

UNIJUI - UNIVERSIDADE REGIONAL DO NOROESTE DO ESTADO DO RIO  
GRANDE DO SUL  
DCEENG - DEPARTAMENTO DE CIÊNCIAS EXATAS E ENGENHARIA  
CIÊNCIA DA COMPUTAÇÃO

EDUARDO MARIANO DOLOVITSCH

DESENVOLVIMENTO DE SITE INFORMATIVO E INTERATIVO SOBRE A LEI  
GERAL DE PROTEÇÃO DE DADOS (LGPD) APLICADA AOS RAMOS DE  
ATIVIDADE COMERCIAL E DE PRESTAÇÃO DE SERVIÇO

Ijuí - RS  
2021

EDUARDO MARIANO DOLOVITSCH

DESENVOLVIMENTO DE SITE INFORMATIVO E INTERATIVO SOBRE A LEI  
GERAL DE PROTEÇÃO DE DADOS (LGPD) APLICADA AOS RAMOS DE  
ATIVIDADE COMERCIAL E DE PRESTAÇÃO DE SERVIÇO

Trabalho de Conclusão do Curso de Ciência da  
Computação – Departamento de Ciências Exatas  
e Engenharia da Universidade Regional do  
Noroeste do Estado do Rio Grande do Sul –  
Unijuí, como requisito parcial para obtenção do  
título de Bacharel em Ciência da Computação.

Orientador: Prof. Me Romário Lopes Alcântara

Ijuí - RS  
2021

EDUARDO MARIANO DOLOVITSCH

DESENVOLVIMENTO DE SITE INFORMATIVO E INTERATIVO SOBRE A LEI  
GERAL DE PROTEÇÃO DE DADOS (LGPD) APLICADA AOS RAMOS DE  
ATIVIDADE COMERCIAL E DE PRESTAÇÃO DE SERVIÇO

Trabalho de Conclusão do Curso de Ciência da  
Computação – Departamento de Ciências Exatas  
e Engenharia da Universidade Regional do  
Noroeste do Estado do Rio Grande do Sul –  
Unijuí, como requisito parcial para obtenção do  
título de Bacharel em Ciência da Computação.

Cidade, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_

BANCA EXAMINADORA

---

Prof. Me Marcos Ronaldo Melo Cavalheiro

Universidade Regional do Noroeste do Estado do Rio Grande do Sul - Unijuí

## **AGRADECIMENTOS**

Agradeço primeiramente a Deus por me disponibilizar a possibilidade de seguir o objetivo de contribuir com meus estudos, para auxiliar as pessoas ao meu redor e por consequência alcançar o sonhado título de bacharel.

Aos meus pais, irmã, família e minha tia, segunda mãe, por toda atenção, amor e colaboração durante todo o período da graduação. Por compreenderem meus momentos de altos e baixos, disponibilizando o apoio necessário para que eu pudesse seguir em frente nesse caminho.

Agradeço aos meus avós, tios, tias, primos, primas e amigos por todo apoio dado, seja ele moral, material e principalmente emocional, dando o incentivo permanente necessário a confecção deste trabalho da melhor maneira possível.

Aos meus professores da universidade, colegas e demais pessoas que fizeram parte dessa caminhada e dispuseram de sua orientação para que ela pudesse seguir pelos melhores caminhos, mesmo que as vezes os mesmos fossem mais tortuosos e difíceis.

Por fim, agradeço também ao meu Orientador Romário Lopes Alcântara, pelo auxílio e orientação no desenvolvimento deste trabalho, o qual posso afirmar, só foi possível devido a muito de seu conhecimento e dedicação também.

"A verdadeira viagem de descoberta não consiste em procurar novas paisagens, mas em ter novos olhos." (Marcel Proust)

## **RESUMO**

Em um cenário atual onde os dados, em sua grande parte pessoais, adquirem patamar de valorização cada vez mais alto frente a sociedade em geral, principalmente no âmbito econômico, surge a Lei Geral de Proteção de Dados Pessoais (LGPD), originada de regulamentação europeia, e com a finalidade de legislar todo e qualquer atividade que envolva tratamento de dados pessoais. Pautado nesta lei, o objetivo principal do trabalho foi desenvolver um recurso contribui com a divulgação e compreensão da lei ao público em geral. Com este intuito, foi realizado um estudo da LGPD, que culmina com o desenvolvimento de uma página web contendo a descrição da lei comentada, etapas de implantação da mesma em qualquer instituição e ferramentas para a criação de comunidade de conhecimento diversificada em torno do assunto.

**Palavras-chave:** LGPD. Direitos. Adequação.

## **ABSTRACT**

In a current scenario where data, mostly personal, acquire an increasingly higher level of valuation in relation to society in general, especially in the economic sphere, the General Law for the Protection of Personal Data (LGPD) arises, originated from European regulations , and for the purpose of legislating any and all activities that involve the processing of personal data. Based on this law, the main objective of the work was to develop a resource that contributes to the dissemination and understanding of the law to the general public. With this in mind, a study of the LGPD was carried out, which culminates in the development of a web page containing the description of the commented law, stages of its implementation in any institution and tools for the creation of a diversified knowledge community around the subject.

**Keywords:** LGPD. Rights. Adequacy.

## LISTA DE ILUSTRAÇÕES

Figura 1 — Atribuições do DPO .....	44
Figura 2 — Princípios de Validação do Consentimento .....	51
Figura 3 — Fundamentos para Política de Tratamento de Dados Pessoais .....	58
Figura 4 — Etapas para desenvolvimento do RIPD .....	63
Figura 5 — Wireframe das Telas de Cadastro .....	71
Figura 6 — Wireframe das Telas de Exibição dos Dados .....	72
Figura 7 — Representação do Padrão MVC .....	76
Figura 8 — Imagem do Diagrama do Banco de Dados .....	78
Figura 9 — Página Home .....	79
Figura 10 — Página de Registro .....	80
Figura 11 — Página de Capítulos Comentados da LGPD .....	81
Figura 12 — Página de Etapas de Implantação da LGPD .....	82
Figura 13 — Página de Setores de Serviço .....	83
Figura 14 — Página de Listagem de Notícias .....	84
Figura 15 — Página de Exibição das Notícias .....	85
Figura 16 — Página do Fórum .....	86
Figura 17 — Página de Comentários .....	87
Figura 18 — Página de Tópico Fixo .....	88
Figura 19 — Página de Listagem de Tópicos Abertos .....	89
Figura 20 — Página de Listagem de Tópicos Fixos .....	90
Figura 21 — Página de Listagem de Links Úteis .....	91
Figura 22 — Página Sobre .....	92
Figura 23 — Página de Cadastro Interna .....	93



## LISTA DE QUADROS

Quadro 1 — Exemplo de Planilha de Mapeamento .....	50
Quadro 2 — Sprint 1 .....	73
Quadro 3 — Sprint 2 .....	73
Quadro 4 — Sprint 3 .....	74

## **LISTA DE ABREVIATURAS E SIGLAS**

TCC	Trabalho de Conclusão de Curso
PLC	Projeto de Lei da Câmara
LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	Regulamento Geral de Proteção de Dados Pessoais
CNPDPP	Conselho Nacional de Proteção de Dados Pessoais e
Privacidade	
PSI	Política de Segurança da Informação
ANPD	Agência Nacional de Proteção de Dados Pessoais
ABNT	Associação Brasileira de Normas Técnicas
NBR	Norma Brasileira
ISO	Organização Internacional de Padronização
FR	Fator de Risco
HTTPS	Protocolo de Transferência de Hypertexto Seguro
TLS	Camada de Transporte Segura
FTP	Protocolo de Transferência de Arquivos
EFS	Sistema de Encriptação de Arquivos
MVC	Model View Controller
EAD	Ensino a Distância
DPO	Data Protection Officer
UE	União Européia

## SUMÁRIO

1	<b>INTRODUÇÃO</b>	12
2	<b>FUNDAMENTOS E CONCEITOS DA LGPD</b>	18
2.1	CAPÍTULO I – DISPOSIÇÕES PRELIMINARES	20
2.2	CAPÍTULO II – TRATAMENTO DE DADOS PESSOAIS	24
2.2.1	<b>Requisitos de Tratamento de Dados Pessoais</b>	24
2.2.2	<b>Requisitos de Tratamento de Dados Pessoais Sensíveis</b>	26
2.2.3	<b>Requisitos de Tratamento de Dados Pessoais de Crianças e Adolescentes</b>	26
2.2.4	<b>Término do Tratamento de Dados</b>	27
2.3	CAPÍTULO III – DIREITOS DO TITULAR	28
2.4	CAPÍTULO IV – TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO	29
2.5	CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS	30
2.6	CAPÍTULO VI – AGENTES DE TRATAMENTOS DE DADOS PESSOAIS	32
2.7	CAPÍTULO VII – SEGURANÇA E BOAS PRÁTICAS	34
2.8	CAPÍTULO VIII – FISCALIZAÇÃO	35
2.9	CAPÍTULO IX – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE	37
2.10	CAPÍTULO X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS	40
3	<b>ADEQUAÇÃO E IMPLANTAÇÃO DA LGPD</b>	42
3.1	DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO	46
3.2	MAPEAMENTO E ADEQUAÇÃO DO FLUXO DE VIDA DOS DADOS	49
3.2.1	<b>Coleta de Dados</b>	50
3.2.2	<b>Armazenamento dos Dados</b>	52
3.2.3	<b>Tratamento de Dados</b>	53
3.2.4	<b>Compartilhamento dos Dados</b>	54
3.2.5	<b>Eliminação dos Dados</b>	55
3.3	ATUALIZAÇÃO DO SISTEMA DE GESTÃO DA INFORMAÇÃO	56
3.4	MONITORAR COM A REALIZAÇÃO DE AUDITORIAS	59
3.5	TREINAMENTOS E CAMPANHAS DE CONSCIENTIZAÇÃO	60
3.6	RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	62
3.7	CRIAÇÃO DE PLANO DE AÇÃO	64
3.8	DEFINIÇÕES ESPECIAIS PELO TIPO DE DADOS	65
4	<b>DESENVOLVIMENTO DO WEB SITE</b>	67
4.1	METODOLOGIA DE DESENVOLVIMENTO	67
4.2	ANÁLISE DE REQUISITOS	69
4.3	WIREFRAME	70

4.4	CRONOGRAMA POR SPRINTS.....	72
4.5	DEFINIÇÃO DAS TECNOLOGIAS.....	74
4.6	MODELAGEM DO BANCO .....	76
4.7	PÁGINAS DESENVOLVIDAS .....	79
5	<b>CONCLUSÃO</b> .....	94
	<b>REFERÊNCIAS</b> .....	98

## 1 INTRODUÇÃO

Diante de um panorama atual, onde dados pessoais ganham cada vez mais valor e, em contrapartida, menor privacidade, no ano de 2018, originado do Plano de Lei da Câmara (PLC) nº 53 e de discussões em torno do General Data Protection Regulation (GDPR), aprovado pela União Europeia em 2016, tivemos em nosso país a publicação da Lei nº 13.709, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD). A presente lei trata da proteção de dados, sejam eles pessoais ou sensíveis, em toda e qualquer situação que envolva os mesmos, destacando atualmente os meios on-line, porém sem deixar de lado os meios físicos.

Embora aparente certa complexidade, as transações envolvendo dados pessoais podem ser exemplificadas por situações do dia a dia, onde podemos citar a realização de uma aquisição de produtos em uma loja de comércio on-line, ou ainda, em uma loja física, onde em ambos os casos são solicitados dados pessoais como nome, telefone e ainda documentações para fins de registro da pessoa no respectivo estabelecimento.

Aqui vale destacar que a LGPD representa o maior avanço legislativo brasileiro em termos de proteção das informações no âmbito da web, pois, embora já houvesse presença de outras legislações abordando o assunto, as mesmas caracterizam-se por se delimitar a tratar de questões relacionadas diretamente a privacidade dos dados, como o Marco Civil da Internet, não abordando questões de dados que fujam a esse domínio e que tenham sido tornados públicos, por intermédio de seus titulares.

Em contrapartida as demais legislações, temos a LGPD, cuja regulação apresenta amplitude maior e aborda os mais diversos meios de difusão dos dados, a qual entrou em vigor a contar de 19 de setembro de 2020, ressalvadas as multas administrativas, que passarão a valer em setembro de 2021, disponibilizando o período de um ano para adequação de empresas e instituições a todos os aspectos da lei.

Como consequência da LGPD e toda sua amplitude, surge um ambiente de segurança, controle e direitos das pessoas sobre seus dados, porém, em contrapartida, devido à complexidade do assunto e as limitações de acesso a estas informações, chegamos ao problemas que iremos abordar neste estudo, o qual consiste em como contribuir na divulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), tanto no que tange a exposição dos direitos do usuário, como nos aspectos a serem observados para adequação de empresas e instituições nos ramos de atividade comercial e de prestação de serviço a esta nova realidade, além de criar uma ferramenta de interação para a sociedade em geral sobre o assunto?

Neste contexto, inicialmente, não se pode ignorar a já existência de um extenso número de ferramentas, como aplicativos e sites visando a divulgação de informações sobre a LGPD. Contudo, estas ferramentas, mesmo apresentando diferentes formas de abordar o assunto, apresentam uma característica em comum, pois abordam a primeira etapa de adequação a lei, disponibilizando recursos grátis que permitam as instituições avaliar seu nível de adequação. Quando segue-se para as demais etapas, cria-se uma relação condicional financeira de acesso ao demais recursos, constituindo um novo ramo de mercado, que é a prestação de serviços para adequação de instituições a LGPD.

Para fins de suprir as duas questões acima, faremos o desenvolvimento de um site, utilizando recursos atuais de desenvolvimento web e voltado a interação com o usuário, com a finalidade de informar usuários leigos e profissionais da área de computação sobre a LGPD, representando sua aplicação em diferentes ramos de atividade como educação, saúde, comércio, financeiro dentre outros. Convém destacar também, que o conteúdo do site será disponibilizado de forma gratuita e contendo ferramentas de interação que possibilitem aos usuários, não apenas usufruir, mas também contribuir com sua experiência e qualificar o conteúdo do site.

Chegando a este momento, você pode estar se perguntando sobre a essencialidade do assunto e se vale dedicar tempo e interesse para procurar conhecimento sobre o mesmo? Em resposta a este questionamento, segue um contexto comum atualmente, que consiste em acordar pela manhã, tomar café,

enquanto atualiza as mídias sociais e visualiza as notícias mais atuais, ou ainda realiza transações financeiras ou comerciais. Embora atos extremamente simples e corriqueiros, quando analisados com mais cuidado e de um prisma de tecnologia da informação, podem ser definidos como os principais meios e ferramentas para impulsionamento da economia mundial.

E antes que se pergunte como posso afirmar isso, basta seguir com alguns dados divulgados pelo Facebook, no ano de 2020, referentes a mídias sociais, onde em todo o mundo, atualmente existem 2.77 bilhões de usuários de mídia social, destacando-se o Facebook com 2.27 bilhões de usuários e o Instagram com 1 bilhão de usuários. Este panorama enfim culmina com uma frase criada por um matemático londrino denominado *Clive Humby* e que tem agitado o mundo dos negócios, que corresponde a “**Data is the new oil**”, ou seja, “**Dado é o novo Petróleo**”.

Essa expressão tem sido bastante utilizada por pessoas no mundo todo, afim de demonstrar a ideia de que os dados se tornaram tão valiosos como o petróleo. E aqui, vale destacar algumas diferenças entre ambos, pois quando falamos de petróleo, sua maior dificuldade está em localizar as reservas do mesmo e gerenciar o fato de que são limitadas. Já quando tratamos de dados, nos incorporamos ao cenário atual, onde como já citado anteriormente, a produção de dados ocorre a todo momento, em escala global e ritmo permanentemente crescente. Dessa forma, chegamos a principal justificativa da valorização dos dados, que é a manipulação dos mesmos.

Este processo de tratamento dos dados, atualmente tem gerado o conhecimento a partir do qual empresas como a NASA, Nike, Microsoft, dentre outras, definem suas ações, em seus mais diversos setores. Adicionalmente a todo impacto causado na economia mundial, verifica-se que a maior parte desses dados, advém de dados pessoais como documentações, dados de contato e endereço, números de cartões de crédito, mensagens pessoais, pesquisas realizadas, histórico de navegação dentre outros. Ou seja, dados que podem afetar seriamente os mais diversos aspectos da vida do indivíduo, e que por muitas vezes ocasionam insegurança e desconfiança por parte dos usuários.

