsabilidade objetiva no caso de qualquer dado ao titular ou a terceiros.

2.2. DOCUMENTOS DE REGISTRO DE TRATAMENTO DE DADOS

Além de todas as imposições já tratadas, a LGPD (2018) impõe a todos os agentes controladores e operadores de dados a elaboração, manutenção e gestão de três tipos de documentos distintos: o Registro de Operações de Proteção de Dados (ROPA), o Relatório de Impacto a Proteção de Dados (RIPD) e o Relatório de Legítimo Interesse (LIA).

Registro de Operações de Tratamento de Dados Pessoais, conhecido como ROPA, de *Record of Processing Activities,* que se refere a um documento que registra todos os dados pessoais coletados para cada processo (BRASIL, 2018).

O ROPA constitui uma base fundamental da conformidade esperada na implementação de um programa de privacidade e proteção de dados, vez que contém as informações necessárias para identificar diversos fatores necessários para a correta gestão do tratamento como, agentes de tratamento, dados pessoais coletados, finalidades de tratamento e processo envolvido, servindo como base para a elaboração do plano de recomendação que permite correlacionar os dados tratados com seus respectivos titulares (VEIGA, 2022).

Apesar da LGPD não prever o conteúdo mínimo necessário para um ROPA e não haver recomendação da ANPD sobre o tema, utiliza-se, em analogia, às recomendações da Autoridade Nacional de Proteção de Dados do Reino Unido (ICO) para o conteúdo mínimo do documento que são (ICO, 2022):

- Dados de contato e informações dos agentes de tratamento e entidades envolvidas;
- As finalidades do processamento, ou seja, qual o propósito a ser atingido com o processamento de dados pessoais;
- Descrição das categorias e tipos de dados pessoais que são necessários para atingir a finalidade;
- Detalhes sobre a transferência internacional de dados e medidas de salvaguardas para a proteção dos dados pessoais;
- Prazo de retenção e demais informações relacionadas a data de expurgo ou anonimização;
- Descrição das medidas técnicas e organizacionais para a proteção de dados.

Este conteúdo é semelhante do recomendado pelo Ministério da Gestão e da Inovação em Serviços Públicos em sua definição de registro de tratamentos para órgãos públicos, sendo o mais próximo de orientação oficial quanto ao conteúdo do ROPA, apesar de não haver qualquer divergência quanto a sua aplicabilidade impositiva (BRASIL, 2018).

Adota-se então o seguinte conteúdo para o ROPA, que compreende as recomendações do ICO e do Ministério da Gestão e da Inovação em Serviços Públicos:

- Identificação do serviço e processo de negócio que trata dado pessoal;
- Identificação dos agentes de tratamento e do encarregado de proteção de dados;
- Identificação da fase do ciclo de vida do tratamento de dados pessoais registrado;
- De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados;
- Escopo e natureza dos dados pessoais envolvidos no processo registrado;
- Finalidade do tratamento de dados pessoais no processo;
- Categorização e identificação dos dados pessoais tratados;
- Frequência de tratamento dos dados pessoais e quantidade de titulares afetados;
- Categoria dos titulares envolvidos no tratamento registrado;
- Se existente compartilhamento de dados com terceiros, com identificação destes terceiros e do motivo do compartilhamento;
- Medidas de segurança aplicadas ao processo;
- Se há transferência internacional de dados, com respectivo indivíduo e forma de mitigação de risco, e;
- Informações sobre contratos que embasem o tratamento e sistemas utilizados no processo registrado.

O segundo documento, agora em forma de relatório, é o Relatório de Impacto a Proteção de Dados Pessoais (RIPD), que é o documento que analisa os tratamentos que possam gerar alto risco aos indivíduos que tiveram seus dados tratados (ANPD, 2023).

O RIPD deve ser elaborado sempre que se identificar as seguintes hipóteses:

- Nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do estado ou atividades de investigação e repressão de infrações penais;
- Quando o tratamento tiver como fundamento a hipótese de legítimo interesse;
- Para tratamentos realizados por agentes do poder público;
- Quando as operações de tratamento envolverem dados pessoais sensíveis e;
- Quando envolverem tratamento de dados de alto risco.

Neste caso são definidos como tratamento de dados de alto risco:

- Tratamento de dados pessoais em larga escala;
- Tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
- Tratamento com uso de tecnologias emergentes ou inovadoras;
- Tratamento que use vigilância ou controle de zonas acessíveis ao público;
- Tratamento que tenha decisões tomadas unicamente com base em tratamento automatizado, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito, ou os aspectos da personalidade do titular, ou;
- Tratamento com utilização de dados pessoais de crianças, de adolescentes e de idosos.

O RIPD deve conter no mínimo a descrição dos tipos de dados pessoais coletados ou tratados, a metodologia usada para o tratamento e para a manutenção da segurança dos dados, a análise do controlador quanto as medidas, salvaguardas e mecanismos de mitigação de riscos adotados devendo ser suficientemente detalhados para uma correta compreensão do tratamento e seus riscos (ANPD, 2023).

O terceiro documento é o Relatório de Análise de Legítimo Interesse (LIA), de *Legitimate Interests Assessment*, que é um teste que deve ser realizado sempre que o controlador e/ou terceiro optar por justificar ou entender aplicável a utilização da base legal do legítimo interesse (BOHRER, 2020).

A base legal do legítimo interesse, prevista na LGPD, é uma hipótese legal que autoriza o tratamento de dados quando houver interesses legítimos do tratamento, desde que não haja conflito com os direitos e liberdades fundamentais da pessoa que teve os dados coletados. Esta base legal exige, como forma de averiguar se não há o conflito com os direitos do titular, a elaboração de um relatório de legítimo interesse (ANPD, 2024).

O relatório de legitimo interesse, LIA, é realizado com a finalidade de testar a viabilidade da opção da base legal do legítimo interesse e, através deste relatório, analisar se o legítimo interesse é a base legal adequada, se a situação está concreta, se houve a minimização dos dados, e por fim, se não há uma sobreposição de interesses entre o controlador e o titular (BOHRER, 2020).

Um exemplo prático da realização de um relatório de legitimo interesse é a hipótese de envio de comunicados eletrônicos para pacientes de um hospital, onde se deve responder os questionamentos do relatório presente no Apêndice A deste trabalho, de modo a concluir, ao final, a licitude ou não deste tratamento (ANPD, 2024).

2.3. METODOLOGIA *BUSINESS PROCESS MANAGEMENT*

Dentro do ambiente hospitalar, os *framework*s mais utilizados para implementar um programa de privacidade e proteção de dados e, de maneira subsequente, aprimorar a segurança da informação do ambiente, são COBIT (*Control Objectives for Information and Related Technologies*) e a Norma ABNT NBR ISO/IEC 27701:2019.

COBIT é um *framework* utilizado por empresas e departamentos de TI para desenvolver, organizar e implementar estratégias de gestão de informação e governança, tendo sua versão mais recente lançada em 2019 (HAES et al, 2020).

Dentre os objetivos do COBIT tem-se uma prevalência para o foco em governança, com uma inclusão recente de um objetivo direcionado para privacidade e proteção de dados em seu sistema de governança aplicáveis ao objetivo de governança/gestão, tendo um viés de melhoria processual e restrição de tratamento de dados sensíveis (SINGH, 2020).

Apesar da recente atualização o COBIT ainda não é totalmente aplicável aos hospitais pediátricos, ante a ausência de aplicabilidade plena e a deficiência de regulação no tocante aos dados de saúde de crianças e adolescentes.

Por sua vez a Norma ABNT NBR ISO/IEC 27701:2019, anteriormente conhecida como ISO 27552, é uma extensão da norma ABNT ISO 27701 que trata de sistemas de gestão de segurança da informação, e veio complementar o sistema de segurança da informação com definições de privacidade e proteção de dados (ABNT, 2022).

O objetivo da nova norma foi aprimorar o sistema de gerenciamento de segurança da informação ao trazer requisitos adicionais para a manutenção de um sistema de gerenciamento de informações de privacidade e se caracteriza como uma extensão certificável, tanto por parte dos profissionais quanto por parte das empresas (ISO, 2019).

A norma ISO tem um enfoque maior na segurança da informação e preferência para exclusão dos tratamentos de dados de crianças e adolescentes, especialmente quando considerados de alto risco, como é o caso de tratamento em massa ou de dados sensíveis (SILVA, 2018).

Para empresas que não prestem serviços hospitalares, ou com coleta de dados majoritariamente voltados a crianças e adolescente, ambos os *frameworks* são bons modelos para a adequação de uma empresa à LGPD.

No entanto, tanto COBIT quanto a Norma ISO não detêm meios adequados para lidar com a propagação de dados sensíveis ou ainda dados de crianças e adolescentes, o que é rotineiro em empresas da saúde, como hospitais (SILVA, 2018), sendo necessária criação de modelo específico para estas organizações.

Business Process Management (BPM) é uma metodologia que auxilia a organização estrategicamente a gerir seu empreendimento, vez que é focada a identificar, desenhar, documentar, medir, monitorar, controlar e melhorar os processos da organização compreendendo também os meios estratégicos pretendidos (AGOSTINELLI et al, 2019)

É uma metodologia de gestão de processos que se utiliza de meios técnicos e visuais para mapeamento e gestão dos processos e, a partir deste momento, com a visibilidade adquirida, é feito uma correta análise tática e estratégica do respectivo processo.

Há diversas vantagens na adoção desta metodologia, como por exemplo, a maior assertividade na gestão e a melhor definição e coordenação das atividades mapeadas e definidas, com potencial melhoria nos resultados advindos destes processos (JÄNTTI e CATER-STEEL, 2017 e PILLAT et al, 2015).

Os benefícios para as organizações são: melhorar o desempenho do negócio através do seu entendimento; simular novas formas para atender o negócio; apoiar a organização em relação às oscilações do mercado; maior controle da duração dos processos e a representação visual dos processos e dos elementos que o compõem (PILLAT et al, 2015 e GATTO, 2020).

Para correto mapeamento dos processos foi criado, pela *Business Process Management Initiative* (BPMI), organização sem fins lucrativos e que tem a finalidade de padronizar as questões de processos de negócio, a *Business Process Management Notation* (BPMN), para uma notação rápida e padronizada de modo a dar visibilidade e gestão a estes processos (PILLAT et al., 2015).

Esta notação tem quatro categorias distintas: objetos de fluxo, que são os eventos, atividades e *gateways*; os objetos de conexão, que são o fluxo de mensagens ou de sequência e a associação entre objetos; as raias ou *swimlanes,* que auxiliam na organização das atividades, com cada uma representando um participante, *lane* ou uma subdivisão; e por fim, os artefatos que são objetos que fornecem informações sobre as atividades que necessitam ser executadas, como dados, anotações e grupos (ABPMP, 2018).

Apresenta-se na Figura 1 todos os objetos do fluxo do BPMN.

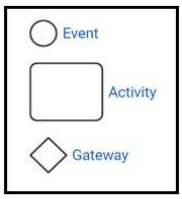


Figura 1 – Objetos de fluxo do BPMN
Fonte: Adaptado de ABPMP (2018)

A Figura 1 apresenta os objetos utilizados na metodologia BPMN, sendo eles: o evento, representado por um círculo; uma atividade, representado por um retângulo; e um ponto de decisão ou *gateway*, representado por um losango.

A Figura 2 exemplifica todos os objetos de conexão.

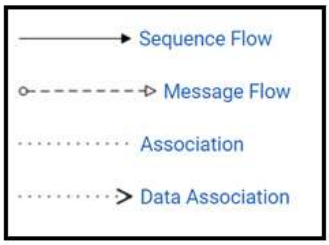


Figura 2 – Objetos de conexão do BPMN
Fonte: Adaptado de ABPMP (2018)

A Figura 2 apresenta os objetos de ligação entre eventos dentro do fluxo de notação da metodologia BPMN. Estes objetos identificam as seguintes conexões: sequencial, oriundo de mensagens, associação e associação entre dados.

A Figura 3 exemplifica as raias ou *swimlanes* do BPMN.

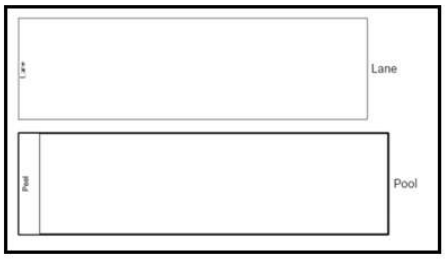


Figura 3 – Raias ou *Swimlanes* do BPMN
Fonte: Adaptado de ABPMP (2018)

A Figura 3 apresenta as *lanes* ou raias onde o fluxo processual é anotado, cada qual representando um indivíduo ou área responsável pela etapa processual. Os objetos de ligação apresentados na Figura dois são responsáveis por ligar as raias.

E por fim, a Figura 4 demonstra os artefatos encontrados na notação.

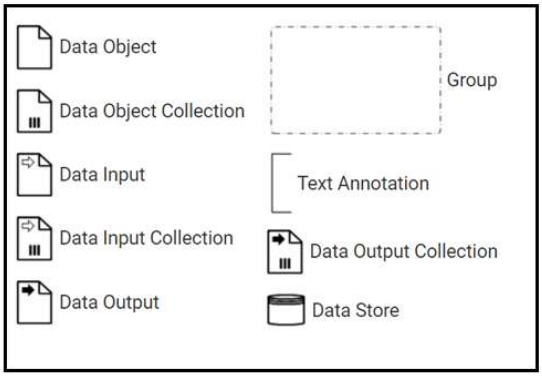


Figura 4 – Artefatos do BPMN
Fonte: Adaptado de ABPMP (2018)

A Figura 4 apresenta os artefatos que são cabíveis de utilização dentro da notação de processo através do BPM. Eles representação questões de data, *input* e *output*, e notações.

Importante citar que o BPM é uma ferramenta para a implementação, e criação de um programa, de privacidade e proteção dos dados, uma vez que dá a visibilidade aos dados trafegados nos tratamentos realizados, e dentro do ROPA, se constitui como poderosa ferramenta para a adequação (AGOSTINELLI et al, 2019).

Em hospitais a adoção da metodologia BPM pode reduzir custos, melhorar a integração da informação, sua segurança e a qualidade de seu uso, com subsequente melhora da qualidade do atendimento ao paciente deste hospital e do trabalho desenvolvido pelos profissionais de saúde (FERREIRA, et al., 2018).

Esta melhoria é decorrente do levantamento profundo dos dados pessoais sensíveis verificados quando do mapeamento de dados utilizando o BPMN e demonstra que a construção de um programa que utiliza mapeamento de dados se beneficia do uso desta metodologia (BERG, 2001).

A utilização de BPM, no mapeamento de processos, é recomendada pela Agência Nacional de Proteção de Dados como forma de construção de boa governança de processos que tratam dados pessoais (ANPD, 2024), havendo comprovação do benefício de incorporar a BPMN no mapeamento de processos (LAPÃO, 2011 e ANDELLINI et al, 2017).

Uma organização hospitalar também se beneficia da implementação do BPM em um mapeamento de processos e em um programa de privacidade e proteção de dados, dando ganho substancial ao programa implementado (SINGH, 2020).

2.4. HOSPITAL PEDIÁTRICO

Historicamente os hospitais não tendem a ser um local feliz para crianças e adolescentes, cumulado com a situação patológica na qual eles se encontram, o próprio ambiente hospitalar sóbrio e destinado a eficiência clínica das condutas, e não na felicidade do paciente, tornava estes estabelecimentos locais temíveis pelos menores, especialmente crianças (SHIELD et al., 2007).

Até o início da década de 1950 acreditava-se que a visita dos pais inibia a cura das crianças e adolescentes (NETHERCOTT, 1993). Passado este período, entendeu-se que as crianças nestes ambientes passariam a sofrer um trauma emocional que poderia trazer consequências na vida adulta (BOWLBY, 1998).

Este processo de revisão sistemática da qualidade do cuidado assistencial, levou a pediatria a afastar a abordagem tradicional que intencionava tratar as crianças e adolescentes como “pequenos adultos”, para uma abordagem centrada na família e voltado ao envolvimento desta última na totalidade de aspectos do cuidado (PALMER, 1993).

Neste novo ambiente a família é reconhecida como especialista no cuidado de seu filho, sendo criado um ambiente onde não há preocupação apenas com a recuperação fisiológica do paciente, mas também com seu bem-estar psicológico (SHIELD et al, 2007).

Como exemplo, cita-se a criação em 1992 do *Institute for Family Centered Care,* estabelecido nos EUA assumindo o papel da anterior *Association for the Care of Children's Health*, cuja tarefa era desenvolver um programa nacional para implementar uma abordagem centrada na família para o cuidado de bebês, crianças e adolescentes. (SHIELD et al., 2007).

Este formato de hospital pediátrico, ou *Children 's Hospital,* acabou por se expandir para o território nacional com a criação de hospitais que focam o seu atendimento exclusivamente em crianças e adolescentes voltados à uma assistência completa para estes indivíduos.

Em um hospital pediátrico os processos assistenciais importam, quase que na totalidade, ao tratamento de dados pessoais, porque se limitam a coleta de dados previstos na LGPD, sendo que em sua maioria são dados sensíveis (HAWRYLISZYN, COELHO e BARJA, 2021).

Estes tratamentos de dados estão vinculados a atividade assistencial eletiva, consultas, procedimentos de urgência e emergência e unidades de internação, sejam convencionais ou de tratamento intensivo, coletando nestes procedimentos diversos dados confidenciais e sensíveis que impõe cuidado.

Como citado, esta criticidade e confidencialidade faz com que hospitais pediátricos se tornem ponto de preocupação no ambiente de proteção de dados, criado no Brasil pela promulgação da LGPD, o que torna urgente que estes

estabelecimentos implementem um programa de cumprimento da LGPD e que o apliquem corretamente, havendo uma correta gestão dos dados de seus pacientes (GREGORI, 2020).

Diante desta urgência, os processos dos hospitais pediátricos brasileiros tiveram que ser totalmente revistos, vez que, com a vigência da LGPD houve uma necessidade de mudança de paradigma, que passou a englobar a proteção de dados e a segurança da informação (KÓS, 2021).

Além disso, o cuidado com a privacidade do paciente, antes vinculada apenas ao prontuário, teve que ser expandida para todo o processo hospitalar não havendo, a priori, uma adequação completa dos *frameworks* existentes para correta implementação e gestão de um programa de privacidade e proteção de dados em hospitais pediátricos (RIVAROLLI e DAL FARRA NASPOLINI, 2023).

2.5. REVISÃO DA LITERATURA

A Revisão da Literatura iniciou-se com a definição dos temas centrais da pesquisa: Privacidade e Proteção de Dados; Dados Sensíveis de Crianças e Adolescentes; Hospital Pediátrico; LGPD; Segurança da Informação.

Posto o alcance de publicações em periódicos internacionais, a pesquisa também ocorreu com a versão dos temas centrais na língua inglesa: *Privacy and Data Protection; Sensitive Data of Children and Adolescents; Pediatric hospital; LGPD; Information security.*

A busca nas bases de dados selecionadas foi realizada da seguinte forma:

- Termos pesquisados isoladamente para observar as publicações sobre este tema;
- Termos pesquisados em pares, para verificar a correlação entre os temas como, por exemplo, hospital pediátrico somado à LGPD, e;
- Todos os termos pesquisados em conjunto, para verificar a existência de obras que abordam os temas aplicados de forma conjunta.

Seguem as *strings* utilizadas, utilizadas em português e inglês:

a) Termos isolados – “Privacidade e Proteção de Dados”, “Dados Sensíveis de Crianças e Adolescentes”, “Hospital Pediátrico”, “LGPD” e “Segurança da Informação”;

b) Termos em pares - “Privacidade e Proteção de Dados” e “Dados Sensíveis de Crianças e Adolescentes”, “Privacidade e Proteção de Dados” e “Hospital Pediátrico”, “Privacidade e Proteção de Dados” e “LGPD”, “Privacidade e Proteção de Dados” e “Segurança da Informação”, “Dados Sensíveis de Crianças e Adolescentes” e “Hospital Pediátrico”, “Dados Sensíveis de Crianças e Adolescentes” e “LGPD, “Dados Sensíveis de Crianças e Adolescentes” e “Segurança da Informação”, “Hospital Pediátrico” e “LGPD”, “Hospital Pediátrico” e “Segurança da Informação”, “LGPD” e “Segurança da Informação”.
c) Termos em conjuntos – “Privacidade e Proteção de Dados” e “Dados Sensíveis de Crianças e Adolescentes” e “Hospital Pediátrico”, “LGPD” e “Segurança da Informação”.

Entre estes temas, o termo Segurança da Informação foi incluído na pesquisa, devido a derivação da Proteção de Dados em temas desta área, no caso de implementação de um programa de privacidade e proteção de dados.

A revisão da literatura foi realizada nas seguintes bases de dados eletrônicos: IEEExplore, PuBMed, Scielo, Scopus e Science Direct, sendo definidos os seguintes critérios de inclusão:

- Ser artigo publicado nas bases relacionadas acima;
- Abordar o tema do trabalho, e;
- Ter sido publicado no período entre 2018 e 2024.

O período temporal acima citado se justifica uma vez que a criação do dever de proteção de dados no Brasil se deu em 2018, data esta que é igual ou anterior a outros marcos legislativos internacionais, como a GDPR, aprovada em 2018, ou a Lei de Privacidade do Consumidor do estado da Califórnia/USA - CCPA, aprovada em 2020.

Por sua vez a escolha destas bases se justificam na medida em que, se por um lado o PuBMed é o repositório mais usado na área da saúde, as bases IEEExplore, Scielo, Scopus e Science Direct são referência quando relacionados a pesquisas vinculadas a tecnologia.

A revisão da literatura foi realizada entre o período do mês de janeiro de 2018, por conta da data inicial do ano de aprovação da LGPD até o mês de abril de 2024, por meio de acesso direto às bases informadas acima e com a leitura dos artigos encontrados. Após a leitura, foram objeto de exclusão os artigos em duplicidade e os que não tinham relação com os temas centrais.

Na revisão da literatura foram encontrados 133 artigos, descartados 17 que estavam duplicados e 49 que não tratavam dos temas da pesquisa. Foram, então, selecionados ao final 67 artigos como verifica-se no Quadro 1.

Base de Dados Pesquisada	Número de Artigos
IEEE Xplore	18
Pubmed	20
Scielo	4
Scopus	9
ScienceDirect	16
Total	67

Quadro 1 – Artigos selecionados

Fonte: O Autor.

Em seguida, realizou-se a análise temporal para identificar o ano das publicações. Os resultados estão apresentados no Quadro 2.

Análise Temporal		
Ano	**Quantidade**	**Percentual**
2018	9	13,43%
2019	12	17,91%
2020	9	13,43%
2021	15	22,39%
2022	7	10,45%
2023	8	11,94%
2024	7	10,45%
Total	67	100,00%

Quadro 2 – Análise temporal para identificar o ano das publicações.

Fonte: O Autor.

Com base nos resultados dos Quadros 1 e 2, nota-se que a maioria das publicações estão concentradas nas bases IEEE, PubMed e Science Direct, sendo a

maioria dos trabalhos publicados em 2021, ou seja, cerca de 3 anos após a aprovação da LGPD, incluindo as novas determinações.

A seguir foi aplicada uma rede de conexão para mapear a correlação dos temas centrais à esta pesquisa seguindo as respectivas etapas:

- Reunir todos os artigos em uma pasta física no *hardware* utilizado;
- Acessar o software Mendeley (2023) e carregar todo o conteúdo;
- Exportar a totalidade das referências no formato .ris;
- Importar o arquivo RIS para o software VosViewer (2023), e;
- Gerar o mapa definindo como alvo as palavras-chave e a ocorrência como “1”.

A Figura 5 apresenta o resultado da rede de conexão, tendo como nodos centrais as palavras *cybersecurity, privacy e data protection*, com interligações com o tema *health*.

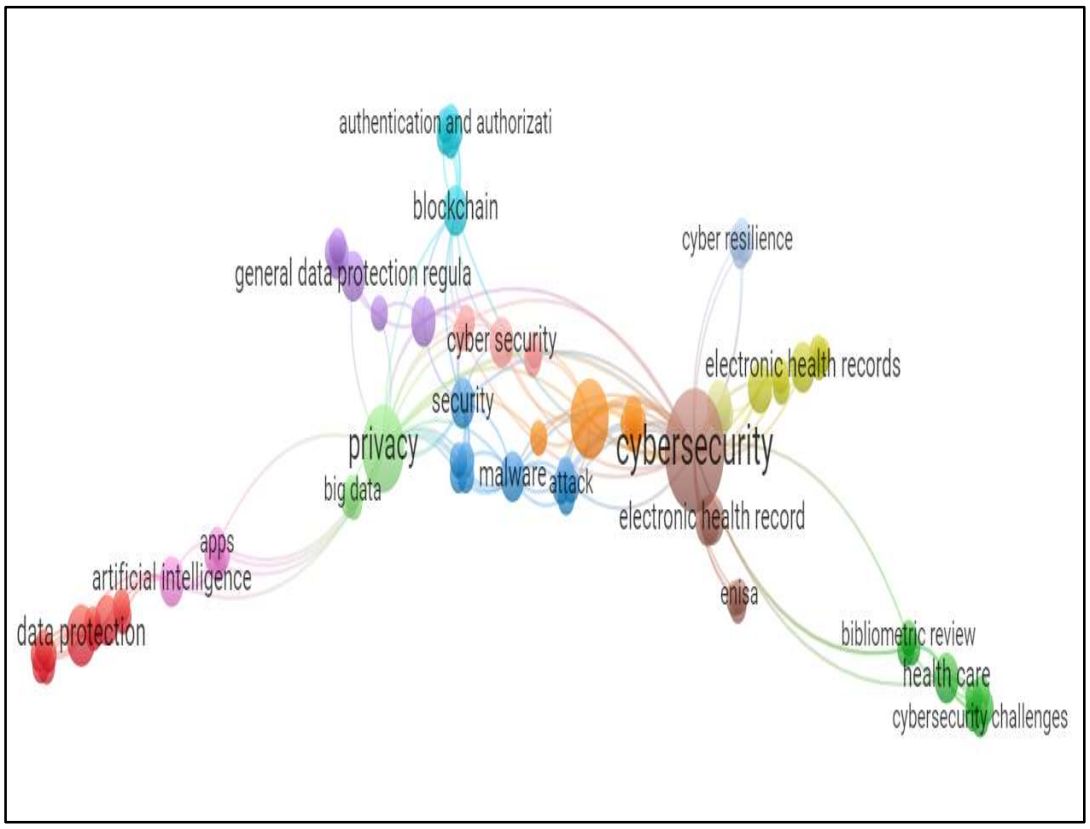


Figura 5 – Resultado da rede de conexão de palavras.

