DESENVOLVIMENTO DE UM *FRAMEWORK* PARA IMPLEMENTAR UM PROGRAMA DE GOVERNANÇA DE DADOS EM UM HOSPITAL PEDIÁTRICO

DEVELOPMENT OF A FRAMEWORK TO IMPLEMENT A DATA GOVERNANCE PROGRAM IN A PEDIATRIC HOSPITAL

Nityananda Portellada[1]
Sarah Loretta Barbosa do Santos[2]
Renato José Sassi[3]

RESUMO

A adoção da Lei Geral de Proteção de Dados (LGPD) pelas organizações gerou medidas para o tratamento de dados como a imposição de uma alteração nos processos baseados na proteção de dados e calçados em governança. **Problemática**: A privacidade e proteção de dados em hospitais pediátricos é prioritária para a gestão do cuidado assistencial do paciente. O cuidado com a privacidade do paciente, antes vinculada apenas ao prontuário, teve que ser expandida para todo o processo hospitalar. **Objetivo:** Foi desenvolver e aplicar um framework para implementar um programa de governança de dados em um hospital pediátrico para aprimorar o cumprimento da Lei Geral de Proteção de Dados. **Métodos:** Trata-se de pesquisa experimental realizada em um hospital de médio porte, com cerca de 180 leitos de internação, amparada por uma revisão bibliográfica. O desenvolvimento do framework foi realizado em 7 fases distintas. **Resultados:** Os resultados preliminares obtidos com a aplicação do *framework* indicam a evolução da maturidade do hospital pediátrico, criando um programa de governança que apoia o mapeamento dos processos organizacionais e a melhoria do ambiente interno.

PALAVRAS-CHAVE: Hospital Pediátrico, Governança de Dados. Proteção de Dados, Business Process Management, Boas Práticas de Segurança da Informação.

ABSTRACT

The adoption of the General Data Protection Law (LGPD) by organizations generated measures for data processing such as the imposition of a change in processes based on data protection and footwear in governance. Problem: Data privacy and protection in pediatric hospitals is a priority for patient care management. Care for the patient's privacy, previously linked only to the medical record, had to be expanded to the entire hospital process. Objective: It was to develop and apply a framework to implement a data governance program in a pediatric hospital to improve compliance with the General Data Protection Law. Methods: This is an experimental research carried out in a medium-sized hospital, with approximately 180 inpatient beds, supported by a bibliographical review. The development of the framework was conducted in seven distinct phases. Results: The preliminary results obtained with the application of the framework indicate the evolution of the maturity of the pediatric hospital, creating a governance program that supports the mapping of organizational processes and the improvement of the internal environment.

KEYWORDS: Pediatric Hospital, Data Governance. Data Protection, Business Process Management, Good Information Security Practices

---

[1] Mestrando no Programa em Informática e Gestão do Conhecimento da Universidade Nove de Julho (UNINOVE) – São Paulo, Brasil. ORCID: 0000-0002-2602-6271

[2] Mestranda no Programa em Informática e Gestão do Conhecimento da Universidade Nove de Julho (UNINOVE) – São Paulo, Brasil. ORCID: 0009-0003-2311-8626

[3] Doutor em Engenharia Elétrica (EPUSP) e docente pesquisador do Programa de Mestrado e Doutorado em Informática e Gestão do Conhecimento da Universidade Nove de Julho. ORCID: 000-0001-5276-4895

1 INTRODUÇÃO

Governança de dados é um tema importante no mundo moderno devido ao acesso sistemático aos dados pessoais nas novas tecnologias. Isso levou à criação de legislações, como a LGPD no Brasil, que impõem medidas obrigatórias de governança de dados.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira inspirada na RGPD ou Regulamento Geral de Proteção de Dados da União Europeia e tem como objetivo a proteção dos dados do indivíduo, buscando garantir que estes tenham controle sobre suas informações e que elas não sejam utilizadas indevidamente.

Tal legislação acaba por criar diversas medidas obrigatórias para o tratamento de dados pessoais como, por exemplo, a imposição de uma alteração essencial na metodologia de trabalhos das empresas, com base na eficiência organizacional baseada na proteção de dados (BOLLIVAR, 2020), o que não é diferente para os hospitais brasileiros.

Tais estabelecimentos tiveram que adequar os seus processos às determinações da LGPD, posto que, com o princípio da minimização dos dados houve uma mudança de paradigma, de um processo voltado apenas ao resultado operacional para um processo voltado para a manutenção dos direitos básicos do titular de dados. Além disto, o cuidado com a privacidade do paciente, antes vinculada apenas ao prontuário, teve que ser expandida para todo o processo (RIVAROLLI e DAL FARRA NASPOLINI, 2023).