E como se não fosse suficiente ter seus dados pessoais, sua localização e suas compras captados e utilizados todos dias, para fins de terceiros, os mesmos tornaram-se alvo de pessoas mal-intencionadas, que podem alterá-los ou até mesmo sequestrá-los, configurando-se o que chamamos de *cybercrime*. Esta nova modalidade criminosa tem mantido um ritmo alarmante em todo o mundo, gerando custos anuais de até US\$ 6 trilhões, conforme (CORREIA, 2020).

E como não poderia deixar de ser, mesmo se tratando de um problema mundial, onde ataques cibernéticos distribuem-se ao redor do mundo, 24 horas por dia, muitas vezes sem qualquer percepção usuário, nosso país destaca-se negativamente frente aos países da América Latina e muitos outros países do mundo. "O Brasil que se encontrava em 2019 na posição 30º, dentre os países que mais sofreram ataques cibernéticos no mundo, agora figura na posição 13, ficando atrás de países como Argélia, Síria, Irã, Turquia e Egito". (FORRESTER, 2020).

E infelizmente, seguindo nessa linha negativa, a situação pode ser ainda mais alarmante, por que, reduzindo nosso escopo para as empresas no país, pelo menos 96% das empresas assumem ter sofrido algum ataque cibernético nos últimos 12 meses, ocasionando, negativamente, impactos de perda de produtividade, de dados de funcionários e ainda perda ou roubo financeiro. Além disso, outro fato que preocupa é existência de políticas de segurança que deveriam ser adotadas por todas as empresas, mas estão presentes em apenas 33% das mesmas, em nosso país, baseado nas informações disponibilizadas por (FORRESTER, 2020).

Avaliando então o cenário retratado, torna-se indispensável a existência de algum tipo de regulamentação que determine uma padronização a ser seguida para manusear os dados, garantindo os conceitos de privacidade e a implantação de um órgão responsável pela fiscalização e aplicação de sanções, caso os direitos fundamentais sejam negligenciados. E para suprir estas necessidades temos a criação da LGPD, sendo considerada um novo marco legal brasileiro de grande impacto, tanto para instituições privadas como para públicas, por tratar da proteção



dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações por qualquer meio conforme, afirmação de (PINHEIRO, 2020).

Em contrapartida a criação da LGPD e a entrada em vigor da mesma recentemente, por um lado, temos a gestão regulamentada de grandes massas de dados pessoais e a contribuição para a redução sensível da intensidade e do número de ataques cibernéticos atualmente. Por outro lado, passa-se a conviver com o fato de aproximadamente 60% das empresas brasileira não estarem prontas para se adequarem as exigências da lei.

Isto se dá, tanto pela falta de conhecimento das instituições sobre a LGPD quanto pela falta de pessoas qualificadas que possam realizar o planejamento de segurança exigido, segundo estudo desenvolvido pela Associação Brasileira de Empresas de Software no ano de 2020. Neste ponto, este trabalho apresentará sua maior contribuição, assumindo a posição de mecanismo para tornar público e acessível, uma das maiores conquistas atuais relacionadas aos nossos direitos frente a sociedade atual.

Para fins de desenvolvimento do estudo será realizado um estudo qualitativo, avaliando todos os artigos que compõe a LGPD, além de demais artigos relacionados a ramos de atividade específicos como saúde e financeiro. Visando garantir a maior diversidade possível de opiniões e análises, será feita análise dos mais diversos documentos como Leis, Regulamentos, Livros, Artigos e até sites informativos sobre o assunto, além de diversas revisões bibliográfica, buscando identificar as orientações em conformidade nos mesmos, que possam ser então divulgadas por meio do site criado ao público em geral.

O trabalho é organizado em 4 capítulos além desta introdução. O primeiro capítulo irá tratar especificamente sobre a LGPD, realizando uma análise comentada dos artigos que constituem a mesma, afim de transmitir ao leitor conhecimentos superficiais a respeito da lei, os quais serão utilizados no desenvolvimento do site. A seguir, no capítulo 2, serão utilizados os conhecimentos do capítulo 1, para elencar procedimentos a serem utilizados com a finalidade de implantação da lei nas

organizações. No Capítulo 3, por sua vez, tratar-se-á de toda a engenharia de desenvolvimento do site, com a apresentação de todo o processo, desde a definição dos requisitos do site, a escolha das tecnologias e ferramentas, passando por seu layout e estrutura dos dados.

Por fim, tem-se o capítulo 4, dedicado aos resultados obtidos, ou seja, o site desenvolvido, demonstrando e avaliando as funcionalidades e contribuições que o mesmo trouxe, além de ressaltar os desafios encontrados e sugestões de melhorias ou trabalhos futuros que possam ser implementados ao mesmo.

## 2 FUNDAMENTOS E CONCEITOS DA LGPD

Partindo de debates originados na União Europeia (UE), em torno da privacidade, tivemos a consolidação do Regulamento Geral de Proteção de Dados Pessoais Europeu, aprovado em abril de 2016 e denominado General Data Protection Regulation (GDPR). Este fato ocasionou grandes efeitos em países por todo o mundo, pois a manutenção de relações comerciais dos mesmos com a UE, ficou condicionada a existência de legislação correspondente a da GDPR, como destaca (POHLMANN, 2019, p. 20) ao afirmar:

Empresas brasileiras que não possam fazer negócios com empresas europeias poderiam ir a quebra, dada a abrangência atual da globalização. Agora tocamos o bolso de grandes empresas! Este é o argumento definitivo, no meu conceito.

E como não poderia ser diferente, nosso país se viu diante da necessidade eminente, que resultou na Lei Geral de Proteção de Dados Pessoais, mais amplamente difundida pela sigla LGPD, e que foi promulgada pelo presidente Michel Temer em 14 de agosto de 2018, sendo alterada pela Medida Provisória 869/2018 e pela Lei n. 13853/2019.

Com sua redação inspirada na lei europeia (GDPR) e focada na proteção de dados pessoais de pessoas naturais, destaca-se por influenciar não apenas pessoas físicas, mas também empresas, pois afetará diretamente os dados que as mesmas possuem de seus funcionários, clientes, terceiros, acionista dentre outros.

Para (PINHEIRO, 2020, p. 12) surgiu com a ideia de proteger direitos fundamentais, como dito em:

O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa de boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança de segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação

que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.

Isto é corroborado por (DONDA, 2020, p. 14), onde ele declara que, “A lei é baseada nos direitos fundamentais de liberdade e de privacidade e no livre desenvolvimento da personalidade da pessoa natural”.

Convém ressaltar que seu tema principal, no caso, a privacidade, já havia sido anteriormente tratado em outras regulamentações, onde podemos destacar o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso a Informação e a Constituição Federal.

Porém a LGPD inovou com a padronização dos atributos da proteção de dados pessoais, cuja ausência ou inobservância dos mesmos ocasionará penalidades, e a criação de duas entidades independentes e especializadas, responsáveis pela gerência de todo ambiente relacionado a LGPD que são a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e Privacidade (CNPDP).

Partindo da sua entrada em vigor na data de 18 de setembro de 2020, assumiu a posição de um novo marco legal brasileiro, causando grande impacto em instituições privadas e públicas, e sendo caracterizada como uma regulamentação extremamente técnica, baseada no pilar fundamental da proteção dos direitos humanos, composta de princípios, direitos e obrigações em relação ao ativo mais valioso da sociedade atual, que são os dados relacionados as pessoas.

A lei compreende 65 artigos distribuídos em 10 capítulos, e para a sua melhor compreensão, faremos em seguida a abordagem de cada um dos capítulos, procurando clarear seus pontos principais, com referências aos artigos e exemplificações.

## 2.1 CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

Como o próprio título já destaca, versa a respeito das disposições gerais da lei, apresentando seu objetivo e escopo de atuação, além de seus fundamentos, princípios de aplicação e as definições dos novos termos introduzidos pela mesma.

Partindo de seu **Art. 1º**, a lei (BRASIL, 2018) já busca retratar claramente sua definição, dispondo sobre o “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado”. Aqui já vale destacar alguns pontos importantes, como a expressão “inclusive nos meios digitais”, a qual deixa claro o fato de que o tratamento não se resume aos meios digitais, mas também a meios manuais, como por exemplo, quando realizamos o preenchimento de algum formulário de forma manual com dados pessoais.

Outro ponto, diz respeito a quem realiza o tratamento, onde tem-se pessoa natural (cidadão com direitos e obrigações na esfera civil), ou ainda pessoa de direito público (entidades ligadas a união, estados, distrito federal, territórios, municípios e autarquias) ou de direito privado (empresas particulares ou ainda estatais, as quais se caracterizam pela contribuição do poder público para o capital).

Complementa seu **Art. 1º** (BRASIL, 2018) com seu objetivo, onde declara “proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural”. Este conteúdo se relaciona com os fundamentos da lei citados no **Art. 2º**, onde temos inicialmente o respeito a privacidade.

Neste ponto destaca-se uma diferença importante entre proteção de dados e privacidade, pois o fato de tornar públicas informações em nossa rede social por exemplo, não subentende que estes dados possam ser utilizados de forma indiscriminada por quem quer que seja, implicando a lei neste ponto, afim de valorizar os direitos do titular sobre seus dados.

O próximo fundamento, e que retrata bem a citação destacada ao fim do parágrafo anterior, é a autodeterminação informativa, o qual garante a pessoa natural total controle sobre seus dados, ou seja, o titular tem o direito de saber quais dados seus as organizações possuem, como foram utilizados, além de determinar se o dado pode permanecer com a organização em questão e se o mesmo pode ser utilizado.

Em seguida, tem-se alguns outros fundamentos já amplamente difundidos na constituição federal como a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, sendo concluído por fundamentos que destoam dos demais, por fazerem referência a sociedade em geral, e não mais a pessoa individual.

Destacando esses fundamentos focados na sociedade, tem-se o desenvolvimento econômico e tecnológico e a livre iniciativa, concorrência e a defesa do consumidor, ressaltando a possibilidade ao legislador de que, quando os dados possam contribuir para a tomada de decisões sociais, políticas e econômicas, os mesmos possam ser utilizados, em alguns casos, em detrimento ao consentimento do titular dos dados, o que será visto como mais detalhes em uma abordagem mais específica a frente.

O **Art. 3º** trata da aplicação territorial da lei, onde retrata que a lei será aplicada a dados que estiverem sido coletados, que sejam tratados, ou ainda para oferta de produtos ou serviços em território nacional, conforme (PINHEIRO, 2020, p. 31) destaca em:

A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional, ou por oferta de serviço para indivíduos no território nacional ou que estivessem no Brasil.

Em contrapartida ao **Art. 3º**, o **Art. 4º** destaca as situações em que a lei não se aplica, onde temos a coleta e tratamento de dados pessoais realizado por pessoa natural para fins apenas particulares, jornalísticos, artísticos, acadêmicos, segurança pública, de estado e defesa nacional.

No **Art. 5º** temos a definição de vários conceitos introduzidos pela lei, e que são de sumária importância para compreensão de todos os aspectos e regulamentações trazidas pela mesma. Destes conceitos, podemos destacar:

**Dado Pessoal:** qualquer informação relacionada a pessoa natural viva identificada ou identificável, destacando que não se restringe a dados comuns como nome e idade, incluindo dados como localização, dados acadêmicos, histórico de compras dentre outros.

**Dado Pessoal Sensível:** relacionados a características da personalidade do indivíduo como origem racial ou étnica, dado genético ou biométrico, além de suas escolhas pessoais, como convicção religiosa e opinião política. Conforme ressalta (POHLMANN, 2019, p. 28) " Podemos considerar que um dado sensível é aquele dado que pode gerar, em algum âmbito, a discriminação ou o preconceito por parte de outras pessoas ".

**Dado Anonimizados:** qualquer dado relativo ao indivíduo que não permita identificação do mesmo, sendo que a operação de anonimização<sup>1</sup> costuma ser aplicada no ato do tratamento dos dados, onde aplica-se técnicas para agrupar ou embaralhar as informações, impossibilitando a associação direta ou indireta dos dados a um indivíduo. Este processo por sua vez, poderá ser fiscalizado e ter seus padrões e técnicas definidos pela ANPD.

**Titular:** pessoa natural a qual se referem os dados pessoais objetos de tratamento.

---

<sup>1</sup>consiste em métodos usados com a finalidade de mascarar e impossibilitar que dados possam identificar seu titular.

**Tratamento:** toda operação realizada para fins de manuseio de dados pessoais, englobando a 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.

**Agentes de Tratamento:** identificados pelo controlador (pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais) e o operador (pessoa física ou jurídica que realiza o tratamento dos dados pessoais em nome do controlador), sendo responsáveis pela indicação do encarregado, que consiste no canal de comunicação entre o controlador, titulares e a ANPD.

**Consentimento:** manifestação livre, informada e inequívoca pela qual o titular acorda com o tratamento de seus dados pessoais para uma finalidade determinada, sendo uma das hipóteses para autorização do tratamento de dados.

**Relatório de Impacto a Proteção de Dados Pessoais:** documentação do controlador composta da descrição dos processos de tratamentos de dados pessoais, bem como as medidas, salvaguardar e recursos para mitigação de riscos.

Para finalização deste capítulo, tem-se o **Art. 6º**, que estabelece a boa-fé e alguns princípios que devem ser observados no tratamento de dados, sendo eles: finalidade (propósito legítimo da coleta), adequação (tratamento compatível com a finalidade), necessidade (tratamento limitado ao mínimo necessário), livre acesso (garantir ao titular consulta, duração e integralidade de seus dados), qualidade dos dados (exatidão, clareza e relevância), transparência (informações claras, precisas e de fácil acesso ao titulares sobre o tratamento e os respectivos agentes de tratamento).

Complementando os princípios, tem-se a segurança (medidas para proteger os dados de acessos não autorizados e situações de destruição, perda, alteração, comunicação ou difusão), prevenção (medidas para prevenir danos em virtude do tratamento de dados), não discriminação (não possibilitar tratamento de dados para



fins discriminatórios ilícitos ou abusivos) e responsabilidade e prestação de contas (demonstração de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados).

## 2.2 CAPÍTULO II – TRATAMENTO DE DADOS PESSOAIS

De posse do conhecimento dos princípios citados anteriormente, chega-se ao capítulo responsável por explicitar as hipóteses para o tratamento dos pessoais, sejam ele dados comuns, como sensíveis ou ainda de crianças e de adolescente, cada um em sua respectiva sessão.

Aqui temos principalmente a hipótese do consentimento, a qual com certeza gera mais dúvidas e será a mais amplamente utilizada, sendo caracterizada por caber ao controlador o fato de comprovar que o consentimento foi obtido em conformidade as solicitações destacadas pela lei. Definidas as hipóteses, o capítulo finaliza tratando sobre o término do tratamento dos dados.

### 2.2.1 Requisitos de Tratamento de Dados Pessoais

Com certeza a hipótese que mais se destaca diz respeito ao consentimento pelo titular presente do **Inciso I do Art. 7º** (BRASIL, 2018) e descrito como “mediante o fornecimento de consentimento pelo titular”. Quando trata-se de consentimento, deve-se observar os princípios retratados anteriormente no **Art. 6º**, como a manifestação livre da escolha por parte do titular, que fica exemplificada pela necessidade de o consentimento ser fornecido de forma escrita ou utilizando de um meio que demonstre claramente a manifestação de vontade do titular.

Convém destacar que mesmo com a presença de consentimento do titular, caso a finalidade de tratamento seja alterada, ou os dados necessitem ser comunicados ou compartilhados com outros controladores, deverá ser informado o titular, tendo esse, direito a solicitação de informações dos dados e seus

tratamentos, assim como de requisitar o cancelamento do consentimento, o qual inclusive, que pode ser realizado a qualquer momento.

Além disso tem-se uma extensa gama de hipóteses que também devem ser consideradas retratadas no **Art. 7º, Incisos II à X**, como o cumprimento de obrigação legal ou regulatória pelo controlador, a pedido do titular dos dados para procedimentos relacionados a contrato cujo titular faça parte, proteção da vida do titular ou terceiro, estudo de órgão de pesquisa (garantida quando possível anonimidade dos dados do titular), proteção de crédito, tutela de saúde (procedimentos realizados por profissionais ou serviços de saúde e autoridade sanitária), exercício de direitos em processo judicial, administrativo ou arbitral, administração pública (tratamento e uso compartilhado de dados para execução de políticas públicas previstas em leis, regulamentos ou convênios) e atender a interesses legítimos do controlado ou de terceiros.