Fonte: Autor.

A Figura 5 apresenta como estão divididos os temas abordados nos artigos selecionados. Os nodos demonstram os pontos de concentração dos assuntos enquanto as linhas demonstram as conexões entre cada um dos nodos.

Os trabalhos abordaram dois pontos principais que se inter-relacionam com 5 pontos teóricos. Tem-se que os trabalhos flutuam, em grande medida, pelos termos privacidade e cyber segurança, sendo tais pontos relacionados com prontuários eletrônicos, proteção de dados, cuidado assistencial, inteligência artificial e legislações de proteção de dados.

Esta distribuição demonstra que a literatura está inclinada a tratar os temas relacionados à proteção de dados e privacidade como tendo relação estrita ao tema segurança da informação e o risco existente no armazenamento de dados de prontuários eletrônicos e nos processos hospitalares, como se denota dos termos *Cybersecurity, Data Protection, GDPR, e Health Care* encontrados na figura 5 e 6.

Por sua vez, a Figura 6 representa a mesma visualização, mas agora associando os temas centrais com a data de publicação, de modo que além de vincular os nodos de concentração, os relacionam com a data de publicação do artigo.

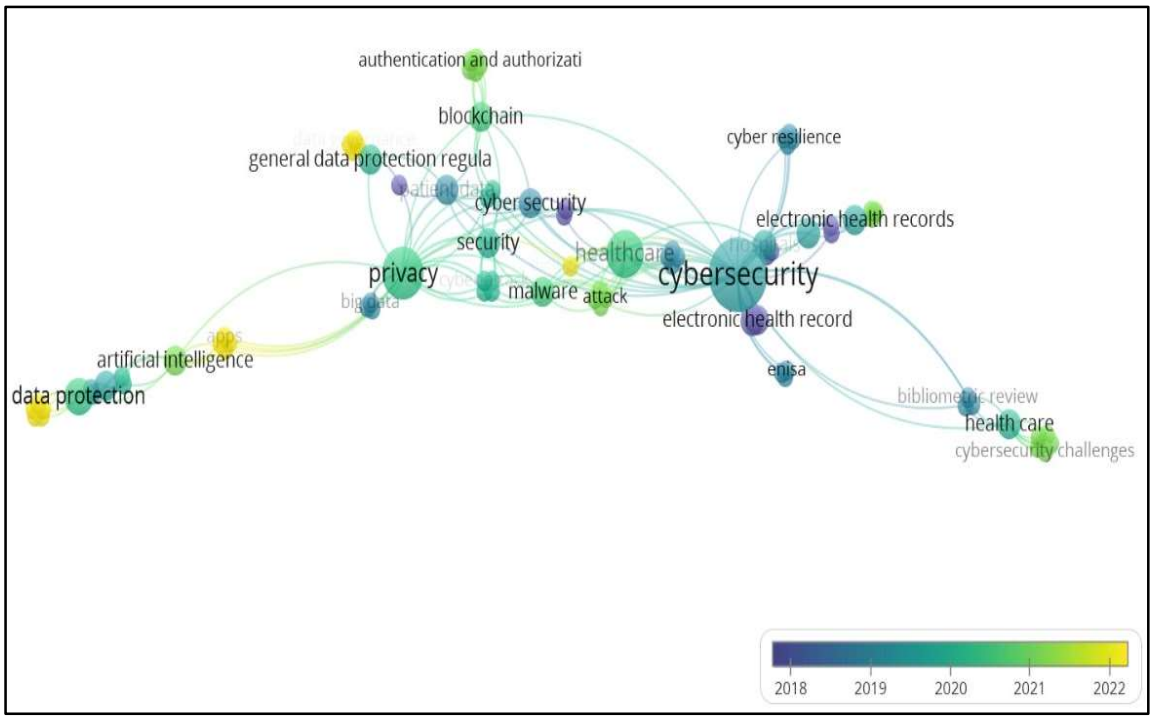


Figura 6 – Resultado da rede de conexão, associando termo e data de publicação.

Fonte: Autor.

A Figura 6 demonstra que, quando da aprovação da LGPD as publicações estavam flutuando em pontos relacionados à segurança da informação de forma clássica e com uma publicação ainda muito incipiente sobre a lei editada, ante a lei ter sido promulgada apenas no segundo semestre de 2018.

Com o avanço da série temporal é notado que as discussões passam a abordar o conceito de privacidade, o dever assistencial e as questões técnicas para cumprimento da lei, tendo em última instância a migração dos trabalhos para o tema de inteligência artificial e riscos cibernéticos.

Apresenta-se no Quadro 3 a relação das 21 obras que mais contribuíram para o desenvolvimento da pesquisa.

NÚMERO	PUBLICAÇÃO	RESUMO E CONTRIBUIÇÃO PARA ESTE TRABALHO
1	ABHISHEK, P. P., NEELIKA C., **A review into the evolution of HIPAA in response to evolving technological environments**, Journal of Journal of Cybersecurity and Information Management, v. 4, n. 2, p. 05-15, 2020. Doi: 10.54216/JCIM.040201)	Analisa a linha temporal da privacidade no ambiente hospitalar através da lei *Health Insurance Portability and Accountability* (HIPAA), explica os desafios enfrentados na implementação da política e dá uma visão dos direitos e responsabilidades de cada parte interessada envolvida, demonstrando a necessidade de adequação. Contribuiu para definir as responsabilidades de cada um dos atores do meio hospitalar, bem como as adequações normalmente encontradas em ambientes clínicos.
2	AGOSTINELLI, S., MAGGI, F; MARELLA, A; SAPIO, F., **Achieving GDPR compliance of BPMN process models.** In International Conference on Advanced Information Systems Engineering. Springer, p. 10–22, 2019.	Recomenda a aplicação do BPM para cumprimento de legislação de privacidade e proteção de dados, auxiliando a organização para gerir seu empreendimento. Contribuiu para a realização dos mapeamentos utilizando o BPM.
3	AHOUANMENOU, S., VAN LOOY, A., POELS, G., **Information security and privacy in hospitals: a literature mapping and review of research gaps.** Inform Health Soc Care. v. 48, n. 01, p. 30-46. 2023. Doi: 10.1080/17538157.2022.2049274.	Analisa a literatura para demonstrar o risco cibernético de hospitais e conclui pela necessidade de proteção dos dados presentes nestes ambientes. Contribuiu para o correto endereçamento das lacunas encontradas no ambiente hospitalar.

4	ÁLVAREZ DÍAZ, J. A.; DURO, E. A.; GUBERT I. C., **Between Huxley and Orwell: Big Data and Health**. Revista Latina de Sociologia. v. 8, n. 2, p. 23-33, 2018. Doi: 10.17979/relaso.2018.8.2.2951.	Aborda a dicotomia entre privacidade e evolução tecnológica no aspecto da saúde, evidenciando as necessidades específicas da área hospitalar. Contribuiu para uma análise completa das necessidades de proteção de dados em hospitais pediátricos e entendimento de seus processos.
5	ANDELLINI, M.; FERNANDEZ RIESGO, S.; MOROLLI, F; RITROVATO, M.; COSOLI, P.; PETRUZZELLIS, S.; ROSSO, N. **Experimental application of Business Process Management technology to manage clinical pathways: a pediatric kidney transplantation follow up case**. BMC Med Inform Decis Mak v. 17, n.1 p. 151-160. 2017. Doi: 10.1186/s12911-017-0546-x -	Demonstrou o uso da metodologia BPM para a gestão de processos na área da saúde. Contribuiu para o mapeamento ser realizado com BPM e apoiou a construção de metodologia própria de documentos para absorção dos aspectos do gerenciamento de TI.
6	ANPD - Autoridade Nacional de Proteção de Dados. **RESOLUÇÃO CD/ANPD Nº 8 - Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD)**. 2024.	Indica a metodologia BPM para o mapeamento de processos com a finalidade de construção de um programa de privacidade e proteção de dados aderente a LGPD. Contribuiu para a realização dos mapeamentos utilizando o BPM.
7	ARAGÃO, S., & SCHIOCCHET, T., **Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde**. Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, v. 14, n. 3, p. 692-708, 2020. Doi: 10.29397/reciis.v14i3.2012	Analisa o impacto da LGPD para o Sistema Único de Saúde e conclui pela necessidade da tomada de medidas para proteção de dados nestes ambientes. Contribuiu para a análise do ambiente hospitalar realizado no trabalho.
8	BERG, M. **Implementing information systems in Healthcare organizations: Myths and challenges**. International Journal of Medical Informatics, v. 64, n. 2, p. 145-156, 2001. Doi: 10.1016/s1386-5056(01)00200-3.	Analisa a implementação de ativos de TI em organizações de saúde e identifica os maiores desafios destes estabelecimentos. Relata que os *frameworks* ISO e COBIT não são os mais adequados para ambientes hospitalares, por haver características não usuais nestes tipos de estabelecimentos. Contribuiu para identificar que alguns *frameworks* não estão de acordo com o ambiente de um hospital pediátrico.

9	BOLIVAR, ANALLUZA ; MONACO, G. F. C. (Org.) **. LGPD NA SAÚDE**. 1. ed. São Paulo: Revista dos Tribunais, v. 1. 431p, 2020.	Discorre sobre a LGPD na área da saúde, sua aplicabilidade, dificuldades encontradas, direitos dos titulares. Contribuiu com o planejamento e criação do programa, ante o discorrido pelo autor.
10	CALAZANS, A., KOSLOSKI, R., e GUIMARAES, F. **Proposta de modelo de medições para contratação do gerenciamento de processo de negócio (*Business Process Management* - BPM).** Journal of Information Systems and Technology Management. n. 13, p. 275-300. 2016. Doi: 10.4301/S1807-17752016000200007.	Indica a metodologia BPM para gerenciamento de processos. Contribuiu com a indicação metodológica acerca da utilização do BPM.
11	COVENTRY, L., BRANLEY, B., **Cybersecurity in healthcare: A narrative review of trends, threats and ways forward**. Maturitas, v. 113, n. 1 P. 48-52. 2018. Doi: 10.1016/j.maturitas.2018.04.008.	Analisa a questão da cibersegurança em ambientes voltados à prestação de serviços de saúde. Contribuiu para o desenvolvimento do trabalho na adoção de uma visão holística da segurança da informação e da contribuição desta para o programa.
12	GREGORI, M. S., **Os Impactos da Lei Geral de Proteção de Dados Pessoais na Saúde Suplementar**. Revista de Direito do Consumidor, São Paulo, v. 127, p. 171-196, 2020. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1268/1189. Acesso em: 23 maio. 2023 às 11:18.	Versa sobre o impacto ás organizações de saúde da aprovação da LGPD. Contribuiu para análise das dificuldades de implementação de um programa de privacidade e proteção de dados nesta entidade.
13	HAWRYLISZYN, L. O., COELHO, N. G. S. C., & BARJA, P. R., **Lei geral de proteção de dados (LGPD): o desafio de sua implantação para a saúde**. Revista Univap, v. 27, n. 54, 2021. Doi: 10.18066/revistaunivap.v27i54.2589.	Discorre sobre a LGPD, suas obrigações e os desafios para organizações de saúde na implementação de programas de proteção de dados. Contribuiu para o trabalho na medida que indicou as necessidades para estes hospitais e dirimiu a melhor forma de abordagem para estes desafios.

14	LAPÃO, L., **Organizational Challenges and Barriers to Implementing IT Governance in a Hospital.** Electronic Journal of Information Systems Evaluation. v. 14, n. 1, p. 37-45, 2011.	Identifica e registra os desafios para implementação de um programa de governança de TI em um hospital. Conclui que a utilização do ISO e COBIT contém barreiras que prejudicam sua utilização em hospitais. Contribuiu para identificar as fragilidades da utilização de *frameworks* para entidades hospitalares e para indicar meio possível de formação de um programa de governança.
15	OLIVEIRA, A. P. de. et al. **A lei geral de proteção de dados brasileira na prática empresarial.** Revista Jurídica da Escola Superior de Advocacia da OAB-PR, Curitiba, v. 4, n. 1, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wpcontent/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 24 jan. 2023, às 18:37.	Trata sobre a aplicação da LGPD no mundo empresarial. Contribuiu para a análise realizada no Hospital, a fim de determinar os pontos necessários de adequação, para o correto cumprimento da LGPD.
16	PELOQUIN, D., DIMAIO, M., BIERER, B., **Disruptive and avoidable: GDPR challenges to secondary research uses of data**. Eur J Hum Genet. v. 28, n. 01, p. 697–705, 2020. Doi:10.1038/s41431-020-0596-x	Analisa as dificuldades trazidas pela GDPR para a pesquisa clínica e atividades assistenciais de pesquisa e propõe a possibilidade de construção de uma solução para atendimento da legislação e a manutenção da atividade de pesquisa. Contribuiu ao discutir a necessidade de um novo *framework* adequado para o ambiente hospitalar, em especial na existência de legislação de proteção de dados.
17	RIVAROLLI, M. A.; DAL FARRA NASPOLINI, S. H. **Privacidade e proteção de dados em nosocômios e clínicas perante a LGPD**. Scientia Iuris, [S. l.], v. 27, n. 1, p. 112–128, 2023. Doi: 10.5433/2178-8189.2023v27n1p112-128.	Analisa o tema em clínicas de saúde cotejando as obrigações legais trazidas pela LGPD e os processos destas organizações. Contribuiu para elaboração do programa.

18	SINGH, D. A. D. S. **Data privacy compliance using COBIT 2019 and development of MISAM audit caselet**, 2020. Dissertação de Mestrado – Concordia University of Edmonton.	Analisa a implementação de um programa de proteção de dados utilizando o *framework* COBIT e desenvolve metodologia própria. Demonstra que apesar de ser possível a implementação de um programa de proteção e dados via COBIT, há fragilidades do *framework* quando em determinados ambientes. Contribuiu para identificar que este *framework* não era o mais adequado para certas áreas como em estabelecimentos de saúde.
19	VERONESE, J. R. P.; ROSSETO, G. M. de F. **O quadrilena da exclusão, inclusão, superexplorações e proteção de dados pessoais de crianças e adolescentes na perspectiva da fraternidade.** Sequência Estudos Jurídicos e Políticos, [S. l.], v. 43, n. 92, p. 1–29, 2023. Doi: 10.5007/2177-7055.2022.e92875.	Discorre sobre a proteção de dados de crianças e adolescentes. Contribuiu na criação e análise do programa voltado a coleta de dados de crianças e adolescentes.
20	XIANG D,; Cai W. **Privacy Protection and Secondary Use of Health Data: Strategies and Methods**. BioMed research international. v. 21, n. 1, p. 01-11, 2021 Doi: 10.1155/2021/6967166.	Versa sobre a proteção de dados para manutenção da privacidade e seu uso em ambientes relacionados a saúde. Contribuiu para a criação do Programa de privacidade e proteção de dados.
21	ZEMMOUDJ, S., BERMAD, N., OMAR, M., **CAPM: Context-Aware Privacy Model for IoT-Based Smart Hospitals,** 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, v. 15, p. 1139-1144, 2019. Doi: 10.1109/IWCMC.2019.8766630.	Propõe um Modelo de Privacidade Consciente do Contexto (CAPM) visando proteger as informações do paciente trocadas e compartilhadas durante sua internação. Contribuiu com sugestão de controles e metodologias para a construção das metodologias próprias desenvolvidas neste trabalho.

Quadro 3 – Relação de Artigos que mais contribuíram para este trabalho.

Fonte: O Autor.

Analisando o Quadro 3 foi possível constatar que a proteção de dados é um tema importante para os hospitais pediátricos, e que os *frameworks* ISO e COBIT não são os mais adequados para implementação de um programa de proteção de dados em hospitais, e que a implementação de um programa passa pela utilização da BPM.

Destaca-se também que, apesar da recomendação da criação de um programa para suplantar as deficiências da ISO 27701 e do COBIT, não foi encontrado trabalho que apresentasse um programa desenvolvido com base no BPM e que trouxesse metodologia para resolução das particularidades de hospitais pediátricos.

Esta dificuldade de implementação se deve a características próprias do ambiente hospitalar como, postos de coleta e exposição de prontuários, escaninhos e suportes de parede, e a falta de preparo dos hospitais para a implementação deste programa, que vai desde a deficiência de conscientização das pessoas, até o planejamento e efetivação dos investimentos necessários para as mudanças trazidas pela LGPD. (HAWRYLISZYN; COELHO; BARJA, 2020).

A implementação de um programa com este objetivo é primordial para estabelecimentos que coletam dados sensíveis de saúde, pois o armazenamento de dados se encontra saturado nesses locais principalmente depois de haver intensa digitalização de processos com o advento da pandemia de SARS-COV19 (ARAGÃO; SCHIOCCHET, 2020 e PINHEIRO, 2019).

A ausência de um mapeamento de processos, procedimento necessário na implementação de um programa de privacidade e proteção de dados, faz com que haja uma baixa gestão dos processos do hospital pediátrico e um déficit na melhoria institucional, posto a melhoria procedimental não estar relacionada à mudança da estrutura, mas sim da qualidade, do resultado e da segurança (THIOLLENT, 1997).

No próximo capítulo serão expostos os materiais e métodos utilizados para criação e implementação do programa de privacidade e proteção de dados.

3 MATERIAIS E MÉTODOS

Neste capítulo, os materiais e métodos utilizados para a realização desta dissertação são apresentados.

3.1 CARACTERIZAÇÃO DA METODOLOGIA DE PESQUISA

A natureza de pesquisa deste trabalho foi definida como uma pesquisa aplicada, vez que adotando a problemática exposta passa a ter como objetivo gerar conhecimento, ou seja, foge do espectro puramente teórico e adota uma aplicação prática (GIL, 2008). Quanto à abordagem metodológica é qualitativa com ambiente de pesquisa diretamente relacionado aos dados coletados (YIN, 2016). É considerada como pesquisa exploratória em seu objetivo porque explora o ambiente do hospital pediátrico para adquirir *insights* (PIOVESAN, e TEMPORINI, 1995).

Pode ser considerada também como pesquisa documental, na medida em que analisa documentos e dados que não são sistematizados como contratos, relatórios, projetos e bases relacionadas aos dados pessoais coletados no hospital pediátrico (KOCHE, 2003). A pesquisa documental foi aplicada para analisar as políticas existentes bem como das documentações de sistema e processos já existentes. Já a pesquisa bibliográfica foi realizada por meio de uma revisão da literatura que pode ser consultada na seção 2.5 deste trabalho.

Por fim, é uma pesquisa de campo em que se pretende a implementação de um programa de privacidade e proteção de dados, por meio da obtenção de informações pertinentes da população pesquisada, seja pela coleta de informações, seja pela coleta documental (GONÇALVES, 2001).

A Figura 7 apresenta com destaque na cor cinza escuro a caracterização da metodologia de pesquisa deste trabalho.

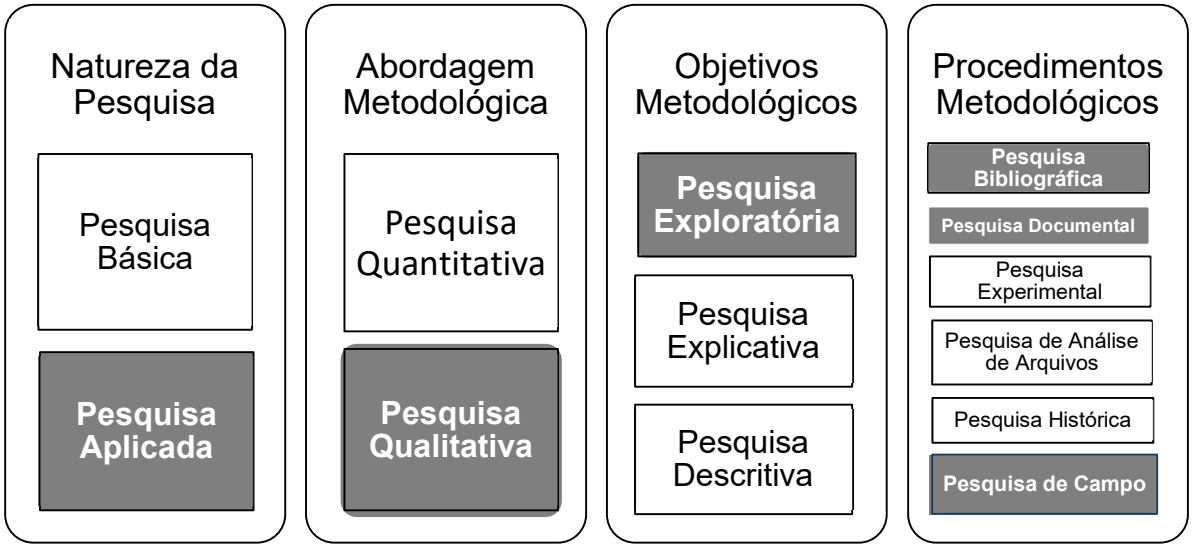


Figura 7 – Caracterização da Metodologia de Pesquisa

Fonte: O Autor.

Foi desenvolvido e aplicado um questionário para validar o programa de privacidade e proteção de dados a ser implementado no hospital pediátrico, com o objetivo de coletar as respostas de dez profissionais da área de segurança da informação, a fim de respaldar o desenvolvimento do programa. No momento da aplicação do questionário foi afirmado que os dados pessoais e a identificação dos participantes não seriam divulgados no trabalho e em publicações derivadas deste. Definiu-se esta premissa para manter o trabalho em conformidade com a Lei Geral de Proteção de Dados, Artigo 7º, Inciso IV. (BRASIL, 2018). O questionário está presente na integra no Apêndice H e mais detalhes sobre sua aplicação e resultados estão presentes na subseção 3.4 deste trabalho.

3.2 CARACTERIZAÇÃO DO HOSPITAL PEDIÁTRICO

O hospital pediátrico que serviu de base para elaboração e implementação do programa é considerado de médio porte, com 180 leitos de internação exclusivos para indivíduos com faixa etária entre 0 e 17 anos, 11 meses e 29 dias. Conta com 52 áreas corporativas, entre as destinadas a assistência ao paciente, atuação administrativa ou de apoio com aproximadamente cinco mil colaboradores diretos e indiretos. O atendimento é majoritariamente direcionado a usuários de plano de saúde ou para

pagamento particular, apesar de haver atendimentos ambulatoriais voltados para o Sistema Único de Saúde (SUS)

Este hospital tem um ambiente extremamente informatizado, com a integralidade dos prontuários e processos digitalizados e com uma abordagem voltada a alta complexidade e a assistência integral. O hospital não autorizou a divulgação de seu nome neste trabalho.

O programa de privacidade e proteção de dados foi aplicado em todas as áreas do hospital pediátrico, de modo a abranger todos os processos deste hospital, bem como realizar a adequação completa da LGPD em todo o ambiente do hospital pediátrico, seja um setor assistencial, um setor de retaguarda ou administrativo.

No início do desenvolvimento do programa foi possível constatar que o hospital pediátrico já havia realizado a implementação parcial de um programa de proteção de dados baseada na ISO 27701, sem haver, entretanto, a finalização da implementação.

Foi possível notar que não havia o cumprimento pleno da LGPD, e que por decorrência da utilização isolada da norma ISO 27701, bem como pela implementação parcial, não havia no hospital pediátrico um mapeamento abrangente de processos, havendo o desconhecimento do funcionamento de muitas áreas não mapeadas.

Esta ausência de mapeamento gerava também uma incompletude no mapeamento de dados, vez que, sem o mapeamento de processos não havia a capacidade de visualização dos dados coletados por cada área, gerando também uma ausência de construção do ROPA, LIA e RIPD exigidos pela LGPD.

Além disto, como os processos não estavam adequadamente mapeados não havia um controle adequado dos riscos inerentes a estes processos, ou dos riscos do tratamento dos dados coletados nestes processos. Outro ponto visualizado no hospital pediátrico foi a completa inexistência de treinamento e conscientização às questões de proteção de dados, o que impactava negativamente no sucesso do programa anterior.

A ausência de gestão de risco, gestão processual e cumprimento pleno da LGPD levou à necessidade de construção de um novo programa de privacidade e proteção de dados, sendo construído um substituto que conseguisse aprimorar o ambiente estando em conformidade à LGPD.

3.3 BASE DE DADOS E PLATAFORMA DE ENSAIOS

O *hardware* utilizado no desenvolvimento do programa de privacidade e proteção de dados foi um computador Intel Core i5-1135G7 Quad Core de 2,42 GHz com 8 GB de memória RAM, 1TB de armazenamento SSD e sistema operacional Windows 10 Pro de 64 bits. Os *softwares* utilizados são apresentados no Quadro 4.