Ocorre que, no caso de hospitais pediátricos, a implementação de um programa de governança de dados é desafiadora pois estes hospitais detêm processos muito diversos, sejam na forma de coleta de dados, seja na regulamentação existente, na medida em que em um hospital pediátrico a coleta de dados sempre envolverá crianças e adolescentes, o que pode não acontecer em uma organização não pediátrica.

Isto faz com que alguns *frameworks* já estabelecidos, como a ISO 27701 e COBIT, respectivamente voltado para atingir requisitos de privacidade e para melhoria no gerenciamento de TI, não estejam de acordo com esta particularidade, pois não compreendem a gestão do ponto de vista de equilibrar os deveres assistenciais com as particularidades acima identificadas (BERG, 2001 e LAPÃO, 2011).

Há uma necessidade de que o *framework* utilizado contenha um mapeamento detalhado de processos e dados, uma análise de risco de todos os processos que tratam dados pessoal, uma metodologia de construção de relatórios de impacto a proteção de dados e a absorção de todos os aspectos da governança de dados. Esta união de técnicas é essencial para um ambiente hospitalar dando meios para melhor aderência da organização ao programa de privacidade e proteção e dados e melhoria da gestão de processos (GOSTIN e NASS, 2009)

Apesar de os hospitais pediátricos buscarem a adequação à LGPD, existem falhas no cumprimento dela, vez que não há facilidade de adequação na utilização dos modelos existentes atualmente (BERG, 2001 e LAPÃO, 2011), o que agrava o risco inerente a privacidade dos titulares envolvidos, posto que o tratamento de dados de crianças e adolescentes são consideravelmente mais críticos, inclusive sendo caracterizado como tratamento de alto risco pela Autoridade Nacional de Proteção de Dados (ANPD) (ANPD, 2022).

Esta falha esta eminentemente relacionada a uma deficiência cultural e de implementação (HAWRYLISZYN, COELHO e BARJA, 2021), posto que a maior parte das implementações de programas de privacidades e proteção de dados me um hospital é feito sem posterior acompanhamento e gestão.

Em um hospital pediátrico o volume de dados admitido do paciente, reforça-se, criança e adolescentes, é extremamente abundante, o que gera, além do erro acima citado, uma dicotomia entre coletar os dados suficientes para o cumprimento do dever de cuidado e a minimização e acesso unicamente entre a equipe assistencial, como médico, enfermeiros e equipe multiprofissional.

Algumas rotinas comuns e práticas para a enfermagem, como placas de identificação na porta, espaço para que armazenamento público do prontuário, passagem de plantão aberta e discussão Inter hospitalar de casos geram patentes riscos a privacidade do paciente, apesar de ser medida de proteção assistencial (SARLET e MOLINARIO, 2021; HAWRYLISZYN, COELHO e BARJA, 2021).

Assim, partindo da premissa construída no sentido de criação de um programa de governança de dados que abarque privacidade, e partindo da premissa de características próprias das organizações hospitalares pediátricos, necessário se faz o desenvolvimento de um framework de privacidade específico para tais locais, que não pretende a substituição dos existentes, mas sim a adaptação às características desta realidade e devido a imposições legais.

O objetivo deste trabalho foi desenvolver um *framework* para implementar um programa de governança de dados em um hospital pediátrico para aprimorar o cumprimento da Lei Geral de Proteção de Dados. Apesar de existirem diversas formas para implementar um programa de privacidade o *framework* se vinculará na diminuição do risco no tratamento de dados organização sem, todavia, prejudicar a operação.

Vislumbra-se com o desenvolvimento desta pesquisa, contribuir para a academia, ao desenvolver um modelo de framework de um programa de governança de dados adaptado para entidades hospitalares pediátricas, de modo que os resultados obtidos na presente poderão ser utilizados por outros pesquisadores para desenvolverem seus próprios métodos.

Esta replicabilidade é importante tendo em vista que a LGPD influenciou uma forte guinada nos hospitais brasileiros, em especial os pediátricos, posto que, com os princípios trazidos no artigo 6º da referida lei (BRASIL, 2018) foi necessário incorporar medidas de segurança da informação, impor o consentimento prévio para a coleta de dados em algumas situações e a minimização da coleta de dados, em antagonismo a uma coleta realizada antes da LGPD que priorizada maximização, ausência de consentimento e desconsideração de boas práticas de governança e segurança.

2 REFERENCIAL TEÓRICO

Nesta seção é apresentada a fundamentação teórica sobre os temas abordados neste trabalho, Hospital Pediátrico, Governança de Dados, Proteção de Dados e Metodologia BPM.