Neste último caso, podemos exemplificar com a manutenção de bases dados que possam ser utilizadas em conjunto com tecnologias de tratamento para gerar atendimentos mais personalizados a seus clientes. Ainda assim deve ser mantido em mente que somente os dados pessoais estritamente necessários para a finalidade definida poderão ser tratados, tendo o controlador a obrigatoriedade de adotar medidas de transparência do tratamento dos dados, inclusive com a existência de relatório de impacto a proteção de dados pessoais, o qual poderá ser solicitado pela ANPD.

Ainda em relação ao interesse legítimo, (POHLMANN, 2019, p. 57), defende que embora seja amparado e justificado pelo bom senso, deve respeitar 3 (três) pilares:

- O legítimo interesse não poderá ser exercido no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção dos dados.
- As finalidades devem ser legítimas.
- O caso deve estar baseado em situações concretas.

No que tange as informações que o titular poderá solicitar, a lei também discorre em seu Art. 9º, especificando dentre elas a finalidade do tratamento, forma e duração do tratamento, identificação e informações de contrato do controlador, sobre o uso compartilhado dos dados, responsabilidades do agente e os direitos do titular.

### **2.2.2 Requisitos de Tratamento de Dados Pessoais Sensíveis**

Caracteriza-se por herdar as hipóteses destacadas no tratamento de dados pessoais, retratado no item anterior, diferenciando-se pela possibilidade de o consentimento partir do seu responsável legal, e pelo desnecessário consentimento nos casos de garantia de prevenção a fraude e à segurança do titular em cadastros de sistemas eletrônicos.

Vale destacar que no caso de dados sensíveis, a comunicação ou compartilhamento de dados entre controladores para fins comerciais e obtenção de vantagens econômicas, fica vedado, principalmente em dados referentes a saúde, salvo quando solicitada portabilidade pelo titular ou em transações financeiras e administrativas resultantes do uso e da prestação de serviços na área de saúde em benefício do titular.

Outro ponto importante, diz respeito aos dados anonimizados, os quais enquadram-se nos que dispendem da necessidade de consentimento, de forma que os mesmos possam ser utilizados para fins de tratamentos com finalidade econômica e de pesquisa. Ressalta-se aqui, a necessidade de comprovada a impossibilidade de identificação do autor dos dados e a garantia de não divulgação dos mesmos no momento da exposição da pesquisa.

### **2.2.3 Requisitos de Tratamento de Dados Pessoais de Crianças e Adolescentes**

Quando nosso escopo incorpora crianças e adolescentes, a lei dispensa cuidados especiais, condicionando seu consentimento a um dos pais ou seu

responsável legal, devendo o controlador realizar todos os esforços para confirmar a identificação do mesmo, além de manter público os tipos de dados coletados e sua forma de utilização, com disposição adequada ao entendimento da criança ou adolescente.

Destaca ainda a possibilidade de obtenção das informações sem consentimento quando destinadas a proteção da criança, localização dos pais ou ainda em atividades como jogos ou aplicações de internet, desde que os dados pessoais disponibilizados sejam estritamente necessários a atividade.

A mesma compreensão fica evidente segundo (GARCIA et al., 2020, p. 12), onde afirma que:

A lei exige o consentimento do responsável legal, papel geralmente exercido pelos pais, quando se trata de dados de menores de 18 anos. Considerando tal público e seu interesse em jogo, a lei endereça um parágrafo para deixar restrita a captura de dados nestes casos, assim como solicita que se trabalhem elementos além dos meramente textuais com o intuito de oferecer melhor experiência e entendimento das crianças e adolescentes ao fornecer seus dados.

Fica evidente também a preocupação da lei para garantir que a origem do consentimento seja de responsáveis ou pais do menor legalmente constituídos, diante de um ambiente digital repleto de recursos para adulterar meios de identificação, como destacado (PINHEIRO, 2020, p. 78):

Merece destaque a preocupação do regulamento em assegurar que o consentimento recebido realmente adveio dos responsáveis/pais do menor. Isso porque o ambiente digital possibilita inúmeros meios de burlar os procedimentos de identificação; dessa forma, cabe aos controladores garantir que o consentimento é real e válido.

#### 2.2.4 Término do Tratamento de Dados

Versando sobre o término de tratamento dos dados, a lei determina em seu **Art. 15 e 16**, que alcançada a finalidade ou o fim previsto do período de tratamento, além da revogação de consentimento por parte do titular ou ainda da ANPD (quando

da violação ao disposto na LGPD), deve ser encerrado o tratamento e realizada a eliminação dos dados. Apenas é autorizada a conservação dos mesmos quando de seu uso para cumprimento de obrigação legal ou regulatória pelo controlador, transferência a terceiro (respeitados os requisitos de tratamento da LGPD), estudo por órgão de pesquisa ou uso exclusivo do controlador, desde que anonimizados os dados.

## 2.3 CAPÍTULO III – DIREITOS DO TITULAR

Dedicado a descrição dos direitos do titular, podemos basear os mesmos nos direitos fundamentais de liberdade, intimidade e privacidade, previstos em nível nacional (Constituição Brasileira) e internacional (Declaração Universal dos Direitos Humanos). Seguindo essas bases, o titular ou representante do mesmo, legalmente estabelecido mediante requisição, poderá solicitar ao agente de tratamento a revogação do consentimento, acesso, correção, anonimização, bloqueio e eliminação dos dados, observados os dispostos a respeito dessas ações na LGPD.

Além disso, poderá também solicitar a confirmação da existência de tratamento ou de compartilhamento dos dados (solicitar informações sobre as entidades ou organizações com as quais os dados foram compartilhados). Feita a requisição, caberá ao controlador disponibilizar os dados em até 15 (quinze) dias a contar da data de solicitação, excetuado os casos em que a ANPD interferir alterando o prazo, em formato simplificado ou completo por meio eletrônico ou sob forma impressa, a critério do titular.

Dentre todos os direitos destaca-se o exposto no **Art. 18 inciso V**, definido como portabilidade dos dados, considerado como um direito novo em nosso ordenamento jurídico, e que irá impactar principalmente em empresas públicas e privadas, garantindo ao titular a possibilidade de compartilhar seus dados que não tenham sido anonimizados, respeitados os segredos comerciais e industriais (dados oriundos da relação do cliente com a instituição em questão), com outras empresas ou instituições. Isto, irá instigar a livre competição econômica entre diferentes instituições, por exemplo, com a divulgação de dados de rendimento do titular.

Em seu **Art. 20**, disponibiliza ao titular a possibilidade de solicitar revisão de decisões tomadas partindo de tratamentos automatizados, muito utilizados hoje em dia, para concessões de crédito ou definição do perfil dos clientes pelas empresas, por meio de tecnologias de Inteligência Artificial e *Big Data*<sup>2</sup>. Aqui temos aspectos contraditórios, pois a lei garante que o titular solicite os critérios e procedimentos utilizados para a análise, porém, ao mesmo tempo, o fato de a empresa disponibilizar seu processo de análise, mesmo que em parte, pode contrariar os segredos de negócio, resguardados como direitos em nosso ordenamento jurídico nacional.

## 2.4 CAPÍTULO IV – TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Inicialmente traz todas as regras a serem respeitadas durante o tratamento de dados pessoais pelo poder público, onde temos algumas semelhanças com as empresas privadas, pois mantém a necessidade de explicitar claramente a finalidade, procedimentos e práticas utilizadas no tratamento, além de haver a necessidade de indicação do encarregado, diferenciando-se pela indicação do interesse público, ou seja, o tratamento deverá ter como objetivo a execução de competências e atribuições legais do serviço público. Podemos destacar que empresas de economia mista respeitarão, por padrão, o tratamento de empresas privadas, excetuados os casos em que estiverem operacionalizando ou executando políticas públicas.

Em relação aos prazos, seguirão os previstos em legislação específica como a Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

---

<sup>2</sup>tecnologia caracterizada pela análise de grandes quantidades de dados para pautar decisões e ações a serem tomadas.

O compartilhamento dos dados, vem retratado em seu **Art. 26**, onde veta o compartilhamento de dados a empresas privadas, com exceção, aos dados que forem acessíveis publicamente, na execução de atividade pública descentralizada, previsão legal respaldada em instrumentos como contratos (comunicados a ANPD), prevenção de fraudes e irregularidades ou proteção a segurança e integridade do titular dos dados. Seguindo essas orientações, em seu comentário ao **Art. 26**, (PINHEIRO, 2020, p. 90) afirma:

Cabe ao Poder Público a garantia de que o uso compartilhado de dados segue os propósitos especiais que concernem à execução das políticas públicas e que, ao mesmo tempo, a ponderação entre a necessidade da publicidade das informações disponíveis ao acesso garante que os direitos dos titulares sejam respeitados. Da mesma forma, a transferência dos dados pessoais às entidades privadas é vetada, com exceção das situações em que os dados são acessíveis publicamente ou em que a execução de um serviço ou medida exigir.

Por fim, estabelece alguns direitos e responsabilidades da ANPD, que devido a seu caráter independente, poderá solicitar relatórios de impacto a proteção de dados, além de informações específicas sobre os dados e as operações de tratamento realizadas sobre os mesmos, pelos órgãos ou entidades públicas, podendo emitir parecer técnico afim de garantir o cumprimento da LGPD.

Dessa forma, compreende a possibilidade de estabelecer normas complementares para atividade de comunicação e uso compartilhado de dados, bem como, nos casos de infração a lei, possui autoridade de garantir que medidas cabíveis e proporcionais sejam tomadas em relação aos órgãos públicos.

## 2.5 CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS

Prevendo o inevitável fluxo internacional de dados pessoais, a lei traz neste capítulo todas as condições a serem avaliadas afim de propiciar a transferência internacional de dados, destacando seu aspecto de semelhança com a GDPR, prevendo a possibilidade de uma padronização internacional no tratamento de dados pessoais, e ganhando um aspecto também econômico, como destacado por Rocha

(2020, p. 14), onde afirma que “Inclusive este foi um dos valores da lei nacional: evitar que o Brasil sofresse qualquer embargo comercial por falta de legislação apropriada, especialmente da Europa, após a promulgação por esta da GDPR”.

Isto fica claro em seu **Art. 33, Incisos I e II**, onde destaca que a transferência de dados depende da garantia por parte do controlador, por meio de cláusulas contratuais, normas corporativas globais, selos, certificados e códigos de conduta regulares, de um grau de proteção de dados pessoais no país de destino que se assemelhe ao existente no Brasil.

Neste ponto, prevê em seu **Art. 34** a possibilidade de avaliação por parte da ANPD, do nível de proteção de dados pessoais do país estrangeiro por meio de fatores como a adoção de medidas de segurança previstas, observância dos princípios gerais de proteção, existência de garantias judiciais e institucionais a respeito dos direitos de proteção, além de outras circunstâncias específicas a transferência e que envolvam os dados.

Essa avaliação estende-se também as cláusulas contratuais, onde a ANPD poderá inclusive designar organismos de certificação sob sua fiscalização para garantir que os direitos, garantias e princípios da LGPD sejam observados, gerando uma padronização dos contratos já diretamente vinculada a especificações da lei, como ressalta (PINHEIRO, 2020, p. 95):

Verifica-se que a imposição de uma padronização do modelo de cláusulas contratuais que devem ser observadas pelas instituições, que seja em suas relações corporativas globais, quer seja em seus códigos internos e certificados, demonstra que as novas regulamentações visam assegurar que os preceitos legais e os princípios, direitos, garantias e deveres trazidos pela lei sejam observados e pactuados em toda a cadeia de valor do negócio, ou seja, que as regras fiquem claras e sejam disseminadas também por meio da governança dos contratos entre as partes.

Adicionalmente as regras acima, apresentam-se outros casos de permissão para transferência internacional como quando for necessário a cooperação jurídica internacional, proteção da vida de titular ou terceiro, devido a compromisso assumido de cooperação internacional, para fins de execução de política pública ou



atribuição legal do serviço público, consentimento do titular ou autorização advinda da ANPD.

## 2.6 CAPÍTULO VI – AGENTES DE TRATAMENTOS DE DADOS PESSOAIS

Capítulo responsável pela descrição dos deveres e responsabilidades do Controlador, Operador e Encarregado. Abordando inicialmente o controlador e o operador, destaca que devem manter registro de todas as operações realizadas durante o processo de tratamento, podendo, inclusive, haver solicitação por parte da ANPD de um relatório de impacto a proteção sobre os dados e as operações citadas anteriormente. Ressalta ainda que o relatório deve conter informações mínimas como a descrição dos tipos de dados coletados e a metodologia utilizada na coleta e segurança das informações.

A manutenção de um registro completo e pleno dos dados, além do aspecto de estar previsto legalmente, apresenta também importante papel em processos e ações judiciais que possam vir a ser impenetradas contra o controlador ou operador, pois a lei possibilita a inversão do ônus da prova, ou seja, a necessidade de que o acusado apresenta provas em detrimento a acusação, nos casos em que a lei entenda a acusação como verosímil e o titular hipossuficiente (sem condições econômico-financeiras).

Dessa forma, o uso das informações terá o papel de demonstrar provas que isentem de responsabilidade os agentes de tratamento, destacando que o tratamento respeitou a legislação e forneceu segurança ao titular quanto ao modo que foi realizado, as técnicas de tratamento utilizadas e o resultado e os riscos que se espera dele.

Em seguida, seu **Art. 39** trata sobre a vinculação entre o controlador e o operador, os quais apresentam relação de solidariedade entre si, inclusive para fins

de cobrança de indenização e multa, onde uma parte pode exigir restituição da outra nos casos de pagamento efetuado.

Contudo, levando em conta que o consentimento do titular é obtido pelo controlador, o mesmo assume responsabilidade maior no que tange ao ciclo de vida dos dados na gestão e governança do negócio. Destaca também, no **Art. 40**, que ambos, controlador e operados, devem pautar suas ações nos os padrões impostos pela ANPD, a qual tem este direito definido e explicitado na LGPD.

No **Art. 41** a lei versa sobre o encarregado (DPO), o qual deverá ser indicado pelo controlador, tendo suas informações de contato divulgadas de forma clara e objetiva. O encarregado por si só pode ser uma pessoa física ou jurídica, estando ele vinculado como funcionário da empresa (excetuando diretores), ou ainda terceiros contratados para realizar a função.

No entanto o ponto principal a ser avaliado, diz respeito as habilidades necessárias ao mesmo, que apresentam grande diversidade em conformidade a diversidade também de atividades que o mesmo irá realizar. Entre suas habilidades podemos destacar relacionamento interpessoal, conhecimentos jurídicos, empresariais, administrativos e técnicos, mais diretamente relacionados com governança de dados e cyber segurança.

Nesta linha (PINHEIRO, 2020, p. 99) afirma:

Logo, poderíamos agrupar as ações do Encarregado em pelo menos 4 grupos distintos: a) atendimento de Titulares (para dentro e para fora); b) relacionamento com Autoridades (Legal Affairs); c) orientação sobre Proteção de Dados Pessoais (suporte para implementação e manutenção da conformidade e campanhas educativas); e d) resposta a incidentes (contenção, mitigação e lições aprendidas).

Devido à está grande lista de conhecimentos, muitas empresas têm utilizado do recurso da constituição de um comitê multidisciplinar na empresa, ou ainda, a contratação de consultorias externas. Este fato tem estabelecido um novo nicho de

negócios, localizado na área de serviço, e que se caracteriza pelo acompanhamento e adequação de instituições a LGPD.

## 2.7 CAPÍTULO VII – SEGURANÇA E BOAS PRÁTICAS

Abordando o tema da Segurança e Boas Práticas, destaca que os padrões mínimos para a proteção de dados pessoais, assim como os prazos e medidas para comunicação e remediação de incidentes, serão definidos pela ANPD. Embora não seja uma definição fixa, pois existe a possibilidade de serem utilizadas técnicas diferentes e suplementares, por parte das instituições, desde que as mesmas sejam comunicadas a ANPD e que tenham a finalidade de assegurar a disponibilidade, integridade e confidencialidade das informações durante todo o ciclo de vida do dado.