Software	Tipo de Aplicação	URL
Bizagi 4.0.0.014	*Software* de uso livre para modelagem de processos que utiliza a notação BPMN aplicado no mapeamento dos processos do hospital (BIZAGI, 2017)	https://www.bizagi.com/pt/plataforma/modeler
Mendeley	*Software* de gerenciamento de referências bibliográficas	https://www.mendeley.com/search/
VOSViewer	*Software* para construir e visualizar redes bibliométricas	https://www.vosviewer.com/

Quadro 4 – *Softwares* utilizados no desenvolvimento do programa de privacidade e proteção de dados.

Fonte: O Autor.

O desenvolvimento do programa foi precedido por uma análise de todos os processos que tratam dados pessoais do hospital pediátrico. Também foram coletados os tipos de dados tratados nestes processos, sendo identificados como: informações de identificação pessoal, dados de identificação eletrônica, dados financeiros, detalhes do plano de saúde do paciente, dados de autorizações e consentimentos, características pessoais, características psicológicas, composição familiar, casamento ou forma atual de coabitação, histórico conjugal, dados residenciais, dados acadêmicos/escolares, dados de profissão e emprego, e dados sensíveis de convicção religiosa, biométricos e referentes à saúde.

Todos os dados coletados foram anonimizados antes da própria coleta diretamente pelo hospital pediátrico, sendo excluída toda característica que pudesse

vincular estas informações a uma pessoa física. A anonimização foi realizada sem possibilidade de reversão, cumprindo o disposto na LGPD quando da utilização de dados para pesquisa preferencialmente anonimizados (BRASIL, 2018)

Os tipos de dados e as fontes de coleta são descritos no Quadro 5.

Tipo de Dados	Fonte de coleta
informações de identificação pessoal, dados de identificação eletrônica, detalhes do plano de saúde do paciente, características pessoais, características psicológicas, composição familiar, casamento ou forma atual de coabitação, histórico conjugal, dados residenciais; dados sensíveis de convicção religiosa, dados biométricos e dados de saúde	Sistema de gestão hospitalar MV Soul e Módulo Prontuário Eletrônico MV PEP, ambos do hospital
dados financeiros	Sistema de gestão financeira Pipefy e Sistema de gestão hospitalar MV Soul, ambos do hospital
dados de autorizações e consentimentos	Data center *on premisse* do hospital
dados acadêmicos/escolares, dados de profissão e emprego	Sistema de gestão de recursos humanos do hospital

Quadro 5 – Fontes de dados coletados.

Fonte: Autor.

3.4 FASES DE DESENVOLVIMENTO E IMPLEMENTAÇÃO DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

O desenvolvimento do programa foi realizado em 4 fases distintas, apresentadas na Figura 8:

- 1ª Fase: Pesquisa Bibliográfica;

- 2ª Fase: Desenvolvimento do Programa de Privacidade e Proteção de Dados
- 3ª Fase: Implementação do Programa de Privacidade e Proteção de Dados;
- 4ª Fase: Cumprimento da Lei Geral de Proteção de Dados;

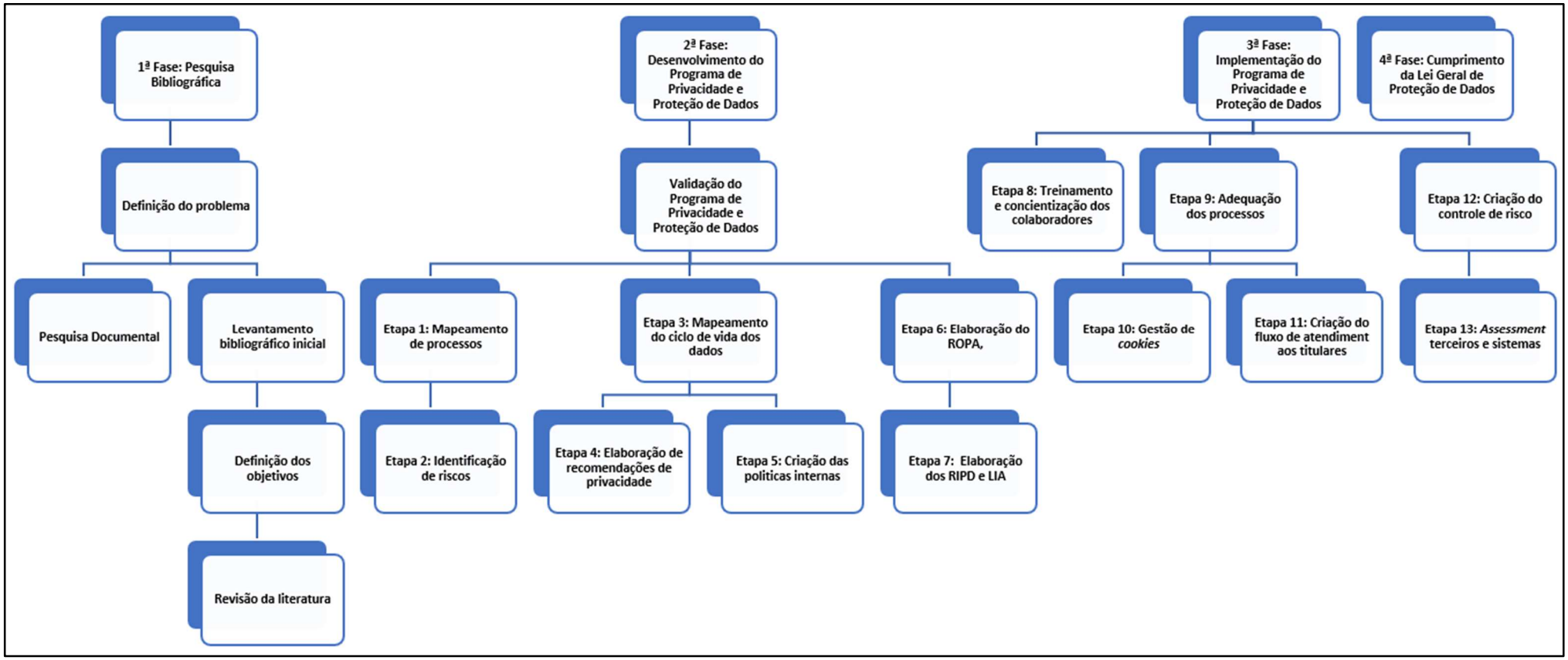


Figura 8 - Fases de desenvolvimento do programa.

Fonte: O Autor.

Descreve-se a seguir as fases de desenvolvimento do programa de privacidade e proteção de dados:

1ª FASE: PESQUISA BIBLIOGRÁFICA

Nesta fase foi definido o problema e realizou-se o levantamento bibliográfico inicial para definir os objetivos, delimitando o escopo da pesquisa e construindo bases metodológicas para apoiar o trabalho, sendo posteriormente realizada a revisão da literatura que pode ser encontrada na seção 2.5. Na mesma fase foi realizada a pesquisa documental com o objetivo de identificar quais eram as problemáticas a serem dirimidas. Nesta etapa foram levantados todos os documentos de gestão de processos, os mapeamentos já realizados, se existentes, os modelos de contratos usados e todas as políticas, regimentos, práticas normas de segurança da informação da organização.

2ª FASE: DESENVOLVIMENTO DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

Antes de iniciada as etapas de desenvolvimento desta fase foi realizada a validação do programa por meio da aplicação de um questionário para dez especialistas da área de segurança da informação. O questionário contém 15 perguntas divididas em perguntas de validação do programa e de caracterização dos respondentes, enviado por e-mail com prazo de dez dias para responder.

Os respondentes têm o seguinte perfil:

- Graduado em Ciência da Computação, Pós-graduado em Redes e Segurança da Informação e exerce gerência de infraestrutura e segurança da informação em um hospital pediátrico;
- Graduado em Filosofia e Gestão Hospitalar, Pós-graduado em Gestão de TI, exerce a função de direção de TI em organizações hospitalares há 29 anos, atualmente é vice-presidente de em empresa de fornecimento de tecnologia para o ambiente hospitalar;
- Graduado em Sistemas da Informação, MBA em Gestão de Pessoas, Especialista em Privacidade e Proteção de Dados, atualmente é

encarregado da área de proteção de dados em uma organização de grande porte da área da saúde;

- Graduado em Ciência da Computação e Direito, MBA em Gestão de TI e Direito Digital, é professor universitário e *Data Protection Officer* (DPO) em um hospital de médio porte;
- Graduado em Gestão de TI, Pós-graduado em Engenharia de Redes, exerce o cargo de especialista em segurança da informação em um hospital pediátrico;
- Graduado em Sistemas da Informação, MBA em Gestão de Sistemas da Informação, atua há mais de 20 anos na área da saúde, exerce o cargo de diretor de TI em um hospital de grande porte.
- Diretor de Segurança da Informação em consultoria especializada em segurança cibernética, atua como assessor e consultor em hospitais de pequeno, médio e grande porte.
- Graduado em Engenharia Mecatrônica, MBA em proteção de dados e em Gestão da Tecnologia da Informação, exerce o papel de *Data Protection Officer* (DPO) em hospital de grande porte;
- Graduado em Medicina, MBA em Gestão Hospitalar e em Transformação Digital, atua em hospitais há mais de 12 anos, exercendo atualmente a posição de diretor operacional em um hospital de grande porte;
- Graduado em Processamento de Dados, MBA em Gestão Empresarial, atua há mais de 10 anos nas áreas governança de dados e compliance, atualmente ocupa o cargo de DPO em uma rede de hospitais de grande porte;

O questionário aplicado está presente, em sua integralidade, no Apêndice H.

Descreve-se a seguir as 7 etapas de desenvolvimento do programa após a validação realizada:

Etapa 1: Mapeamento de processos - Nesta etapa é realizada a identificação de quais processos tratam dados pessoais com a finalidade de formalizar os processos de todas as áreas, utilizando a notação do *Business Process Model and Notation* (BPM CBOK, 2014).

Etapa 2: Identificação de riscos - Tendo sido mapeados os processos, são identificados os ativos utilizados e elaborado um mapeamento de riscos de cada um destes processos. Esta etapa é a que embasará as demais etapas.

Etapa 3: Mapeamento do ciclo de vida dos dados - Identificando os processos que tratam dados pessoais, bem como os riscos de cada processo, é realizado um inventário, identificando todo o ciclo de vida dos dados, do início à sua exclusão e, quais dados são coletados em cada uma das atividades.

Este mapeamento é realizado identificando qual processo se relaciona, quais dados coletados neste processo, local de armazenamento dos dados, qual a finalidade de coleta, e qual é o prazo de retenção dos dados coletados. Nesta etapa também é identificada a justificativa legal para utilização dos dados pessoais, utilizando-se a metodologia disponibilizada no Apêndice B.

Etapa 4: Elaboração de recomendações de privacidade - Com base nos riscos identificados na etapa 2 e nos processos que tratam dados pessoais identificados na etapa 3, é formulado um plano de recomendações para cada processo mapeado com a finalidade de adequar o processo às necessidades regulatórias trazidas pela LGPD.

Etapa 5: Criação das políticas internas - Nesta etapa serão elaboradas todas as políticas de proteção de dados e de segurança da informação para cumprirem a imposição de governança trazida pela LGPD conforme recomendações da etapa 4.

Etapa 6: Elaboração do ROPA - Neste momento é construído o ROPA, documento necessário para formalizar, registrar e acompanhar os tratamentos de dados, conforme recomenda a LGPD. Os processos que receberão o registro através do ROPA são os identificados na etapa 3 e um modelo de ROPA pode ser encontrado no Apêndice D.

Etapa 7: Elaboração dos RIPDs e LIAs - Nesta etapa são elaborados os RIPDs e LIAs, que são ferramentas para análise do risco identificado na etapa 2 e mapeado na etapa 3. Os documentos utilizam metodologia própria, baseada nas indicações da LGPD, e podem ser encontrados nos Apêndices A e C. Estes documentos foram desenvolvidos com metodologia própria baseada nas obrigações trazidas na Lei Geral de Proteção de Dados.

3ª FASE: IMPLEMENTAÇÃO DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

Nesta fase implementa-se o programa de privacidade e proteção de dados no hospital pediátrico, de acordo com as etapas a seguir:

Etapa 8: Treinamento e conscientização dos colaboradores - Conscientização de todos os colaboradores do hospital de forma a educá-los quanto às mudanças necessárias para conformidade com a LGPD e treinamento acerca das novas políticas criadas na etapa 5.

Etapa 9: Adequação dos Processos - Com base nas recomendações e análise da etapa 4 são realizadas todas as alterações de processos, sistemas e pessoas, para cumprimento das recomendações geradas na etapa anterior. Nesta etapa é feita a mitigação dos riscos identificados e é escriturado o risco remanescente para acompanhamento. Além disso, nesta etapa é realizada a implementação de melhorias nos processos mapeados.

Etapa 10: Gestão de *Cookies* - Implementação da gestão correta dos *cookies* dos sites e sistemas utilizados, em atendimento ao guia orientativo da ANPD (ANPD, 2022). A gestão correta destes *cookies* é de suma importância para o programa de proteção de dados, vez que os *cookies* são considerados dados pessoais e muitas vezes são a porta de entrada destes dados na organização através de uma coleta direta.

Etapa 11: Criação de Fluxo de Atendimento aos Titulares - Implementado o canal de atendimento aos titulares, para atender o artigo 18 da LGPD e às solicitações dos indivíduos que tiveram seus dados tratados nos termos das políticas criadas na etapa 5.

Etapa 12: Criação do Controle de Risco - Tendo sido verificado o risco inicial e o risco após a implementação, é extravasado a sua gestão de modo a construir Matriz de Risco para controle e acompanhamento das medidas identificadas nas etapas 3 e 7.

A Matriz de Risco é uma ferramenta para se mensurar de forma qualitativa o risco de um processo ou organização usando duas variáveis que são classificadas previamente e relacionadas a certo grau de severidade. Estas variáveis são a frequência e o impacto quando associadas aquele evento, sendo possível chegar a

um valor final de chance de acontecimento deste evento, denominado risco (MARTIN; SANTOS e DIAS FILHO, 2004). A Matriz de Risco desenvolvida neste trabalho está presente no Apêndice E.

Etapa 13: *Assessment* de Terceiros e Sistemas - Identificados os sistemas e terceiros envolvidos nos processos mapeados nas etapas 1 e 3, é elaborado um *Assessment* abrangente de terceiros que se relacionam com o hospital e dos sistemas utilizados, para identificação das lacunas existentes e criação de plano de ação personalizado para cada terceiro ou sistema.

O *Assesment* é realizado através do acesso ao ambiente do terceiro, ou do sistema, utilizando os requisitos e metodologia disposta no Apêndice F, de modo a conseguir averiguar o nível de maturidade deste parceiro e/ou sistema, com a finalidade de implementar as mudanças necessárias constatadas no *Assessment*.

4ª FASE: CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Nesta fase, compara-se as melhorias obtidas com a implementação do programa de privacidade e proteção de dados, demonstrando o cumprimento da LGPD através de indicadores pertinentes a proteção de dados, como número de processos mapeados, riscos encontrados, políticas elaboradas, incidentes verificados, práticas impostas, treinamentos realizados e melhorias implementadas.

No Capítulo 4 serão apresentados e discutidos os resultados da implementação do programa de privacidade e proteção de dados no hospital pediátrico.

4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo são apresentados e discutidos os resultados relacionados a implementação do programa de privacidade de proteção de dados em um hospital pediátrico.

As seguintes fases e resultados são apresentados neste capítulo:

- 2ª Fase: Desenvolvimento do Programa de Privacidade e Proteção de Dados;
- 3ª Fase: Implementação do Programa de Privacidade e Proteção de Dados;
- 4ª Fase: Cumprimento da Lei Geral de Proteção de Dados;

4.1 2ª FASE: DESENVOLVIMENTO DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

O questionário foi encaminhado de maneira virtual para dez respondentes, sendo que, antes dos 10 dias de prazo oferecido, houve o recebimento das respostas de todos os respondentes. O questionário é composto por 15 perguntas, divididas entre 4 perguntas de qualificação do respondente e 11 perguntas técnicas voltadas para a validação do programa.

Analisando as respostas foi possível verificar que todos os respondentes validaram a proposta de desenvolvimento de um Programa de Proteção de Dados voltado para hospital pediátrico. Esta validação foi reforçada também pela indicação da importância do Mapeamento de Processos usando BPMN, do Mapeamento de Dados, do RIPD, ROPA e LIA, aplicados conjuntamente. O questionário aplicado, as respostas e a análise dos resultados são apresentadas no Apêndice H.

Nota-se, então que o programa, além de ser benéfico ao hospital pediátrico, está de acordo com as técnicas indicadas pelos respondentes, especialistas nas áreas afins, o que demonstra a importância de sua criação e utilização.

Ademais, foram desenvolvidas as 7 etapas que compreendem esta fase: Mapeamento de Processos; Identificação de Riscos; Mapeamento do ciclo de vida dos dados; Elaboração de recomendações de privacidade; Criação de políticas internas; Elaboração do ROPA e Elaboração dos RIPD e LIA.

a) ETAPA 1: MAPEAMENTO DE PROCESSOS

No tocante à gestão de processos do hospital pediátrico, havia uma situação em que os processos não eram mapeados, sendo que cada área não tinha formalizado as suas atividades e os sub processos que levam à conclusão oficial desta atividade.

Isto comprometia, de sobremaneira, a gestão e desenvolvimento das atividades do hospital pediátrico, ainda mais sendo considerado que há uma grande rotatividade de funcionários da área assistencial, como enfermeiros e médicos.

Após o mapeamento foi possível identificar 533 processos com a aplicação da metodologia BPM para possibilitar a identificação de riscos presentes na Etapa 2, e o mapeamento do ciclo de vida dos dados da Etapa 3. Um exemplo de processo mapeado nesta etapa foi o “processo de comunicação de óbito” realizado pela área da psicologia, que pode ser visualizado na Figura 9.

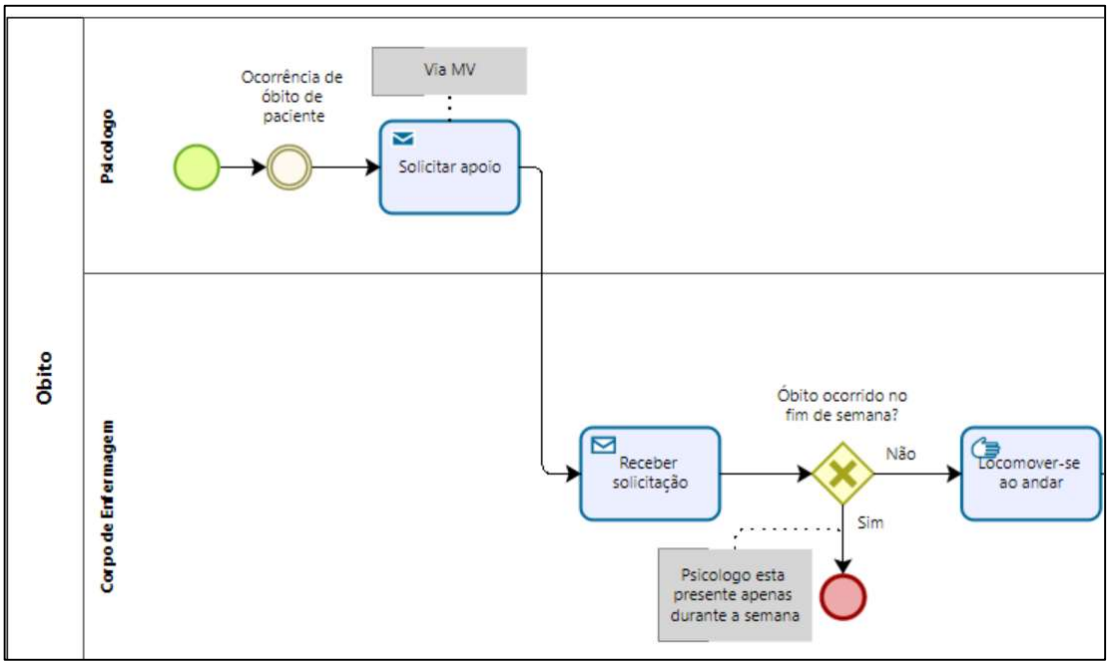


Figura 9 - Processo Comunicação de Óbito

Fonte: O Autor.

A Figura 9 demonstra o início do processo de comunicação quando da ocorrência de um óbito. Ademais, foram mapeados todos os processos realizados no hospital pediátrico.

Nesta etapa foi possível ter como resultado a visibilidade pela primeira vez de todos os processos de negócio presentes no hospital pediátrico, sendo possível

constatar, de maneira gerencial, todas as condutas realizadas por todas as equipes do hospital.

b) ETAPA 2: IDENTIFICAÇÃO DE RISCOS

Visualizado o mapeamento de processos realizado na Etapa 1 e o desenho dos 533 processos organizacionais, foi realizada uma análise destas atividades com a finalidade de identificar os riscos de privacidade de cada uma delas.

Para tanto foi utilizada uma planilha identificadora de risco contendo as seguintes informações: ID do risco, processo relacionado, ativo envolvido, categorização do risco, risco existente e fatores do risco. Um exemplo de risco encontrado no processo de “evolução de prontuários” é apresentado na Figura 10.

ID do Risco	Processo	Ativo	Categoria do Risco	Riscos	Explicação do Risco	Fatores de Risco
R.1	Evolução do prontuário	MV	Risco de TI	Acesso indevido ao sistema	Acessos indevidos a sistema, sem comprometimento do file server, podem acarretar em vazamentos de dados e afetar a confidencialidade e integridade dos sistemas	1) Compartilhamento de senha 2) Expor a senha em locais publicos. 3) senhas fracas 4) Gestão de acesso comprometida,

Figura 10 - Risco do processo evolução do prontuário

Fonte: O Autor.

A identificação dá a organização a capacidade de conhecer e gerir seus riscos e, após devida classificação, permite o entendimento das lacunas existentes para correção e implementação de melhorias previstas na priorização estratégica da organização. O modelo de planilha utilizado pode ser integralmente visualizado no Apêndice E.

Esta etapa possibilitou a visão dos riscos organizacionais de maneira abrangente, o que permite a melhor construção do programa de privacidades e proteção de dados que permitiram a criação de indicadores, planos e medidas mitigatórias, tal como planos de melhoria, correção dos processos em desacordo com a LGPD e acompanhamentos dos processos.

c) ETAPA 3: MAPEAMENTO DO CICLO DE VIDA DOS DADOS

Esta etapa teve como objetivo mapear os dados pessoais coletados pelos processos identificados na Etapa 2, identificando, através desta etapa, quais dados são coletados, de que forma é feito a coleta e o que é realizado com estes dados.

A partir da sistematização e formalização destes processos foi possível identificar o ciclo de vida dos dados para identificar informações sobre a natureza destes tratamentos, como, por exemplo, volume de coleta de dados de crianças e adolescentes, base legal aplicável, criticidade e interrelações entre tais dados.

Este mapeamento é realizado identificando qual processo se relaciona, quais dados coletados neste processo, onde tais dados estão armazenados, qual a finalidade de coleta e qual é o prazo de retenção dos dados coletados, através do questionário que pode ser encontrado no Apêndice B.

Importante citar que o mapeamento do ciclo de vida dos dados tem como finalidade identificar quais dados são tratados na organização, de modo a registrar em um documento formal e visível quais são os tratamentos de dados realizados nos processos do hospital pediátrico.

Deste mapeamento é possível verificar que a grande maioria dos dados pessoais coletados no hospital pediátrico é de crianças e adolescentes, um tipo de tratamento de dados que demanda mais cuidado e detém bases legais próprias (BRASIL, 2018), como se verifica da Figura 11 abaixo, onde 55% de todos os dados tratados se relacionam a crianças e adolescentes.

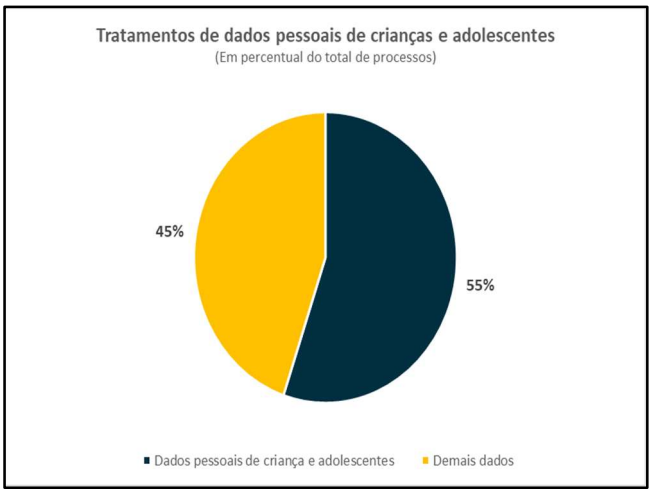


Figura 11 - Percentual de tratamentos de dados que envolvem crianças e adolescentes.

Fonte: O Autor.

Além desta conclusão, é possível a partir deste mapeamento, identificar no hospital pediátrico quais são as bases legais utilizadas em cada tratamento de dados, sendo que bases legais são as autorizações da LGPD que permite tratar tais dados.

A identificação correta da base legal adequada para aquele tratamento é primordial para que seja possível entender a necessidade regulatória para cada um daqueles tratamentos, na medida em que bases legais diferentes implicam em requisitos diversos trazidos pela LGPD.

Da elaboração desta fase foi possível identificar que para dados pessoais sensíveis o exercício regular de direito, a tutela da saúde e a obrigação legal preponderam em relação aos demais, o que demonstra o risco envolvido.

Com base neste mapeamento de dados foi possível constatar que o hospital detém 533 processos ativos, sendo que 357 processos coletam dados de crianças e adolescentes, demonstrando uma necessidade de maior rigor no tratamento destes dados. O modelo completo utilizado no mapeamento do ciclo de vida dos dados está presente no Apêndice B deste trabalho.

Fazendo a divisão dos processos que tratam os dados pessoais coletados por área, obtém-se o seguinte resultado apresentado no Quadro 6.