2.1 HOSPITAL PEDIÁTRICO

Segundo Shield et al., (2007) Historicamente um hospital não tende a ser um local feliz para crianças e adolescentes, cumulado com a situação patológica a que eles sem encontram, o próprio ambiente hospitalar, destinado a sobriedade das relações e na eficiência clínica das condutas, não necessariamente na eficiência da felicidade do paciente, tornava estes estabelecimentos locais temíveis pelos menores, especialmente crianças.

Até o início da década de 50, acreditava-se inclusive que a visita dos pais inibia a cura das patologias das crianças e adolescentes o que gerava um ambiente isolado do convívio

familiar para estes pacientes pediátricos, em um hospital que tendia a tratar estes infantes como autônomos (SHIELD *et al,* 2007, 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 (SHIELD *et al,* 2007 e BOWLBY, 1971 e 1973).

O 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, com o envolvimento desta última na totalidade de aspectos do cuidado (PALMER, 1993).

Neste ambiente a família é reconhecida como especialista no cuidado de seu filho (SHIELD et al, 2007), sendo criado um ambiente onde não se preocupa mais 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 Em 1992, *o Institut for Family Centered Care* foi estabelecido nos EUA, assumindo o papel da *Association for the Care of Children's Health*, cuja tarefa era desenvolver um programa nacional para aprimorar a implementação de uma abordagem centrada na família para o cuidado de bebês, crianças e adolescentes. (SHIELD et al, 2007).

Este formato de *Children´s Hospital* acabou por ser expandido para o território nacional com a criação de hospitais exclusivamente pediátricos, voltados para uma assistência completa para estas crianças e adolescentes.

Em um hospital nesta formatação os processos assistenciais do dia a dia importam, quase que na totalidade, no tratamento de dados pessoais, porque se limitam a coleta de dados previstos no LGPD (BRASIL, 2018), sendo que em sua maioria são dados sensíveis (HAWRYLISZYN, COELHO e BARJA, 2021).

Estes tratamentos estão vinculados a atividades assistenciais eletivas, consultas, procedimentos de urgência e emergência e unidade de internação, sejam convencionais sejam de tratamento intensivo.

Um hospital então é um dos pontos com celeuma dentro de toda a cadeia de consumo, na medida que detém criticidade nos dados ao qual controla, o que implica em uma urgência na implementação de um programa de compliance com a LGPD e na correta gestão dos dados de seus pacientes (GREGORI, 2020).

Além disto, o cuidado com a privacidade do paciente, antes vinculada apenas ao prontuário, teve que ser expandida para todo o processo (RIVAROLLI e DAL FARRA NASPOLINI, 2023), o que leva a necessidade de implementação de um programa de privacidade e proteção dos dados dos pacientes deste hospital.

2.2 GOVERNANÇA DE DADOS

Governança é um termo amplo que se refere à maneira como uma organização ou sistema é gerenciado, administrado e supervisionado. O conceito de governança é aplicado em várias áreas, como empresas, governos, instituições sem fins lucrativos e até mesmo em nível global. (MACHADO FILHO, 2020).

A governança tem como objetivo estabelecer um conjunto de regras, processos, políticas e práticas que orientem as decisões e as ações dos indivíduos e grupos responsáveis pela

administração de uma entidade. Ela busca garantir a transparência, a prestação de contas, a equidade, a responsabilidade e a eficácia das organizações. (MACHADO FILHO, 2020).

No contexto empresarial, a governança refere-se ao sistema pelo qual as empresas são dirigidas e controladas. Ela abrange aspectos como a estrutura de poder e autoridade, a relação entre acionistas, diretores e executivos, a divulgação de informações financeiras e não financeiras e a proteção dos direitos dos acionistas.

Já no âmbito governamental, a governança refere-se aos processos e mecanismos pelos quais as instituições políticas são organizadas, regulamentadas e controladas, abrangendo aspectos como a divisão de poderes, a prestação de serviços públicos, a tomada de decisões, a transparência e a participação do cidadão. (KREUZBERG et al 2019).

A governança também pode ser aplicada em outros setores, como organizações sem fins lucrativos, organizações internacionais e até mesmo na governança global, onde se busca estabelecer mecanismos de cooperação e coordenação entre os países. (MACHADO FILHO, 2023).

Em resumo, o conceito de governança envolve a definição e implementação de estruturas, processos e práticas que visam assegurar uma gestão adequada, responsável e eficiente das organizações e sistemas, promovendo a transparência, a responsabilidade e o alcance de objetivos comuns (VIEIRA et al 2019).

Governança de dados por sua vez é o processo de controle, acesso, gestão, armazenamento e proteção dos dados da empresa como um ativo, que foca no quesito qualidade, o que abrange segurança da informação, uso ético do dado e privacidade deste dado (VENTURA e COELI, 2018).

A governança de dados, antes uma ferramenta afastada e incomum passou a ser mais utilizada com a criação das legislações de proteção de dados, aos quais pode-se citar a LGPD, posto que estas legislações impuseram medidas de gestão e proteção dos dados pessoais (BERGAMINI, CRISTOVAM e HAHN, 2021).