No caso de ocorrência que possa acarretar risco ou dano ao titular, caberá ao controlador comunicar a ANPD, em prazo razoável, definido pela própria autoridade, mencionando minimamente informações como a descrição da natureza dos dados atingidos, medidas técnicas e de segurança utilizadas, riscos relacionados, informações dos titulares envolvidos e as medidas que foram ou serão adotadas para reverter ou reduzir os prejuízos.

Caso os prazos para resolução das situações se estendam além dos previamente estabelecidos, deverá ser comunicado ainda, a razão da demora em reverter a situação. A autoridade de posse destes dados avaliará a gravidade, decidindo as medidas a serem adotadas e se corresponde ao caso de expandir a divulgação do ocorrido para outros meios de comunicação, tornando a informação pública ao maior número possível de pessoas.

Para evitar estas ocorrências, a lei em seu **Art. 50**, procura ampliar e destacar as competências dos controladores e operadores, na formulação de regras de boas práticas e de governança, de forma que contenham informações como o regime de funcionamento, os procedimentos em geral, normas de segurança, padrões técnicos

(serão estimulados pela ANPD), as obrigações de todos os envolvidos no tratamento, ações educativas e os mecanismos de supervisão e mitigação de riscos.

Aqui vale destacar a natureza mutável das situações que envolvam dados, onde a lei destaca que deve ser levado em conta a estrutura, a escala, volume de suas operações, além da sensibilidade dos dados tratados e a gravidade dos dados para os titulares, sendo necessária, a constante atualização, divulgação e real implementação dos processos dentro da organização. Ressaltando a necessidade da real implementação, ou seja, que saia do papel, como afirma (GARCIA et al., 2020, p. 16):

Porém, não basta que isso esteja somente no papel: é preciso que esteja, de fato, acontecendo, com atualizações periódicas e amplamente conhecidas na Organização. Com essa preocupação, a LGPD deixa claro que é preciso levar em consideração a estrutura, o volume e a escala de cada tratamento de dados, com capacidade de resposta para a ANPD em qualquer tempo, para os Titulares ou mesmo outros órgãos que possam solicitar essas informações.

Dessa forma passa-se a ter um programa de governança aplicável a todo conjunto de dados, com mecanismos de supervisão e planos de resposta a incidentes, garantindo confiança por parte do titular e também da ANPD, que pode solicitar a demonstração da efetividade do programa adotado para fins de fiscalização.

## 2.8 CAPÍTULO VIII – FISCALIZAÇÃO

Chegando ao capítulo VIII, trata-se das informações que despertam o maior interesse e que mais destacam-se dentre a grande diversidade de publicações sobre o assunto, que corresponde as sanções impostas pela lei. Inicialmente, a lei garante o princípio da ampla defesa, definindo que a aplicação das sanções ocorrerá apenas depois de todos os processos administrativos que garantam ao acusado todos os recursos para sua defesa.

Comprovada a culpa, e por consequência, a imposição de sanção, as mesmas seguem uma gradação, embora a lei destaque que em sua aplicação, não haja qualquer padrão a ser seguido, podendo ser imputada uma sanção de gravidade maior, a ser julgada segundo os procedimentos que serão relatados mais abaixo.

Contudo, seguindo a linha da gradação e orientações constantes nos artigos da LGPD (BRASIL, 2018) , as sanções iniciam com advertência, passando por multa simples ou diária, em valores de até 2% (dois por cento) do faturamento de pessoa jurídica de direito privado, grupo ou conglomerado no Brasil em seu último exercício, até um valor total de R\$ 50.000.000,00 (cinquenta milhões de reais).

Em seguida, existe ainda a possibilidade de publicação das informações, bloqueio ou eliminação dos dados pessoais relacionados com a infração, e ainda, suspensão parcial dos bancos de dados e total do exercício de atividades de tratamento pelo período máximo de 6 (seis) meses, com prorrogação por igual período.

Existem também outros dois princípios, presentes na Constituição Brasileira, da proporcionalidade e razoabilidade, os quais devem ser levados em conta quando da definição das sanções. Conforme estes princípios, serão avaliados fatores objetivos e subjetivos para definição da sanção, estando entre eles: a gravidade e natureza da infração e dos direitos afetados, boa-fé, vantagem obtida pretendida, condição econômica, reincidência, grau do dano, cooperação e a adoção reiterada e demonstrada de mecanismos, procedimentos, boas práticas e medidas tanto preventivas como corretivas, todos referentes ao infrator.

Com isto, se mantém a ideia de implementar sanções de intuito preventivo e que não corram o risco de inviabilizar uma organização, ainda mais, quando levamos em conta o momento atual, onde a diversidade de técnicas e recursos destinados a burlar sistemas de segurança, cresce em ritmo acelerado, em contrapartida ao baixo investimento e atenção dispendida as questões de segurança em nosso país.

Um exemplo claro para uma situação de inviabilização seria uma empresa *startup*<sup>3</sup>, cujos investimento apresentam uma limitação clara, e que muitas vezes impossibilita a adoção das medidas de segurança que se deseja, sofrer uma sanção de bloqueio dos bancos de dados ou do tratamento dos mesmos, gerando abrupta queda no faturamento e por consequência o fechamento da empresa. Contudo, a lei já demonstra esta preocupação em seu **Art. 55 inciso XVIII** onde a LGPD atribui a ANPD:

Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresarias de caráter incremental ou destrutivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

A existência de um artigo tratando dessa questão de forma específica, já deixa claro a preocupação da lei quanto a afetar economicamente de forma negativa instituições, além de que o fato de que a LGPD será gerenciada por um agência nacional, predispondo que a aplicação de sanções será norteadas pelos princípios do direitos administrativo, onde destacam-se a proporcionalidade ou razoabilidade, como (PINHEIRO, 2020, p. 111) destaca:

Importante destacar que o princípio da proporcionalidade ou razoabilidade é amplamente apontado pela doutrina e jurisprudência nacional como uma derivação do art. 5º, V, da Constituição Federal, sendo muito vinculado ao exercício do direito administrativo. Como a regulação dos dados pessoais será efetuada por uma agência nacional, a aplicação das sanções deve seguir os mesmos nortes e princípios do direito administrativo.

## 2.9 CAPÍTULO IX – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Responsável por legislar sobre as autoridades criadas para fins de execução e manutenção da LGPD, o referido capítulo tem seu início com determinações

---

<sup>3</sup>conceito amplamente difundido atualmente, que corresponde a companhias ou empresas que estejam iniciando suas atividades.

relativas a Autoridade Nacional de Proteção de Dados Pessoas (ANPD). Criada com o intuito de trazer segurança, confiabilidade e estabilidade na aplicação da LGPD, bem como assumir o papel de elo para ligação entre as mais diversas partes como o titular, ente privado, ente público e as demais autoridades reguladoras e fiscalizadoras existentes nos três poderes.

Tem sua importância destacada no Brasil, devido ao grande número de artigos existentes na LGPD com dependência explícita da autoridade, tanto para adequações quanto para atividades de fiscalização, auditoria, sanções, dentre outras responsabilidades imputadas a ANPD.

Seguindo a disposição dos artigos, no **Art. 55-A** fica definida a criação da ANPD, com natureza jurídica inicial e transitória de órgão da administração pública federal, sendo que o fato de ser transitória, possibilita que em 2 (dois) anos da sua criação, possa ser transformada em uma autarquia. Este fato é importante pois permitiria a extensão da independência da autoridade, já definida no **Art. 55-B**.

Após a criação da ANPD, parte-se para composição, onde temos o Conselho Diretor, definido como o órgão máximo, composto de 5 (cinco) diretores escolhidos pelo presidente da república dentre brasileiros com reputação ilibada e nível superior de educação e conhecimento técnico. Ocuparão mandatos de 4 anos, ficando responsáveis pelo regimento interno da ANPD e nos casos de vacância do cargo, terá o prazo remanescente inteirado pelo sucessor do mesmo.

Para complementação da sua composição, temos o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas especializadas para suporte à aplicação da LGPD.

Outro destaque importante fica por parte do Conselho Nacional de Proteção de Dados, que apresenta uma complexa composição de 23 representantes, sendo 5 (cinco) do Poder Executivo Federal, 1 (um) do Senado Federal, 1 (um) da Câmara de Deputados, 1 (um) do Conselho Nacional de Justiça, 1 (um) do Conselho

Nacional do Ministério Público, 1 (um) do Comitê Gestor da Internet no Brasil, 3 (três) de entidades da sociedade civil com atuação na proteção de dados, 3 (três) de instituições (científicas, tecnológicas e inovação), 3 (três) de confederações sindicais, 2 (dois) de entidades representantes do setor empresarial e 2 (dois) do setor laboral. Terão à sua disposição mandatos de 2 (dois) anos com a possibilidade de 1 (uma recondução) e atuação não remunerada.

Voltando a ANPD, após criada e composta, suas competências iniciam pela sua responsabilidade em criar ou editar as diretrizes, normas, orientações e procedimentos, por meio de estudos nacionais e internacionais, para garantir o zelo pela proteção de dados pessoais e pela observância dos segredos comerciais e industriais. Geradas as regulamentações, fica a seu cargo a divulgação dessas informações a população, com a escolha das melhores técnicas e recursos de publicitar os mesmos.

No aspecto de divulgação, retratado acima, fica claro que sua atuação deverá ser próxima ao público nacional e internacional. No caso do nacional, será importante a manutenção de canais de comunicação com entidades públicas, agentes de tratamento diversos e a sociedade em geral, para fins de dirimir dúvidas e sanar solicitações, que podem compreender desde sugestões até questões judiciais. Por outro lado, internacionalmente sua atuação estará presente na promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países.

Destacando que sua finalidade vai além do estabelecimento e divulgação de políticas, fica sobre sua competência exclusiva, prevalecendo suas competências sobre outras entidades da administração pública, a fiscalização, instauração de auditorias (inclusive em relação a entidades ou órgãos da administração pública), apreciação de petições de titulares e aplicação de sanções quando comprovada a negligência aos artigos da LGPD. Quando as infrações se originarem de órgãos ou entidades da administração pública federal, deverá comunicar os órgãos de controle interno, assim como, quando as mesmas corresponderem a infrações penais, às autoridades competentes.



Mesmo diante de todas suas particularidades, mantém similaridades com os demais órgãos da administração pública, principalmente no que tange a transparência, sendo ela financeira, onde deverá tornar público por meio de relatórios o detalhamento de suas receitas e despesas, ou ainda técnica, com a elaboração de relatórios de gestão anuais acerca de seus planejamentos e atividades realizadas.

Conforme (PINHEIRO, 2020, p. 46), afirma:

De maneira geral, pode-se afirmar que a constituição da ANPD é essencial para que o enforcement da Lei de Proteção de Dados seja possível, ou seja, é esse regulamento que torna a aplicação da lei possível. Isso ocorre porque um regulamento com previsão de sanções sem órgão fiscalizador não tem efetividade nem garantia de funcionamento.

Ficando evidenciada a importância da criação, composição e implantação da ANPD, para fins de retirar a LGPD de seu papel secundário, para sua posição de destaque dentro da sociedade atual, de encontro ao que vem ocorrendo em todo o mundo.

## 2.10 CAPÍTULO X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Em suas disposições finais ressalta alterações na Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), em relação a exclusão dos dados pessoais, conforme orientação impostas pela LGPD, além da notificação de empresas estrangeiras em todos os atos processuais previstos pela LGPD, independente de procuração ou disposição contratual.

Reforça ainda que a autoridade nacional deve estabelecer normas para adequação progressiva dos bancos de dados e que a LGPD seja aplicada, em caráter especial, no tocante a matéria de proteção de dados pessoais.

Além disso, conforme afirma (PINHEIRO, 2020, p. 123):

É muito importante que a LGPD seja aplicada de forma especial no tocante à matéria de proteção de dados pessoais, não excluindo a aplicação das demais leis de forma complementar ou subsidiária, sejam nacionais ou tratados internacionais, que devem ser interpretados de maneira harmoniosa e integradora.

Isto destaca o papel da LGPD complementar e não substitutivo, afim de seja aplicada sem excluir a aplicação de outras leis e princípios previstos no ordenamento jurídico brasileiro ou nos tratados internacionais, interagindo com os mesmos em harmonia.

### 3 ADEQUAÇÃO E IMPLANTAÇÃO DA LGPD

Quando se faz referência a LGPD, a atualidade e especialidade do assunto ocasiona muitas dúvidas. Do lado dos titulares dos dados, a principal questão são os direitos que os mesmos passarão a ter e o que irá mudar, quando por exemplo, acessamos uma rede social ou uma simples página *web*, embora como já destacado anteriormente, a lei não se restrinja a esses meios. Por outro lado, temos as empresas e instituições, onde a extensa divulgação centralizada nas sanções geram grande preocupação sobre a adequação a lei, focando o questionamento em onde devo começar e o que devo fazer.

Para suprir esses questionamentos, far-se-á uso de todas as disposições já tratadas anteriormente, aliando as mesmas com recursos e tecnologias, para moldar um passo a passo e gerar sugestões que possibilitem uma adequação segura, rápida e que se adapte aos mais diversos ramos de órgãos ou instituições.

Mas e então, por onde você deve começar? A complexidade dos aspectos da lei e sua característica multidisciplinar, sugere duas opções amplamente difundidas, e que em ambos os casos apresentam pontos positivos e negativos.

No primeiro caso, tem-se a terceirização, ou seja, a contratação de uma empresa especializada na área, com a qual ficará a responsabilidade de avaliação, implantação e acompanhamento dos processos de *compliance*<sup>4</sup>. da empresa em relação a LGPD. Embora seja uma opção interessante no que tange a especialização e experiência trazida pelo terceiro contratado, exige que muitas informações da empresa tenham que ser compartilhadas, aliado ao alto nível de investimento necessário.

No segundo caso, tem-se a opção, que ao meu ver, corresponderia a melhor, onde é formado um comitê responsável pelos aspectos relacionados a LGPD, composto de colaboradores da instituição em questão e liderado pelo DPO, ou

---

<sup>4</sup>em uma tradução livre para a língua portuguesa, significa cumprir, obedecer e executar aquilo que foi determinado" conforme (ASSI, 2018).

ainda, por algum profissional que contenha conhecimentos avançados no que tange a segurança da informação. O restante do comitê será composto das mais diversas áreas como destaca (DONDA, 2020, p. 23):

Esse grupo de trabalho que tem como responsabilidade a análise e a proteção dos dados deve contar com a participação de membros de diversas áreas, principalmente os líderes dos setores que estão diretamente ligados ao tratamento de dados na corporação.

Vale ressaltar que a magnitude da empresa também irá influenciar neste processo, pois para empresas de menor porte, onde um ou poucos profissionais assume todo o gerenciamento das tecnologias, esta função pode vir a ser assumida pelo mesmo. Isto se dá pelo fato de que investimentos visando a contratação de um profissional específico para função de DPO, figuram totalmente fora da disponibilidade de orçamento da instituição, além da necessidade de dispor de tempo para que o profissional se familiarize com todos os processos e tecnologias utilizados pela instituição.

Com isso, o perfil de profissional de TI genérico, portador de conhecimento nas mais diversas áreas, inclusive de áreas além da tecnologia, como a jurídica, começa a tornar-se cada vez mais indispensável nas instituições, pois isto vem de encontro a diversidade de atribuições que o mesmo, na função de DPO, haverá de suprir, como representado na imagem abaixo:

Figura 1 — Atribuições do DPO



Fonte: Data Diligence Consultoria e Acessoria Empresarial LTDA (2020, p. 15)

Considerando a criação e composição do comitê como o primeiro passo, listaremos a seguir todos os passos detalhados para orientar a completa implantação da LGPD em uma organização, devendo a mesma avaliar e aplicar os passos que se enquadram a sua realidade. Podemos listar na ordem indicada:

1. Realizar um diagnóstico baseado na identificação, localização e tratamentos dispensados aos dados pessoais, bem como a gestão de consentimentos, para identificar o nível de conformidade e quais investimentos serão necessários a adequação. Destacando que existem

ferramentas automatizadas atualmente, que podem corresponder como importante recurso no desenvolvimento desta atividade;

2. Revisão e atualização das políticas de privacidade, bem como de cláusulas contratuais, sejam elas relacionadas com titulares, funcionário ou ainda com parceiros e fornecedores. Neste último caso, deve ser avaliado se os fornecedores de ferramentas para gestão de informações como nuvem, big data e mídias sociais, adequaram suas atividades aos requisitos impostos pela LGPD;

3. Mapeamento e compreensão do fluxo e ciclo de vida dos dados, avaliando a necessidade de armazenamento dos mesmos, controles de acesso, controles de segurança, riscos e vulnerabilidades e monitorando todo o tratamento de dados para garantir a manutenção de conformidade presente no ambiente;

4. Atualização do Sistema de Gestão da Informação, principalmente no que tange a Política de Segurança da Informação (PSI), destacando as gestões de consentimento;

5. Monitorar todo ambiente, inclusive com a realização de auditorias;

6. Ministrando treinamentos e campanhas de conscientização;

7. Geração de relatórios de impacto a proteção de dados pessoais, também conhecido por RIPD, o qual deve conter todos os processos de tratamento, bem como os riscos e providências de segurança aplicados aos dados;

8. Criação de um plano de ação para situações emergenciais;

Seguindo a listagem acima, discorrer-se-á mais profundamente a respeito de alguns passos, destacando que o item 2 será tratado juntamente ao item 4, devido as questões de privacidade e contratuais integrarem, normalmente, a PSI. A finalidade será esclarecer informações e sugerir rotinas e ferramentas que auxiliem no desenvolvimento dos mesmos.

