DOI: 10.24325/issn.2446-5763.v7i20p380-396

South American Development Society Journal

Vol.: 07, | Nº.: 20 | **Ano:** 2021 | **ISSN:** 2446-5763 | **DOI:** 10.24325/issn.2446-5763.v7i20p380-396
Data de Submissão: 24/04/2021 | **Data de Publicação:** 31/08/2021

LGPD O NOVO DESAFIO PARA AS ORGANIZAÇÕES: EXEMPLOS DE FRAMEWORKS PARA DIAGNOSTICAR ESTE NOVO CENÁRIO

Prof. Dr. Marcelo T Okano - CEETEPS – Unidade de Pós-graduação, Extensão e Pesquisa
https://orcid.org/0000-0003-1680-7821

Lamara Ferreira - CEETEPS – Unidade de Pós-graduação, Extensão e Pesquisa
https://orcid.org/0000-0002-9790-9485

Henry de Castro Lobo dos Santos - UNICAMP – Faculdade de Tecnologia
https://orcid.org/0000-0003-1400-3811

Prof. Dr. Edson L Ursini - UNICAMP – Faculdade de Tecnologia
https://orcid.org/0000-0002-1597-4057

Resumo

A temática “dados pessoais” está em alta devido ao lançamento da Lei Geral de Proteção de Dados (LGPD), também conhecida como Lei nº 13.709/2018, e trata de qualquer relação entre o tratamento de informações classificadas como dados pessoais por qualquer meio, seja pessoa física ou jurídica, a proteção de dados pessoais. Este novo cenário para as empresas e organizações exigirá diversas adaptações e ajustes nos processos que envolvam dados pessoais, um diagnóstico inicial, para verificar se estes processos estão adequados ou não a LGPD, será necessário para orientar e organizar os procedimentos. Isso posto, este artigo tem o objetivo de levantar e discutir os modelos ou frameworks existentes na literatura para diagnosticar se os processos estão adequados ou não a LGPD. O objetivo desta pesquisa foi alcançado, pois identificou-se e discutiu-se dois modelos ou frameworks existentes na literatura para diagnosticar se os processos estão adequados ou não a LGPD. A importância destes frameworks é grande, pois facilita e organiza os diagnósticos dos processos das empresas em relação ao LGPD.

Palavras-chave: LGPD; Framework LGPD; LGPD model Canvas

Abstract

The theme “personal data” is on the rise due to the launch of the General Data Protection Law (LGPD), also known as Law No. 13.709 / 2018, and deals with any relationship between the treatment of information classified as personal data by any means, whether natural or legal, the protection of personal data. This new scenario for companies and organizations will require several adaptations and adjustments in the processes that involve personal data, an initial diagnosis, to verify if these processes are suitable or not the LGPD, it will be necessary to guide and organize the procedures. That said, this article aims to raise and discuss the models or frameworks existing in the literature to diagnose whether the processes are suitable or not to LGPD. The objective of this research was achieved, since two models or frameworks existing in the literature were identified and discussed to diagnose whether the processes are suitable or not to LGPD. The importance of these frameworks is great, as it facilitates and organizes the diagnostics of companies' processes in relation to LGPD.

Keywords: LGPD; LGPD Framework; LGPD model canvas

Introdução

O mundo passa por constantes transformações que de alguma forma mudam a trajetória e a história da humanidade (Okano, 2017)**.** Atualmente**,** a temática “dados pessoais” está em alta devido ao lançamento da Lei Geral de Proteção de Dados (LGPD), também conhecida como Lei nº 13.709/2018, e trata de qualquer relação entre o tratamento de informações classificadas como dados pessoais por qualquer meio, seja pessoa física ou jurídica, a proteção de dados pessoais (PINHEIRO, 2018).

A LGPD estipula que pessoas físicas ou jurídicas processem dados pessoais de acordo com o direito público ou privado, e seu objetivo é proteger os direitos básicos de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas, incluindo mídia digital (Artigo 1) (MACIEL, 2018).

De acordo com Maciel (2018), a LGPD aplica-se a todas as operações de tratamento realizadas no Brasil, com o objetivo de ofertar bens, serviços ou tratar dados de indivíduos localizados no país ou ainda, que tenham sido coletados no território nacional.