A LGPD, em seu artigo 50, é expresso a determinar que as empresas devem implementar um programa de governança que possibilite uma gestão abrangente relativa à proteção de dados pessoais, inclusive com adoções de boas práticas (BRASIL, 2018). Além disto há a criação de um direito à informação ao titular de dados, o que demanda o estabelecimento de um canal de comunicação e consequentemente a implementação de um programa de governança.

A proteção de dados assim se torna um ponto motivador para a tomada de condutas para construção de um programa de governança, seja pela imposição legal, seja pelo ganho estratégico na implementação de um programa de privacidade e proteção de dados (BERGAMINI, CRISTOVAM e HAHN, 2021).

2.3 PROTEÇÃO DE DADOS

A proteção à privacidade está prevista na Constituição Federal, artigo 5º, inciso X (BRASIL, 1988) bem como no Marco Civil da Internet, lei 12.965/2014 (BRASIL, 2014), sendo que após a massificação dos computadores portáteis, passou a ser uma preocupação global, o que levou a promulgação de legislações restritivas (BOLLIVAR e MONACO, 2020).

Apesar de parecer muito natural na discussão jurídica e tecnologia atual o conceito de privacidade é discutido somente a partir do final do século XIX (MILLER, 1971), sendo bastante conhecido a sua origem lendária, através de cunho do termo *privacy* por Louis D.

Brandeis em seu trabalho *The Right to Privacy* (ASHMAN, 1971), onde a privacidade é definida como o direito de ser deixado em paz (BRANDEIS e WARREN, 1890).

Importante citar que a construção de Brandeis, apesar de massificar o uso do termo, não foi em realidade inovador, honra que cabe a um Juiz da Suprema Corte do Estado de Michigan, que em julgado paradigma criou o termo *the right to be let alone* sem, entretanto, vinculá-lo a um conceito (ZANON, 2013).

No Brasil, com o advento da Constituição da República Federativa do Brasil o termo privacidade passa a assumir feições mais modernas e conhecidas (DONEDA, 2006), ficando consignado, no já citado artigo 5° Inciso X da CF/88 que a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis, derivando daí também a inviolabilidade de correspondência, comunicações telemáticas e demais comunicações de cunho privado.

A privacidade, portanto, é um direito a personalidade do indivíduo, que mantém em sua projeção os valores inatos da sociedade ao qual está inserido (GUERRA, 2004), sendo reconhecido a proteção à privacidade na Declaração Universal dos Direitos Humanos, em seu artigo 12 (ONU, 1948).

Do ponto de vista semântico Privacidade pode ser definida, com base na interpretação legal, como o direito que uma pessoa tem, ou seja, uma faculdade, de constranger os outros ao respeito e de resistir a violação de sua intimidade (GUERRA, 2004).

Importante destacar que a privacidade somente existe com a existência da Proteção de Dados, vez que tendo em vista que o direito à privacidade é um direito negativo e de eficácia limitada (MORAES, 2014) é necessário manter a proteção deste direito não através de outro direito, que seria subjugado pela mesma problemática, mas sim através da criação de um dever imposto a todos para manter e guardar a privacidade (BURKART, 2021).

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

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 procedimentos para correta utilização dos dados coletados, para, em *última ratio* 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 jurídica própria (OLIVEIRA et al, 2019) ambos se relacionam intrinsicamente, posto que enquanto a Privacidade do indivíduo é o que exige que as empresas adotem medidas de proteção de dados, está última é a conduta que, se realizado, mantem a privacidade intacta.

Assim, para criar este dever dentro do ordenamento jurídico, que contava com o direito à privacidade parcialmente ineficaz (GRECO FILHO, 1986) promulgou-se a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 12.709/2018, que trouxe uma importante contribuição para a operacionalização da proteção dos dados pessoais, e que foi amplamente inspirado na General Data Protection Regulation da União Europeia (EU, 2016).

A LGPD implementa então a necessidade de construção de um programa de privacidade e proteção de dados, programa este que é construído através de um programa de governança de

dados, na medida em que obriga adoção de medidas de segurança da informação, gestão e controle de todos os dados coletados (BERGAMINI, CRISTOVAM e HAHN, 2021).

2.4 *BUSINESS PROCESS MANAGEMENT*

Business Process Management (BPM) é uma metodologia que auxilia a organização estrategicamente gerir seu empreendimento, posto que é focada a identificar, desenhar, documentar, medir, monitorar, controlar e melhorar os processos da organização compreendendo também os meios estratégicos pretendidos (GATTO, 2019 e CALAZANS, KOSLOSKI e GUIMARÃES, 2016).

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).