### 3.1 DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO

Em nosso passo inicial, a ideia é abordar e avaliar toda a política adotada pela empresa, que envolva a segurança da informação. Neste ponto faz-se necessário o apoio por parte das gerências da empresa, de forma que comunicar de forma clara os conceitos trazidos pela lei, dando ênfase a importância de implantação da mesma, é indispensável, pois como destaca (POHLMANN, 2019, p. 69), "Antes os dados eram da empresa. Agora eles serão dos titulares, e os controladores terão responsabilidade de serem, simplesmente, os Fiéis Depositários destes dados".

Embora este seja um assunto de extrema importância, onde todas as empresas deveriam adotar as melhores práticas e garantir todos os níveis de segurança, na realidade ficamos diante de um panorama onde poucas empresas tem o interesse e recursos para buscar o ideal. Em função disso, considero interessante abordar de maneira superficial e com foco maior na LGPD, os pilares que fundamentam a segurança da informação, definidos como confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Tratando da **Confidencialidade**, a mesma objetiva que apenas pessoas devidamente autorizadas, tenham acesso a determinadas informações, impossibilitando, por exemplo, a divulgação de dados pessoais e sensíveis, de forma descontrolada, gerando riscos aos portadores desses dados. Os recursos usados baseiam-se na definição de permissões de acesso, seja a banco de dados, recursos on-line e de compartilhamento, e culminando com o uso de recursos de criptografia (mascarando os dados para impedir sua compreensão por pessoas não autorizadas).

Em seguida, tem-se a **Integridade**, que visa garantir de que as informações armazenadas ou em processo de armazenamento não serão manipuladas ou alteradas. Isto assume papel destacado, quando tratamos da integridade de

informações nos bancos de dados, *backups*<sup>5</sup>, *logs*<sup>6</sup>. e nos mecanismos de proteção utilizados.

Outro ponto fundamental, destacado atualmente com a intensificação do uso de ferramentas on-line, diz respeito a informação estar permanentemente disponível, que corresponde a **Disponibilidade**. Para auxiliar nesta implementação, destacam-se ferramentas como *clusters*<sup>7</sup>, e sistemas alicerçados em recursos de *cloud* (nuvem), onde os prestadores do serviço apresentam como uma de suas principais características a recorrência das atividades, de forma que caso um de seus servidores apresente problemas, a tarefa é retomada por outro, garantindo a manutenção do serviço.

Por fim, tem-se dois pilares, que se destacam frente a LGPD, sendo a **Legalidade**, que como o nome já diz, institui que todas as tarefas que envolvam segurança da informação estejam pautadas e respeitem a Legislação sobre assunto, a qual foi extremamente diversificada e complementada com o advento da LGPD.

E a **Autenticidade**, onde visa-se garantir que as pessoas envolvidas em ações com dados pessoais possam ser identificadas ágil e incontestavelmente. Aqui vale destacar que este princípio deve caminhar em conformidade com a LGPD, de forma que não deve ser possível identificar os titulares dos dados por meio de seus dados divulgados, mas apenas por intermédio dos responsáveis de tratamento, mediante solicitações amparadas pela Lei.

Mediante os princípios tratados acima, segue-se para a avaliação da empresa, quanto a sua política de segurança, de forma que o recurso amplamente utilizado corresponde a um questionário, contendo perguntas de cunho genérico e técnico. No âmbito genérico, utiliza-se questões que procurem avaliar a área de atuação da empresa, sua magnitude e os processos internos que a mesma realiza, de forma que possa ser definida uma prioridade dentre os processos que irão passar

---

<sup>5</sup>cópia de segurança.

<sup>6</sup>registros de atividades realizadas no sistema.

<sup>7</sup>união de computadores, para realizar atividades de processamento em conjunto.



por adequação. Neste ponto, uma sugestão é seguir a linha de abordagem de (POHLMANN, 2019), utilizando o conceito de Fator de Risco (FR).

Fator de Risco é um número, entre 2 e 1.800, que indica o grau de risco que o item representa para sua empresa. Se FR for menor ou igual a 150, ele apresentará um risco desprezível, não sendo necessária nenhuma ação corretiva sobre o item. Sendo maior que 150, apresenta risco de compliance ou de continuidade do negócio, para a empresa, sendo o risco, proporcional ao número. Assim, um item que apresente um FR de 1.800 necessita de cuidado muito mais urgente que um item que apresenta índice 200, por exemplo. Isto permite que os itens sejam agrupados por ordem decrescente, no relatório de compliance, de forma que você possa, facilmente, determinar àqueles que necessitam de cuidado mais urgente.

Seguindo este conceito, atribui-se um determinado valor a cada item, estando esses valores dentro de uma janela, como por exemplo, de 0 a 100, de forma que ordenando os itens pelo seu valor, em ordem decrescente, definimos quais itens terão preferência frente aos demais no processo de implantação da LGPD. Uma forma de representação dos dados acima corresponde a Declaração de Apetite de Risco, desenvolvida internamente na empresa, por integrantes da alta gerência e focada nos riscos entorno da empresa, listando, quantificando e qualificando os mesmos. Dentre os questionamentos que está sessão deve responder, (POHLMANN, 2019, p. 97) destaca:

- Quais riscos a organização consegue assumir sem prejuízos significativos?
- Quais riscos a organização não está disposta a assumir?
- Quais riscos são considerados extremos, e precisam ser evitados a qualquer custo?
- Quantos riscos a empresa pode absorver (quantitativamente)?
- Quantos eventos paralelos são tolerados pela política de riscos da empresa?

Complementando o questionário, tem-se a sessão técnica do mesmo, onde serão avaliadas as tecnologias e recursos utilizados na empresa, para garantir a segurança de suas atividades, desde a contratação de colaboradores e serviços, aquisição de equipamentos, incorporação de funcionários, desenvolvimento das atividades, ciclo dos dados, até o desligamento de funcionário e compartilhamento e divulgação de dados para ambiente externo.

Finalizado o questionário, passa-se a execução de um paralelo entre as informações obtidas pela avaliação e as regulamentações de segurança da informação, onde temos destacada a LGPD, pilar central de nosso estudo, e também a família de normas da ABNT NBR ISO/IEC 27000, que trata fundamentalmente, e de forma detalhada, todas as práticas a serem dotadas para confecção de uma Política de Segurança da Informação.

### 3.2 MAPEAMENTO E ADEQUAÇÃO DO FLUXO DE VIDA DOS DADOS

O próximo passo exige muita participação dos integrantes do comitê e consiste em identificar o fluxo dos dados dentro da instituição, desde a sua coleta até o término do seu tratamento, culminando com sua eliminação ou armazenamento, quando assim previsto pela lei. Convém destacar que o fluxo de dados vem ocorrendo de maneira descontrolada e cada vez mais intensa, com a valorização do dado, porém, com a entrada em vigor da LGPD, passa a ser regulamentado e amplamente gerenciado, conforme destaca (DONDA, 2020, p. 35):

O que antes acontecia indiscriminadamente agora deve obedecer à lei, que determina que certos dados somente podem ser tratados seguindo os princípios da LGPD, e isso vale para todo o tratamento de dados no ciclo. Por isso, é importante o conhecimento de como o ciclo ocorre na empresa para que sejam tomadas as medidas necessárias.

Vale destacar que o ciclo de vida dos dados envolve muitas etapas como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, modificação e eliminação, sendo que para nossa finalidade de estudo abordaremos a coleta, armazenamento, operação, tratamento, compartilhamento e eliminação dos dados. Por isso, segue abaixo um exemplo inicial de uma planilha para mapeamento de dados, para auxiliar na compreensão e servir como ponto de partida para realizar esta atividade.

Quadro 1 — Exemplo de Planilha de Mapeamento

Dado	Tipo	Fonte	Motivo	Amparo Legal	Processos	Eliminação	C	MI	MC
Nome	Pessoal	RH	Saúde	Obr. Legal	BD	3 meses	S	N	S
Sangue	Sensível	RH	Saúde	Saúde	Avaliação Física	1 mês	S	N	S

Fonte: Adaptado de Pohlmann (2019, p. 72)

Na planilha acima, procura-se agrupar informações do ciclo de vida dos dados, com informações adicionais de Consentimento (C), Menor de Idade (MI) e a identificação se corresponde a um dado crítico dentre os processos da empresa (MC). O conjunto de informações já destaca o processo dispendioso e detalhista a ser executado, cujo conhecimento dos dados faz-se muito importante, de forma que o auxílio dos responsáveis dos setores da instituição é praticamente indispensável.

Pode-se destacar, ainda, alguns softwares utilizados desde a descoberta dos dados (*Data Discovery*), controle de prevenção de perda de dados (*Data Loss Prevention*) e classificação de dados (*Data Classification*), os quais contribuem amplamente no processo de mapeamento.

### 3.2.1 Coleta de Dados

Dentre as etapas de fluxo dos dados, a coleta pode ser definida como a primeira etapa, sendo caracterizada na LGPD pelos fundamentos do consentimento (ciência clara e explícita do titular) e transparência, sendo essa comumente representada pelas declarações de privacidade.

Recomenda-se que a composição da declaração contenha informações relativas a quais dados pessoais serão coletados, como serão utilizados, por quanto tempo, como e com quem serão compartilhados, e informações para contato com os responsáveis pela declaração em questão, de forma que titular dos dados possa exercer seu direito de acesso aos dados solicitados, mediante requerimento documental.

Já em relação ao consentimento, a lei traz algumas recomendações e exigências para a validação do mesmo, além de abordar os dados tornados públicos pelos titulares, onde destaca a necessidade de comunicação e solicitação de consentimento ao titular, apenas quando a finalidade a qual os dados foram disponibilizados for alterada.

Figura 2 — Princípios de Validação do Consentimento



Fonte: Data Diligence Consultoria e Acessoria Empresarial LTDA (2020, p. 31)

Deve-se ainda ter muita atenção aos vícios de consentimento, que corresponde a situações e ações que invalidam o consentimento disponibilizado, seja ela de fonte escrita, digital, áudio ou vídeo. Dentre eles podemos destacar erros, dolo, coação, estado de perigo, fraude, simulação, dentre outros. Para garantir maior clareza, (POHLMANN, 2019, p. 60), dispõe um exemplo simples que corresponde a "uma tela de um aplicativo web que apresente o consentimento, seguido de uma caixa de aceitação, onde a aceitação já esteja marcada".

Convém destacar também, a grande diversidade de meios para a coleta de dados, os quais são abrigados pela LGPD como cadastro *on-line*, formulários escritos, recebimento de dados de terceiros, e-mail dentre outros, que ocasiona grande diversidade de recursos de segurança a serem adotados.

A tendência está em eliminar a utilização de formulários escritos, voltando a comunicação dos dados de forma digital, usando além de formulários digitais, e-mail, ferramentas *cloud* (Google Drive) e servidores FTP, onde é possível utilizar recursos de segurança como firewall, criptografia (exemplo *Formsite*), que garantam a segurança na disponibilização dos dados do usuário e no processo de transferência dos mesmos até seu local de armazenamento. Aqui temos também meios físicos como pendrives e hds externos, onde farei uma recomendação pessoal e que tem sido adotada pela maioria das empresas, que corresponde a descontinuidade de utilização destes meios.

Para melhorar a compreensão desta etapa, podemos exemplificar uma coleta de dados, com o acesso e cadastro de dados em uma página web. Neste ponto temos vários detalhes a serem levados em contas, desde a declaração de privacidade, a exposição do propósito de utilização de *cookies*, assim como a utilização de certificados digitais do tipo TLS, identificados pela extensão HTTPS na *url* do navegador, e que primam pela segurança na camada de comunicação das informações.

### 3.2.2 Armazenamento dos Dados

Quando se chega ao armazenamento dos dados, o primeiro passo é identificar todos os locais de armazenamento dos dados, sejam eles físicos, onde podemos citar os populares arquivos em pastas, ou digitais, onde temos nossos bancos de dados, sendo eles locais ou ainda na nuvem.

Nos casos locais, devemos observar alguns pontos importantes na garantia da segurança dos dados como o acesso privilegiado aos bancos físicos e digitais presentes na instituição, segurança física, criptografia (dados em repouso e em

trânsito), anonimização, redundância de dados (inclusive com backups externos seguros), auditoria (prevenir ataques e gerar logs das atividades do usuário) e o hardening do servidor. Caracterizando o hardening, (DONDA, 2020, p. 45), define que “irá blindar o sistema com proteções, políticas de segurança e a eliminação de serviços e recursos desnecessários para a função do servidor”.

Já por parte de bancos de dados na nuvem, a responsabilidade de adoção das práticas de segurança passa para a empresa ou serviço contratado, cabendo ao DPO da instituição, a observância e confirmação de que o serviço contratado estará de acordo com a LGPD. Estas informações devem ser disponibilizadas pelo prestador do serviço por meio do termo de serviço ou documentação contratual, destacando neste caso, a importância da familiarização com conceitos jurídicos, seja por parte do próprio DPO, ou de algum profissional na instituição que lhe preste auxílio.

### 3.2.3 Tratamento de Dados

Nos tratamentos e operações dos dados, as atividades costumam ser realizadas em estações de trabalho, para as quais devemos dispensar alguns cuidados. Dentre eles temos a criptografia, tanto dos dados no disco por meio de recursos nativos como o *bitlocker* ou ainda sistemas de criptografia de arquivos como *Encrypting File System* (EFS), assim como a manutenção de antivírus e firewall ativo, registrado e atualizado.

Além das estações de trabalho formais, temos a grande difusão, ocasionada em grande parte pela pandemia, das estações de trabalho remotas com a utilização de VPN. Nestes casos é importante a criação de redes seguras e criptografadas por parte da instituição, para que seus colaboradores façam uso, além de cuidados quanto a engenharia social, conscientizando-os da importância de apenas utilizar conexões seguras, e tomar cuidados para que as informações de acesso não fiquem disponíveis a demais pessoas.

Outro cuidado de sumaria importância está relacionado a política de senhas, onde podemos sugerir algumas rotinas importantes: estabelecer a mudança frequente de senhas com maior complexidade (contenham maiúsculas, minúsculas, números e caracteres especiais), utilização de software *self-service password* (permite ao usuário próprio controle sobre a senha, permitindo lembrar e alterar a mesma) e a utilização de autenticação multifator (uso de biometrias e *tokens* além da senha). Vale destacar que, biometria é caracterizada como dado sensível, e por isso, conforme tratando anteriormente na lei, deve ser dispensada uma atenção especial quando da utilização da mesma.

O controle de acesso também figura como importante cuidado, nas atividades de operações dos dados, pois estende-se além das estações de trabalho, fazendo referência aos dados armazenados nos mais diversos locais, e especificando quais operações podem ser realizadas por qual usuário. Esse recurso pode ser utilizado para fins de limitar as possibilidades de ataques aos dados, desde que o usuário com nível mais alto de acesso, não seja atingido.

Dentre os muitos tipos de atribuições podemos destacar o *Mandatory Access Control List* (MACL), onde apenas o administrador pode definir quem e qual o nível de acesso a um objeto, e o *Discretionary Access Control List* (DACL), onde o acesso pode ser definido por qualquer usuário, de acordo com a capacidade de conceder permissão disponibilizada ao mesmo.