Todas as empresas terão que se adaptar a essa nova lei e a partir de agosto de 2021, pois a privacidade dos dados pessoais envolve as organizações em todos os níveis e sofrerão penalidades legais se não cumprirem as suas exigências.

A Agência Nacional de Proteção de Dados (ANPD) deve fiscalizar o cumprimento da lei por parte dessas empresas, incluindo a aplicação de multa de até 50 milhões de reais por infrações. Novos direitos foram concedidos, incluindo a possibilidade de solicitar acesso aos seus dados pessoais em formato legível por máquina. Para cumprir esse direito, a empresa deve estabelecer procedimentos internos para devolver os dados ao titular em tempo hábil (LOHMANN et al., 2021).

Este novo cenário para as empresas e organizações exigirá diversas adaptações e ajustes nos processos que envolvam dados pessoais, um diagnóstico inicial, para verificar se estes processos estão adequados ou não a LGPD, será necessário para orientar e organizar os procedimentos.

Isso posto, este artigo tem o objetivo de levantar e discutir os modelos ou frameworks existentes na literatura para diagnosticar se os processos estão adequados ou não a LGPD. Justifica-se a relevância do artigo pela novidade do tema e a falta de literatura referente ao assunto.

2 Referencial conceitual

Este tópico aborda os principais conceitos estudados neste artigo como LGPD, privacidade de dados e framework conceitual.

2.1 LGPD

A Lei de Proteção de Dados Pessoais (também conhecida como LGPD) é uma lei promulgada pelo Presidente Brasileiro Michel Temer em 14 de agosto de 2018 e originada do nº 53/2018. Trata-se de uma legislação altamente técnica que reúne uma série de itens de controle para assegurar que as garantias prestadas sejam cumpridas com base na proteção dos direitos humanos (Pinheiro, 2019).

O espírito da lei é proteger os direitos básicos de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas. Ela fornece um pré-requisito de honestidade e credibilidade para todos os tipos de processamento de dados

pessoais. Agora, o processamento de informações pessoais deve estar em conformidade com uma série de aspectos, na vida do uso da informação: Usar informação dentro do ciclo que identifique ou possa identificar uma pessoa e é relevante para ela, incluindo categorias de dados sensíveis (Pinheiro, 2019).

Segundo Maciel (2018), a LGPD traz como fundamentos para a utilização de dados pessoais:

1. o respeito à privacidade;

2. a autodeterminação informativa;

3. a liberdade de expressão, de informação, de comunicação e de opinião;

4. a inviolabilidade da intimidade, da honra e da imagem;

5. o desenvolvimento econômico e tecnológico e a inovação;

6. a livre iniciativa, a livre concorrência e a defesa do consumidor; e

7. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os principais conceitos do LGPD estão no Quadro 01:

Quadro 01 – Principais conceitos

Tratamento dos dados	- Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Pinheiro, 2019). - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (Brasil, 2018)
Dados pessoais	- Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de

	automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva (PINHEIRO, 2019). - Informação relacionada a pessoa natural identificada ou identificável; (BRASIL, 2018).
Dados pessoais sensíveis	- São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (PINHEIRO, 2019) - 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 natura (BRASIL, 2018).
Dado anonimizado	- São os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento (PINHEIRO, 2019). - Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (BRASIL, 2018).
Titular	- Pessoa a quem se referem os dados pessoais que são objeto de algum tratamento (PINHEIRO, 2019). - Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018).
Consentimento	- Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Não é o único motivo que autoriza o tratamento de dados, mas apenas uma das hipóteses (PINHEIRO, 2019). - Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

	(BRASIL, 2018).
Controlador	- Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018).
Operador	- Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).
Encarregado	- Pessoa natural, indicada pelo controlado, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional (PINHEIRO, 2019). - Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).
Agentes de tratamento	- O controlador que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal (PINHEIRO, 2019). - O controlador e o operador (BRASIL, 2018).

Fonte: Pinheiro (2019) e Brasil (2018).

2.2 Privacidade de dados

O aumento da capacidade de armazenamento de dados e informações por meio de novas tecnologias de armazenamentos como *Datawarehouse*, Data Mining, big data, *cloud computing*, e etc. acelerou a necessidade cada vez maior de cuidar e proteger este ativo das organizações.

De acordo com Brito & Machado (2017), garantir a privacidade dos indivíduos tem impacto direto na qualidade dos dados publicados, visto que a privacidade e a utilidade dos dados são princípios inversamente proporcionais. Quanto maior a privacidade, menor será a utilidade dos dados para análise, e vice-versa.