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* ou BPMN, para uma notação rápida e padronizada (GATTO, 2019 e PILLAT et al., 2015).

Importante citar que o BPMN é uma ótima ferramenta para a implementação, ou criação de um framework, de privacidade e proteção dos dados, posto 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).

3 METODOLOGIA

A Trata-se de uma pesquisa experimental realizada em um hospital pediátrico de médio porte situado na cidade de São Paulo, com cerca de 180 leitos de internação. Realizou-se uma revisão da literatura, buscando artigos publicados no período de 2018 a 2023. O período selecionado, tendo em vista que a LGPD foi aprovada no ano de 2018, havendo imposição legal quanto a proteção de dados apenas partir deste ano.

Ademais, a revisão foi realizada nas seguintes bases eletrônicas Portal de Periódicos Capes, IEEExplore, PuBMed e Scielo. Foram empregando os seguintes descritores na língua portuguesa e na língua inglesa: Hospital Pediátrico, Proteção de Dados, COBIT 2019, Boas Práticas de Segurança da Informação, Governança de Hospital Pediátrico.

A partir da pesquisa realizada foram selecionados 88 artigos analisados com base nos seguintes critérios de seleção:

- Referir-se à privacidade e proteção de dados;

-Tratar do tema de proteção de dados aplicado à saúde;

- Tratar do impacto da LGPD na área da saúde.

Dos 88 artigos selecionados foram desconsiderados os que obedeciam aos seguintes critérios de exclusão:

-Artigos fora do período proposto;

-Não tratam sobre o tema;

-Não disponíveis de forma online e;

-Apareceram em duplicidade nas bases de dados consultadas.

Foram então considerados 50 trabalhos que atenderam ao critério de seleção.

A criação do *framework* foi procedida por uma análise de todos os processos que tratam dados pessoais do hospital pediátrico, sendo também coletado os tipos de dados coletados nestes processos, sendo identificado os seguintes tipos de dados: Informações de identificação pessoal; Dados de identificação eletrônica; Dados Financeiros; Detalhes do Plano de Saúde do Paciente; Dados de Autorizações ou 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 a saúde.

O desenvolvimento do *framework* foi realizado em sete fases distintas apresentadas na Figura 1.

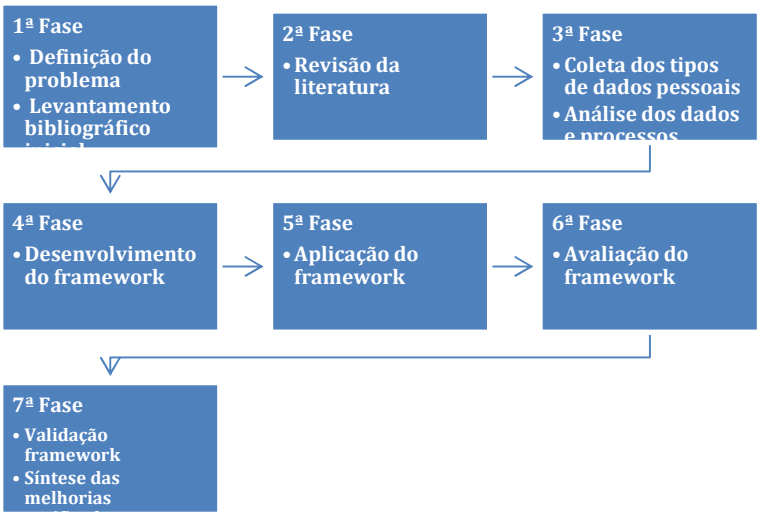

Figura 1: Fases do desenvolvimento do *framework* para implementar um programa de governança dados em um hospital pediátrico.
Fonte: Os Autores.

Descreve-se a seguir as sete fases de desenvolvimento do *framework*:

-1ª Fase: Definição do problema, realização do levantamento bibliográfico inicial.

-2ª Fase: Foi realizada a revisão da literatura, de modo a construir os conceitos e fundamentos teóricos do trabalho e determinar a lacuna de pesquisa na literatura;

-3ª Fase: Coleta dos tipos de dados pessoais tratados no ambiente do hospital, realização do mapeamento de dados e de processos e análise do risco identificado em cada um dos processos previamente mapeados.

-4ª Fase: Com base no plano de recomendação e dados levantados, desenvolve-se o framework para criação de um modelo reproduzível de programa de governança de dados;

-5ª Fase: Aplica-se o Framework na organização e, adota-se as medidas indicadas;

-6ª Fase: Os resultados da aplicação do Framework são avaliados. Esta fase encontra-se em desenvolvimento;

-7ª Fase: Validação dos resultados e indicadores e síntese das melhorias verificadas no ambiente. Esta fase encontra-se em desenvolvimento.