Área	Número de Processos
Administração de Pessoal	23
Instituto de Pesquisa	22
Relacionamento Médico e Residência	20
Unidade de Tratamento Intensivo	20
Atendimento	19
Desenvolvimento Humano	16
Centro de Excelência	13
Medicina do Trabalho	13
Unidade de Internação	13
Serviço Auxiliar de Diagnóstico	12
Agendamento	11
Centro Cirúrgico	11
Hotelaria	11
Serviços de Arquivo Médico e Estatística	11
Marketing	10
Farmácia	10
Recurso de Glosa	9

Controladoria	8
Segurança do Trabalho	7
Tecnologia da Informação	7
Faturamento	6
Manutenção	6
Jurídico	6
Financeiro	5
Fonoaudiologia	5
Hospital Dia	5
Nutrição	5
Psicologia e Serviços Social	5
Portaria e Segurança	5
Telemedicina	5
Voluntariado	5
Central de Guias	4
Comercial	4
Compras	4
Fisioterapia	4
Núcleo de Informação em Saúde	4
Comitê de Ética e Pesquisa	3
Engenharia Clínica	3
Almoxarifado	2
Central de Material Esterilizado	2
Central de Transporte Interno	2
Auditoria	1
Total de Processos	357

Quadro 6 - Número de Processos que tratam dados pessoais coletados por área de negócio.

Fonte: O Autor.

A partir da análise das informações contidas no Quadro 6, é possível visualizar quais são as áreas com maior tratamento de dados, e o grande volume de dados coletados, o que já demonstra por estes motivos alguns pontos focais de risco.

Da simples leitura destes resultados, é possível concluir pela necessidade de implementação de um programa de privacidade e proteção de dados em um hospital pediátrico ante a necessidade de controle, gestão e tratamento adequado destes dados oriundos de crianças e adolescentes e em grande medida sensíveis.

d) ETAPA 4: ELABORAÇÃO DE RECOMENDAÇÕES DE PRIVACIDADE

Após a realização das etapas 2 e 3 foi possível verificar quais dos processos do hospital pediátrico tratam dados pessoais, bem como quais os riscos existentes em

cada um destes processos. Esta etapa analisa em conjuntos estas duas características para construir recomendações que devem ser atendidas para tornar aquele processo, ou aquele tratamento de dados de acordo com os preceitos e necessidades trazidas pela LGPD.

Estas recomendações serão implementadas na fase seguinte e podem ser de algumas naturezas como: alteração de processo, interrupção de processo, adequação de ferramentas, recomendações ou implementação de ferramentas. Para cada uma das recomendações foi criado um plano de ação e este trabalho é desenvolvido no próprio mapeamento do ciclo de vida dos dados.

Na Figura 12, podem ser visualizadas recomendações de privacidade geradas para o processo de “Plataforma de Eventos e EAD” e identifica o detalhamento de funcionamento desses processos, quais são os riscos visualizados e o plano de ação direcionado para mitigação destes riscos.

NOME DO PROCESSO	FINALIDADE	DETALHAMENTO	PLANO DE AÇÃO DIRECIONADO
Plataforma de Eventos e EAD	Realizar eventos e cursos online	Realizam eventos online como congressos, workshop, webinars, entre outros. Possuem uma plataforma em que divulgam os eventos e os interessados podem realizar a inscrição. Para a inscrição na plataforma, solicitam o nome, RG, CPF, email, endereço, telefone, carreira, CRM e UF. Encaminham no email o link do evento. Retiram da plataforma a lista de presença dos cursos com o nome e email dos participantes. Podem ter inscrições realizadas por pessoas jurídicas (razão social, CNPJ, telefone e email - possuem clientes MEI/ME/EIRELI) ou pessoas físicas. Realizam a divulgação do cursos através do site do instituto, redes sociais e sites de associações parceiras. Ao final do curso, disponibilizam uma pesquisa de satisfação na GN1, que é fator condicionante à liberação do certificado.	1. Atualizar o contrato com sistema para inserir clausulado de proteção de dados pessoais e segurança da informação. 2. Incluir, no momento da inscrição na plataforma, acesso às Políticas de Privacidade, de Cookies e Termos de Uso da plataforma para assegurar ao titular informações sobre tratamento de dados pessoais; 3. Avaliar cadastro na plataforma para os cursos online e eventos para excluir a coleta de dados desnecessários à finalidade pretendida 4. Assegurar mecanismo de opt-out para os titulares em comunicações, por e-mail, sobre eventos e cursos disponibilizados. 5. Elaborar tabela de temporalidade de guarda de base de dados de inscritos para que, findo o prazo, sejam os dados descartados ou anonimizados.

Figura 12 - Recomendações de privacidade para o processo Plataforma de Eventos e EAD.

Fonte: O Autor.

A elaboração deste documento permitiu, após mapear os processos e identificar seus riscos, endereçar quais medidas que serão tomadas na fase de implementação, como por exemplo realizar uma alteração contratual, ser transparente com políticas de privacidade ou mitigar riscos e inconformidades presentes.

e) ETAPA 5: CRIAÇÃO DAS POLÍTICAS INTERNAS

Identificada a criticidade dos tratamentos mapeados através das etapas anteriores e elaboradas as recomendações para adequação do hospital pediátrico, passou-se à etapa de construção das políticas da organização com a geração de 27 políticas de privacidade e segurança da informação, como se visualiza no Quadro 7.

Estas políticas foram criadas após o mapeamento dos processos e do mapeamento do ciclo de vida dos dados e foram validadas posteriormente por meio de reuniões com as áreas de negócio, de forma a se criar documentos que atendessem as necessidades para cumprimento pleno da LGPD, bem como para encontrar soluções as prioridades das próprias áreas de negócio, em especial ao departamento de TI com questões relacionadas à Segurança da Informação.

No Quadro 7 constam as políticas criadas nesta etapa.

Políticas de Privacidade e Segurança da Informação
Política de Backup e Restauração
Plano de Resposta a Incidentes de Segurança da Informação
Política de Segurança da Informação
Política de Uso de Internet
Política de Senhas
Política de E-mail
Política de Mesa Limpa
Política de Dispositivos Móveis
Política de Governança de Dados Pessoais
Política de Utilização do Wi-Fi
Política de Uso de Comunicadores Instantâneos
Política de Controle de Acesso Lógico
Manual de Concessão de Dispositivos Móveis
Política de Privacidade
Regimento de Acesso Remoto
Regimento de Segurança Física do Datacenter
Regimento de Uso do Serviço de Impressão e Digitalização
Regimento de Controle de Acesso ao Banco de Dados
Regimento de Avaliação de Impacto à Privacidade (PIA/PbD)
Regimento de Atendimento de Requisições do Titular
Regimento de Gestão de Incidentes de Violação de Dados Pessoais
Regimento de Relatório de Impacto à Proteção de Dados (RIPD)
Política de Classificação e Uso da Informação
Regimento de Avaliação da Governança e Proteção de Dados Pessoais em Terceiros
Regimento de Avaliação de Aplicação do Legítimo Interesse
Regimento de Prevenção de Perda de Dados
Política de Acesso Lógico

Quadro 7 - Políticas elaboradas na etapa 5.

Fonte: O Autor.

A construção destas políticas teve a finalidade de trazer normas e regulação para o hospital pediátrico, como regras para acesso a informações sigilosas, gestão de rede e regras de uso e descarte, garantindo um nível mínimo de governança recomendado pela LGPD.

f) ETAPA 6: ELABORAÇÃO DO ROPA

Tendo realizado o mapeamento dos processos e o mapeamento do ciclo de vida dos dados, foi possível identificar quais processos tratam dados pessoais e desta forma registrar tais tratamentos segundo a LGPD (BRASIL, 2018).

Foram realizados os registros de todos os 357 processos que tratam dados pessoais em modelo próprio construído nos termos do Apêndice D deste trabalho. A Figura 13 apresenta o registro de tratamento de dados do processo “documento de admissão para prestador de serviço”.

Registro de Atividades de Processamento de Dados						
1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais						
1.1 - Empresa / Área	HISICompras					
1.1 - Processo de negócio	Documento de admissão para prestador de serviço					
1.2 - Nº Referência / ID	RPA0333					
1.3 - Data de Criação do Inventário	21/07/2021					
1.4 - Data Atualização do Inventário	28/03/2023 - 3ª Versão					
2 - Agentes de Tratamento e Encarregado	Nome	Endereço		CEP	Telefone	E-mail
2.1 - Controlador	[redacted]					
2.2 - Encarregado						
2.3 - Operador						
3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação	
3.1 - Em qual fase do ciclo de vida o tratamento ocorre	Sim	Sim	Sim	Não	Não	

4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados	
4.1 - Descrição do Fluxo do tratamento dos dados pessoais	Ao contratar qualquer empresa prestadora de serviço é solicitado por e-mail o envio da documentação para o departamento de SESMT do HIS os seguintes dados (nome da empresa, serviço prestado, data do inicio do trabalho, quantos funcionários que serão disponibilizados e duração dos serviços que serão prestados, junto essas informações é extremamente enviar cópia de registro empregatício (carteira de trabalho), cópia do ASO, Cópia de certificados, Relação de EPIs, caso seja empresa subcontratada deverá apresentar contrato de prestador, e por fim o agendamento da integração de segurança fornecida pelo HIS. Para fins qualificatórios da empresa é necessário o envio por e-mail ao setor documentos como prova de quitação, certidão de regularidade com órgãos públicos e certidão negativa de protesto.

5 - Escopo e Natureza dos Dados Pessoais	
5.1 - Abrangência da área geográfica do tratamento	Brasil
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	Diretamente

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento Dados Pessoais	V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados
6.2 - Hipótese de Tratamento Dados Sensíveis	II (...) d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
6.3 - Finalidade	Solicitar documentação de admissão para prestadores de serviços
6.4 - Resultados pretendidos para o titular de dados	Inicio da prestação de serviços
6.5 - Benefícios esperados para a empresa	Gestão da mão de obra terceirizada que acessará o hospital

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	mpo Retenção dos Dad	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal	Nome, E-mail, Telefone	Indeterminado	Informação direta da	File Server
7.1.2 - Informações de identificação atribuídas por instituições	RG e CNPJ, Carteira de Trabalho	Indeterminado	Informação direta da	File Server
7.1.3 - Dados de identificação eletrônica	NA			
7.1.4 - Dados de localização eletrônica	NA			
7.2 -Dados Financeiros	Descrição	mpo Retenção dos Dad	Fonte Retenção	Nome Base de
7.2.1 - Dados de identificação financeira	NA			
7.2.2 - Recursos financeiros	NA			

Figura 13 - ROPA do processo “Documento de admissão para prestador de serviço”.

Fonte: O Autor.

A Figura 13 mostra o ROPA desenvolvido para o processo “Documento de admissão para prestador de serviço” realizado no departamento de compras do hospital pediátrico. Nas duas figuras é possível visualizar a característica do

tratamento, sua finalidade, dados tratados e demais características primordiais para um ROPA.

Com a finalização e implementação do ROPA, passou a ter agora vinculados em um unido documento de controle todos os requisitos e informações pertinentes daquele tratamento, podendo, além de cumprir a determinação da LGPD, dar visibilidade a todos os envolvidos com aquele tratamento, como por exemplo fornecedores, banco de dados utilizados, ativos vinculados e contratos firmados eventualmente com os envolvidos.

g) ETAPA 7: ELABORAÇÃO DOS RIPDs E LIAs

Após a identificação dos riscos na Etapa 2, e após identificar quais os riscos são considerados como altos ou muito altos, foram construídos 123 relatórios de impacto à proteção de dados (RIPD), relatório este que formaliza os processos que podem gerar alto risco aos indivíduos que tiveram os dados coletados.

O RIPD utilizado foi desenvolvido com metodologia própria, devido ao fato de não haver um padrão aprovado pela ANPD para tal documento até o presente momento e pode ser encontrado no Apêndice C deste trabalho.

As Figuras 14, 15 e 16 reproduzem o RIPD do processo de medicamento quimioterápico da farmácia do hospital pediátrico.

1. DADOS DO CONTROLADOR			
Dados do Controlador	**Agentes de Tratamento envolvidos** *Indicar todos os agentes de tratamento envolvidos (operadores e outros controladores, se aplicável)*	**Dados do Encarregado pelo Tratamento de Dados Pessoais** *Indicar nome, e-mail e telefone do Encarregado*	**Departamento/Área envolvida**
Sede na Avenida Angélica, nº 1.987, complemento: 3º subsolo ao 16º andar, Higienópolis, CEP 01227-200, no município de São Paulo, estado de São Paulo, CNPJ sob nº. 61.213.674/0002-40	Corpo Clínico e Prestadores dos processos.		Farmácia
Necessidade de elaboração do RIPD *Aponte o motivo pelo qual a elaboração do RIPD é necessário*	Tendo em vista que os processos da área envolve a utilização de dados sensíveis, necessário a elaboração deste RIPD		

2. DESCRIÇÃO DO TRATAMENTO DE DADOS PESSOAIS			
Para descrição detalhada do tratamento de dados pessoais, é importante considerar a possibilidade de consultar a documentação que demonstre os fluxos de tratamento de dados pessoais da empresa, como, por exemplo o Registro das Atividades de Tratamento (*Record of The Processing Activities* - RoPA)			
Natureza	**Escopo**	**Contexto**	**Finalidade**
Para este RIPD é considerado o processo de **Medicamento quimioterápico:** Possuem uma empresa terceira que manipula medicamentos quimioterápicos. A prescrição de quimioterapia é enviada fisicamente para a farmácia quando o paciente está internado. Quando se trata de um paciente com programação eletiva de internação para administração de quimioterapia a prescrição é enviada pelo setor de agendamento por e-mail para os farmacêuticos. Após validação da prescrição, o farmacêutico encaminha a prescrição por e-mail para a empresaparceira para manipulação. No recebimento do medicamento realiza a conferência do rótulo com a solicitação realizada. A via original da prescrição fica arquivada no prontuário do paciente e a cópia da mesma é armazanada em armário sem chave no departamento, em sala com acesso restrito. Após 2 anos a cópia arquivada é destruída e descartada;	No processo são tratados dados sensíveis de saúde e são tratados dados pessoais como Nome, idade, data de nascimento, carteirinha do SUS, medicamento, prescrição, CID, remedios e diagnóstico. O volume de tratamento é maior que 100 titulares dia. A abrangência geografica é todo território brasileiro, com enfase maior no estado de São Paulo, onde se localiza o hospital.	A natureza do titular de dados com a empresa é de paciente. O titulares não exercem controle sobre os dados. Todos os tratamentos coletam obrigatoriamente dados de menores, ante a especialidade do Hospital; O tratamento ao titular atende sua espectativa ante se tratar de processo imprescindível para manutenção da qualidade do atendimento assistêncial realizado em beneficios dos pacientes da organização.	O resultado pretendido ao titular é a manutenção da saude do titular (Paciente). Os beneficiós esperados para a sociedade empresarial é a manutenção da missão de assistência de excelência aos menores.

Figura 14 - RIPD do processo “Medicamento quimioterápico” executado pela farmácia do hospital pediátrico.

Fonte: O Autor.

A Figura 14 apresenta o conteúdo do RIPD, especialmente a definição do controlador, a natureza do tratamento, o contexto inserido no tratamento, a finalidade, suas bases legais, finalidades e objetivos.

	4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS				5. ACEITAÇÃO DO RISCO
	DESCREVA A FONTE DE RISCO E A NATUREZA DO IMPACTO POTENCIAL SOBRE OS TITULARES	PROBABILIDADE DE DANO	GRAVIDADE DO DANO	RISCO GERAL	RISCO ACEITO? (Sim / Não)
R1	**Risco de Vazamento dos dados dos titulares**	3. Significativo	3. Significativo	9. Significativo	**Não**
R2	**Dano à integridade física do titular (ausência de atendimento por ausência de encaminhamento prescrição)**	2. Limitado	3. Significativo	6. Limitado	**Não**

Figura 15 - RIPD do processo “Medicamento quimioterápico” executado pela farmácia do hospital pediátrico.

Fonte: O Autor.

A Figura 15 apresenta a identificação dos riscos deste tratamento, sendo elencado a fonte de risco, a probabilidade de dados, a gravidade do dano, o cálculo do risco geral e a eventual aceitação do risco.

6. IDENTIFICAÇÃO DE MEDIDAS/CONTROLES PARA MITIGAÇÃO DE RISCOS					
MEDIDAS DE MITIGAÇÃO OU ELIMINAÇÃO RISCOS NÃO ACEITOS (Impacto e/ou Probabilidade)	NOVA PROBABILIDADE DE DANO	NOVA GRAVIDADE DO DANO	RISCO RESIDUAL	EFEITO SOBRE O RISCO	MEDIDA APROVADA/ EM PRÁTICA (Sim / Não)
Documentos fisicos devem ser aquivados em locais com controle de acesso e acaso não seja mais necessário deve ser descartado via fragmentadora de papel.	1. Insignificante	3. Significativo	3. Insignificante	Risco Reduzido ou eliminado	Sim
realizar controle das solicitações e prescrições para atendimento do paciente corretamente	1. Insignificante	3. Significativo	3. Insignificante	Risco Reduzido ou eliminado	Sim

Figura 16 - RIPD do processo “Medicamento quimioterápico” executado pela farmácia do hospital pediátrico.
Fonte: O Autor.

A Figura 16 apresenta as medidas de mitigação adotadas para os riscos encontrados, o novo cálculo de risco, e qual o risco residual encontrado.

Nesta etapa também foram identificados os processos que têm como base legal o legítimo interesse, que é definido como o interesse da empresa ou individuo para aquele tratamento de dados sem afetar os direitos dos titulares. Assim, foram identificados 46 processos que são calcados no legítimo interesse e que, por força das disposições da LGPD, exigem a elaboração de um LIA.

Para este relatório foi desenvolvido um modelo próprio, diante da ausência de definição da ANPD, até o presente momento sobre o modelo a ser utilizado para elaboração de um LIA. O modelo está reproduzido no Apêndice A deste trabalho.

A Figura 17 apresenta o LIA dos processos de gerenciamento de redes sociais e envio de e-mail pelo marketing do hospital pediátrico.

ANÁLISE DO LEGÍTIMO INTERESSE PARA TRATAMENTO DOS DADOS PESSOAIS – MARKETING – PROCESSOS DE GERENCIAMENTO DE REDES SOCIAIS E ENVIO DE E-MAIL MARKETING		
1. FINALIDADE LEGÍTIMA (ART. 10, CAPUT E INCISO I DA LGPD).		
ID.	**QUESTIONAMENTO/ORIENTAÇÕES**	**RESPOSTA**
1.	**QUAL É A FINALIDADE DO TRATAMENTO DOS DADOS PESSOAIS.** DETALHAR QUAL O OBJETIVO QUE SE PRETENDE ATINGIR COM O TRATAMENTO DOS DADOS PESSOAIS	O tratamento dos dados é realizado com a finalidade de verificar a qualidade do atendimento realizado no hospital bem como para atender as reclamações postadas pelos pacientes e/ou responsáveis nas redes sociais. Além disto o tratamento tambem é realizado para comunicação coorporativa através de e-mail marketing.
2.	**O TRATAMENTO É NECESSÁRIO PARA ATENDER UM OU MAIS OBJETIVOS ORGANIZACIONAIS?** SE O TRATAMENTO É NECESSÁRIO PARA ATINGIR UM OBJETIVO COMERCIAL LEGAL, É PROVÁVEL QUE SEJA LEGÍTIMO PARA OS FINS DESTA AVALIAÇÃO.	Sim, o tratamento é necessário para atingir um dos objetivos da organização, como a manutenção da qualidade do atendimento e da missão assistencial da organização, que demanda comunicação das atividades.

Figura 17 - LIA dos processos de gerenciamento de redes sociais e envio de e-mail pelo marketing.
Fonte: O Autor.

A Figura 17 demonstra o modelo de LIA utilizado para o programa implementado no hospital pediátrico, onde se denota a averiguação da finalidade do tratamento, qual sua necessidade e posterior averiguação de conformidade neste tratamento.

Os resultados sumarizados da Fase 2 são apresentados no Quadro 8.

Etapas	Resultados
1- Mapeamento de Processos	Com o mapeamento foi possível identificar 533 processos, possibilitando a formalização das atividades destes processos e a visualização dos riscos presentes nestas atividades, sendo realizado posteriormente o mapeamento do ciclo de vida dos dados.
2 - Identificação de Riscos	Nesta etapa, após o mapeamento acima, foi utilizada uma planilha identificadora de risco que deu para o hospital a capacidade de conhecer e gerir seus riscos.
3 - Mapeamento do Ciclo de Vida dos Dados	Identificado que 357 processos coletam dados de crianças e adolescentes, foi possível demonstrar a necessidade de maior rigor no

	tratamento dos dados coletados pelo hospital pediátrico e foi possível construir as recomendações de privacidade e os documentos do programa.
4 - Elaboração de Recomendações de Privacidade	Tendo havido a completa elaboração das etapas anteriores, foi analisado cada um dos processos que tratam dados pessoais para verificar se existe necessidade de adequação destes processos para cumprimento da LGPD, sendo formalizada cada recomendação para cada um destes processos.
5 - Criação de Políticas Internas	Foram criadas todas as políticas para implementação do programa de privacidade e proteção de dados bem como para o correto cumprimento da LGPD, permitindo o correto conhecimento e cumprimento das regras trazidas pela lei à organização.
6 - Elaboração do ROPA	Foram elaborados todos os registros de tratamento de dados, medida obrigatória perante a LGPD, e formalizado todo o ciclo de vida dos dados visualizado na etapa 3, o que dá gestão aos tratamentos realizados e permite uma correta individualização do risco.
7 - Elaboração dos RIPD e LIA	Nesta etapa foram criados os RIPD e LIA de modo a identificar, formalizar e gerir os riscos identificados na etapa 2, de modo a não só os geri-los, mas mitigá-los ou excluí-los

Quadro 8 – Resultados sumarizados da Fase 2.

Fonte: O Autor.

A realização completa desta fase permitiu construir uma base para a implementação do programa de privacidade e proteção de dados no hospital pediátrico porque pela primeira vez foi possível visualizar de maneira clara e perene todos os dados tratados, o que permite uma análise completa do ambiente e o desenvolvimento das etapas presentes na Fase 3.

4.2 3ª FASE: IMPLEMENTAÇÃO DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

Nesta fase foram implementadas as recomendações geradas e construídos controles necessários para aprimorar o cumprimento da LGPD pelo hospital pediátrico.

Esta fase é composta de 5 etapas: Treinamento e Conscientização de Colaboradores; Adequação de Processos; Gestão de *Cookies*; Criação de Fluxo de Atendimento aos Titulares; Criação do Controle de Risco e *Assessment* de Terceiros e Sistemas.

a) ETAPA 8: TREINAMENTO E CONSCIENTIZAÇÃO DE COLABORADORES

Nesta etapa iniciou-se o treinamento dos colaboradores do hospital pediátrico, bem como a conscientização geral do hospital, com a finalidade de orientá-los sobre o cumprimento das novas políticas implementadas, e sobre as determinações da LGPD e melhores práticas para seu cumprimento.

Foi desenvolvido um treinamento com duas aulas presenciais com duração de 2 horas especificamente desenhadas para treinar os colaboradores a respeito das questões trazidas pela LGPD.

Ressalta-se que, além do treinamento, foi desenvolvida uma cartilha para orientar o colaborador, conforme demonstrado na Figura 18.

Figura 18 –Cartilha para orientação dos colaboradores.

Fonte: O Autor.

Dos 2.024 colaboradores selecionados participaram 1.987, um percentual de presença de 98,17%. Por motivo de afastamento laboral, 37 colaboradores não participaram do treinamento.

Além dos treinamentos foi implementado no hospital pediátrico um sistema para simulação de *phishing,* de modo a verificar se os colaboradores estão seguindo a orientação de não clicarem em *links* encaminhados por e-mails não reconhecidos. A simulação é feita bimestralmente e todos os colaboradores que clicarem nestes *links* são encaminhados para um treinamento.

A Figura 19 exemplifica um modelo de *e-mail* reconhecido enviado como parte do treinamento no decorrer da implementação.

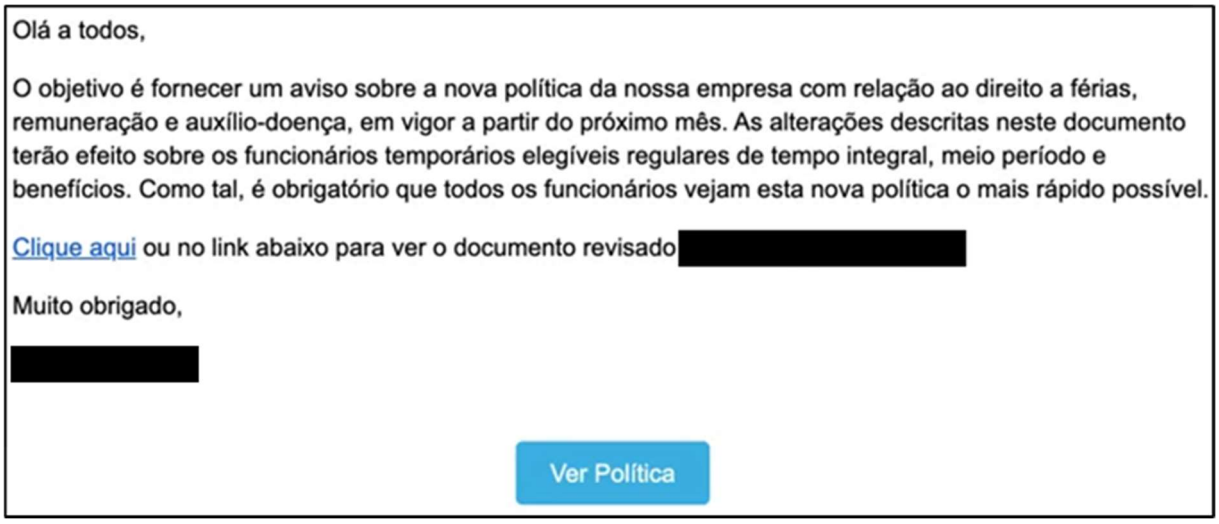


Figura 19 – Modelo de e-mail enviado para simulação de *phishing*.
Fonte: O Autor.