O conceito de privacidade está relacionado a pessoas, com mais precisão com o direito que as pessoas precisam manter um espaço pessoal, sem interferência de

outras pessoas ou organizações. Desta forma, depende deles para decidir manter suas informações sob o seu controle único ou informar, decidir quem, quando e onde suas informações estarão disponíveis (Brito & Machado, 2017).

Conforme Freitas (2021), a política de privacidade é um dos instrumentos de implementação do *privacy by design* e faz parte da estrutura de documentos para a proteção de dados. A política objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo princípios da Lei Geral de Proteção de Dados Pessoais (LGPD).

O conceito de *Privacy by Design* foi proposto para servir como uma diretriz sobre como abordar essas questões. *Privacy by Design* consiste em uma série de princípios que podem ser aplicados desde o início do desenvolvimento de sistemas para mitigar preocupações de privacidade e alcançar conformidade de proteção de dados (GÜRSES et al, 2011).

Cavoukian (2009) apresenta os seguintes princípios orientadores:

1. Proativo e não reativo; preventivo e não corretivo;

2. Privacidade como padrão;

3. Privacidade incorporada ao design;

4. Funcionalidade completa: soma positiva e não soma zero;

5. Segurança ponta a ponta: proteção durante todo o ciclo de vida;

6. Visibilidade e transparência;

7. Respeito pela privacidade do usuário.

A política de privacidade é única e orientada ao serviço e à organização responsável, inclusive no que tange à linguagem utilizada, algumas mais formais, outras informais. Não importa a forma, é preciso garantir que o conteúdo seja conciso, de fácil acesso e compreensão. Utilizar aspectos visuais, como vídeos e imagens, pode ser um bom instrumento para facilitar o entendimento da política (Freitas, 2021).

2.3 Framework conceitual

De acordo com o CAMBRIDGE DICTIONARY (2021), o termo framework é um sistema de regras, ideias ou crenças que é usado para planejar ou decidir algo ou as ideias, informações e princípios que formam a estrutura de uma organização ou plano.

A WIKIPEDIA (2021) define framework, ou arcabouço conceitual, como um conjunto de conceitos usado para resolver um problema de um domínio específico. Framework conceitual não se trata de um software executável, mas sim de um modelo de dados para um domínio.

O framework conceitual será utilizado para descrever e comparar os modelos e procedimentos descritos nos artigos pesquisados.

O framework conceitual deve destacar os principais conceitos e estruturas utilizadas na pesquisa e as relações entre eles. Esta construção deve ser feita em formato de texto, mas pode ser auxiliada por gráficos ou diagramas. O importante a notar aqui é que a "estrutura conceitual" informa ao leitor o conceito no qual a pesquisa se baseia, como lê-la, quais conversas foram feitas com pesquisas anteriores e quais aspectos do fenômeno foram analisados (AZEVEDO, 2016).

3. Metodologia

Esta pesquisa pode ser classificada como exploratória pois de acordo com Gil (2002), tem objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de ideias ou a descoberta de intuições.

Para atingir o objetivo desta pesquisa foi utilizada a revisão bibliográfica sobre os temas LGPD, privacidade de dados e framework conceitual. Tentou-se fazer uma pesquisa bibliométrica nas bases Scopus e WOS, mas o resultado foi insatisfatório, retornou seis documentos e nenhum deles foi selecionado. Então, foi realizado uma revisão descritiva com o Google Acadêmico e foram selecionados 2 documentos.

Conforme Paré et al. (2015), as revisões descritivas procuram determinar até que ponto um corpo de estudos empíricos em uma área de pesquisa específica apoia ou revela quaisquer padrões ou tendências interpretáveis com respeito a proposições, teorias, metodologias ou descobertas pré-existentes.

Os frameworks selecionados estão descritos a seguir:

- O framework LGPD Model Canvas, criado por Lamara Ferreira, foi inspirada nos métodos ágeis, nos pilares do modelo Privacy by Design, nos benefícios do Design Thinking e no modelo Business Model Canvas e pode ser aplicado nas empresas que buscam se adequar a LGPD.
- O FRAMEWORK LGPD, criado por Silva (2021), utiliza as referências bibliográficas relacionadas às principais leis mundiais de proteção e privacidade de dados como GDPR, CCPA e LGPD. Foi elaborado um modelo composto por cinco fases: de iniciação, conhecimento, validação, desenvolvimento e encerramento.