#### 3.2.4 Compartilhamento dos Dados

Com a disposição da LGPD, esta etapa passa a apresentar mais fatores e recursos a serem observados, devido a diversas especificações que a Lei para os casos com exigência de consentimento, ou ainda, outras situações que se sobrepõe ao consentimento como o cumprimento de obrigação legal ou regulatória, execução de contratos e acordos de integração internacional.

Primeiro, focando nos casos de consentimento, mesmo após a coleta dos dados de forma consentida, a LGPD exige que a empresa solicite autorização do

titular para compartilhamento dos mesmos, informando de forma clara e explícita com quem serão compartilhados e qual a finalidade do compartilhamento, excetuados os casos previstos em lei citados anteriormente. Além disso, a lei também garante o direito ao titular de solicitar a portabilidade de seus dados, ou seja, que seus dados sejam compartilhados com outra instituição que o mesmo definir. Esta análise fica clara nas palavras de (GARCIA et al., 2020, p. 13):

Entre os direitos dos usuários estão: confirmação da existência de tratamentos consentidos, a revogação de seu consentimento de acesso aos dados, assim como devida correção, anonimização, bloqueio ou eliminação do que não concordar; portabilidade a terceiro que indicar; informações sobre possíveis compartilhamentos

Solucionada a questão de consentimento, entramos nos recursos de segurança na transferência dos dados e principalmente no fato de que, quando a transferência destinar outro país, caberá ao DPO, e Operador, por meio da ANPD, garantir que as determinações especificadas pela LGPD, estejam sendo utilizadas também no país de destino, sendo isso, necessário ao prosseguimento do processo de compartilhamento.

### **3.2.5 Eliminação dos Dados**

Ao fim do ciclo de vida dos dados, chegamos ao seu descarte ou eliminação, que apesar de parecer um processo simples, depende de algumas avaliações importantes, sejam elas quanto ao momento da eliminação dos dados ou aos meios utilizados para tal. A lei define que após cumprida a finalidade dos dados, os mesmos devam ser eliminados, cabendo as empresas a justificativa legal e informação aos titulares das novas finalidades e do tempo caso desejem mantê-los.

Além disso, sugere-se a utilização de empresas especializadas e softwares específicos na eliminação dos dados, para impedir de sobremaneira qualquer possibilidade de recuperação dos mesmos, correspondendo a um processo mais complexo do que parece conforme afirma (DONDA, 2020, p. 90):



Na prática, a eliminação dos dados é um processo simples, mas exige atenção quando houver a necessidade de descarte físico de equipamentos, pois, do ponto de vista de segurança da informação, devemos ter certeza de que os dados foram eliminados de maneira a não permitir que pessoas mal-intencionadas possam recuperar as informações excluídas e comprometer a privacidade ou o ambiente.

### 3.3 ATUALIZAÇÃO DO SISTEMA DE GESTÃO DA INFORMAÇÃO

De forma clara e simples, um sistema de gestão das informações são processos adotados para estabelecer e implementar a segurança dentro de uma instituição, visando garantir a confidencialidade, integridade e disponibilidade de seus ativos. Como tratamos mais diretamente sobre informação, focaremos nosso estudo na PSI, que consiste em um documento que define diretrizes, planos, regras, e procedimentos de processos, com linguagem compreensível a todos, a respeito das questões de segurança adotadas e obrigatórias na empresa.

A melhor maneira de implementar uma Política de Segurança, detalhada e seguindo as regulamentações de forma completa, consiste em seguir a família de normas da ABNT NBR ISO/IEC 27000, as quais para melhor compreensão segue abaixo uma descrição detalhada de sua distribuição:

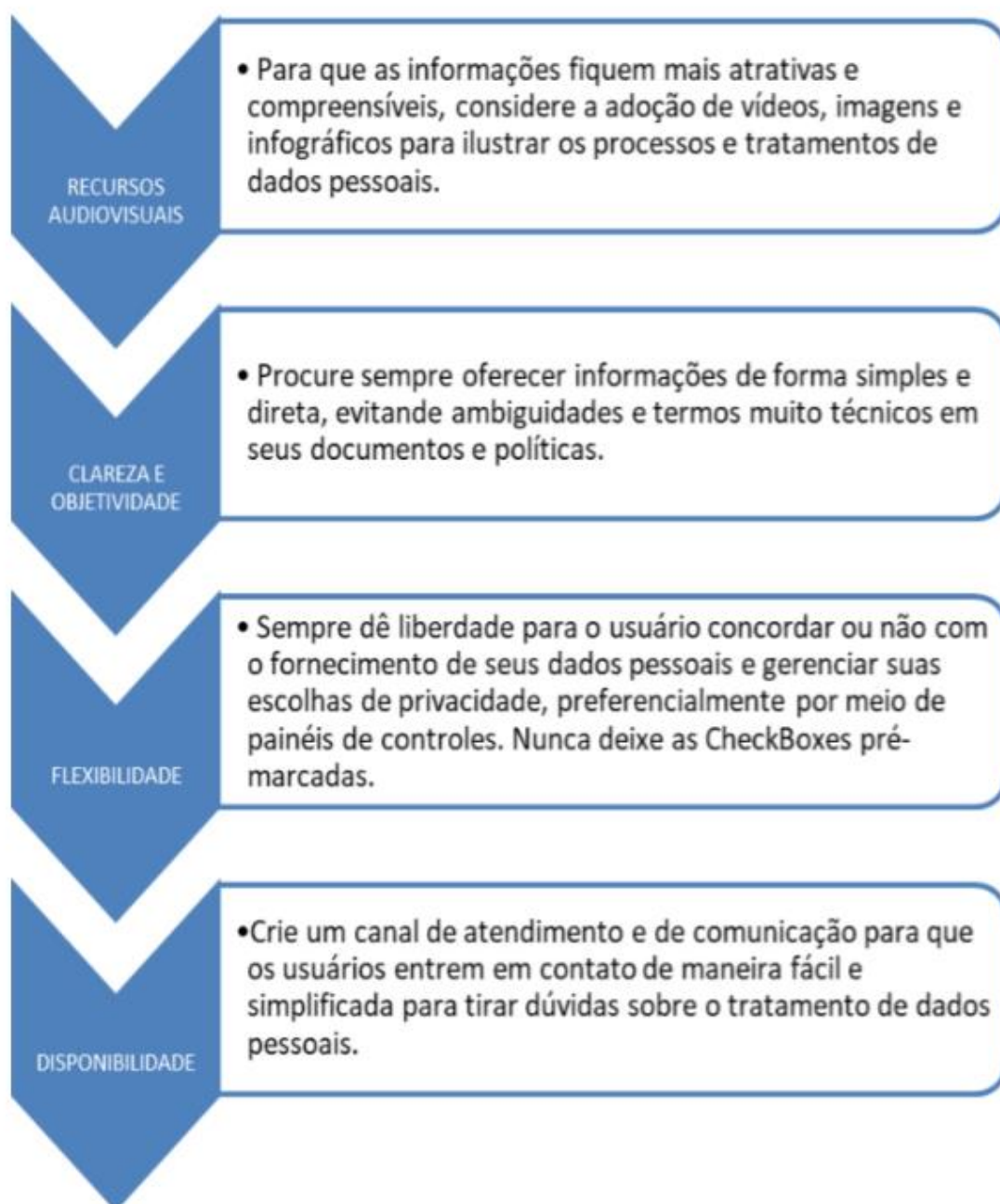
- ISO/IEC 27000: define a nomenclatura utilizar nas normas da família;
- ISO/IEC 27001: norma responsável pelos processos para certificação das empresas e instituições;
- ISO/IEC 27002: norma contendo as práticas para implementações dos controles de segurança;
- ISO/IEC 27003: guia de boas práticas;
- ISO/IEC 27004: norma destinada aos procedimentos de monitorização, medição, análise e avaliação;
- ISO/IEC 27005: trata da gestão dos riscos de segurança da informação;

Devidamente constituída a PSI, e diante da LGPD, cabe aos responsáveis a revisão e atualização da PSI, com a adição de uma Política de Tratamento de Dados Pessoais, com a finalidade de transmitir aos demais colaboradores, de forma compreensível, conceitos e processos trazidos pela LGPD, além de demonstrar a importância dessas implementações. Visando esta atualização, (DONDA, 2020, p. 31) sugere:

Você pode criar um documento a parte ou adicionar em sua PSI já existente pontos importantes sobre o tratamento de dados pessoais, indicando o que é a LGPD, quais as responsabilidades dos envolvidos, quais os níveis de acesso e o uso permitido das informações, se é permitido ou não fornecedor dados a terceiros etc.

Na confecção desta Política de Tratamento de Dados Pessoais, a melhor abordagem consiste em seguir os fundamentos para compreensão, interpretação e implementação das normatizações estabelecidas pela LGPD, definidos no seu Art. 6º da LGPD, os quais podem ser visualizados com mais clareza na figura a seguir.

Figura 3 — Fundamentos para Política de Tratamento de Dados Pessoais



Fonte: Data Diligence Consultoria e Acessoria Empresarial LTDA (2020, p. 15)

Outro aspecto importante e que tem sido tratado em conjunto ou incorporado a PSI, diz respeito as cláusulas contratuais, sejam elas entre as pessoas integrantes da instituição ou entre a instituição e outros agentes externos. Aqui, com a LGPD, temos a exigência de revisão contratual, sob penalidade de suspensão de contratos,

pois muitas instituições virão a exigir a comprovação de adequação da empresa para seguirem sua relação contratual com a mesma.

Para facilitar esta revisão, podemos elencar alguns pontos a serem adicionados ao contrato como informações de tratamento e consentimento quanto aos dados, declaração de *compliance* ou documento de mesmo valor semelhante e comprovem o *compliance* da instituição com a LGPD, determinação clara de responsabilidade das partes do contrato, quanto aos dados pessoais que estarão presentes nessa relação.

### 3.4 MONITORAR COM A REALIZAÇÃO DE AUDITORIAS

Após a implantação da LGPD, passamos a realização de auditorias, atuando com papel dissuasivo, ou seja, o conhecimento por parte dos usuários de que todos os seus passos e atividades realizadas serão detalhadamente registradas, emitindo um alerta que impedirá a tomada de ações mal-intencionadas. Contudo, com a vinda da LGPD, as auditorias ganharão importância ainda maior, pois a própria lei solicita que seja mantido um registro em tempo real de todas as operações de tratamento de dados, o que culmina em grande diversidade de relatórios.

O caráter distribuído dos dados por diversos sistemas diferentes e a extensa produção de dados, além da necessidade imposta pela LGPD de pronta comunicação de incidentes de segurança a ANPD, corroboram com a utilização de softwares de auditoria, em detrimento a técnicas nativas para desempenhar tal função.

Sempre destacando que a presença do software deve estar aliada a eficiente utilização do mesmo como (DONDA, 2020, p. 64) afirma “Para ser bem eficiente, o software de auditoria deve ser igual a uma central de monitoramento de vídeo, consolidando todos os eventos em um painel único, pois o monitoramento de eventos deve ser simples e eficiente”.

Após implantado o monitoramento, nos deparamos com outro desafio, que faz referência ao gerenciamento dos diversos *logs* gerados, sejam eles originários de sistemas, bancos de dados, antivírus, *firewalls* dentre outros. Dessa forma, podemos sugerir algumas soluções que auxiliem na centralização dos logs, para fins de identificar com agilidade e integridade violações de segurança nos mais diversos dispositivos e sistemas.

Estas ferramentas são definidas como *log management* ou gerenciadores de logs, compostos de funções como coletar e armazenar massivos volumes de dados, processar e normalizar logs, os mantendo por prazos mais extensos protegidos de adulteração ou destruição, e possibilitando com os mesmos a análise e geração de relatórios.

Ainda em complemento aos gerenciadores de logs, existem softwares atualmente que garantem possibilidades além, como correlacionar eventos de diferentes fontes de dados, detectar e alertar sobre ameaças, contendo *dashboard* para visualização em tempo real e *threat intelligence* (informações a respeito de ameaças e seus atores que auxiliam na mitigação de eventos prejudiciais no ciberespaço). Estas ferramentas são conceituadas por *Security Information and Event Management* (SIEM), onde podemos destacar o *Intrust* (Quest), *Splunk* e *IBM QRadar*.

### 3.5 TREINAMENTOS E CAMPANHAS DE CONSCIENTIZAÇÃO

Chega-se enfim, ao passo onde passa-se a iterar diretamente com o agente que mais impacta na segurança de informação, tanto para o bem como para o mal, que o usuário. Este, por sua vez, encontra-se no centro de uma das principais questões que permeiam a segurança da informação, onde afirma-se de modo unanime, o fato de que as pessoas são o elo mais fraco da cadeia.

Dessa forma, cabe aos responsáveis pela segurança da informação na organização a tomada de iniciativas que visem converter o elo fraco, em um

importante integrante e contribuinte para que a PSI seja divulgada e executada com excelência, pois como já citado anteriormente, a execução da segurança da informação em uma organização, depende da contribuição e participação de todas as pessoas da mesma, pois como afirma (POHLMANN, 2019, p. 71).

Se lhe parece estranho, comentamos que o usuário bem treinado é um dos mais eficientes pontos de segurança que a empresa pode ter (com um custo muito baixo). Pelo contrário, um usuário despreparado é uma ameaça constante à segurança da organização, aos seus ativos, e por conseguinte, aos titulares de dados tratados pela organização.

Para garantir este ambiente de colaboração, a aplicação de treinamentos e campanhas de conscientização torna-se indispensável, embora seja um grande desafio, a simplificação dos conceitos relativos a segurança da informação, tornando os mesmos compreensíveis a qualquer pessoa, independentemente do nível de instrução do mesmo.

Visando a facilidade e amplitude de compreensão, torna-se importante aliar tecnologias atuais, juntamente com atividades interativas, que de alguma forma solicitem a pró atividade do “aluno”, pois as práticas mais adotadas atualmente, como por exemplo cursos EAD, não apresentam garantia alguma de que o usuário tenha realmente obtido os conhecimentos necessário e assimilado a importância da sua contribuição dentro da organização.

Para isso, farei a sugestão de alguns recursos que podem ser utilizados, e que tem demonstrado melhores resultados como:

- Uso de páginas web interativas, com vídeos, instruções e atividades avaliativas que solicitem por parte do usuário, a utilização dos conceitos obtidos para determinar decisões frente a simulações de situações do dia a dia na organização;
- Boletins por E-mail para fins de lembrar regulamentações e práticas a serem adotadas;
- Distribuição de folhetos ilustrados, com recursos ilustrados e chamativos;

- Seminários presenciais e palestrar com face da manhã, realizados em períodos de tempo pré-definidos, para atualizar os colaboradores da organização a respeito da PSI. Estas atividades promoverão uma maior concentração dos colaboradores, por serem momentos de foco totalmente definido na segurança da informação, em contrapartida a cursos individuais onde demais atividades do dia a dia podem ocasionar o desvio de atenção.

Aqui vale ainda destacar um exemplo prático adotado pelo Comitê Gestor de Internet do Brasil, onde foi criada e distribuída uma Cartilha de Segurança para Internet, acompanhada de periódicos contendo conteúdo específico, para auxiliar na divulgação.