Por fim, nesta etapa foi construído um planejamento para comunicação constante com toda a equipe, através do envio de *e-mail marketing*, acerca de assuntos pertinentes à privacidade e proteção de dados, bem como dicas e orientações de conduta. Estas comunicações são realizadas semanalmente para todos os colaboradores do hospital pediátrico.

A Figura 20 exemplifica uma das comunicações encaminhadas.

Figura 20 – Comunicação enviada para os colaboradores do hospital pediátrico.

Fonte: O Autor.

b) ETAPA 9: ADEQUAÇÃO DOS PROCESSOS

Nesta etapa utilizou-se as recomendações de privacidade geradas na etapa 4 para adequar os processos mapeados no decorrer do desenvolvimento do programa. Para cada processo mapeado foi observado se há recomendações de adequação e, em última instância, se está passível de melhoria para ganho de efetividade.

Esta atividade foi realizada para os 533 processos mapeados e pode envolver mudança no corpo do processo, com supressão, alteração ou criação de atividades, a implementação de um sistema ou ainda a troca de sistema já utilizado.

De todos os processos mapeados, após a elaboração das recomendações da Etapa 4, foram realizadas adequações em 189 processos, sendo que tais processos foram objetos desta adequação por ter sido identificado uma oportunidade de melhoria no fluxo de processo ou ainda por haver, inerente ao processo, um descumprimento patente perante a LGPD.

Utilizando-se como exemplo o processo “exame não coberto” do setor do caixa, onde havia a prática manual e sem sistema de gestão, foi realizada a implementação de um sistema de envio de documentos eletrônicos para evitar atraso na cobrança e perda de tempo humano.

As Figuras 21 e 22 mostram as alterações realizadas.

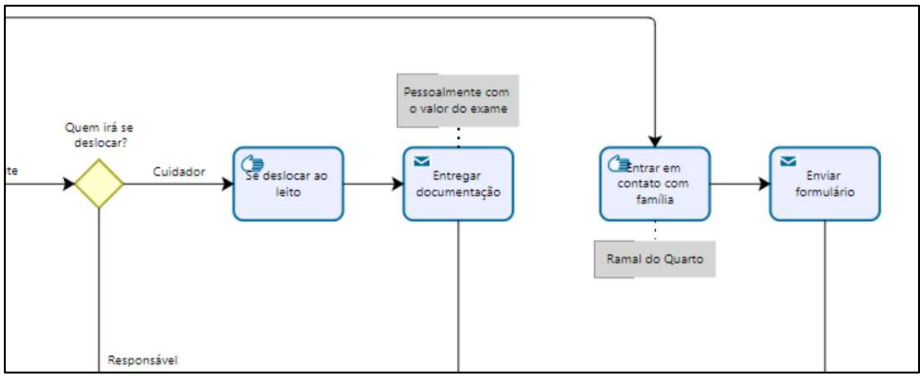


Figura 21 – Etapa processual antes da adequação a LGPD.

Fonte: O Autor.

A Figura 21 mostra a atividade realizada pelo colaborador do caixa do hospital pediátrico quando há algum exame não coberto pelo plano de saúde do paciente, sendo necessário o deslocamento do colaborador para o leito com a finalidade de averiguar a forma de pagamento do exame.

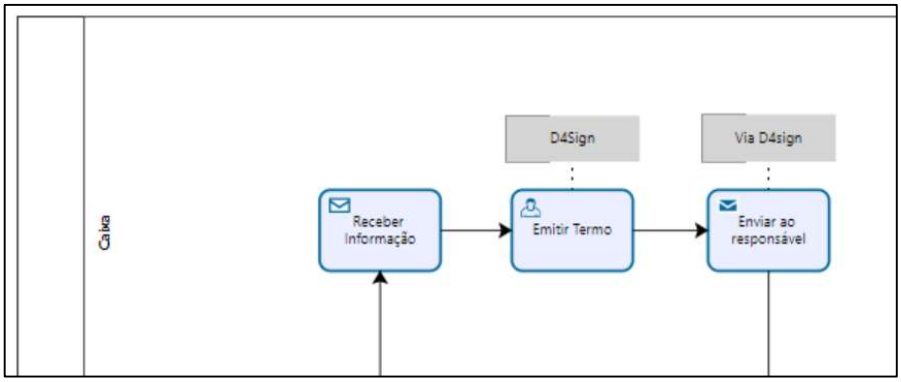


Figura 22 – Etapa processual após adequação a LGPD.

Fonte: O Autor.

Já na Figura 22, que representa o processo após a implementação da recomendação, é possível ver que com adoção de ferramenta tecnológica, uma forma de mitigar riscos de vazamento de dados, ante a ausência de coleta de documentação física, o processo foi simplificado sem a necessidade de deslocamento ao leito.

Com esta alteração foi possível obter, além da diminuição de risco, a simplificação que foi determinante para o ganho de eficiência deste processo, que passou a ter 17 atividades e não mais 31 como originalmente visualizado.

c) ETAPA 10: GESTÃO DE *COOKIES*

Após a realização da etapa 4 foi possível constatar que o hospital pediátrico detém um *site* de acesso público, onde são coletados *cookies* dos visitantes, sendo necessária a gestão destes *cookies*, que é classificado como um dado pessoal nos termos da LGPD (BRASIL, 2018).

Assim, foi construído um sistema de gestão destes dados coletados para possibilitar que o titular que visite a página do hospital pediátrico possa escolher se deseja que estes dados sejam coletados, especialmente no que atine aos *cookies* que não são essenciais ao funcionamento do *site.*

A recomendação de criação de um sistema de gestão de *cookies* está de acordo com a regulamentação da ANPD presente no guia orientativo "*Cookies* e Proteção de Dados Pessoais" (ANPD 2022).

A implementação foi realizada através de um programa específico para coleta e manutenção dos *logs* de cada usuário, implementado diretamente na página eletrônica do hospital pediátrico, e gerido diretamente pelo responsável pela privacidade no hospital.

A Figura 23 apresenta o resultado coletado diretamente do *site* do hospital pediátrico.

Figura 23 - Forma de coleta e gestão dos *cookies* do *site* do hospital pediátrico.

Fonte: O Autor.

d) ETAPA 11: CRIAÇÃO DE FLUXO DE ATENDIMENTO AOS TITULARES

A LGPD determina que os titulares de dados podem solicitar perante o hospital pediátrico os seguintes direitos: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados pessoais; portabilidade dos dados a outro fornecedor de serviço ou produto; informação sobre o compartilhamento de dados; informação sobre a possibilidade de não fornecer consentimento ou revogação do consentimento dado (BRASIL, 2018).

Para atendimento dessas solicitações foi construído um canal de atendimento aos titulares que se encontra em atividade e está vinculado ao endereço eletrônico do hospital e, através dele os titulares podem solicitar ao responsável quaisquer dos direitos expostos acima.

O canal foi criado através de sistema próprio e está apresentado na Figura 24.

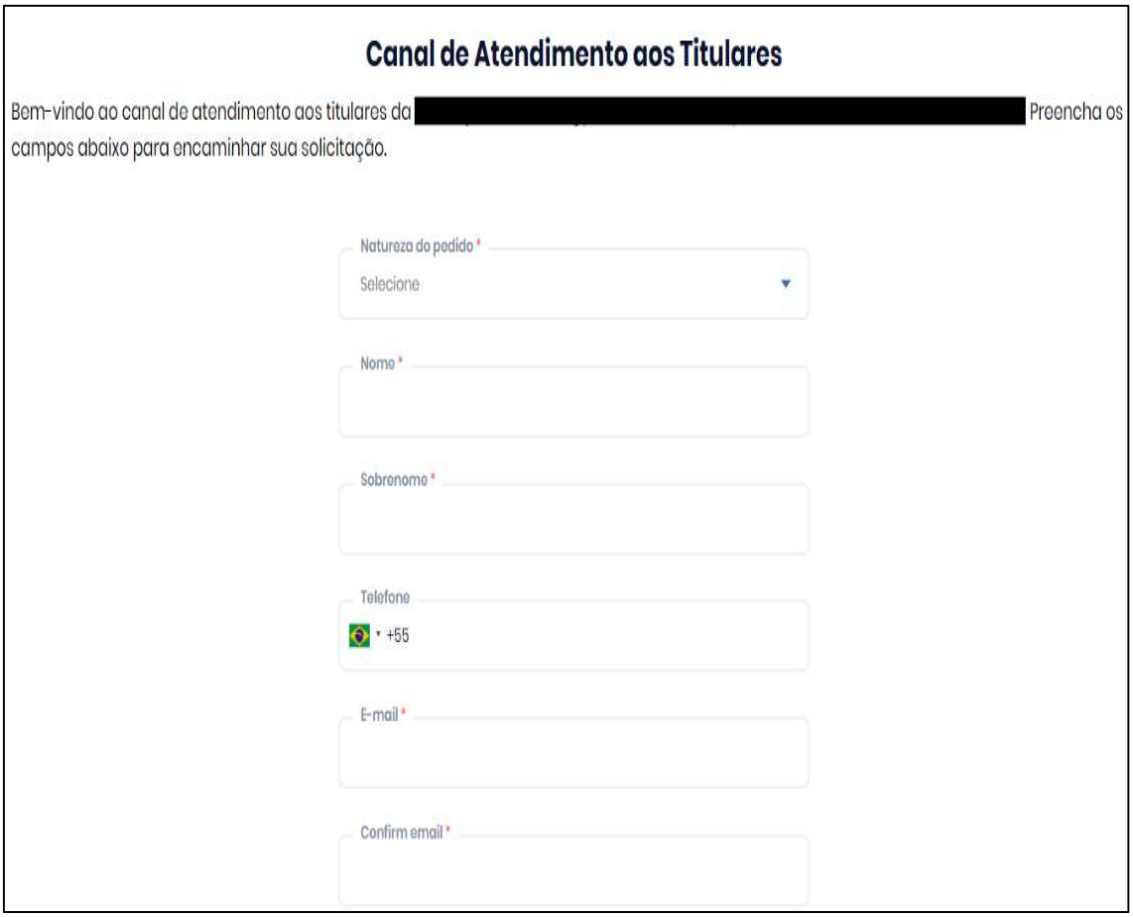


Figura 24 - Canal de Atendimento aos Titulares.

Fonte: O Autor.

Com a implementação deste canal foi possível criar um canal direto para atendimento das pessoas relacionadas ao hospital e que tiveram seus dados coletados, o que melhorou a celeridade de atendimento, inclusive da obtenção de cópia de prontuários e a forma do atendimento.

e) ETAPA 12: CRIAÇÃO DO CONTROLE DE RISCO

Identificados os riscos nas etapas anteriores, foi realizada uma análise de cada um dos riscos com base em uma análise quantitativa dos processos mapeados com a metodologia BPM, utilizando uma Matriz de Risco desenvolvida especificamente para o ambiente hospitalar.

O risco foi conceitualizado como a multiplicação da probabilidade da ocorrência pelo impacto observado no caso de ocorrência deste risco, conforme a equação 1.

$$Risco = Probabilidade * Impacto \ (1)$$

Por se tratar de riscos que podem acarretar o impacto a múltiplos indivíduos, decidiu-se que o impacto deveria ser calculado com base nestes múltiplos indivíduos atingidos, ou seja, para todo o risco é definido um impacto para os seguintes elementos que compõem a equação 2, desenvolvida com metodologia própria baseada em Martin; Santos e Dias Filho (2004).

Na equação 2 as siglas representam cada uma das formas de impactos possíveis dentro da equação, entre as suas diversas naturezas. Desta forma, *"Pa"* significa impacto aos pacientes; *"Cot"* impacto aos colaboradores do hospital; *"Ma"* impacto ao meio ambiente; *"Ah"* impacto ao ambiente do hospital; *"Ti"* impacto aos ativos de TI; *"Im"* impacto a imagem do hospital pediátrico; *"Fi"* impacto financeiro; e; *"Jre"* impacto jurídico ou regulatório.

Assim, a definição acima é expandida para significar o cálculo completo do risco compreendendo os agentes possivelmente impactados, conforme a equação 2.

$$Risco = Probabilidade * \frac{Impacto(Pa+Cot+Ma+Ah+Ti+Im+Fi+Jr\ )}{8} \ (2)$$

Quanto à valoração de cada item, eles foram identificados entre 1 e 5, sendo que 1 identifica “muito baixo” e 5 “muito alto”, com base na recomendação da ISO 27001 e da ISO 31000 (ABNT 2018 e 2021), conforme a Figura 25.

Figura 25 – Valoração do Risco.

Fonte: O Autor.

Utilizando a equação 2 para cálculo do risco, com a valoração adequada, chegou-se em cada um dos processos com valores entre 0 e 25. A Matriz de Risco com os respetivos valores é apresentada na Figura 26, criada com metodologia própria baseada em Martin; Santos e Dias Filho (2004).

Risco	**Probabilidade**				
Impacto	**1. Muito Baixo**	**2. Baixo**	**3. Moderado**	**4. Alto**	**5. Muito Alto**
5. Muito Alto	4,00 a 9,00	9,01 a 16,00	9,01 a 16,00	16,01 a 25,00	16,01 a 25,00
4. Alto	4,00 a 9,00	4,00 a 9,00	9,01 a 16,00	9,01 a 16,00	16,01 a 25,00
3. Médio	1,01 a 3,99	4,00 a 9,00	4,00 a 9,00	9,01 a 16,00	9,01 a 16,00
2. Baixo	1,01 a 3,99	1,01 a 3,99	4,00 a 9,00	4,00 a 9,00	9,01 a 16,00
1. Muito Baixo	0,01 a 1,00	1,01 a 3,99	1,01 a 3,99	4,00 a 9,00	4,00 a 9,00

Figura 26 – Matriz de Risco

Fonte: O Autor.

Apresenta-se na Figura 26 a Matriz de Risco para classificar cada um dos resultados obtidos com a equação 2. Assim, um risco entre 0,0 e 1,0 é classificado como muito baixo, destacado na figura na cor azul; entre 1,01 e 3,99 é classificado como baixo, destacado na figura na cor verde; entre 4,0 e 9,0 é classificado como médio, destacado na figura na cor amarela; entre 9,01 e 16,00 é classificado como

alto, destacado na figura na vermelho; e, acima de 16,0 classificado como muito alto, destacado na figura na cor preta.

Diante destes resultados, adotou-se as medidas apresentadas na Figura 27 para cada um dos riscos classificados, sendo que para riscos considerados muito baixos nenhuma medida é tomada.

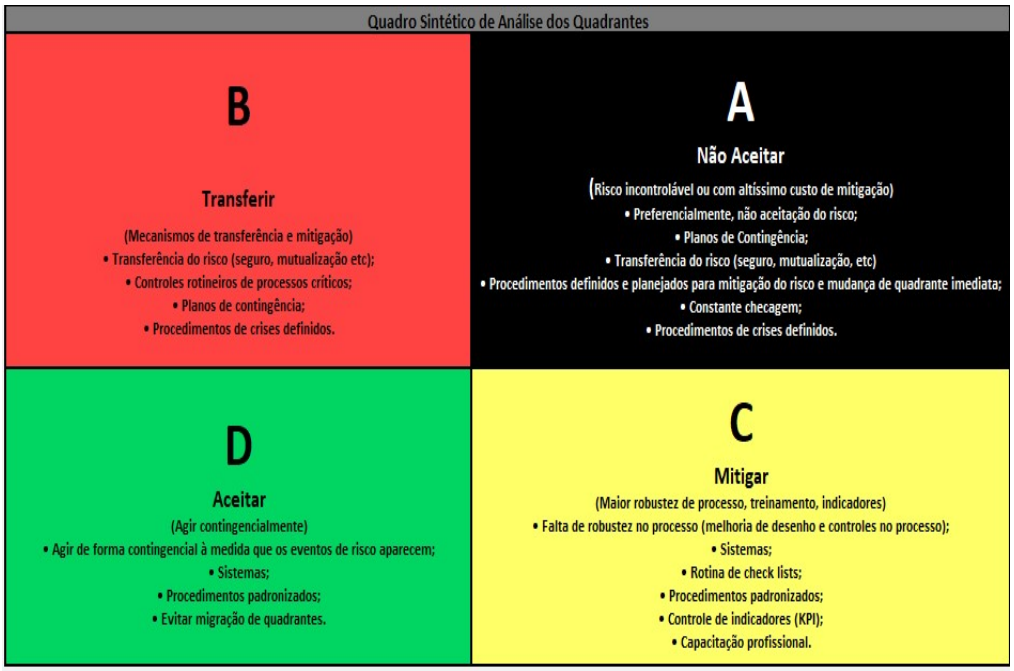


Figura 27 – Medidas tomadas em decorrência do risco.

Fonte: O Autor.

Como exemplo, utilizando o risco de TI, preencheu-se a equação 2 com os dados deste processo, chegando ao resultado presente na Figura 28.

Identificação do Risco				Perfil do Risco										
ID do Risco	Ativo	Categoria do Risco	Probabilidade	Impacto do Risco Corporativo									Nota Final do Risco	Rating Risco
				Pacientes	Cuidadores/ Terceiros	Meio Ambiente	Ambiente Hospitalar	TI	Imagem	Financeiro	Jurídico / Regulatório	Impacto Geral do Risco Corporativo		
R.1	MV	Risco de TI	3	5	2	0	3	3	4	3	4	3,458333333	10,375	Alto

Figura 28 – Exemplo de cálculo de risco.

Fonte: O Autor.

A Figura 28 demonstra na prática o uso das equações 1 e 2 que calculam o valor final de risco com base no impacto de cada um dos meios coorporativos e com base na probabilidade dada para este risco em especial. Neste exemplo, observa-se que este risco é classificado como alto, sendo adotado uma mitigação, constituída em controle eficiente de acesso ao sistema e um plano de contingência na eventualidade de concretização deste risco.

f) ETAPA 13: *ASSESSMENT* DE TERCEIROS E SISTEMAS

Como última etapa de implementação do programa de privacidade e proteção de dados foi iniciado o *assessment* de todos os parceiros do hospital pediátrico, seja ele um prestador ou um fornecedor de sistema.

Este *assessment* teve como finalidade entender qual o nível de maturidade do programa de privacidade e proteção de dados destes parceiros. Foram indagados todos os parceiros que tratam dados pessoais do hospital pediátrico, ou seja, os indivíduos, empresas ou não, que são operadores de dados e desta forma detém o dever de cuidado com os dados coletados. A medida visa mitigar a chance de um incidente em um parceiro que possa contaminar de maneira transversa o ambiente do hospital pediátrico, prejudicando-o.

O *assessment* é realizado através do envio de um formulário que deve ser respondido pelos parceiros de modo que seja explicado, e comprovado, quais as medidas tomadas no ambiente daquele parceiro. O formulário foi construído com metodologia própria e pode ser encontrado no Apêndice F deste trabalho.

As respostas são avaliadas em 4 níveis: “atende”, “atende parcialmente”, “não atende” e “não aplicável”. Este último nível é utilizado quando a questão não é aplicável para aquela troca de dados em questão. Para que seja considerado como aprovado, o parceiro deve atingir um nível mínimo de 70% de “atende” ou “atende parcialmente”.

No caso de não atingimento deste percentual, é dado um prazo para adequação do parceiro e, para cada resposta diferente de “atende” é gerado um plano de ação para que o parceiro possa se adequar.

Analisando os 764 parceiros, apenas 37% atingiram o valor mínimo estipulado, sendo criado um plano de ação específico. Atualmente os parceiros estão no período concedido para adequação e sendo acompanhados.

No Quadro 9 os resultados obtidos com a implementação da Fase 3 estão sumarizados.

Etapas	Resultados
8- Treinamento e Conscientização de Colaboradores	Com a realização do treinamento dos colaboradores foi possível melhorar as condutas praticadas na organização, de forma a mitigar riscos de tratamentos indevidos e aprimorar o cumprimento da LGPD no hospital pediátrico. A implementação de conscientização constante permitiu ser ágil na comunicação organizacional e reforçar as orientações necessárias.
9 - Adequação dos Processos	Com a adequação dos processos foi possível não só corrigir inadequações relacionadas ao cumprimento da LGPD como também permitir uma revisão abrangente dos processos identificados com melhoria de eficiência e segurança aos envolvidos, inclusive pacientes.
10 – Gestão de *Cookies*	Foi implementada uma metodologia de gestão dos *cookies* coletados no site do hospital pediátrico e nos sistemas web utilizados, permitindo não só a gestão do consentimento para coleta destes dados, mas o cumprimento integral da determinação da ANPD sobre o tema.
11 – Criação de Fluxo de Atendimento aos Titulares	Tendo havido a implementação do canal de atendimento aos titulares, foi possível construir um vínculo direto entre o indivíduo que teve seu dado coletado e o hospital pediátrico, passando este canal a assumir demandas outrora pulverizadas na organização, como a entrega de prontuários, com ganho de gestão e segurança.
12 - Criação do Controle de Risco	Criada uma metodologia de risco, através do uso de planilha eletrônica, para conhecer, identificar e gerir corretamente os riscos organizacionais, sendo possível a criação e acompanhamento de planos de mitigação destes riscos, uma medida também imposta pela LGPD.
13 - *Assessment* de Terceiros e Sistemas	Realizado um *assessment* de terceiros e sistemas da organização para averiguar o grau de maturidade destes participantes dos processos do hospital, o que possibilitou a identificação dos não aderentes e a implementação de plano de melhoria para cada um destes identificados.

Quadro 9 – Resultados sumarizados da Fase 3

Fonte: O Autor.

No Quadro 9 os resultados da fase 3 estão sumarizados, focando no treinamento de colaboradores, agora prática implementada, na melhoria dos processos do hospital pediátrico, adequados à LGPD e ao controle de riscos, sejam internos ou em terceiros.

4.3 4ª FASE: CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Nesta fase foram implementadas as recomendações geradas e construídos os controles necessários para que o objetivo deste trabalho fosse atingido ao desenvolver e implementar um programa de privacidade e proteção de dados em um hospital pediátrico utilizando-se do *Business Process Management* para apoiar o cumprimento da LGPD.

Apresenta-se no Quadro 10 os itens alterados com a implementação do programa.

Atividades	**Antes da Implementação do Programa**	**Cumprimento da LGPD, após a Implementação do Programa**
Gestão de Processos	Os processos não eram mapeados e apresentavam inconsistências entre as equipes do hospital. Vários processos careciam de padronização e, por este motivo eram realizados de maneiras diferentes pelos colaboradores, comprometendo a qualidade da atividade.	Com o mapeamento foi possível identificar 533 processos, possibilitando a formalização das atividades e a visualização dos riscos presentes. Foi melhorada a relação entre as equipes, com previsibilidade e gestão das atividades, possibilitando a melhoria dos processos mapeados.
Gestão de Riscos	Não havia gestão de riscos.	Foi criada uma metodologia para gestão de riscos que abrangeu todos os processos mapeados no hospital pediátrico, com a qualificação dos riscos de cada processo e de cada área. Houve a criação e acompanhamento de planos de mitigação destes de riscos para todas as áreas do hospital.

Gestão de Dados	Não havia gestão dos dados.	Foram mapeados todos os dados coletados pelo hospital pediátrico com a identificação dos tipos de dados, formalizando as operações de coleta e tratamento através de 357 ROPAs, o que possibilitou a elaboração dos relatórios RIPD e LIA.
Privacy by design	Não havia um programa ou gestão de questões de privacidade e proteção de dados.	Foram adequados todos os processos da organização que tratam dados pessoais. Foi construído um procedimento para que todo processo ou produto criado pela organização passe por uma análise prévia quanto as questões de proteção de dados.
Estruturação e formalização	Não havia políticas abrangentes de segurança da informação e proteção de dados.	Foram criadas todas as políticas para implementação do programa de privacidade e proteção de dados e para o correto cumprimento da LGPD, havendo uma melhoria também no tocante a segurança da informação.
Conscientização e Treinamento	Não havia treinamento sobre questões de proteção de dados ou de segurança da informação.	Foi criado um plano de treinamento para todos os colaboradores, sendo possível melhorar as condutas praticadas na organização, diminuindo-se os riscos de tratamento e aprimorando o cumprimento da LGPD no hospital pediátrico.
Atendimento aos titulares	Não havia fluxo para atendimento de titulares clientes, pacientes ou colaboradores.	A implementação do canal de atendimento aos titulares possibilitou construir um vínculo direto entre o indivíduo que teve seu dado coletado e o hospital pediátrico, passando este canal a assumir demandas outrora pulverizadas na organização, como a entrega de prontuários, com ganho de gestão e segurança.
Adequação a legislações de dados	O hospital não tinha aderência à LGPD, vez que não tinha mapeamento de dados e processos, inexistia políticas adequadas e havia diversos descumprimentos da legislação.	Após o mapeamento dos dados, dos treinamentos realizados e da adequação dos processos identificados, o hospital pediátrico pode ser considerado como aderente à LGPD.
Gestão de Terceiros e Parceiros	Não havia gestão de terceiros e parceiros.	Foi criado um *assessment* de terceiros e parceiros para averiguar o grau de maturidade perante a LGPD destes terceiros com a finalidade de criar um plano de adequação e acompanhamento individualizado.

Procedimento para contratação de sistemas	Os sistemas eram adquiridos e implementados sem uma correta análise quanto a questões de segurança e proteção de dados.	Foi criado um processo para aquisição de sistemas onde há uma análise prévia quanto aos requisitos relacionados à segurança da informação e proteção de dados.