O desenvolvimento deste *framework* vai apoiar a implementação do programa de governança de dados no hospital pediátrico na medida em que dará meios para que seja aprimorado a gestão de dados da organização, com a construção de uma proteção de dados efetiva no ambiente hospitalar. Por sua vez as fases 3, 4 e 5 foram subdivididas em seis etapas para a correta análise do ambiente, desenvolvimento do *framework* e implementação dele no hospital.

Apresenta-se na Figura 2 as seis etapas de implementação de um programa de privacidade e proteção de dados em um hospital pediátrico.

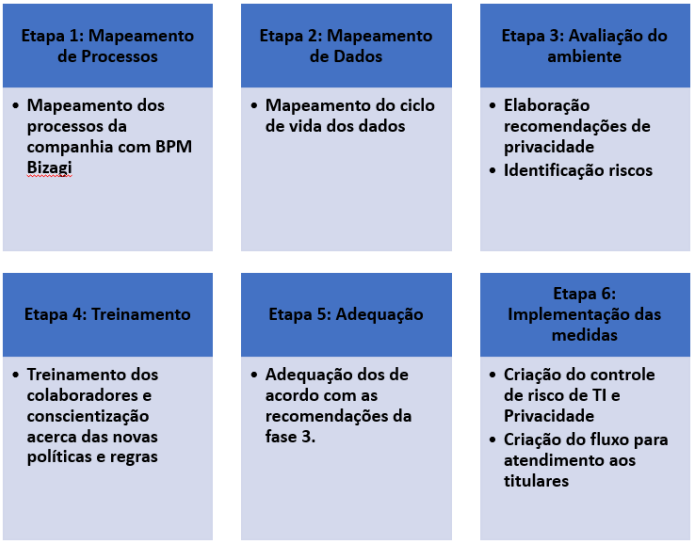

Figura 2 - Etapas de implementação do programa de privacidade e proteção de dados em um hospital pediátrico.
Fonte: Os Autores.

Descreve-se a seguir as etapas de implementação do programa de privacidade e proteção de dados:

-Etapa 1 (Fase 3): Mapeamento de Processos – Nesta etapa é realizado toda a identificação dos processos do hospital utilizando a notação do *Business Process Model and Notation* (BPM CBOK, 2014).

-Etapa 2 (Fase 3): Mapeamento de Dados – Identificado os processos que tratam dados pessoais é realizado um inventário, identificando todo o ciclo de vida dos dados, do início à sua exclusão e, quais dados são coletados e cada um dos processos.

-Etapa 3 (Fase 3): Avaliação do Ambiente - Com base no mapeamento de processo realizado e com base da existência de base legal, são identificados os riscos existentes e formulado um plano de recomendações para cada processo mapeado.

-Etapa 4 (Fase 3): Treinamento – Conscientização de todos os colaboradores do hospital de forma a educá-los quanto as mudanças necessárias para conformidade com a LGPD e treinamento acerca das novas políticas.

-Etapa 5 (Fase 4): Adequação – Com base nas recomendações e análise realizadas na etapa 3 são realizadas todas as alterações, de processos, sistemas e pessoas, para cumprimento

das recomendações gerada na etapa anterior. Nesta etapa é feito a mitigação dos riscos identificados e é escriturado o risco remanescente para acompanhamento.

-Etapa 6 (Fase 5): Implementação – Terminada a implantação das medidas necessárias é criado os mecanismos de controle dos processos, através de planilha que pode ser automatizada e é implementado o canal de atendimento aos titulares, para atender o artigo 18 da LGPD.

4 RESULTADOS E DISCUSSÃO

No tocante a 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 a conclusão oficial desta atividade. Isto prejudica, de sobremaneira a gestão e desenvolvimento das atividades do hospital pediátrico, ainda mais sendo considerado que a uma rotatividade de funcionários assistenciais, como enfermeiros e médicos, e acabam por levar o conhecimento processual desenvolvido.

Após o início da implementação do programa de privacidade e proteção de dados foram mapeados 533 processos, com a sua formalização realizando a metodologia BPMN, o que significou a identificação de 357 processos onde há tratamento de dados pessoais.

Iniciando a gestão destes processos, foi desenvolvido um registro para cada uma das atividades coletam, produzem, recepcionam, classificam, utilizam, acessam, reproduzem, transmitem, distribuem, processam, arquivam, armazenam, eliminam, avaliam ou controlam dados pessoais.