4. Resultados e análises

4.1 LGPD *Model Canvas*

A inspiração para este modelo foi o Business Model Canvas, que de acordo com Clark (2013) o quadro de modelo de negócios confere um atalho visual para simplificar organizações complexas. Na mesma perspectiva, Clark (2013) reforça que as imagens ajudam a transformar suposições não verbalizadas em informações explícitas. E que informações explícitas nos ajudam a pensar e comunicar mais efetivamente.

Diante destes conceitos e inspirado nestas poderosas ferramentas, o framework LGPD Model Canvas sugere que a privacidade seja considerada logo do início do projeto, desde a concepção e seja incorporada durante todo o processo e desta forma, o método LGPD Model Canvas será aplicado em dois momentos:

AS IS: Como se fosse uma “foto do momento atual da empresa” onde todos os processos existentes, que realizam o tratamento de dados pessoais serão levantados. No entanto, para que adequação seja efetiva de fato, a equipe de colaboradores da empresa precisa efetivamente “colocar a mão na massa” e visualizar como a privacidade e proteção de dados, influência e reflete no seu dia a dia nos serviços empresariais. Esta ideia vai de encontro com as considerações de Vidal (2006), que diz que o ponto mais vulnerável em um sistema computacional também é o componente humano. Desta forma, somente documentos, ferramentas, tecnologias, treinamentos

de conceitos, não podem resolver todas as questões de privacidade e *compliance* nas organizações.

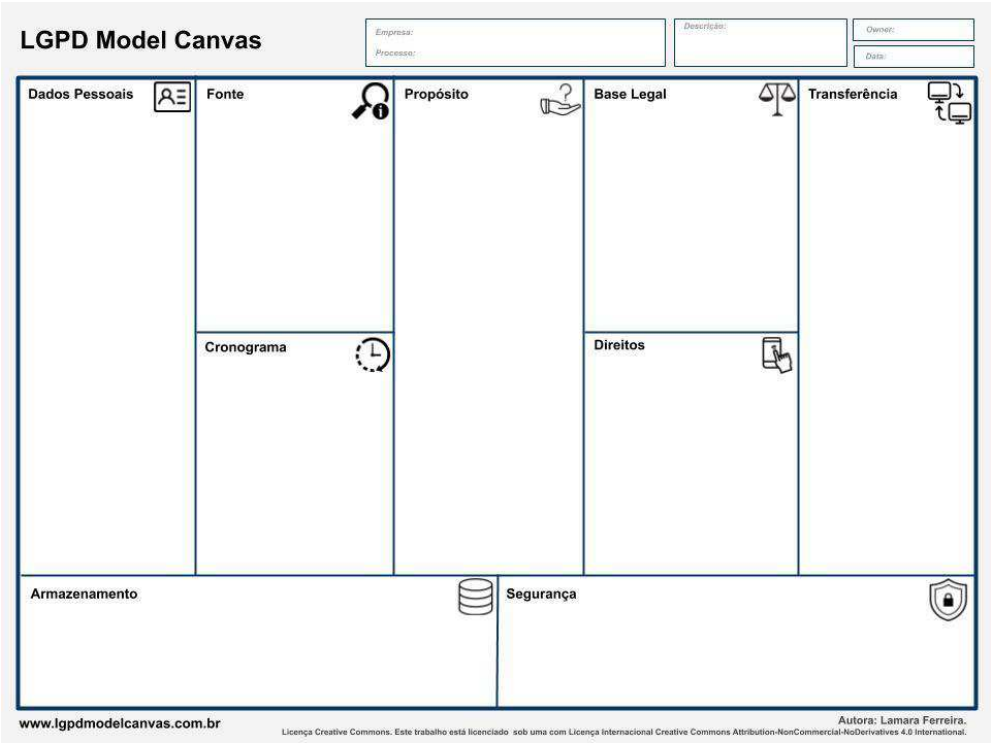
Neste cenário, visando criar uma dinâmica participativa, colaborativa, ágil e eficaz, o LGPD *Model Canvas* pode ser aplicado e incorporado às práticas e rotinas da empresa, assim como ocorrem com os métodos ágeis. Desta forma, a empresa cresce em aprendizagem organizacional, torna a privacidade parte da sua cultura e forma pessoas que serão os facilitadores internos, para tratar no dia a dia, das questões de privacidade ao longo dos projetos de forma proativa e sem silos (departamentos).