Quadro 10 – Quadro comparativo no ambiente do hospital pediátrico.

Fonte: O Autor

Com base na comparação apresentada no Quadro 10, nota-se que mudanças significativas foram realizadas no hospital com a implementação do programa, o que significou em alterações, que levaram a organização à aderência à LGPD.

A implementação do programa permitiu que fosse construída uma gestão eficiente das atividades dos colaboradores do hospital pediátrico que trouxe melhoria além da extensão do programa de proteção de dados pretendido. A partir do momento da implementação de uma metodologia BPM houve uma melhoria substancial à qualidade das atividades do hospital e a criação de gestão antes inexistente.

Após a conscientização, construção documental e adoção das recomendações para resolução das lacunas encontradas foi possível aprimorar o ambiente de proteção de dados da organização e, como consequência indireta, melhorar os processos do hospital pediátrico com ganho operacional e de segurança ao paciente.

Do ponto de vista da gestão de risco houve uma sensível melhora na metodologia utilizada na organização, de uma ausência quase completa de análise dos riscos de proteção de dados e de segurança da informação para uma organização que mapeou e criou controles e ações perante os riscos identificados no desenvolvimento e implementação do programa.

Além disto, a criação de um procedimento revisor de processos, gestores e sistemas, todos alinhados com a priorização da proteção de dados, melhorou o ambiente organizacional, sendo determinante para a formação do programa de proteção de dados.

A partir da implementação do programa foi possível identificar, atender e abordar os titulares de dados relacionados aos dados tratados pelo hospital pediátrico, o que melhorou qualidade do atendimento dos titulares e dos demais clientes do hospital.

Os Relatório de Impacto a Proteção de Dados (RIPD) e o Relatório de Legitimo Interesse (LIA) permitiram a visibilidade dos tratamentos de dados considerados de risco ou ainda que tem como base o legítimo interesse. Analisando os resultados obtidos foi possível averiguar a vantagem de implementação do programa de proteção de dados para toda a organização.

Os resultados obtidos com a implementação do programa corroboram com os trabalhos de Aragão e Schiocchet (2021); Hawryliszyn; Coelho e Barja (2021); Agostinelli et al (2019); Calazans; Kosloski e Guimarães (2016), que recomendaram o desenvolvimento e aplicação de um programa de privacidade e proteção de dados baseado no mapeamento de processos e de dados, como alternativa frente as dificuldades apresentadas pela Norma ISO 27701 e o COBIT quando aplicados em ambiente de hospital pediátrico. Os resultados corroboram também com o resultado do questionário que validou a proposta de desenvolvimento do programa de privacidade e proteção de dados.

Resultante do desenvolvimento e da implementação do programa foi criado um Guia para apoiar hospitais pediátricos e outras organizações da área da saúde a cumprirem com a LGPD no seu ambiente organizacional. O Guia é composto por três fases e pode ser encontrado no Apêndice G, deste trabalho:

- 1ª Fase: Preparação da Implementação, composta pelas etapas de Identificar e mapear processos da organização, identificar e mapear dados tratados na organização, identificar e gerir riscos, elaborar e formalizar o RIPD e LIA, e, elaborar políticas de segurança da informação e proteção de dados.
- 2ª Fase: Implementação do Programa, composta pelas etapas de treinamento e conscientização, adequação de processos, criação da gestão de *cookies*, criação do fluxo de atendimento aos titulares, indicação do DPO, e, *Assessment* de terceiro e sistemas.
- 3ª Fase: Pós-implementação e Avaliação, onde se construí um ciclo de revisão e reanálise de todo o ambiente da organização, havendo a nova análise a cada alteração de processo, ou ainda a cada 12 meses, para um acompanhamento cuidadoso dos riscos encontrados.

5 CONCLUSÕES

A privacidade e proteção de dados no ambiente de um hospital pediátrico é complexa e a implementação de um programa nestes moldes passa por dificuldades de execução, ante as próprias características deste ambiente e dos dados coletados e tratados. No entanto, apesar desta complexidade, o hospital pediátrico deve cumprir adequadamente os requisitos trazidos pela Lei. No caso deste trabalho este cumprimento se deu pelo desenvolvimento e implementação de um programa de privacidade e proteção de dados baseado na metodologia BPM.

A revisão bibliográfica e o levantamento documental permitiram levantar características do ambiente pediátrico e de sua relação com a proteção de dados e a questão da privacidade em uma organização hospitalar voltada ao atendimento de crianças e adolescentes. Foi possível identificar a importância da utilização da metodologia BPM neste hospital, vez que o mapeamento de processos é o ponto inicial para um bom entendimento do ambiente organizacional e do mapeamento sistemático dos dados coletados e tratados pelo hospital pediátrico. O mapeamento realizado possibilitou obter informações que identificassem o risco envolvido nestes processos e coleta de dados, risco este relacionado a proteção de dados e segurança da informação, o que permitiu a construção de uma metodologia para mitigação e gestão perene destes riscos.

O hospital pediátrico conta agora com políticas e processos voltados para a proteção de dados e correta gestão de dados dos titulares relacionados a esta organização. Houve ainda uma criação e melhoria da gestão da segurança da informação com o patrocínio de mudanças de regras e costumes, embasados pelos treinamentos realizados. Houve um aprimoramento no cumprimento da LGPD, com a formalização de documentos exigidos por esta lei, como o ROPA, RIPD, LIA e o correto adereçamento do atendimento aos titulares e gestão dos terceiros.

O objetivo de pesquisa do trabalho foi atingido, uma vez que o programa implementado no hospital pediátrico através do uso do Business Process Management garantiu o cumprimento da LGPD, como pode ser observado nas comparações apresentadas no Quadro 10, antes da implementação e após a implementação do programa. A questão de pesquisa por sua vez foi respondida de maneira afirmativa porque com o desenvolvimento do programa foi possível identificar

que este desenvolvimento deve ser amparado por um mapeamento de processos e dados, na gestão de risco e na utilização dos documentos necessários à conformidade como o RIPD, o LIA e o ROPA, corroborando com a literatura pesquisada e com a validação do programa por parte dos profissionais da área de segurança respondentes do questionário aplicado.

A relevância deste trabalho reside em ter sido aplicado em uma área tão importante como a área da saúde e em hospitais pediátricos que tratam de pacientes vulneráveis tanto fisicamente, psicologicamente e emocionalmente que necessitam ter as suas informações extremamente protegidas. A relevância pode ser comprovada ao se verificar os resultados do questionário confirmando a importância do desenvolvimento e implantação do programa e da revisão da literatura que apontou a importância em desenvolver um programa nos moldes desenvolvido neste trabalho. O Guia para apoiar a implementação desenvolvido a partir do programa tem como objetivo orientar e apoiar a implementação do programa em outros hospitais pediátricos e instituições da área da saúde, considerando as características de cada instituição.

Desta forma, procurou-se mostrar neste trabalho que é possível construir um programa de privacidade e proteção de dados em um hospital pediátrico que seja passível de cumprimento, perene e que atenda de um lado os rigores da LGPD e do outro as particularidades das informações hospitalares de crianças e adolescentes. A realização do trabalho procurou mostrar também que a aplicação prática de um programa de privacidade e proteção de dados, além de mitigar riscos regulatórios, cria um diferencial estratégico e negocial para a organização.

As contribuições deste trabalho são as seguintes:

- Para a pesquisa acadêmica: foi desbravado um assunto ainda pouco estudado, e que pode servir de direcionamento para novas pesquisas relacionadas ao tema do cumprimento da LGPD em hospitais pediátricos e em outras organizações da área da saúde.

- Para hospitais e organizações da área da saúde: a construção de um ambiente onde a coleta de dados é feita com qualidade. A melhoria da segurança da informação e da proteção dos dados reduz tanto o risco de vazamento de dados coletados quanto o risco de qualquer penalidade ou condenação judicial.

- Para os pacientes, melhoria na gestão de seus dados decorrente da implementação do programa de privacidade e proteção de dados, visto que há ampliação do sigilo e proteção de seus dados, evitando que sejam utilizados para fraudes e outras atividades ilícitas, além de salvaguardar direitos e garantias individuais do paciente ao melhorar o atendimento assistencial.

Considera-se como limitação do trabalho a impossibilidade de comparar os resultados obtidos com os de outro hospital pediátrico ou com a literatura levantada porque o programa implementado contempla as características únicas dos processos e dados do hospital pediátrico selecionado. Além disso, destaca-se que não foi encontrado outro hospital pediátrico que tenha implementado um programa com as características semelhantes ao desenvolvido neste trabalho.

Por fim, também se considera como limitação a dificuldade de extração dos dados utilizados para pesquisa no hospital pediátrico, ante ao fato de tais dados não estarem estruturados em um banco de dados único.

Indica-se como continuidade da pesquisa a aplicação do modelo em outras instituições hospitalares, uma vez que poderá se validar o modelo em outras organizações, pediátricas ou não e também, a inclusão de outra metodologia no programa, como o NIST, um padrão de segurança criado pelo *National Institute of Standards and Technology*, apontado pelos respondentes do questionário que validaram o programa.

Os estudos apresentados neste trabalho não têm a pretensão de esgotar o assunto, pelo contrário, buscou-se contribuir para o processo de proteção de dados em ambientes hospitalares.

REFERÊNCIAS BIBLIOGRÁFICAS

ABHISHEK, P. P., NEELIKA C., **A review into the evolution of HIPAA in response to evolving technological environments**, Journal of Journal of Cybersecurity and Information Management, v. 4, n. 2, p. 5-15. 2020. Doi: 10.54216/JCIM.040201.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2022.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – código de prática para controles de segurança da informação – Requisitos. ABNT, 2022.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701 – Tecnologia da informação – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. ABNT, 2019.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 31000 – Gestão de Risco – Princípios e Diretrizes. ABNT, 2018.

ANDELLINI, M.; FERNANDEZ RIESGO, S.; MOROLLI, F; RITROVATO, M.; COSOLI, P.; PETRUZZELLIS, S.; ROSSO, N. **Experimental application of Business Process Management technology to manage clinical pathways: a pediatric kidney transplantation follow up case**. BMC Med Inform Decis Mak, v. 17. n. 2, p. 151-160. 2017. Doi: 10.1186/s12911-017-0546-x.

AHOUANMENOU, S., VAN LOOY, A., POELS, G., **Information security and privacy in hospitals: a literature mapping and review of research gaps**. Inform Health Soc Care. v. 48, n. 1, p. 30-46. 2023. Doi: 10.1080/17538157.2022.2049274.

ALBUQUERQUE, A., **Disclosure de incidentes de segurança do paciente sob a ótica do Direito do Paciente**. Cadernos Ibero-Americanos de Direito Sanitário, [S. l.], v. 11, n. 3, p. 70–90, 2022. Doi: 10.17566/ciads.v11i3.925. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/925. Acesso em: 20 maio. 2023.

ALBUQUERQUE, A. As vulnerabilidades das instituições de saúde e o cyber risco . Disponível em https://medicinasa.com.br/cyber-risco-saude/#:~:text=Cerca%20de%2050%25%20dos%20incidentes,pagamento%20de%20um%20%E2%80%9Cresgate%E2%80%9D, Acessado em 23 de maio de 2023 às 10:56.

ÁLVAREZ DÍAZ, J. A.; DURO, E. A.; GUBERT I. C., **Between Huxley and Orwell: Big Data and Health**. Revista Latina de Sociologia. v. 8, n. 2, p. 23-33, 2018. Doi: 10.17979/relaso.2018.8.2.2951.

ANDERSON, T; **Governança Digital**. Senac. São Paulo, 2022.
ANPD – Autoridade Nacional de Proteção de Dados. Base Jurídica. Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica, 2023, acessado em 23 de maio de 2023 às 11:03.

ANPD – Autoridade Nacional de Proteção de Dados. Guia Orientativo de *Cookies*. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf, 2022, acessado em 04 de outubro de 2023 às 20:20.

ANPD - Autoridade Nacional de Proteção de Dados. Competência da ANPD. Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/competencias-da-anpd. 2023. Acessado em 23 de maio de 2023 às 11:04.

ANPD - Autoridade Nacional de Proteção de Dados. Relatório de Impacto a Proteção de Dados Pessoais. Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. 2023. Acessado em 23 de maio de 2023 às 11:05.

ANPD - Autoridade Nacional de Proteção de Dados. Guia orientativo: Hipóteses legais de tratamento de dados pessoais legítimo interesse. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse. 2024. Acessado em 27 de abril de 2024 às 17:11.

ANPD - Autoridade Nacional de Proteção de Dados. RESOLUÇÃO CD/ANPD Nº 8 - Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD). 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-8-de-5-de-setembro-de-2023-508638337. Acessado em 12 de maio de 2024 às 07:20.

ANPD - Autoridade Nacional de Proteção de Dados. RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. ANPD, 2022.

ANPD - Autoridade Nacional de Proteção de Dados - RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023 - Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. ANPD, 2023.

ABPMP, Association of Business Process Management Professionals. **Guia para o Gerenciamento de Processos de Negócio Corpo Comum de Conhecimento**. São Paulo- SP: ABPMP, 2018. Disponível em https://www.abpmp-br.org/educacao/bpm-cbok/ acessado em 21 de maio de 2023.

ABRAHAM, A., CHATTERJEE, D., SIMS, R.R. **Muddling through cybersecurity: Insights from the U.S. healthcare industry**. Business Horizons. v. 62, n. 4, p. 539-548, 2019. Doi: 10.1016/j.bushor.2019.03.010.

AGOSTINELLI, S., MAGGI, F; MARELLA, A; SAPIO, F., **Achieving GDPR compliance of BPMN process models**. In International Conference on Advanced Information Systems Engineering. Springer, p. 10–22, 2019.

ÁLVAREZ DÍAZ, J. A., DURO, E. A., GUBERT I. C., MARTINEZ C. A. C., SOTOMAYOR, M. A., LÓPEZ L., DURO A., MOYA, R. N., SOROKIN, P. **Entre Huxley y Orwell: Big Data y salud.** Rev Lat Sociol. v. 8, n. 2, p. 23-33, 2018. Doi: 10.17979/relaso.2018.8.2.2951.

ARAGÃO, S. M. de; SCHIOCCHET, T. **Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde**. Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, [S. l.], v. 14, n. 3, p. 693-708, 2020. Doi: 10.29397/reciis.v14i3.2012.

ARGAW, S.T.; et al. **Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks.** BMC Med Inform Decis Mak v. 20, n.1, p. 146-156, 2020. Doi: 10.1186/s12911-020-01161-7.

ALODAYNAN, A. M. e ALANAZI, A. A., **A survey of cybersecurity vulnerabilities in healthcare systems**. International Journal of Advanced and Applied Sciences, v. 8, n. 12, p. 48-55, 2021. Doi: 10.21833/ijaas.2021.12.007.

BARRETO JUNIOR., I. F., **Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells**. In: DE LUCCA, N.; SIMÃO FILHO, A., DE LIMA, C. R. P.. Direito & Internet III: Marco Civil da Internet. 1ed. São Paulo: Quartier Latin, v. 2, p. 100-127, 2015.

BASTOS, Celso Ribeiro. **Curso de Direito Constitucional**, 17 ed. São Paulo: Saraiva, 1989.

BERG, M. **Implementing information systems in Healthcare organisations: Myths and challenges**. International Journal of Medical Informatics, Volume 64, Issue 2, p 145-156, 2001.

BOLIVAR, ANALLUZA ; MONACO, G. F. C. (Org.) . **LGPD NA SAÚDE**. 1. ed. São Paulo: Revista dos Tribunais, v. 1, p. 431, 2020.

BOWLBY, J., **Apego e perda, Vol. 2. Separação: angústia e raiva,** 3ª ed. São Paulo: Martins Fontes. 1998 (Trabalho original publicado em 1973).

BOTELHO, M. C., & CAMARGO, E. P. do A., **A aplicação da Lei Geral de Proteção de Dados na saúde**. Revista De Direito Sanitário, 21, e0021. 2021. Doi: 10.11606/issn.2316-9044.rdisan.2021.168023.

BPM CBOK. **Guia para o Gerenciamento de Processos de Negócio** – Corpo Comum de Conhecimento. ABPMP CBOK V3.0, 2014.

BRANDEIS, L. D., e WARREN, S. D. **The Right of Privacy**. Harvard Law Review, Vol. 4, n. 5, p. 193-220, 1890.

BRASIL. LEI Nº 8.069, DE 13 DE JULHO DE 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília. DF. Diário Oficial da União, 1990.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília. DF. Diário Oficial da União, 2018.

BURKART, D., VINCENZI V., **Proteção de dados e o estudo da LGPD**. 2021. Disponível em: <http://hdl.handle.net/11449/204091>. Acessado em 17/05/2023 às 18:48.

CALAZANS, A., KOSLOSKI, R., e GUIMARAES, F. **Proposta de modelo de medições para contratação do gerenciamento de processo de negócio (*Business Process Management* - BPM).** Journal of Information Systems and Technology Management. n. 13, p. 275-300. 2016. Doi: 10.4301/S1807-17752016000200007.

CAPPELLETTI, M., **O que é: Guia de Implementação**. 2018. Disponível em: URL. https://marcelocappelletti.com.br/glossario/o-que-e-guia-de-implementacao/. Acesso em: 03 de março de 2024.

CHINTHAPALLI K., **The hackers holding hospitals to ransom.** BMJ; n. 357: j2214, 2017 Doi:10.1136/bmj.j2214.

COSTA, M. M., **A era da vigilância no ciberespaço e os impactos da nova lei geral de proteção de dados pessoais no brasil: reflexos no direito à privacidade**. 2018. Monografia (Trabalho de Conclusão do Curso de Graduação em Direito – Faculdade de Direito da Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: https://pantheon.ufrj.br/handle/11422/8252. Acesso em: 20 maio de 2023 às 17:33.

COVENTRY, L., BRANLEY, B., **Cybersecurity in healthcare: A narrative review of trends, threats and ways forward**. Maturitas, v. 113, n. 1, p. 48-52. 2018. Doi: 10.1016/j.maturitas.2018.04.008.

DE HAES, S.; VAN GREMBERGEN, W.; JOSHI, A.; HUYGH, T., **COBIT as a *Framework* for Enterprise Governance of IT**. In International Conference on Advanced Information Systems Engineering. Springer, p. 125-162, 2020.

DONEDA, D., **Considerações iniciais sobre os bancos de dados informatizados e o direito a privacidade à privacidade**, 2000. Problemas de direito civil-constitucional. Rio de Janeiro: Renovar. Fl. 111, 136.

DONEDA, D., **Da Privacidade à proteção de Dados Pessoais**, Rio de Janeiro, Renovas, 2006, p. 8.

FERNANDES, A. A.; DINIZ, J. L.; ABREU, V., F.; et al. **Governança Digital 4.0**. Brasport. Rio de Janeiro, 2019.

FERRAZ JÚNIOR, T. S. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Revista Da Faculdade De Direito, Universidade De São Paulo, v. 88, p. 439-459. 1993. Disponível em <http://www.revistas.usp.br/rfdusp/article/viewFile/67231/69841>. Acesso em 23 de maio de 2023 às 09:30.

FERREIRA, G. S. A.; SILVA, U. R.; COSTA, A. L.; PÁDUA, S. I. D. d. D. **The promotion of BPM and lean in the health sector: main results**, Business Process Management Journal, v. 24, n. 2, p. 400-424. 2018. Doi: 10.1108/BPMJ-06-2016-0115.

FINKELSTEIN, M. E.; FINKELSTEIN, C. **Privacidade e lei geral de proteção de dados pessoais**. Revista de Direito Brasileiro. v. 23, n. 9, p. 284-301, 2019. Doi: 10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343.

GATTO, D., **Sistema Especialista no Apoio à Classificação de Criticidade De Versão De Software**, 2020. Dissertação de Mestrado – Universidade Nove de Julho.

GIL, A. C., **Métodos e Técnicas de Pesquisa Social**. 6ª Edição, São Paulo: Atlas, 2008.

GOSTIN, L.; NASS, S. **Reforming the HIPAA Privacy Rule: Safeguarding Privacy and Promoting Research**. JAMA : the journal of the American Medical Association. 301, p. 1373-5, 2009. Doi: 10.1001/jama.2009.424.

GRECO FILHO, V. **Tutela Constitucional das liberdades**, São Paulo: Saraiva, 1989.

GREGORI, M. S., **Os Impactos da Lei Geral de Proteção de Dados Pessoais na Saúde Suplementar.** Revista de Direito do Consumidor, São Paulo, v. 127, p. 171-196, 2020. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1268/1189. Acesso em: 23 maio. 2023 às 11:18.

GUERRA, S. C. S., **O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado**. Rio de Janeiro: Ed. América Jurídica. 2004, p. 37.

GUIMARÃES, G. P., DELIA, I. M., STOCCO, T., & AMARAL, C. S. T., **Transformação digital no setor de healthcare**. Brazilian Journal of Health Review, v. 6, n. 2, p. 5570–5583. 2023. Doi: 10.34119/bjhrv6n2-088.

HAWRYLISZYN, L. O., COELHO, N. G. S. C., & BARJA, P. R., **LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): O DESAFIO DE SUA IMPLANTAÇÃO PARA A SAÚDE.** Revista Univap, v. 27, n. 54, 2021. Doi: 10.18066/revistaunivap.v27i54.2589.

ICO, **Records of processing and lawful basis**. 2022. Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-of-processing-and-lawful-basis/ Acesso em 10 de outubro de 2023 às 19:58.

ISACA. **COBIT 2019 *Framework*: Governance and Management Objectives**. [S.l.:s.n.], 2019.

JÄNTTI, M; CATER-STEEL, **A. Proactive Management of IT Operations to Improve IT Services**. JISTEM-Journal of Information Systems and Technology Management, v. 14, n. 2, p. 191-218, 2017.

JESUS, D.C., **Proposta de um projeto de conformidade a partir das práticas da ISO 27701 para implementação de um programa compliance de proteção de dados à luz da LGPD na Universidade de Rio Verde**; Trabalho de Conclusão do Curso. Universidade do Vale do Rio dos Sinos; 2022.

KOCHE, J. C., **Fundamentos de Metodologia Científica. Petrópolis**: Vozes, 2003.

KÓS, M. V. M. M. d., **A Lei Geral de Proteção de Dados Aplicada à Saúde: O Impacto da Adequação da Lei em Instituições Brasileiras.** 2021. Dissertação de Mestrado – Universidade do Porto – Faculdade de Economia.

KOSTALOVA, J.; TETREVOVA, L.; SVEDIK, J., **Support of Project Management Methods by Project Management Information System**, Procedia - Social and Behavioral Sciences, Pardubice, Czech Republic v. 210 p. 96-104, 2015, Doi: 10.1016/j.sbspro.2015.11.333.

LAPÃO, L., **Organizational Challenges and Barriers to Implementing IT Governance in a Hospital**. Electronic Journal of Information Systems Evaluation. 2021.

LEONARDI, M., **Tutela e privacidade na internet**. São Paulo: Saraiva. 2011. p. 52.

MARTIN, N.C.; SANTOS, L.R.; DIAS FILHO, J.M. **Governança Empresarial, Riscos e Controles Internos: A Emergência de um Novo Modelo de Controladoria**. Revista Contabilidade & Finanças USP, São Paulo, n. 34, p. 7-22, janeiro/abril 2004.

MENDES, L. S. **Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental**. 2ª. tiragem. São Paulo: Saraiva, 2019.

MORAES, A., **Direito constitucional**. 30. ed., São Paulo: Atlas. 2014. p. 81.

NACHROWI, E.; NURHADRYANI, Y.; SUKOCO, H. **Evaluation of governance and management of information technology services using cobit 2019 and itil 4**. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), v. 4, n. 4, p. 764 – 774, Aug. 2020.

NEVES, D. L. F.; LOPES , T. S. DE A.; PAVANI, G. C.; SALES, R. M., **A segurança da informação de encontro às conformidades da LGPD**. Revista Processando o Saber, v. 13, p. 186-198, 2021.

NETHERCOTT S., **A concept for all the family: family centred care, a concept analysis**. Professional Nurse. v. 8, n. 12. p. 794–797. 1993.

NUNES, P., ANTUNES, M., SILVA, C. **Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions**. Procedia Computer Science, v. 181, p. 173-181, 2021. Doi: 10.1016/j.procs.2021.01.118.

OLIVEIRA, A. P. de. et al. **A lei geral de proteção de dados brasileira na prática empresarial**. Revista Jurídica da Escola Superior de Advocacia da OAB-PR, Curitiba, v. 4, n. 1, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wpcontent/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 24 jan. 2023, às 18:37.

OLIVEIRA, D, **Sistemas, Organização e Métodos e Uma Abordagem Gerencial**. 18ª ed. São Paulo: Atlas, p. 480, 2009.

ONU - Assembleia Geral da Nações Unidas, **Declaração Universal dos Direitos Humanos** (217 [III] A). Paris. 1948.

PASSO, MARIA Z. L. B. **Porque a Área a Saúde Precisa se Preocupar com a Proteção de Dados Pessoais**. RJLB, v. 8, n. 2, p. 1301-1317, 2022.

PELOQUIN, D., DIMAIO, M., BIERER, B., **Disruptive and avoidable: GDPR challenges to secondary research uses of data**. Eur J Hum Genet. v. 28, p. 697–705. 2020. Doi:10.1038/s41431-020-0596-x.

PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira**. 2021. Dissertação (Mestrado em Direito) - Faculdade de Direito, Programa de Pós-Graduação em Direito, Universidade Federal do Ceará, Fortaleza, 2021.

PILLAT, R. M. OLIVEIRA, T. C.; ALENCAR, P. S.; COWAN, D. D. **BPMN: A BPMN extension for specifying software process tailoring. Information and Software Technology**, v. 57, p. 95-115, 2015.