A partir da sistematização e formalização destes registos foi possível identificar uma série de informações sobre a natureza destes tratamentos, como volume de coleta de dados de crianças e adolescentes, base legal aplicável, criticidade e interrelações entre tais dados

A Figura 03 demonstra dentre os processos que tratam dados pessoais a porcentagem de tratamento de dados de crianças e adolescentes:

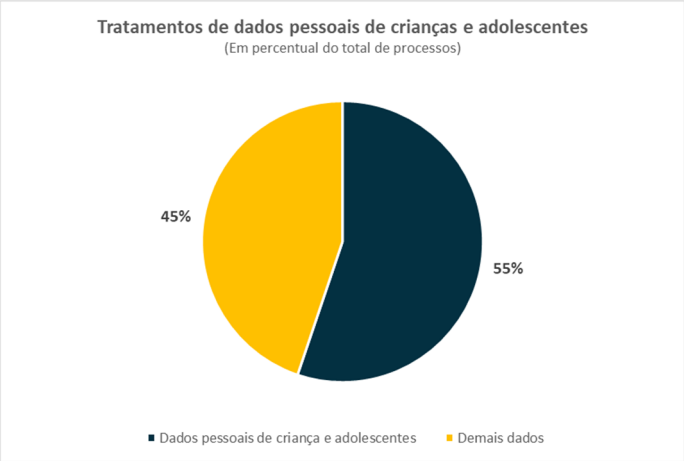

Figura 03 - Porcentagem de tratamentos de dados que envolvem crianças e adolescentes.
Fonte: Os Autores

Fazendo a divisão dos processos que tratam dados pessoais por área, tem-se os seguintes resultados quanto às cinco áreas que mais tratam dados pessoais apresentados no Quadro 1.

Área	Número de Processos
Administração de Pessoal	23
Instituto de Pesquisa	22
Relacionamento médico e Residência	20
Unidade de Tratamento Intensivo	20
Atendimento	19

Quadro 1: Número de Processos que tratam dados pessoais por área de negócio.
Fonte: Os Autores.

Também foi possível averiguar que o hospital pediátrico trata em sua grande maioria dados sensíveis, como se verifica da Figura 04.

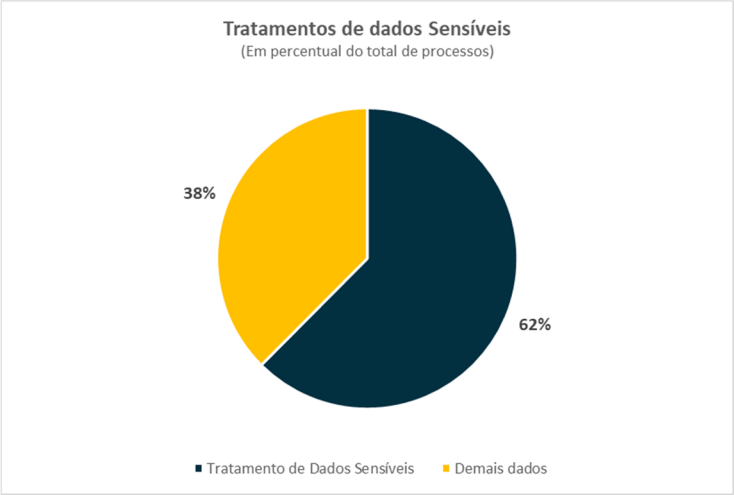

Figura 04 - Porcentagem de tratamentos de dados que envolvem dados sensíveis.
Fonte: Os Autores.

Passou-se, então para construção das políticas da organização. Apresenta-se no Quadro 2, as quatorze mais importantes do total de vinte e sete políticas.

Passou-se, então, para a construção das políticas da organização. Apresenta-se no Quadro 2, as quatorze políticas mais importantes do total de vinte e sete.

	Políticas
1	*Backup* e Restauração
2	Resposta a Incidentes de Segurança da Informação
3	Segurança da Informação
4	Uso de *Internet*
5	Senhas
6	*E-mail*
7	Classificação e Uso da Informação
8	Governança de Dados Pessoais
9	Controle de Acesso ao Banco de Dados

10	Uso de Comunicadores Instantâneos
11	Controle de Acesso Lógico
12	Prevenção de Perda de Dados
13	Privacidade
14	Acesso Remoto

Quadro 2: Políticas criadas.
Fonte: Os Autores.

O *framework* apoiou a elaboração destas políticas posto que trouxe um norte para as determinações necessárias para aprimoramento do ambiente de governança de dados esperados, bem como direcionou a metodologia necessária para avaliação do ambiente e elaboração dos textos.

Ademais a construção destas políticas tem a finalidade de trazer normas e regulação para a organização, trazendo um nível mínimo de governança e implementando o artigo 50 da LGPD (BRASIL, 2018).

5 CONSIDERAÇÕES FINAIS

Espera-se que a implementação do programa de governança de dados contribua para o aprimoramento dos processos institucionais, posto que o mapeamento de processos e o mapeamento de dados implementa uma gestão de negócio, resulte na melhoria contínua do ambiente hospitalar, inclusive no tocante ao dever assistencial.