Desta forma, ao aplicar o framework LGPD Model Canvas, seja para o mapeamento AS IS (presente) ou TO BE (futuros), a organização deverá levar em conta o processo de brainstorming para concepção da cultura de privacidade. De acordo com Brown (2010) o brainstorm demostra o seu valor quando a meta é abrir uma ampla variedade de ideias. Reforça que outras abordagens são importantes para fazer escolhas, mas que não há nada melhor do que uma boa sessão de brainstorming para criá-las.

Durante o brainstorming com os colaboradores da empresa serão levantados a vivenciar a cultura organizacional, para que possam incluir a privacidade no centro dos processos, como um valor fundamental para toda a organização, corroborando com as ideias da metodologia *Privacy by Design*. Durante esta etapa é questionado a missão, a visão e os valores da organização. Logo em seguida, é a privacidade é relacionada neste contexto: O que significa a privacidade de dados pessoais para a organização e como ela se relaciona com a sua missão, visão e valores.

É iniciado o preenchimento, Figura 01, seguindo a ordem da direita para a esquerda e de cima para baixo, iniciando em “Dados Pessoais” e finalizando em “Segurança”.

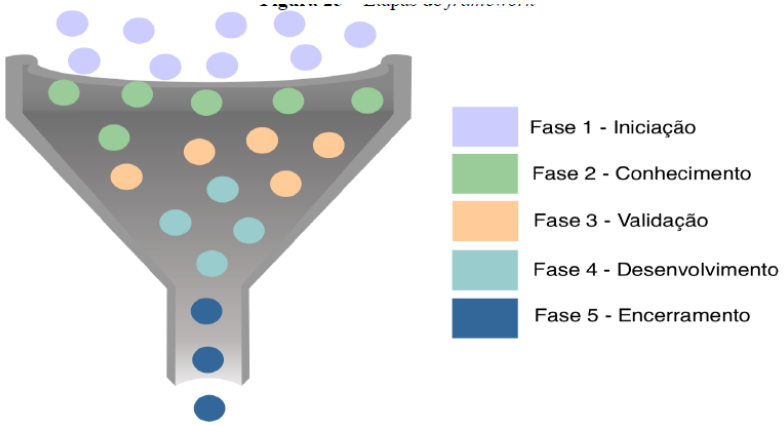
Figura 01 – LGPD Model Canvas



4.2 Framework lgpd

Criado por Silva (2021) contêm 5 fases para diagnosticar os processos para o LGPD, vide Figura 02.

Figura 02 – Fases do Framework LGPD



Fonte: Silva (2021)

Fase 1 - Iniciação

O início desta fase se dá através de uma reunião com a alta gestão da empresa, com o objetivo de obter apoio para desenvolvimento do projeto. Na sequência, é desenvolvida uma carta em que o mais alto cargo CEO/Diretor da organização deverá comunicar a toda a empresa sobre a iniciativa. O comunicado deve atingir todos os colaboradores, externos e internos, em formato digital ou físico quando necessário. A carta descreve um breve histórico da organização, aborda sobre os dias atuais, a necessidade de conformidade, fala sobre a equipe responsável pelo desenvolvimento externo e responsável interno e por fim envolve todos os departamentos e terceiros que trabalhem dentro da organização.

Nesta fase, é ainda necessário criar um comitê de governança de dados e definir um responsável por ele, que será responsável por criar, manter e melhorar a governança dos dados pessoais. Os membros do comitê devem ser pessoas que conheçam a fundo as atividades do seu setor ou departamentos. Após definido esse comitê, o próximo passo é definir uma agenda de treinamentos com os respectivos membros para treiná-los em proteção e privacidade de dados, além de fazê-los ciente dos aspectos gerais da lei geral de proteção de dados.

Fase 2 – Conhecimento

Nesta fase, será necessário listar o cenário de proteção de dados da empresa, de forma a reconhecer quem envia informações pessoais, quais tipos de dados são coletados, como a empresa recebe esses dados, como eles são armazenados e quem tem ou poderia ter acesso a esses dados.