PINHEIRO, Patrícia Peck. **LGPD e saúde: os fins justificam os meios?** Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveissaude. Acesso em: 27 out. 2023, às 14:13.

PIOVESAN, A., & TEMPORINI, E. R., **Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública**. Revista de Saúde Pública, v. 29, n. 4, p. 318–325. 1995. Doi: 10.1590/s0034-89101995000400010.

PMI - PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project Management Body of Knowledge and the Standard for Project Management**, 7th Edition, Pennsylvania: PMI, 2021.

PREIBUSCH, S., KÜBLER, D., & BERESFORD, A. R., **Price versus privacy: an experiment into the competitive advantage of collecting less personal information**. Electronic Commerce Research, v. 13, n. 4, p. 423–455. 2013. Doi: 10.1007/s10660-013-9130-3.

RIVAROLLI, M. A.; DAL FARRA NASPOLINI, S. H. **Privacidade e proteção de dados em nosocômios e clínicas perante a LGPD**. Scientia Iuris, [S. l.], v. 27, n. 1, p. 112–128, 2023. Doi: 10.5433/2178-8189.2023v27n1p112-128.

ROMERO, M. **Arquitetura híbrida baseada em business process management, arquitetura corporativa e mineração de processos para apoiar o mapeamento e redesenho inteligente de processos organizacionais**, 2020. Tese de Doutorado – Universidade Nove de Julho.

SALGADO LEME R, BLANK M., **Lei Geral de Proteção de Dados e segurança da informação na área da saúde.** Cad. Ibero Am. Direito Sanit. v. 9, n.3, p. 210-224, 2020.

SARLET, G. B. S.; MOLINARO, C. A. **Questões Tecnológicas, Éticas e Normativas da Proteção de Dados Pessoais na Área da Saúde em um Contexto de Big Data**. Direitos Fundamentais e Justiça, Belo Horizonte, v. 13, n. 41, p. 183-212, 2019. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/811/964. Acesso em: 28 abril. 2023 às 14:12.

SAKAMOTO, L.S. et al., **Professional Guidance of the DPOs-BR in Corporate Governance in Logistics Chains. In: Kim, D.Y., von Cieminski, G., Romero, D. (eds) Advances in Production Management Systems. Smart Manufacturing and Logistics Systems: Turning Ideas into Action**. APMS 2022. IFIP Advances in Information and Communication Technology, v. 664. Springer, Cham. 2022 Doi: 10.1007/978-3-031-16411-8_8.

SHIELDS, L., PRATT, J., DAVIS, L., HUNTER, J., **Family-centred care for children in hospital**, Cochrane Database of Systematic Reviews. v. 24, n. 01, p. 01-27, 2007. Doi: 10.1002/14651858.CD004811.

SHIN, S.; et al. **Proposal for a Privacy Impact *Assessment* Manual Conforming to ISO/IEC 29134:2017**. In: Saeed, K., Homenda, W. (eds) Computer Information Systems and Industrial Management. CISIM. Lecture Notes in Computer Science(), vol 1. Springer, Cham, p. 486-498, 2018. Doi: 10.1007/978-3-319-99954-8_40.

SILVA-JUNIOR, D. do N.; ARAUJO, J. L. de; NASCIMENTO, G. G. do. **As ações dos profissionais diante da privacidade e da confidencialidade de usuários de um hospital geral**. pers.bioét., Chia, v. 21, n. 2, p. 219-232, Dec. 2017. Doi: 10.5294/pebi.2017.21.2.3.

SINGH, D. A. D. **S Data privacy compliance using COBIT 2019 and development of MISAM audit caselet**, 2020. Dissertação de Mestrado – Concordia University of Edmonton.

SOARES, N. V.; DALL´AGNOL, C. M. **Privacidade dos pacientes: uma questão ética para a gerência do cuidado em enfermagem**. Acta paul. enferm. v. 24, n. 5, p. 683-688, 2011. Doi: 10.1590/S0103-21002011000500014.

XIANG D,; Cai W. **Privacy Protection and Secondary Use of Health Data: Strategies and Methods.** BioMed research international. v. 21, n. 1, p. 01-11, 2021 Doi: 10.1155/2021/6967166.

YIN, R. K.; **Pesquisa Qualitativa do Início ao Fim**. 2.ed, Porto Alegre, 2016.

THIOLLENT, M., **Pesquisa-ação nas organizações**. São Paulo: Atlas, 1997.

VEIGA, T.M., **A LGPD nos escritórios de advocacia previdenciária: o registro das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade**. Revista Jurídica da Escola Superior de Advocacia da OAB-SC, Santa Catarina, 2021. Disponível em: https://oabsc.s3.saeast-1.amazonaws.com/arquivo/update/331_58_617abcaa47d41.pdf#page=153. Acesso em: 09 de abr. 2023 às 11:23.

VERONESE, J. R. P.; ROSSETO, G. M. de F. **O quadrilena da exclusão, inclusão, superexploraçãoes e proteção de dados pessoais de crianças e adolescentes na perspectiva da fraternidade**. Seqüência Estudos Jurídicos e Políticos, [S. l.], v. 43, n. 92, p. 1–29, 2023. Doi: 10.5007/2177-7055.2022.e92875.

VETIS-ZAGANELLI, M.; BINDA FILHO, D. L. **A Lei Geral de Proteção de Dados e suas implicações na saúde: as avaliações de impacto no tratamento de dados no âmbito clínico-hospitalar**. Rev. Bioética y Derecho, Barcelona, v. 54, p. 215-232, 2022.

WARREN, S., BRANDEIS, L., **The Right to privacy**. Disponível em http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm . Acesso em 23 maio 2023 às 10:27.

ZANON, J. C. **Direito à proteção dos dados pessoais**. São Paulo, Revista dos Tribunais, 2013.

ZARPELON, S. P. A.; KLEIN, L. P.; BUENO, D. **Metas internacionais de segurança do paciente na atenção primária à saúde: uma revisão integrativa**. Rev. OFIL·ILAPHAR, Madrid, v. 32, n. 4, p. 377-386, 2022. Doi: 10.4321/s1699-714x20220004000011.

ZEFERINO, D**., Proteção de dados: como adequar a sua empresa à LGPD?** In: Certifiquei: segurança da informação. 29 jul. 2020. Disponível em: https://www.certifiquei.com.br/protecao-dados/. Acesso em: 20 maio. 2023 às 15:34.

ZEMMOUDJ, S., BERMAD, N., OMAR, M., **CAPM: Context-Aware Privacy Model for IoT-Based Smart Hospitals**, 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, v. 15, p. 1139-1144, Doi: 10.1109/IWCMC.2019.8766630.

APÊNDICE A - Formato do LIA desenvolvido para aplicação no hospital pediátrico.

1. Qual é a finalidade do tratamento dos dados pessoais.
2. O tratamento é necessário para atender um ou mais objetivos organizacionais?
3. Qual a situação concreta do tratamento?
4. O tratamento é necessário para atender um ou mais objetivos específicos de terceiros?
5. Existe alguma referência legal ou normativa que esteja atrelada ao tratamento pretendido?
6. Por que o tratamento pretendido é importante para a empresa?
7. O tratamento é importante para terceiros?
8. Existe outra maneira de alcançar o objetivo?
9. São usados apenas os dados minimamente necessários?
10. Existe alguma outra base legal, como consentimento, execução do contrato ou obrigação legal, ou outra prevista no rol do art. 7º?
11. O titular espera que este tratamento de dados ocorra?
12. O tratamento pretendido agrega valor a um produto ou serviço que ele utiliza?
13. É provável que o tratamento tenha um impacto negativo nos direitos do titular?
14. É provável que o tratamento resulte em dano injustificado ou prejuízo ao titular?
15. Pode ocorrer um prejuízo para a empresa caso o tratamento não ocorra?
16. Pode ocorrer um prejuízo para terceiros caso o tratamento não ocorra?
17. O tratamento é do interesse do titular cujos dados pessoais estão relacionados?
18. Os interesses legítimos do titular estão alinhados com a parte dos interesses legítimos para o tratamento pela empresa?
19. Quais são os benefícios para o titular ou a sociedade?
20. O processamento limita direitos dos titulares?
21. Os dados pessoais serão obtidos diretamente do titular ou indiretamente?

22. O tratamento pode ser considerado intrusivo ou inadequado pelo titular?
23. Será ou é fornecido um aviso sobre este tratamento ao titular? Em caso afirmativo, como ele será feito?
24. O titular pode se opor a este tratamento? Se não, explique.
25. O escopo do tratamento pode ser modificado para reduzir/mitigar riscos ou danos à privacidade?
26. Quais são as medidas e instrumentos empregados para assegurar os direitos dos titulares dos dados pessoais e evitar que os dados sejam eventualmente tratados de modo indevido?
27. Qual as medidas de mitigação dos riscos?
28. Há mecanismo de oposição (opt-out)?

APÊNDICE B - Modelo de mapeamento de ciclo de vida dos dados desenvolvidos no projeto.

1. Qual o seu departamento?
2. Quais as atividades que você participa que processam dados pessoais de indivíduos? Informar nome dos serviços ofertados à sociedade ou nome dos processos de negócio que realizam tratamento dos dados pessoais.
3. Quais os tipos de processamento de dados pessoais envolvidos em cada atividade listada?
4. Quem são os titulares dos dados pessoais processados em cada atividade? Especifique qual é o relacionamento da empresa com o indivíduo cujos dados pessoais estão sendo processados.
5. Quais os sistemas, websites, dispositivos etc., que você utiliza para efetuar cada processamento?
6. Quais tipos de dados pessoais você processa?
7. Liste todos os elementos de dados pessoais que você utiliza em cada processo e os organize por ferramentas às quais eles pertencem.
8. Quais são as fontes dos dados em cada ferramenta?
9. Com quem você compartilha os dados?
10. Você é o Controlador ou Operador dos Dados Pessoais em questão?
11. Qual a Base Legal (finalidade) para o processamento dos dados pessoais?
12. Qual o ciclo de vida dos dados pessoais?
13. Para cada processo, indique por quanto tempo você armazena os dados.
14. Quais são as informações do controlador dos dados pessoais para esta atividade?
15. Quais são as informações do operador dos dados pessoais para esta atividade?
16. Descreva o fluxo do tratamento dos dados pessoais, descreva como (de que forma) os dados pessoais são coletados, retidos/armazenados, processados/usados e eliminados.
17. Indique a abrangência geográfica do tratamento.

18. Informe o resultado pretendido para o titular de dados.
19. Informe os benefícios esperados para a empresa.
20. Qual a frequência de tratamento dos dados pessoais?
21. Qual o volume de dados pessoais tratados?
22. Quais são as medidas de segurança adotadas nessa atividade?
23. Existem contratos de serviços e/ou soluções de TI que tratam dados pessoais nessa atividade?

APÊNDICE C – Modelo de Relatório de Impacto a Proteção de Dados - RIPD.

Segue modelo de Relatório de Impacto a Proteção de Dados – RIPD – desenvolvido no escopo do presente trabalho.

1. DADOS DO CONTROLADOR

Quem é o Controlador deste tratamento?

Qual é o nome, e-mail e telefone do encarregado de proteção de dados?

Qual o motivo pelo qual a elaboração do RIPD é necessária?

2. DESCRIÇÃO DO TRATAMENTO DE DADOS PESSOAIS

Como os dados pessoais são coletados, armazenados, tratados, usados e eliminados?

Qual é a origem dos dados pessoais e qual foi o meio utilizado para sua coleta?

Com quem esses dados pessoais são compartilhados?

Quem são os outros agentes de tratamento (operadores ou outros controladores) envolvidos no tratamento de dados?

A empresa adotou algum tipo de nova tecnologia que envolva tratamento dos dados pessoais?

Quais medidas de segurança são adotadas atualmente?

Quais tipos de dados são tratados? Há tratamento de dados sensíveis?

Qual o volume dos dados pessoais a serem coletados e tratados?

Qual a extensão e frequência em que os dados são tratados?

Quanto tempo os dados pessoais serão mantidos, retidos ou armazenados?

Qual o número de titulares de dados afetados pelo tratamento?

Qual a abrangência da área geográfica do tratamento?

Qual a natureza do relacionamento da empresa com o titular de dados pessoais?

Qual o nível ou método de controle que os titulares exercem sobre os dados pessoais?

O tratamento envolve o tratamento de dados pessoais de crianças e/ou adolescentes?

O tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais?

Descrever as medidas para garantia da privacidade e da proteção de dados e de segurança da informação adotadas pela empresa.

Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.

Informar os benefícios esperados para empresa, para um terceiro ou para a sociedade como um todo.

3. CONSULTAS E ANÁLISE DO TRATAMENTO DE DADOS PESSOAIS

Quais são as partes interessadas, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento?

O que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise?

Qual a base legal para o tratamento dos dados pessoais?

Caso o fundamento legal seja embasado no legítimo interesse do controlador, ele é indispensável? Há outra base legal possível de se utilizar para alcançar o mesmo propósito e, esse tratamento de fato auxilia no propósito almejado?

Como será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados) e minimização dos dados?

Quais medidas são adotadas a fim de assegurar que o operador realize o tratamento de dados pessoais?

Como estão implementadas as medidas que assegurem o exercício pelo titular dos direitos previstos pela legislação de proteção de dados?

Como a empresa pretende fornecer informações de privacidade para os titulares dos dados pessoais?

Há transferência internacional de dados? Quais são as salvaguardas para as transferências internacionais de dados?

4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Descreva a fonte de risco e a natureza do impacto potencial sobre os titulares:

Qual a probabilidade de danos? (Baixo, Médio, Alto e Muito Alto)

Qual o impacto do risco? (Baixo, Médio, Alto e Muito Alto)

Valor do risco final (Baixo, Médio, Alto e Muito Alto)

5. ACEITAÇÃO DO RISCO

Risco Aceito?

6. IDENTIFICAÇÃO DE MEDIDAS/CONTROLES PARA MITIGAÇÃO DE RISCOS

Identifique medidas adicionais que serão adotadas para reduzir ou eliminar riscos identificados como significativo ou máximo no item 4.

Qual a nova probabilidade de Danos? (Baixo, Médio, Alto e Muito Alto)

Qual o novo impacto do risco? (Baixo, Médio, Alto e Muito Alto)

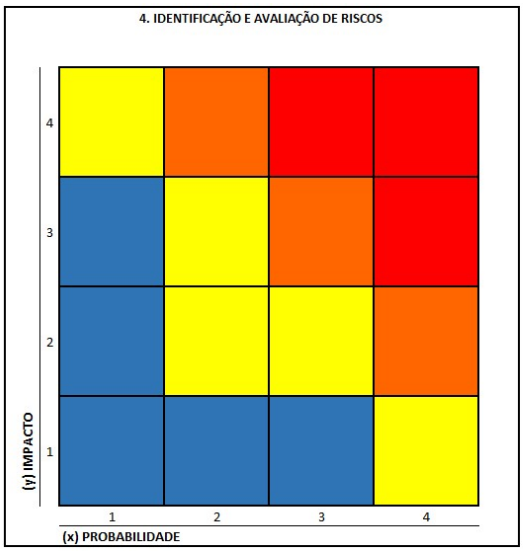
Valor do novo risco final (Baixo, Médio, Alto e Muito Alto)

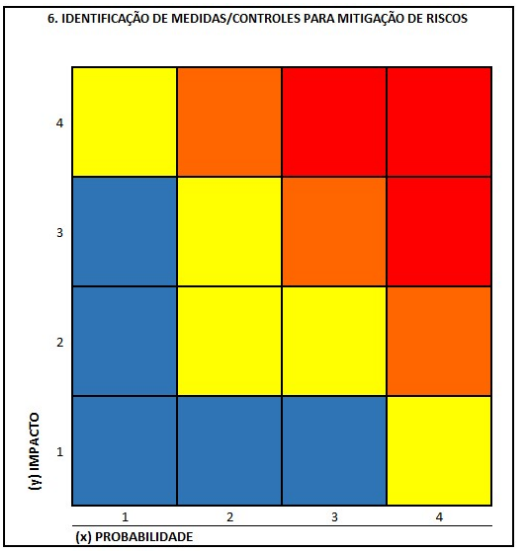
Qual o risco residual? (Baixo, Médio, Alto e Muito Alto)

Qual o efeito sobre o risco? (mitigado, excluído ou majorado)

Medida aceita?

Demonstrativo gráfico dos itens 4 e 6 calculados com base nas respostas dos itens.





APÊNDICE D - Modelo de ROPA desenvolvido no escopo do presente trabalho.

Registro de Atividades de Processamento de Dados	
1 - Identificação dos serviços/processo de negócio de tratamento de dados pessoais	
1.1 - Área/Processo de negócio	
1.1 - Processo de negócio	
1.2 - Nº Referência/ID	
1.3 - Data de Criação do Inventário	
1.4 - Data Atualização do Inventário	

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador					
2.2 - Encarregado					
2.3 - Operador					

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					

4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados	
4.1 - Descrição do Fluxo do tratamento dos dados pessoais	

5 - Escopo e Natureza dos Dados Pessoais

5.1 - Abrangência da área geográfica do tratamento	
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento Dados Pessoais	
6.1 - Hipótese de Tratamento Dados Sensíveis	
6.2 - Finalidade	
6.4 - Resultados pretendidos para o titular de dados	
6.5 - Benefícios esperados para a empresa	

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				
7.2 -Dados Financeiros	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.2.1 - Dados de identificação financeira				
7.2.2 - Recursos financeiros				

7.2.3 - Dívidas e despesas				
7.2.4 - Situação financeira (Solvência)				
7.2.5 - Empréstimos, hipotecas, linhas de crédito				
7.2.6 - Assistência financeira				
7.2.7 - Detalhes do Plano no Paciente				
7.2.8 - Transações financeiras				
7.2.9 - Atividades profissionais				
7.2.10 - Autorizações ou consentimentos				
7.3 - Características Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.3.1 - Detalhes pessoais				
7.3.2 - Descrição Física				
7.4 - Hábitos Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.4.1 - Hábitos				
7.4.2 - Estilo de vida				
7.4.3 - Viagens e deslocamentos				
7.4.4 - Contatos sociais				
7.4.5 - Uso de mídia				
7.5 - Características Psicológicas	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.5.1 - Descrição Psicológica				
7.6 - Composição Familiar	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados

7.6.1 - Casamento ou forma atual de coabitação				
7.6.2 - Histórico conjugal				
7.6.3 - Familiares ou membros da família				
7.7 - Interesses de lazer	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.7.1 - Atividades e interesses de lazer				
7.8 - Associações	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)				
7.9 - Processo Judicial/Administrativo/ Criminal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.9.1 - Suspeitas				
7.9.2 - Condenações e sentenças				
7.9.3 - Ações judiciais				
7.10 - Hábitos de Consumo	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.10.1 - Dados de bens e serviços				
7.11 - Dados Residenciais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.11.1 - Residência				
7.12 - Educação e Treinamento	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados

7.12.1 - Dados acadêmicos/escolares				
7.12.2 - Qualificação e experiência profissional				
7.13 - Profissão e emprego	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.13.1 - Emprego atual				
7.13.2 - Recrutamento				
7.13.3 - Rescisão de trabalho				
7.13.4 - Carreira				
7.13.5 - Absentismo e disciplina				
7.13.6 -Avaliação de Desempenho				
7.14 -Outros (Especificar)	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.14.1 - Outros (Especificar)				

8 - Categorias de Dados Pessoais Sensíveis	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
8.1 - Dados que revelam origem racial ou ética				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências políticas				

8.8 - Dados referentes à saúde				
8.9 - Dados referentes à vida sexual ou orientação sexual				
8.10 - Dados genéticos				
8.11 Dados de Imagem (Vídeo e Fotográfico)				
8.12 - Dado de Imagem (Câmera de Vigilância)				
8.13 - Dado de Voz				
8.14 - Outros Dados biométricos				

9 - Frequência e totalização das categorias de dados pessoais tratados	
9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes?		
10.4 - Além de crianças e adolescente, trata dados de outro grupo vulnerável		

11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1		

12 - Medidas de Segurança/Privacidade	Tipo de medida de segurança e privacidade	Descrição do(s) Controle(s)
12.3 - Medida de Segurança/Privacidade 1		

13 - Transferência Internacional de Dados Pessoais	País	Adequado ?	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1				

14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Contrato	Objeto do Contrato	E-mail do Gestor do Contrato
14.1 - Contrato nº 1			

APÊNDICE E – Documento para registro e gestão de risco.

Segue modelo de documento utilizado para identificar e classificar o risco desenvolvido no escopo do presente trabalho.

ID do Risco	Ativo	Categoria do Risco	Riscos	Explicação do Risco
R.1	**MV**	Risco de TI	Acesso indevido ao sistema	Acessos indevidos ao sistema, sem comprometimento do file server, podem acarretar em vazamentos de dados e afetar a confidencialidade e integridade dos sistemas

Fatores de Risco	Descrição do Impacto	*Dono do Risco(Main Risk Owner)*	
		Nome	Diretoria
1) Compartilhamento de senha 2) Expor a senha em locais públicos 3) Senhas fracas 4) Gestão de acesso comprometida	1) Vazamento de dados pessoais 2) Exposição negativa da imagem da empresa. 3) Prejuízos financeiros por multas de 0,1% a 20% do faturamento bruto ou R$50 milhões 4) Ação judicial e/ou administrativa contra a organização 5) Publicação do nome da empresa n 6) Suspensão ou interdição das atividades 7) Dano moral e subjetivo aos pacientes 8) Reparar integralmente o dano causado	Diretor Técnico	Técnica

Probabilidade	Impacto do Risco Corporativo									
	Pacientes	Cuidadores /Terceiros	Meio Ambiente	Ambiente Hospitalar	TI	Imagem	Financeiro	Jurídico / Regulatório	Impacto Geral do Risco Corporativo	Nota Final do Risco
3	5	2	0	3	3	4	3	4	3,458333333	10,375

APÊNDICE F - Modelo de *assessment* de terceiros e sistemas desenvolvido no escopo do presente trabalho.

1. O terceiro adota um inventário contendo o registro de suas operações de tratamento de dados pessoais com informações sobre a categoria de titulares, finalidade de tratamento, base legal e outros?
2. O terceiro possui um Encarregado pelo tratamento de dados pessoais?
3. O terceiro celebra Acordo de Confidencialidade com os seus colaboradores na prestação de serviços relacionados ao tratamento de dados pessoais?
4. O terceiro possui treinamento periódico sobre proteção de dados?
5. O terceiro adota mecanismos sobre análise de privacidade e proteção de dados pessoais desde a concepção (Privacy by Design), de seus produtos, serviços ou projetos, e realiza avaliações constantes, inclusive antes da implementação daqueles? Em caso positivo, detalhar como é realizado.
6. O terceiro possui política ou norma de proteção de dados que aborda as formas adequadas de tratamento de dados pelos seus colaboradores e terceiros, bem como alocando responsabilidades sobre os tratamentos?
7. As práticas de descarte ou destruição segura das informações garantem que esses dados não sejam recuperados?
8. Há algum registro ou tabela que detenha/centralize as informações de tempo de retenção dos dados pessoais estabelecidas pela empresa e/ou pela legislação vigente aplicável?
9. O terceiro possui procedimentos/mecanismos para garantir que as solicitações de requisição dos titulares sejam atendidas de forma segura e comunicadas, se necessário?
10. O terceiro possui mecanismos/procedimentos que requeiram a comunicação/notificação caso haja um tratamento indevido por parte de um subcontratado?
11. Há um plano de contingência que inclui notificar a empresa sobre incidentes com violação de dados pessoais?
12. Possui controles que protejam e limitem o acesso a dados pessoais e/ou sensíveis de clientes ou colaboradores da Empresa?

13. O terceiro realiza avaliações periódicas de segurança de rede? Identificar se regras de firewall são aplicadas para conter o acesso a sites e códigos maliciosos.

14. O terceiro mantém um inventário atualizado dos ativos utilizados para dar suporte no tratamento/armazenamento de dados?

15. O terceiro adota acesso restrito e com controles de autenticação no ambiente onde se armazenam e tratam dados pessoais?

16. O terceiro promove patchs para garantir a segurança nos sistemas utilizados no tratamento de dados pessoais e/ou sensíveis de clientes ou colaboradores da Empresa?

17. O terceiro possui antivírus e *antimalware*, atualizados e licenciados, em todos os equipamentos que processam dados pessoais e/ou sensíveis de clientes ou colaboradores da Empresa?

18. O terceiro possui documentado um plano para garantir a disponibilidade dos dados, por exemplo um plano de backup e *restore* implementado?

19. O terceiro possui planos de continuidade de negócios e realiza testes de recuperação após incidentes?

20. A empresa realiza a transmissão segura de dados pessoais, inclusive por e-mails e mensagens instantâneas?

21. O terceiro possui criptografia nos dispositivos que irão acessar ou processar dados?

22. O terceiro possui gerenciamento de acesso aos ambientes físicos onde são armazenados dados da Empresa?

23. O terceiro mantém anônimos os dados utilizados em ambientes de desenvolvimento ou homologação?

24. O terceiro possui um inventário dos serviços utilizados em nuvem?

25. O contrato firmado com o fornecedor de serviços de nuvem atende os requisitos de disponibilidade?

APÊNDICE G – Guia para Apoiar a Implementação do Programa de Privacidade e Proteção de Dados.

Com base no programa implementado no hospital pediátrico foi desenvolvido um guia para servir de roteiro para hospitais e outras organizações de saúde que se interessarem em desenvolver e implementar um programa de privacidade e proteção de dados.

Este guia, presente neste apêndice, deve ser usado para apoiar a construção, em qualquer entidade da área da saúde, de um programa de privacidade e proteção de dados que, além de estar de acordo com os requisitos trazidos pela LGPD, não impactará o funcionamento da assistência prestada por este hospital ou entidade da saúde.