O aprimoramento dos processos do hospital pediátrico contribuirá para uma melhor tutela da saúde dos pacientes de hospital, posto que, além de terem seus dados tratados de maneira protegida, e respeitando seus direitos e garantias individuais, haverá uma governança de dados em toda a coleta que propiciará uma diminuição em erros advindos do tratamento equivocado de dados pessoais, como identificação equivocada de pacientes e outros erros da assistência que tem como fator base um erro de tratamento de dados.

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, e em última instancia, contribuindo para uma infância feliz.

O objetivo foi alcançado na medida em que a construção de um framework para um programa de privacidade e proteção de dados foi capaz de construir um ambiente com diminuição de risco ao hospital pediátrico, uma melhoria na gestão de processos e o aprimoramento da proteção aos dados dos titulares, sejam eles pacientes ou colaboradores.

A replicabilidade do framework é importante para todo o ambiente hospitalar na medida em que possibilita aos hospitais pediátricos a utilização deste mesmo modelo para dar um salto de qualidade e contribuir para própria formação da organização, com resultados esperados benéficos aos seus pacientes e sociedade.

Entende-se que o presente trabalho é limitado por ter sido desenvolvido com base no paradigma de um hospital, exclusivamente pediátrico, ou seja, que detém apenas processos que se relacionam, ou Inter relacionam com dados de crianças e adolescentes.

Assim, o framework desenvolvido não é reproduzível para qualquer entidade hospitalar que não seja pediátrica, posto que as características marcantes desta última são diversas dos demais hospitais.

REFERÊNCIAS

ANDERSON, T; **Governança Digital**. 1ª edição, São Paulo: Editora Senac, 2022.

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. Brasília: ANPD, 2022.

AGOSTINELLI, S., MAGGI, F; MARELLA, A; SAPIO, F. Achieving GDPR compliance of BPMN process models. **International Conference on Advanced Information Systems Engineering**. Springer, v. 455, p. 10–22, 2019.

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

BOLIVAR, A., MONACO, G. F. C. **LGPD NA SAÚDE**. 1ª edição, São Paulo: Revista dos Tribunais, 2020.

BOWLBY, J.; **Attachment and loss.** 2ª Edição, Harmondsworth, UK: Penguin, 1971.

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

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

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

BURKART, D., VINCENZI V. **Proteção de dados e o estudo da LGPD**. Dissertação de Mestrado – Faculdade de artes, Arquitetura e Comunicação, Universidade Estadual Paulista "Júlio de Mesquita Filho", Bauru, 2021

BERGAMINI, J. C. L., CRISTOVAM, J. S. d. S., HAHN, T. M. Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). **Interesse Público TJDF**, v. 23, n. 129, p. 75-102, 2021.

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

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

GATTO, D., **Sistema Especialista no Apoio à Classificação de Criticidade de Versão de Software**. Dissertação de Mestrado – Programa de Pós-graduação em Informática e Gestão do Conhecimento, Universidade Nove de Julho, São Paulo, 2020.

GOSTIN, L., NASS, S. Reforming the HIPAA Privacy Rule: Safeguarding Privacy and Promoting Research. **JAMA: the journal of the American Medical Association**. v. 301, p. 1373-1375, 2009.

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.

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.

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, p. 5570–5583, 2023.

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, p. 01-13, 2021.

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.

KREUZBERG, F., VICENTE, E. F. R. Para onde estamos caminhando? Uma análise das pesquisas em governança corporativa. **Revista de Administração Contemporânea**, v. 23, p. 43-66, 2019.

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

MACHADO FILHO, Cláudio Pinheiro. **Responsabilidade social e governança: o debate e as implicações**. São Paulo: Pioneira Thomson Learning, 2020.

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

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

OLIVEIRA, A. P. 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, p. 01-29, 2019.

PALMER, S. J. Care of sick children by parents: a meaningful role. **Journal of Advanced Nursing**, v. 18, n. 2, p. 185–191, 1993.

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, n. 01, p. 95-115, 2015.

RIVAROLLI, M. A., DAL FARRA NASPOLINI, S. H. Privacidade e proteção de dados em nosocômios e clínicas perante a LGPD. **Scientia Iuris**, v. 27, n. 1, p. 112–128, 2023.

SHIELDS, L., PRATT, J., DAVIS, L., HUNTER, J., Family□centred care for children in hospital. **Cochrane Database of Systematic Reviews**, v. 1, n. 1, p. 01-29, 2007.

VENTURA, M., COELI, C. M. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. **Caderno de Saúde Pública**, Rio de Janeiro, v. 34, n. 7, p. 3-7. 2018

VIEIRA, J. B., BARRETO, R. T. S. **Governança, gestão de riscos e integridade**. Brasília: Escola Nacional de Administração Pública, 2019.

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

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.