Na fase 2, é importante ainda enumerar os regulamentos e as normas de proteção de dados e a privacidade que afetam sua empresa ou organização, no nível local nacional ou internacional como por exemplo caso sua empresa possua negociações com a Europa e precise de alguma forma coletar ou tratar dados de cidadãos europeus, o GDPR deverá ser consultada.

Fase 3 – Validação

Com a fase de levantamento finalizada, é necessário, primeiramente, identificar se as informações obtidas estão de acordo com os princípios da LGPD.

É ainda imprescindível analisar, estudar e entender o impacto que essas regras de proteção de dados e privacidade, regulamentos e normas podem ter para a empresa. Executar uma auditoria inicial de dados pessoais e uma avaliação de proteção de dados da empresa. Ao realizar essa auditoria, cada empresa ou organização deve identificar os riscos de proteção de dados e privacidade para indivíduos, riscos de conformidade e quaisquer riscos relacionados à empresa ou organização para que possam evitar multas por não conformidade, procedimentos potenciais de litígios individuais por danos à reputação, que pode levar à perda de negócios, conforme ilustrado na Figura 03.

Figura 03– Planilha AIPD

	Etapa 1	Etapa 2	Etapa3
Cód.	Identificar a necessidade de uma apid- Descreva o motivo para criar essa AIPD	Descreva os Fluxos de Informação	Severidade
1	A implantação de um novo sistema ERP para atender de forma centralizada os dois hospitais irá armazenar os dados pessoais diretos indiretos e sensíveis dos pacientes.	Devido a fusão o armazenamento dos dados pessoais dos paciente serão todos centralizados em um único ERP centralizado no hospital A, ou seja independente do hospital que o paciente está frequentando os seus dados estarão armazendos de forma central.	15
1	A implantação de um novo sistema ERP para atender de forma centralizada os dois hospitais irá armazenar os dados pessoais diretos indiretos e sensíveis dos pacientes.	Devido a fusão o armazenamento dos dados pessoais dos paciente serão todos centralizados em um único ERP centralizado no hospital A, ou seja independente do hospital que o paciente está frequentando os seus dados estarão armazendos de forma central.	10
2	O backup dos arquivos pessoais de todos os pacientes dos dois hospitais será armazenado em no hospital B e gerenciado pela empresa Main Safe.	Os dados pessoais de todos os pacientes serão armazenados em um backup no hospital B para garantir a segurança.	5
2	O backup dos arquivos pessoais de todos os pacientes dos dois hospitais será armazenado em no hospital B e gerenciado pela empresa Main Safe.	Os dados pessoais de todos os pacientes serão armazenados em um backup no hospital B para garantir a segurança.	6

Fonte: Silva (2021)

Fase 4 – Desenvolvimento

Nesta fase, é necessário nomear um encarregado de dados, que será o responsável por receber e responder as solicitações dos titulares, interagir com a ANPD e manter todos os documentos que foram desenvolvidos atualizados. É também necessário o desenvolvimento de uma matriz de informando a responsabilidade de cada um dos membros do comitê e desenvolver uma política de segurança de dados pessoais. É

necessário ainda desenhar os fluxos de dados pessoais para que seja possível entender o caminho que a informação percorre na organização. Por fim é desenvolvido um plano de ações com todas as atividades que a empresa precisa executar para ficar em conformidade com a LGPD.

Fase 5 – Encerramento

Com base nas etapas 1 a 4, é possível emitir um relatório contendo: a análise e os resultados das atividades; um orçamento contendo fundos, recursos, sistemas e ferramentas necessárias e um conjunto de planos de ação específicos para executar a proteção e a privacidade completas dos dados processo e cada fase. Esse relatório deve ser revisado e aprovado para que recursos e pessoal sejam empregados para projetar, desenvolver e operar sua proteção de dados e privacidade programa para a empresa que você gerencia. Com esse plano em mãos, a empresa estará pronta para avançar e implementar a proteção de dados e planos de privacidade para os dados pessoais que ela coleta, usa, processa e mantém.

O resultado da fase 5 é preparar a empresa (diretoria, gerência e equipe) para ser mais eficaz ao lidar com os riscos de proteção de dados e privacidade. No final dessa fase, é gerado um documento que indique em qual nível a empresa está em relação a cada item analisado.

4.3 Discussão

Os dois frameworks permitem diagnosticar e avaliar se os processos analisados estão adequados a LGPD, ambos utilizam instrumentos como entrevistas e questionários para obter os dados para fazerem as análises. Não foi objetivo deste artigo testar os frameworks no campo, mas ambos apresentaram as pesquisas empíricas nos documentos.