### 3.6 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

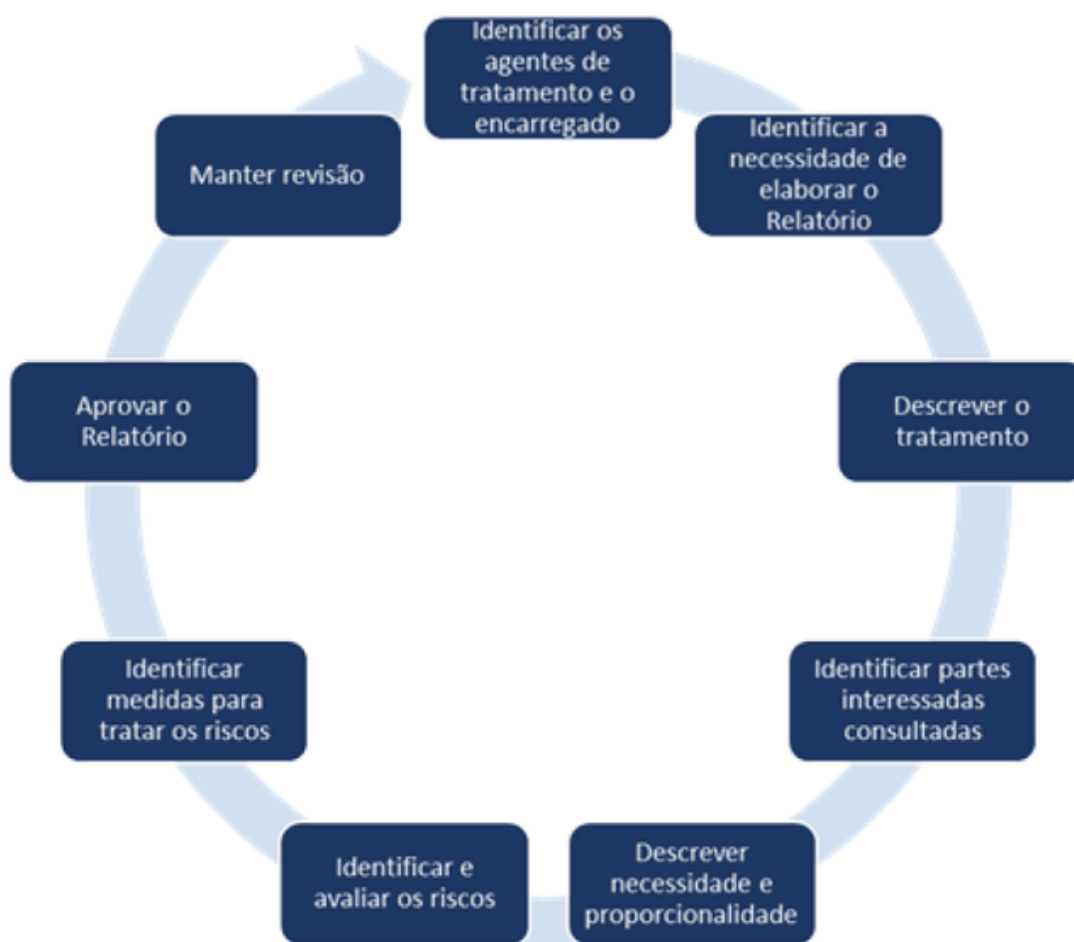
Mais amplamente conhecido por RIPD, consiste em um documento extremamente importante no processo de conformidade com a LGPD dentro das organizações, sendo o responsável por demonstrar os dados pessoais coletados, tratados, usados, compartilhados bem como os riscos associados aos dados pessoais sensíveis e que podem afetar os direitos fundamentais dos titulares, destacando-se aqui a privacidade. Isto segue a definição e caracterização de (DONDA, 2020).

Este documento deverá ser criado pelo controlador (empresa controladora), e nele deverão constar todos os detalhes sobre os dados e como é feito o seu tratamento desde a coleta, o que inclui especificar a base legal usada até o fim do ciclo de vida, informação em que devem constar ainda todas as medidas utilizadas na proteção e na garantia da privacidade.

Levando em conta os riscos destacados, o relatório deve conter as medidas adotadas ou que se objetiva adotar na prevenção e mitigação dos riscos. Vale destacar que seu papel vai muito além do informativo, pois um RIPD completo, apresentando processos e tratativas bem documentadas, definirá como diferencial a favor na avaliação e definição de sanções contra a organização e seus agentes de tratamento de dados.

No que se refere a sua estrutura, a LGPD destaca em seu **Art. 5º e 38**, algumas informações que devem compor o conteúdo do mesmo como os tipos de dados coletados, como é feita a coleta e quais medidas são adotadas para garantir a segurança dos dados. Contudo para dar uma ideia inicial da estrutura do relatório, faremos uso da figura abaixo, sem entrar em detalhes em cada uma das fases, pois, isto fará do estudo mais detalhado que seguirá no desenvolvimento do TCC.

Figura 4 — Etapas para desenvolvimento do RIPD



Fonte: Donda (2020)

Sua estrutura apresenta abordagem semelhante à de (POHLMANN, 2019, p. 180), que descreve os itens para confecção do relatório:

O relatório para a ANPD deve conter um cronograma dos fatos que aconteceram, informar as medidas de segurança que haviam, e identificar



os motivos do vazamento. Também deve informar as medidas tomadas pela empresa para conter o problema, a comunicação original aos titulares, sobre o vazamento, e as medidas adicionais de proteção tomadas após o incidente, com a finalidade de que o mesmo não volte a ocorrer.

### 3.7 CRIAÇÃO DE PLANO DE AÇÃO

Para fins da formatação de um Plano de Ação para situações emergenciais, o primeiro passo consiste em utilizar ferramentas e recursos para identificar as vulnerabilidades existentes dentre os ativos, sejam elas de hardware, software, redes, pessoas e ambientes físicos. Realizada esta detecção, deve ser criada uma relação de prioridade entre as vulnerabilidades e os ativos que elas afetarão, pois determinados ativos oferecem mais riscos na execução dos processos e manutenção da empresa, e por consequência, devem ter prioridade em seu tratamento.

Dentre as rotinas utilizadas nos planos de recuperação, costuma-se focar em tecnologias de backup, replicação e redundância nos ambientes de hardware e software. Estas visam garantir a confidencialidade, integridade e disponibilidade dos dados, levando-se em conta o objetivo do Ponto de Recuperação e do Tempo de Recuperação. Em relação ao ponto de recuperação, é possível exemplificar com o período que se deseja ter backup de dados disponíveis, e o tempo de recuperação corresponde ao período necessário a recuperação completa dos dados, partindo da cópia de segurança existente.

Pode-se enquadrar no plano de ação, as medidas e documentações que podem vir a ser solicitadas por parte da ANPD, para fins de fiscalização por parte da mesma. As mesmas correspondem as políticas adotadas e os registros de processamento dos dados. Ressalta-se ainda, os casos de processos judiciais solicitados por usuários, onde a presença de RIPDs, Política de Tratamento de Dados Pessoais e Privacidade, avaliações de risco, documentos de solicitação de dados de usuários e solicitações de consentimento, representam papel fundamental favorável aos responsáveis pela segurança da informação na instituição.

Deve-se ressaltar também, que mesmo tomadas todas as providências possíveis, ainda podemos vir a ter problemas, e a comunicação do ocorrido, tanto ao titular dos dados como a ANPD deve fazer parte também do Plano de Ação. Em relação a ANPD, o documento indicado corresponde ao RIPD, repleto de informações detalhadas sobre o incidente, envolvidos e documentações como o comunicado de prestação de contas ao titular.

Como já retratado quando da comunicação a ANPD, faz se necessário comunicar aos titulares dos dados, o incidente ocorrido, e o mesmo é feito por intermédio de um comunicado de prestação de contas. Este deve ser encaminhado prontamente ao incidente ocorrido, informando de maneira clara ao titular o que ocasionou e descrevendo o mesmo, além de destacar as medidas tomadas para que fosse solucionado e não volte a acontecer. Não esquecendo de instruir o titular, caso seja necessária alguma ação por parte do mesmo.

### 3.8 DEFINIÇÕES ESPECIAIS PELO TIPO DE DADOS

Aqui far-se-á uma classificação e observação de comportamento dos dados, pelas peculiaridades que alguns tipos de dados trazem consigo, como por exemplo os dados referentes a saúde, os quais podem ser encaixados, quase que em sua totalidade, como dados sensíveis.

Isto ressalta a atenção que deve ser dada na adequação a LGPD dos processos que envolvam esses dados, pois embora boa parte deles dispense de consentimento do titular, por se enquadrarem em base legal, tutela de saúde, proteção a vida ou cumprimento de obrigação legal, isto apenas afeta a etapa de coleta dos dados, sendo que as demais operações com os mesmos deverão observar os princípios de segurança da informação e da LGPD. Esta análise é corroborada por (POHLMANN, 2019, p. 145):

Da mesma forma que em casos anteriores, ressaltamos que o enquadramento em uma base legal como uma das citadas, não exime a empresa dos demais pontos de exigência a nível de segurança para a empresa. Somente dispensa o consentimento, mas as exigências legais relativas ao tratamento dos dados seguem sendo exatamente as mesmas.

Em relação aos dados contábeis e financeiros, além de sua importância vital nos processos da instituição e seu caráter sigiloso, devemos atentar para os dados financeiros que estejam aliados a titulares, pois esse vínculo lhes confere a etiqueta de dados sensíveis.

Além disso, vale destacar que muitos dados serão gerados neste ramo, partindo de tratamento realizado por tecnologia de Inteligência Artificial, e neste ponto a LGPD traz uma inovação, possibilitando aos titulares questionarem os parâmetros, os métodos e resultados dessa análise.

Outro importante tipo de dado corresponde aos dados de titulares em processo de contratação por alguma instituição, pois aqui temos uma situação incomum, onde a instituição passa a ter posse de dados pessoais e inclusive sensíveis, originados por exemplo das avaliações psicológicas, de titulares externos a mesma. Vale destacar que os processos pelos quais os titulares passaram e que darão origem a intensa gama de dados, devem partir sempre do consentimento por parte do titular, gerando termos específicos de consentimento, a cada etapa de seleção.

Chegando ao fim do tour pela LGPD e do passo a passo para implantação da mesma, você estará de posse de informações que servirão para dar prosseguimento ao estudo, com o desenvolvimento de uma página web, interativa e onde os conhecimentos estarão particionados em ramos de atividade, devido a particularidade específicas de cada ramo em relação as disposições da LGPD, e procurando destacar duas visões distintas, onde teremos de um lado a visão do profissional de implantação e do outro, do usuário e seus direitos frente a essa nova realidade.

## 4 DESENVOLVIMENTO DO WEB SITE

Entrando na etapa de desenvolvimento propriamente dito do web site, adotado o desenvolvimento particionado em etapas, que estarão retratadas de forma mais detalhada abaixo. Convém ressaltar que as etapas utilizadas visaram um desenvolvimento ágil, porém, mantendo a integridade e adaptação do desenvolvimento, as novas funcionalidade e recursos que surgiram durante todo o processo de constituição do site.

Dentre as etapas, tem-se inicialmente a definição da metodologia de desenvolvimento, seguido da análise de requisitos, a geração de um *wireframe*<sup>8</sup>, o cronograma, definição das tecnologias, modelagem do banco de dados, finalizando com a criação do site.

Ao fim do capítulo, disponibilizado algumas imagens referentes ao site desenvolvido, destacando a finalidade da página, bem como os conceitos de interface do usuário e da LGPD aplicados a mesma. Vale destacar também, o site ficou hospedado, possibilitando ser acessado por qualquer pessoa para obter e contribuir com o incremento de conhecimento no mesmo.

### 4.1 METODOLOGIA DE DESENVOLVIMENTO

No que tange a organização e desenvolvimento do site, far-se-á uso da metodologia ágil SCRUM, caracterizada por métodos mais informais e simplicidade, que garantam maior agilidade ao desenvolvimento, frente ao panorama atual de constantes atualizações. A escolha por esta metodologia apresenta ainda pontos adicionais positivos, como ressalta (PRESSMAN; MAXIM, 2015)

A engenharia de software ágil combina filosofia com um conjunto de princípios de desenvolvimento. A filosofia defende a satisfação do cliente e a entrega de incremental prévio; equipes de projetos pequenas e altamente

---

<sup>8</sup>mapa do site, ou seja, uma representação em forma de imagem de como as páginas do site ficarão distribuídas e relacionadas entre si.

motivadas; métodos informais; artefatos de engenharia de software mínimos e, acima de tudo, simplicidade no desenvolvimento geral. Os princípios de desenvolvimento priorizam a entrega mais que a análise e projeto (embora essas atividades não sejam desencorajadas); também priorizam a comunicação ativa e contínua entre desenvolvedores e clientes.

Com a finalidade de contribuir na organização das tarefas, faremos a distribuição de todo o processo em *sprints*, ou seja, blocos de tarefas, com prazos pré-estabelecidos no momento de planejamento, e que estarão disponíveis mais a frente, em uma sessão específica para os mesmos.

Em relação ao ambiente de desenvolvimento, o mesmo foi configurado em uma máquina local, com sistema operacional Windows, utilizando um pacote de serviços denominado WAMPP, de origem francês e que se destaca pela facilidade de uso e por já conter uma interação pré-estabelecida entre todos os recursos necessários ao desenvolvimento.

Este pacote é composto de uma ferramenta online, para criação e gerenciamento de banco de dados *MySQL*, chamada *PhpMyAdmin*. Além dela, temos um framework de desenvolvimento, que fará a composição do *Front-End*, e sua interação do banco de dados, conhecido como Laravel.

O Laravel consiste em um framework *open source* (código livre), escalável, que utiliza a linguagem PHP e o padrão MVC (*Model, View e Controller*), criando uma camada para a lógica da aplicação, uma para a visualização dos dados e outra que faz a interação entre as duas anteriores, rodeado de uma atuante comunidade, que contribuí muito para a sua constante evolução e atualização.

Convém destacar que o mesmo disponibiliza grande facilidade na interação do *Front-End* com o banco de dados, com recursos de consulta em banco de dados que primam pela agilidade no desenvolvimento, além de integridade e segurança, o que vem de encontro a requisitos muito destacados pela LGPD.

Deve-se ainda ressaltar que iremos fazer uso do gerenciamento de versões por meio do *Git*, ou seja, teremos um recurso onde iremos controlar todo o desenvolvimento, inclusive tendo acesso a versões anteriores para restauração, de acordo com a necessidade.

Por fim, no que se refere a hospedagem, foi adquirida e utilizada uma hospedagem da *HostGator*, pois embora tenhamos outras possibilidade de hospedagem grátis, as mesma não nos disponibilizam os recursos de segurança e as adequações a LGPD, inclusive, que o presente serviço de hospedagem já apresenta, e que fica devidamente evidenciado na utilização de seus recursos e em suas políticas contratuais e de privacidade disponibilizadas.

## 4.2 ANÁLISE DE REQUISITOS

Em nosso projeto, o processo de análise de requisitos se deu através dos estudos sobre a LGPD e seu processo de implantação, expostos nos capítulos anteriores. Estes estudos possibilitaram que fossem definidas as informações que seriam mais interessantes de serem divulgadas em relação a LGPD, bem como as melhores forma de expor as mesmas, cumprindo com a finalidade da análise de requisitos, como (PRESSMAN; MAXIM, 2015) ambos autores afirmam declarando que "A análise de requisitos resulta na especificação de características operacionais do software, indica a interface do software com outros elementos do sistema e estabelece restrições que o software deve atender".

Conforme resultado das análises, segue abaixo a lista de requisitos apurados:

- Cadastro dos Usuário do Site, com seus respectivos perfis;
- Cadastro de Notícias atuais sobre a LGPD que serão exibidas na página Inicial;
- Cadastro Interno dos Capítulos, Artigos e Incisos da LGPD;
- Cadastro de links relacionados a LGPD, inclusive dos órgãos oficiais;
- Cadastro dos Setores de Serviço;

- Proposta de Questionário para avaliar Adequação da Instituição a LGPD;
- Sugestão de Dados a serem verificados por Setor de Serviço;
- Cadastro de Passos de Adequação a LGPD, contendo textualização, imagens, vídeos e links de acesso;
- Listagem de Situações por Setor de Serviço, de forma a compartilhar experiências de fatos ocorridos relacionados a LGPD;
- Criação de Página com comportamento semelhante a um Fórum, cuja finalidade será incentivar a integração entre pessoas relacionadas a LGPD, de forma que as mesmas possam compartilhar dúvidas e experiências, que após avaliadas por responsável competente irão se tornar conteúdo permanente no site;
- Sessão simplificada de informações da LGPD, para transmitir informações de forma atrativa a todos e qualquer pessoa que acesse o site;
- Área no site para avaliação e sugestão de melhorias ao próprio site.