A utilização deste guia importará na economia de tempo e dinheiro pelas organizações de saúde, que não mais necessitarão dispender altos volumes de trabalho de seus colaboradores para desenvolver um programa autônomo, vez que já há um modelo a ser seguido.

O guia é dividido em três partes: preparação para a Implementação e Implementação do Programa.

Etapa 1 – Preparação da Implementação

Nesta etapa se pretende preparar a organização para receber o programa desenvolvido, de modo a ser possível obter sucesso na implementação e preparar as fundações de um programa de proteção de dados baseados nas melhores práticas.

A preparação do ambiente é composta da identificação e mapeamento dos processos e dados da organização, a identificação de riscos, formalização de políticas organizacionais e construção dos relatórios de impacto (RIPD), do registro de tratamento de dados (ROPA) e da análise do legitimo interesse (LIA), conforme detalhado nos itens a seguir:

a) Identificar e Mapear Processos da Organização

Para o sucesso do programa de privacidade e proteção de dados, bem como para identificar todas as atividades que são realizadas dentro das áreas da organização se faz necessário a construção de um profundo mapeamento de processos utilizando-se da metodologia BPM, sendo determinadas todas as etapas dos processos visualizados e formalizada em um arquivo passível de análise e

perpetuação. A recomendação para utilização da metodologia BPM é realizada com base na indicação realizada pela ANPD e pela literatura recomendar esta utilização.

O mapeamento de processos deve ser revisto a cada ano e deverá sempre ocorrer em qualquer alteração destas atividades.

b) Identificar e Mapear os Dados Tratados na Organização

Em posse de todos os processos da organização, e após realizar o mapeamento dos dados utilizando-se da metodologia BPN, é necessário identificar quais dados são tratados na execução dos processos mapeados, de modo a verificar quais dados foram coletados, o motivo da sua coleta, sua base legal, o ciclo de vida dos dados, qual o tempo de manutenção e qual a forma de exclusão, se existente.

Todo mapeamento de dados é formalizado através de um ROPA, utilizando o modelo reproduzido no Apêndice D. Estes relatórios são atualizados anualmente e são armazenados em um local seguro e passível de ser consultados pela área responsável.

c) Identificar e Gerir Riscos

Vez que a LGPD determina uma avaliação sistemática dos riscos organizacionais e de privacidade, é necessário, neste momento, identificar e gerir os riscos envolvidos nos processos mapeados ou ainda na coleta dos dados identificados na fase “b”. Esta análise é realizada de acordo com metodologia própria indicada no capítulo 4 e se relaciona às seguintes etapas:

- Identificar riscos;
- Formalizar riscos em documento de controle;
- Calcular risco com base na metodologia indicada no capítulo 4;
- Analisar as medidas mitigatórias para diminuição, se necessário, do risco encontrado e;
- Identificar os tratamentos classificados como de alto risco ou que tenham como base o tratamento de dados de menores, o legítimo interesse, ou que envolvam dados sensíveis.

d) Elaborar e Formalizar o RIPD e o LIA

Havendo a formalização dos processos e do mapeamento do ciclo de vida dos dados coletados, e havendo a classificação sistemática dos riscos, deve-se elaborar

os RIPD e LIA com base no modelo presente no apêndice C para formalizar os tratamentos tidos como de risco, e realizar a análise deste tratamento, com base nas orientações presentes na LGPD.

e) Elaborar Políticas de Segurança da Informação e Proteção de Dados

Para manutenção do programa, e adequação a LGPD, devem ser criadas políticas para estabelecer diretrizes e procedimentos para toda a organização no tocante a segurança da informação e proteção dados. Recomenda-se a utilização das políticas indicadas no Capítulo 4 ou ainda a utilização dos controles presentes nas boas práticas de segurança.

Entende-se que o minimamente aceitável é a existência de políticas que envolvam segurança, privacidade, backup e restauração, senhas, e-mail, acesso aos ambientes (lógicos e físicos), de conduta, de dispositivos móveis e no tocante a governança.

Etapa 2 – Implementação do Programa

Após a preparação da organização, e havendo a construção dos mapeamentos de processo, de dados, da RIPD, do LIA e dos ROPAs já é possível passar para a etapa dois deste guia, ou seja, iniciar a implementação do programa de privacidade e proteção de dados.

Esta etapa é composta das seguintes fases:

a) Treinamento e Conscientização

Um bom treinamento aos colaboradores do hospital ou entidade de saúde é fundamental para o sucesso de um programa de privacidade e proteção de dados, uma vez que o fator humano é essencial para que seja mantido os requisitos de governança necessários para que haja o pleno cumprimento da LGPD.

Em posse de todas as políticas aprovadas e de um mapa de processos e dados, deve ser realizado um treinamento abrangente para todos os colaboradores da organização, treinamento este que deve conter questões de segurança da informação, proteção de dados, e temas atuais da organização para conscientização.

Após este treinamento é importante construir um programa de conscientização constante que sirva como reciclagem do treinamento para trazer assuntos pontuais sobre estes temas. Importante citar que este programa de

conscientização engloba simulação de *phishing*, que é uma forma de ataque e que traga atualidade ao tema.

b) Adequação de Processos

Visualizando o mapeamento de processos, o mapeamento de dados e a elaboração dos relatórios de impacto e legitimo interesse, passa-se a identificar os processos que necessitam de alteração e, com base nas recomendações presentes no ROPA, realizar as alterações necessária nesses processos para cumprimento da LGPD.

Deve se priorizar os processos com maior risco e cuja adequação demandar menor trabalho possível, de forma a maximizar o retorno esperado. Após este ponto, focando no maior risco, deve se criar um plano institucional para mitigar todos os riscos encontrados e ao final, adequar todos os processos à LGPD e a ideia de implementar a proteção de dados na organização.

Nesta fase deve se privilegiar o apoio da alta gestão das alterações recomendadas, de modo a vincular o alto da organização e suas decisões com a base da organização e a nova orientação.

c) Criação da Gestão de *Cookies*

Vez que *cookies* são considerados dados pessoais, se faz necessário alterar todos os sites organizacionais para gerir corretamente os *cookies* da organização, e adequar o site a qualquer imposição da LGPD. Deve se priorizar um sistema que possibilite uma coleta adequada, construção de log e gestão adequada dos óbices à coleta dos visitantes deste site.

d) Criação do Fluxo do Atendimento aos Titulares

Para atendimento dos titulares deve ser criado dentro da organização um fluxo para atendimentos de qualquer solicitação do titular de dados, nos termos do artigo 18 da LGPD. Recomenda-se que haja identificação clara no site da organização, no ambiente físico e em todos os contatos com os titulares, sendo deixado claro que o titular pode e deve entrar em contato com o responsável pelo tratamento de dados. O canal ideal deve ter registro de log e facilidade de acesso.

e) Indicação do Responsável pelo Tratamento de Dados

Em atendimento a LGPD deve ser indicado um responsável pelo tratamento de dados da organização. Indica-se que o responsável tenha autonomia de decisão e trabalhe, idealmente, respondendo diretamente a alta gestão da organização.

f) *Assessment* de Terceiros e Sistemas

Nesta fase dever ser realizado um levantamento de todos os parceiros do hospital pediátrico e de todos os sistemas informatizados usados pela organização, com a finalidade de replicar aos parceiros e aos sistemas utilizados o programa de privacidade e proteção de dados.

Isto é feito através de um mapeamento da maturidade do parceiro, utilizando-se o questionário indicado no apêndice F. Após a resposta por parte do parceiro, deve ser desenvolvido um programa de adequação das atividades dos terceiros de acordo com as questões identificadas no questionário utilizado.

Por fim, no tocante aos sistemas utilizados pela organização, deve ser criado um procedimento de análise de requisitos de segurança e proteção de dados e análise dos riscos envolvidos também na utilização deste sistema.

Etapa 3 – Pós-implementação e Avaliação

Após a implementação do programa de privacidade e proteção de dados é necessário que seja construído um ciclo de revisão e reanálise de todo o ambiente da organização, havendo a nova análise a cada alteração de processo, ou ainda a cada 12 meses.

Além disto deve ser realizado um acompanhamento cuidadoso dos riscos encontrados, sendo revisitado todos os pontos com atenção para evitar majoração adicional do risco. Este acompanhamento deve se valer da fórmula de cálculo de risco constante no apêndice E.

Recomenda-se que os treinamentos sejam revisados anualmente e no tocante a algumas questões pontuais seja perene.

APÊNDICE H – Questionário para validação do programa de privacidade e proteção de dados.

UNIVERSIDADE NOVE DE JULHO (UNINOVE) –
PROGRAMA DE MESTRADO E DOUTORADO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO (PPGI)

Mestrando: Nityananda Portellada
E-mail: nityananda.portellada@uni9.edu.br; nityananda.portellada@gmail.com
Celular: 11 970886636
Orientador: Prof. Dr. Renato José Sassi
E-mail: sassi@uni9.pro.br

Objetivo da aplicação do questionário: Validar a Proposta de Desenvolvimento e Aplicação de um Programa de Privacidade e Proteção de Dados para um Hospital Pediátrico.

O questionário composto por 15 questões é parte integrante da pesquisa realizada pelo aluno de mestrado, Nityananda Portellada

Por conta da necessidade de privacidade e proteção dos dados dos pacientes em um hospital pediátrico, propõe-se o desenvolvimento de um programa voltado, especificamente para esse tipo de hospital. O Programa proposto será formado pelas seguintes metodologias, com suas respectivas aplicações, descritas a seguir:

- Mapear os processos com *Business Process Model and Notation* (BPMN);
- Mapear o ciclo de vida dos dados;
- Aplicar o *Record Of Processing Activities* (ROPA) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- Utilizar o *Legitimate Interests Assessment* (LIA) para a análise dos tratamentos de dados com base no legítimo interesse;
- Aplicar os princípios de segurança da informação nos tratamentos de dados;
- Realizar *Assesment* de Terceiros e de Sistemas quando à segurança da informação e proteção de dados.

Desta forma, busca-se com a aplicação do questionário validar a proposta de desenvolvimento do programa.

A pesquisa tem caráter essencialmente acadêmico, e que os dados pessoais dos participantes serão mantidos em total anonimato, não sendo utilizados para outras finalidades. Para mais informações, por favor, utilize os endereços de e-mail ou o número do telefone celular disponibilizados acima.

Antecipadamente, agradeço a atenção dispensada.
Nityananda Portellada

Questões
1) Qual é a sua área de atuação? a) Privacidade e Proteção de Dados. b) Segurança da Informação. c) Ambas as áreas. d) Outra área de atuação. Caso tenha selecionado o item "**d**", por favor, escreva a sua área de atuação.
2) Há quanto tempo você atua na área selecionada na questão 1? a) Menos de 1 ano. b) De 1 a 3 anos. c) De 4 a 6 anos. d) De 7 a 9 anos. e) Mais de 10 anos, inclusive.
3) Qual é o porte do hospital que você trabalha? a) Grande porte. b) Médio porte. c) Pequeno porte. d) Outro. Caso tenha selecionado o item "**d**", por favor, escreva o porte do hospital.
4) Qual é o tipo de hospital que você trabalha? a) Hospital Pediátrico. b) Hospital Geral. c) Hospital Especializado. d) Hospital Dia. e) Outro tipo. Caso tenha selecionado o item "**e**", por favor, escreva o tipo do hospital.
5) Em se tratando de privacidade e proteção de dados em um hospital, qual abordagem você usa ou consideraria usar? a) COBIT. b) ISO 27701. c) A combinação de ambas as abordagens. d) Outra(s) abordagem(ns). Caso tenha selecionado o item "**d**", por favor, escreva a(s) abordagem(ns).

6) Dentre os itens a seguir, qual(is) você considera vantajoso(s), de acordo com a(s) abordagem(ns) selecionada(s) na questão 5?

a) Aumento de eficiência organizacional.
b) Aumento da Segurança da informação.
c) Atendimento às normas da Lei Geral de Proteção de Dados Pessoais (LGPD).
d) Aumento da transparência organizacional.
e) Outra(s) vantagem(ns).

Caso tenha selecionado o item "**e**", por favor, escreva a(s) vantagem(ns).

7) Dentre os itens a seguir, qual(is) você considera desvantajosos(s), de acordo com a(s) abordagem(ns) selecionada(s) na questão 5?

a) Implementação trabalhosa.
b) Necessidade de alteração dos processos.
c) Não ampara completamente a adequação às normas da LGPD.
d) Necessita do amparo de outra(s) abordagem(ns).
e) Outra(s) desvantagem(ns).
f) Não tem desvantagem.

Caso tenha selecionado o item "**e**", por favor, identifique a desvantagem.

8) O mapeamento de processos com BPMN pode ser uma alternativa à(s) abordagem(ns) selecionada(s) na questão 5.

a) Discordo totalmente.
b) Discordo.
c) Neutro.
d) Concordo.
e) Concordo totalmente.

9) O mapeamento de processos com BPMN em conjunto com o Mapeamento de Dados pode ser uma alternativa para a redução de vulnerabilidades e riscos de segurança, privacidade e proteção de dados em um hospital.

a) Discordo totalmente.
b) Discordo.
c) Neutro.
d) Concordo.
e) Concordo totalmente.

10) A aplicação do ROPA para registrar e controlar os processos que tratam dados pessoais, do RIPD para registrar e analisar riscos de processos considerados altos ou que envolvam tratamento de dados e do LIA ao registrar e analisar riscos de processos, cuja base legal é o legítimo interesse do titular dos dados, é relevante para a privacidade e proteção de dados em um hospital.

a) Discordo totalmente.
b) Discordo.
c) Neutro.
d) Concordo.
e) Concordo totalmente.

11) O *Assessment* de Terceiros e Sistemas para identificação da aderência à LGPD dos parceiros de negócios e sistemas é essencial para manutenção e sucesso da proteção de dados em um hospital.

a) Discordo totalmente.
b) Discordo.
c) Neutro.
d) Concordo.
e) Concordo totalmente.

12) Aplicar um programa de privacidade e proteção de dados desenvolvido especialmente para hospitais pediátricos é justificável e importante.

a) Discordo totalmente.
b) Discordo.
c) Neutro.
d) Concordo.
e) Concordo totalmente.

13) Você validaria uma proposta de desenvolvimento e aplicação de um programa de privacidade e proteção de dados para hospitais pediátricos que apresentasse a associação de BPMN, Mapeamento dos Dados, RIPD, ROPA e LIA?

a) Sim.
b) Não.

Use este espaço, caso queira comentar.

14) Você incluiria outra metodologia, método ou técnica ao programa de privacidade e proteção de dados, além das descritas na questão 13?

a) Sim.
b) Não.

Use este espaço, caso queira comentar.

15) Por favor, faça os comentários que achar necessário.

Seguem a análise das respostas realizadas na validação do programa de privacidade e proteção de dados.

Pergunta	Alternativas	Numero de Respostas
1. Qual é a sua área de atuação?	a) Privacidade e Proteção de Dados.	4
	b) Segurança da Informação.	1
	c) Ambas as áreas.	4
	d) Outra área de atuação.	1 (Gestão de TI)

Quadro 11 – Área de atuação dos respondentes da pesquisa encaminhada.

O quadro 11 demonstra que dos 10 respondentes a maioria atua na área de Proteção de Dados ou tem uma atuação mista entre Proteção de Dados e Segurança da informação.

Pergunta	Alternativas	Numero de Respostas
2. Há quanto tempo você atua na área selecionada na questão 1?	a) Menos de 1 ano.	0
	b) De 1 a 3 anos.	0
	c) De 4 a 6 anos.	5
	d) De 7 a 9 anos.	1
	e) Mais de 10 anos, inclusive.	4

Quadro 12 – Tempo de atuação dos respondentes da pesquisa encaminhada.

O quadro 12 possibilitou identificar que a totalidade dos respondentes é de profissionais experientes com mais de 4 anos de experiência, com 4 respondentes tendo atuado na área a mais de 10 anos.

Pergunta	Alternativas	Numero de Respostas
3. Qual é o porte do hospital que você trabalha?	a) Grande porte.	5
	b) Médio porte.	3
	c) Pequeno porte.	0
	d) Outro.	2 (Plano de Saúde e Farmacêutica)

Quadro 13 – Porte do hospital onde os respondentes trabalham.

Do quadro 13 é possível identificar que 7 respondentes trabalham em hospitais de grande ou médio porte.

Pergunta	Alternativas	Numero de Respostas
4. Qual é o tipo de hospital que você trabalha?	a) Hospital Pediátrico.	3
	b) Hospital Geral.	4
	c) Hospital Especializado.	0
	d) Hospital Dia.	1
	e) Outro tipo.	2 (Outros estabelecimentos de saúde)

Quadro 14 – Tipo de hospital em que os respondentes trabalham.

Das respostas da pergunta 4, é possível identificar que a grande maioria, 7 respondentes, atuam ou em hospitais pediátricos, com atendimento exclusivo a indivíduos até 18 anos incompletos, ou em hospitais gerais, que atendem qualquer paciente independentemente da idade.

O perfil extraído das respostas das questões qualificadoras para os respondentes são indivíduos que atuam nas áreas de Privacidade e Proteção de Dados, com mais de 4 anos de experiência; com metade dos indivíduos com experiência maior de 7 anos que trabalham em hospitais e que se relacionam com entidades de médio e grande porte.

O quadro 15 traz perguntas relacionadas às abordagens passíveis de utilização em um programa de proteção de dados de um hospital e que se fixam em citar expressamente dois modelos comumente utilizados, o COBIT e a norma ISO 27701.

Pergunta	Alternativas	Numero de Respostas
5. Em se tratando de privacidade e proteção de dados em um hospital, qual abordagem você usa ou consideraria usar?	a) COBIT.	0
	b) ISO 27701.	3
	c) A combinação de ambas as abordagens.	5
	d) Outra(s) abordagem(ns).	2 (NIST)

Quadro 15 – Metodologias utilizadas em programas de proteção de dados em hospitais.

Nota-se que, do quadro acima, a grande maioria dos respondentes identificam que a combinação dos dois modelos são os mais indicados para o questionado, ou seja, a implementação de um programa de proteção de dados.

Em continuidade é possível averiguar, no quadro 16, que a maior parte dos respondentes indicam que o uso do COBIT e da ISO 27701 contribuem para o aumento da segurança da informação e o atendimento às normas da LGPD, sendo importante citar que esta questão possibilitava a escolha de mais de uma opção.

Pergunta	Alternativas	Numero de Respostas
6. Dentre os itens a seguir, qual(is) você considera vantajoso(s), de acordo com a(s) abordagem(ns) selecionada(s) na questão 5?	a) Aumento de eficiência organizacional.	4
	b) Aumento da Segurança da informação.	8
	c) Atendimento às normas da Lei Geral de Proteção de Dados Pessoais (LGPD).	8
	d) Aumento da transparência organizacional.	3
	e) Outra(s) vantagem(ns).	0

Quadro 16 – Vantagens para uso das metodologias indicadas na questão 5.

Após a indagação quanto as vantagens dos modelos escolhidos, o quadro 17 indica as desvantagens relacionadas com a abordagem indicada na questão 5, sendo que esta questão também possibilitava a escolha de mais de uma opção.

Pergunta	Alternativas	Numero de Respostas
7. Dentre os itens a seguir, qual(is) você considera desvantajosos(s), de acordo com a(s) abordagem(ns) selecionada(s) na questão 5?	a) Implementação trabalhosa.	2
	b) Necessidade de alteração dos processos.	0
	c) Não ampara completamente a adequação às normas da LGPD.	3
	d) Necessita do amparo de outra(s) abordagem(ns).	3
	e) Outra(s) desvantagem(ns).	1 (Implementação lenta)
	f) Não tem desvantagem.	3

Quadro 17 – Desvantagens para uso das metodologias indicadas na questão 5.

Questionados sobre a possibilidade de ser adotado um mapeamento de processos com BPMN na metodologia indicada na questão 5, os respondentes, em sua maioria, 9 respondentes, indicaram concordar ou concordar completamente com a adoção desta forma de mapeamento, como se vê no quadro 18.

Pergunta	Alternativas	Numero de Respostas
8. O mapeamento de processos com BPMN pode ser uma alternativa à(s) abordagem(ns) selecionada(s) na questão 5.	a) Discordo totalmente.	0
	b) Discordo.	1
	c) Neutro.	0
	d) Concordo.	7
	e) Concordo totalmente.	2

Quadro 18 – Questionamento sobre o uso de BPMN na abordagem selecionada na questão 5.

Neste mesmo sentido, os respondentes indicaram, em sua totalidade, que o uso do BPMN junto ao mapeamento de dados é uma ótima alternativa para a redução de vulnerabilidades e melhora da proteção de dados da organização, como visto no quadro 19.

Pergunta	Alternativas	Numero de Respostas
9. O mapeamento de processos com BPMN em conjunto com o Mapeamento de Dados pode ser uma alternativa para a redução de vulnerabilidades e riscos de segurança, privacidade e proteção de dados em um hospital.	a) Discordo totalmente.	0
	b) Discordo.	0
	c) Neutro.	0
	d) Concordo.	10
	e) Concordo totalmente.	0

Quadro 19 – Questionamento sobre a melhoria trazida pelo uso da BPMN.

Indicadas as abordagens de escolha para a implementação de um programa de proteção de dados, juntamente com suas vantagens e desvantagens, citando ao final o benefício de se utilizar o mapeamento de processo com BPMN, passa-se a indicação nos quadros 20 e 21, sobre a utilização, respectivamente, do ROPA, RIPD e LIA, e do uso de *Assessment* de Terceiros.

Pergunta	Alternativas	Numero de Respostas
10. A aplicação do ROPA para registrar e controlar os processos que tratam dados pessoais, do RIPD para registrar e analisar riscos de processos considerados altos ou que envolvam tratamento de dados e do LIA ao registrar e analisar riscos de processos, cuja base legal é o legítimo interesse do titular dos dados, é relevante para a privacidade e proteção de dados em um hospital.	a) Discordo totalmente.	0
	b) Discordo.	0
	c) Neutro.	0
	d) Concordo.	1
	e) Concordo totalmente.	9

Quadro 20 – Questionamento sobre a relevância do uso de ROPAs, LIAs e RIPDs.

O quadro 20 indica a adesão de todos os respondentes a utilização do ROPAs, RIPDs e LIAs, havendo 9 respostas concordando totalmente com o questionamento e 1 resposta concordando apenas.

Pergunta	Alternativas	Numero de Respostas
11. O Assessment de Terceiros e Sistemas para identificação da aderência à LGPD dos parceiros de negócios e sistemas é essencial para manutenção e sucesso da proteção de dados em um hospital.	a) Discordo totalmente.	0
	b) Discordo.	0
	c) Neutro.	0
	d) Concordo.	5
	e) Concordo totalmente.	5

Quadro 21 – Questionamento sobre a relevância do uso do *Assessment* de Terceiros e Sistemas.

O quadro 21 indica a adesão de todos os respondentes quanto a relevância da realização de *Assessment* de Terceiros e Sistemas para o sucesso da implementação de um programa de proteção de dados em um hospital.

Após estas indagações, foi questionado se os respondentes concordam com a afirmação de que “Aplicar um programa de Privacidade e Proteção de Dados desenvolvido especialmente para hospitais pediátricos é justificável e importante”, como se verifica do quadro 22.

Pergunta	Alternativas	Numero de Respostas
12. Aplicar um programa de privacidade e proteção de dados desenvolvido especialmente para hospitais pediátricos é justificável e importante.	a) Discordo totalmente.	0
	b) Discordo.	1
	c) Neutro.	0
	d) Concordo.	4
	e) Concordo totalmente.	5

Quadro 22 – Questionamento sobre a relevância de um programa de privacidade e proteção de dados especialmente construído para um hospital pediátrico.

Do quadro 22 é possível identificar que 1 respondente discordou da afirmação, tendo os demais respondentes afirmado que concordam ou concordam totalmente com a afirmação, o que demonstra a importância do programa de Privacidade e Proteção de dados criado especialmente para um hospital pediátrico, como proposto.

Assim, passou-se a indagar os respondentes acerca da validação de um programa de proteção de dados unicamente para hospitais pediátricos que associem o mapeamento com BPMN, Mapeamento de Dados, RIPD, LIA e ROPA, como se verifica do quadro 23.

Pergunta	Alternativas	Numero de Respostas
13. Você validaria uma proposta de desenvolvimento e aplicação de um programa de privacidade e proteção de dados para hospitais pediátricos que apresentasse a associação de BPMN, Mapeamento dos Dados, RIPD, ROPA e LIA?	a) Sim.	10
	b) Não.	0

Quadro 23 – Questionamento sobre a validação da proposta de programa de proteção de dados como descrito.

É possível verificar que, do quadro 23, todos os respondentes validaram a proposta de um programa voltado para um hospital pediátrico, o que valida também o presente trabalho, que se propôs construir tal proposta. Foi dado na pergunta seguinte a possibilidade de indicar se o respondente incluiria outra metodologia no programa citado na questão 13, como se nota no quadro 24.

Pergunta	Alternativas	Numero de Respostas
14. Você incluiria outra metodologia, método ou técnica ao programa de privacidade e proteção de dados, além das descritas na questão 13?	a) Sim.	4
	b) Não.	6

Quadro 24 – Questionamento sobre a inclusão de outra metodologia no programa validado na questão 13.

Houve 6 respondentes que indicaram não ser necessário a inclusão de outra metodologia ao programa de privacidade voltado para hospitais pediátricos e 4 respondentes indicando a inclusão de outra metodologia, como o NIST, um padrão de segurança criado pelo *National Institute of Standards and Technology*.

A 15ª pergunta deixou aberto ao respondente a possibilidade de tecer comentários que entendesse necessários, de modo que dois respondentes indicaram

ser vantajoso a realização de um treinamento concomitante a implementação, o que de fato foi realizado no programa.