Cada framework utiliza-se de métodos teóricos diferentes, mas ambos analisam os processos para verificar a privacidade de dados.

O Framework LGPD está preparado para empresas brasileiras do setor químico e LGPD model Canvas permite avaliar os processos de qualquer setor de empresa ou organização.

5. Conclusão

O objetivo desta pesquisa foi alcançado, pois identificou-se e discutiu-se dois modelos ou frameworks existentes na literatura para diagnosticar se os processos estão adequados ou não a LGPD. A importância destes frameworks é grande, pois facilita e organiza os diagnósticos dos processos das empresas em relação ao LGPD.

Além de permitir que as empresas e organizações possam enxergar a LGPD de uma forma mais organizada, prever os recursos que irão ser afetados neste novo cenário e o mapeamento de processos permitiu um engajamento maior entre as áreas das empresas.

Percebeu-se que a aplicação do framework permitiu que os próprios usuários com as suas experiências, visões e vivências sobre os processos que tratam dados pessoais complementem estas informações.

Estes dois exemplos de frameworks podem servir de inspiração para outros que venham a complementar os diagnósticos e análises dos processos da LGPD.

Como estudo futuro, recomenda-se a automatização dos frameworks com o uso das Tecnologias da Informação e Comunicação (TIC).

Referencias

AZEVEDO, Debora. Revisão de Literatura, Referencial Teórico, Fundamentação Teórica e Framework Conceitual em Pesquisa–diferenças e propósitos. Working Paper, 2016. Disponível em:< https://unisinos. academia. edu/DeboraAzevedo/Papers>. Acesso em: 08 de maio de, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, 2018.

BRITO, Felipe Timbó; MACHADO, Javam Castro. Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. Jornadas de atualização em informática, p. 91-130, 2017.

BROWN, Tim. Design Thinking: uma metodologia poderosa para decretar o fim das velhas ideias. Rio de Janeiro: Campus, 2010.

CAMBRIDGE DICTIONARY. Disponível em https://dictionary.cambridge.org/pt/dicionario/ingles/framework acesso em: 09/05/2021.

Cavoukian, Ann. «Cavoukian, Ann. "7 Foundational Principles"» (PDF). "Privacy by Design The 7 Foundational Principles". "Information and Privacy Commissioner of Ontario". 2009

Clark, T.; Osterwalder, A.; Pigneur Y. Business Model You: o modelo de negócios pessoal. Alta Books, Rio de Janeiro, RJ, Brasil. 2013

FREITAS, Carla. Como elaborar uma política de privacidade aderente à LGPD? Disponível em https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais Acesso em 09/05/2021

GIL, Antonio Carlos et al. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2002.

GÜRSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering privacy by design. Computers, Privacy & Data Protection, v. 14, n. 3, p. 25, 2011.

LOHMANN, Pedro A.; ALBUQUERQUE, Carlos; MACHADO, Raphael. Revisão Sistemática para o Processo de Avaliação de Impacto sobre a Proteção de Dados Pessoais e à Privacidade. Disponível em https://www.researchgate.net/profile/Carlos-Albuquerque-7/publication/349924412_Revisao_Sistematica_para_o_Processo_de_Avaliacao_de_Impacto_sobre_a_Protecao_de_Dados_Pessoais_e_a_Privacidade/links/6047852e92851c077f297eac/Revisao-Sistematica-para-o-Processo-de-Avaliacao-de-Impacto-sobre-a-Protecao-de-Dados-Pessoais-e-a-Privacidade.pdf Acesso 08/05/2021.

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

OKANO, Marcelo T. IOT and industry 4.0: the industrial new revolution. In: International Conference on Management and Information Systems September. 2017. p. 26.

PARÉ, Guy et al. Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, v. 52, n. 2, p. 183-199, 2015.

PINHEIRO, Patricia Peck Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patricia Peck Pinheiro. – São Paulo: Saraiva Educação, 2018.

SILVA, Rogério Hermínio da. Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, Florianópolis, 2021.

VIDAL, M. T. V. L. Segurança em redes. Niterói: UFF,2006.

WIKIPEDIA. Disponível em https://pt.wikipedia.org/wiki/Framework Acesso em: 09/05/2021.