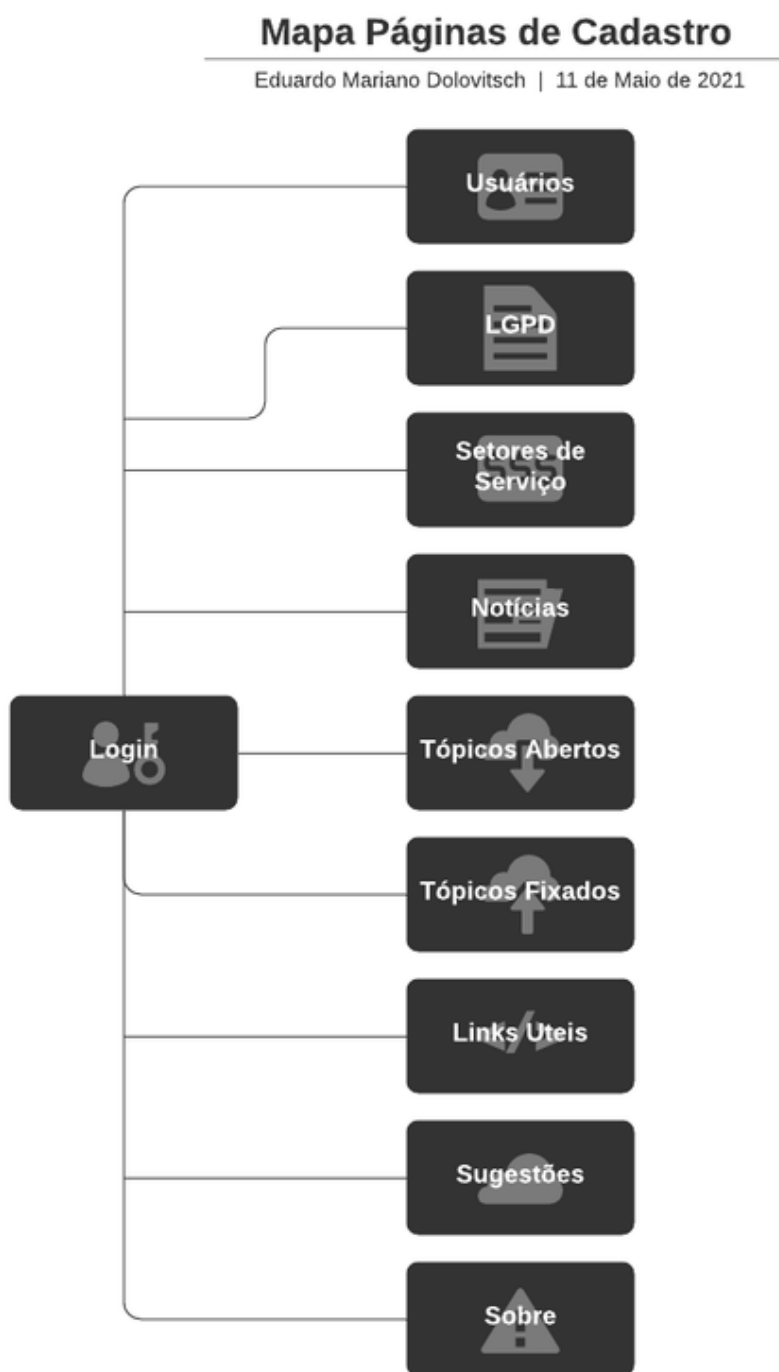
De posse dos requisitos foi realizado o *WireFrame* do Site, ou seja, o mapeamento do mesmo para facilitar a identificação e disposição das páginas. Vale ainda destacar que foram criados 2 (dois) *wireframes*, sendo um referente a página de cadastro dos dados e outra para as páginas de exibição dos mesmos.

#### 4.3 WIREFRAME

Muito utilizados no design de interface, os *wireframes* consistem em um protótipo da interface que será replicada na página web, bem como da distribuição e relacionamento entre as páginas que serão criadas e irão compor o site como um todo. Possibilita a verificação de dependência entre as páginas, de forma a estruturar o desenvolvimento em nível de prioridades.

Segue abaixo as imagens dos *wireframe*, de forma que o leitor tenha já uma ideia de como as páginas foram distribuídas.

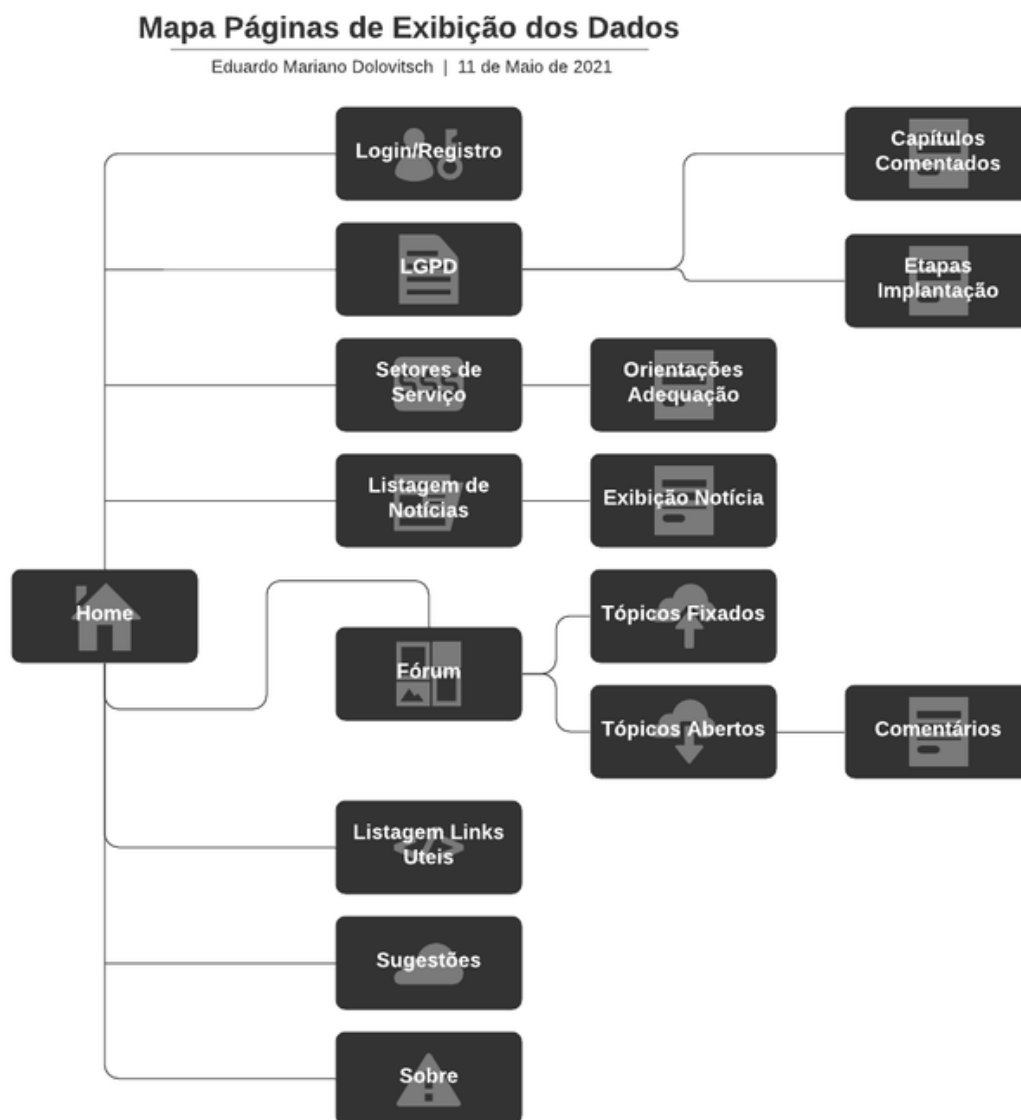
Figura 5 — Wireframe das Telas de Cadastro



Fonte: O autor (2021)



Figura 6 — Wireframe das Telas de Exibição dos Dados



Fonte: O autor (2021)

#### 4.4 CRONOGRAMA POR SPRINTS

Segue nesta seção o cronograma de desenvolvimento, dividido em Sprint, conforme a metodologia ágil adotada, para o desenvolvimento do site.

Quadro 2 — Sprint 1

Tarefa	Data Início	Data Fim
Análise de Requisitos	10/05/2021	10/05/2021
Definição das Tecnologias	10/05/2021	10/05/2021
Criação do Mapa do Site (Wireframe)	11/05/2021	11/05/2021
Modelagem do Banco de Dados	11/05/2021	11/05/2021
Configuração do Ambiente de Desenvolvimento	12/05/2021	12/05/2021

Fonte: O autor (2021)

O primeiro *sprint* foi dedicado ao planejamento do desenvolvimento, buscando informações dos requisitos, e gerando a modelagem do site e do banco de dados. Além disso, de posse dos requisitos, foi possível estabelecer as melhores tecnologias e configurar o ambiente de desenvolvimento da melhor maneira possível.

Quadro 3 — Sprint 2

Tarefa	Data Início	Data Fim
Estruturação da Página Inicial	13/05/2021	14/05/2021
Desenvolvimento da Página de Login e Registro	14/05/2021	14/05/2021
Desenvolvimento da Página de Cadastros	15/05/2021	19/05/2021
Desenvolvimento da Página de Setores de Serviço	20/05/2021	22/05/2021
Desenvolvimento da Página de Links Importantes	23/05/2021	23/05/2021
Desenvolvimento da Página de Listagem e Exibição de Notícias	24/05/2021	24/05/2021
Desenvolvimento da Página do Fórum	25/05/2021	25/05/2021
Desenvolvimento da Página de Exibição de Tópicos Abertos e Fixos	27/05/2021	27/05/2021
Desenvolvimento Página Sobre	28/05/2021	28/05/2021
Desenvolvimento Página de Capítulos da LGPD	29/05/2021	29/05/2021
Desenvolvimento da Página de Etapas de Implantação da LGPD	29/05/2021	29/05/2021

Fonte: O autor (2021)

No segundo *sprint* ficou distribuído o desenvolvimento nas páginas do site, iniciando pela página inicial, de login e cadastros, pois por meio das informações cadastradas na presente página, serão supridas as informações que irão compor as demais páginas.

Quadro 4 — Sprint 3

Tarefa	Data Início	Data Fim
Utilização e Avaliação da Página	30/05/2021	16/06/2021
Realização de Correções e Melhorias	30/05/2021	16/06/2021

Fonte: O autor (2021)

Por fim, no *sprint* 3, realiza-se a hospedagem da página, e a utilização da mesma, para apurar seu funcionamento quanto a agilidade, compreensão e facilidade ao usuário, sendo que a partir desta análise foram realizadas atualizações, para atingir a versão final da página.

#### 4.5 DEFINIÇÃO DAS TECNOLOGIAS

De posse da análise requisitos e do mapeamento do site, é possível ter uma ideia mais clara das necessidades de desenvolvimento, no que tange principalmente aos recursos web necessários. Em função disso, leva-se em conta alguns fatores como o número de páginas, o tempo para desenvolvimento, os recursos para exibição dos dados e interação com o usuário na interface, para chegar a uma definição comum da tecnologia a ser utilizada no desenvolvimento, que é o *Framework Laravel*.

O Laravel consiste em um framework de desenvolvimento rápido baseado na linguagem PHP e de código livre. Desenvolvido por Taylor B. Otwell, com sua primeira versão lançada em junho de 2011, sob a licença MIT, com o propósito de ser uma alternativa avançada ao *CodeIgniter*, tem passado por muitas atualizações com o passar do tempo, trazendo cada vez mais funcionalidade para agilizar o desenvolvimento, dentre os quais podemos destacar:

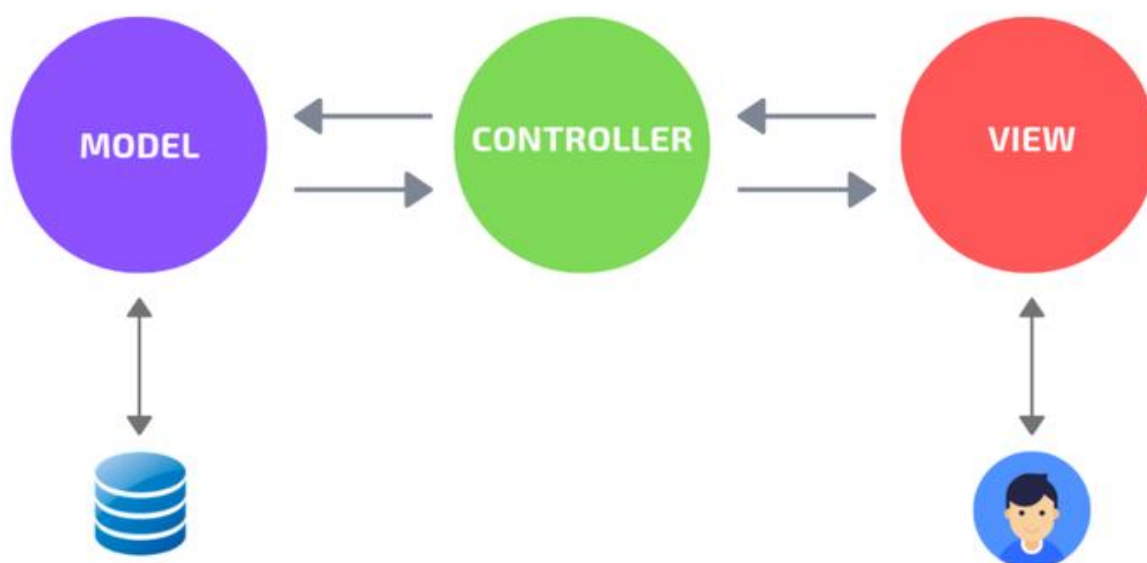
- Sistemas de Template (Blade), possibilitando o reaproveitamento de sessões pré-definidas no restante das páginas do site;
- Modulo de Autenticação Pré-Pronto incluindo as telas de login, e todos os recursos para logar, deslogar, alterar e recuperar senha;
- Sistema de Rotas para mapeamento das páginas vinculadas a URLs;
- Documentação vasta e muito intuitiva, localizada no link <https://laravel.com/docs>;
- Eloquent, QueryNuider e Migrate.

Este último listado, destaca-se, principalmente em nosso projeto, onde o recurso de *migrate* permite que sejam definidas as tabelas do banco, assim como seus campo e tipos dentro do *Framework Laravel*, e a partir disso, com comandos relativos ao *migrate*, desde que configurado corretamente o banco de dados, o Laravel gera as tabelas no Banco.

Após isso, é possível utilizar comando próprio do Laravel (*Eloquent*), para realizar consultas no banco, incluindo filtros, ordenações e agrupamentos, sem a necessidade de escrever SQL puro. Ou seja, o Laravel realiza todas as interações de criação, inserção, alteração, consulta e deleção de dados do banco, tornando os processos mais rápidos e íntegros, a agilizando em muito o desenvolvimento.

Destaca-se ainda por utilizar o padrão MVC (*Model, View e Controller*), onde temos 3 camadas bem definidas, facilitando em muito a organização e manutenções do projeto. Para exemplificar e compreender o padrão MVC, usaremos uma requisição, na qual o *Controller* solicita ao *Model* as informações que virão do banco de dados, e o *Model* por sua vez, obtém as informações do banco, retornando as mesmas ao *Controller*, que então as encaminha para a *View*, a qual ficará responsável por renderizá-las e exibi-las ao usuário. Isto fica ainda mais claro na imagem abaixo:

Figura 7 — Representação do Padrão MVC



Fonte: De Andrade (2020)

Além disso, será utilizado no *Front-End* também as bibliotecas do *Bootstrap*, as quais dispõem de grande quantidade de componentes para páginas web, já pré-formatados, principalmente no que tange a responsividade de dispositivos. Na criação da codificação, será utilizada a ferramenta *Visual Studio Code*, que consiste em um editor de texto avançado, onde existe a possibilidade de inserção de diversos componentes adicionais, que auxiliam no desenvolvimento, denominados como *plugins*.

Outro ponto de destaque deste editor, diz respeito a sua interação nativa com ferramentas de gerenciamento de versões como o *GitHub*, da qual faremos uso em nosso projeto, pois propiciam que tenhamos controle sobre todo o desenvolvimento, inclusive com o histórico e versões anteriores do projeto para restauração.

#### 4.6 MODELAGEM DO BANCO

O Sistema de Gerenciamento de Banco de Dados escolhido foi o MySQL, devido a sua gratuidade, facilidade de manuseio e principalmente a interação do

mesmo com o Framework Laravel, a qual é extremamente completa e de fácil implementação.

Embora tenha sido feita uma modelagem inicial banco por meio do *Visual Paradigm*, com o desenvolvimento integrado das páginas web com o banco de dados, passou-se a utilizar a modelagem originada diretamente do MySQL, que após diversas mudanças e adequação que surgiram no transcorrer do desenvolvimento, culminaram na representação abaixo, onde temos um diagrama trazendo as tabelas para utilização do web site, com suas devidas relações.

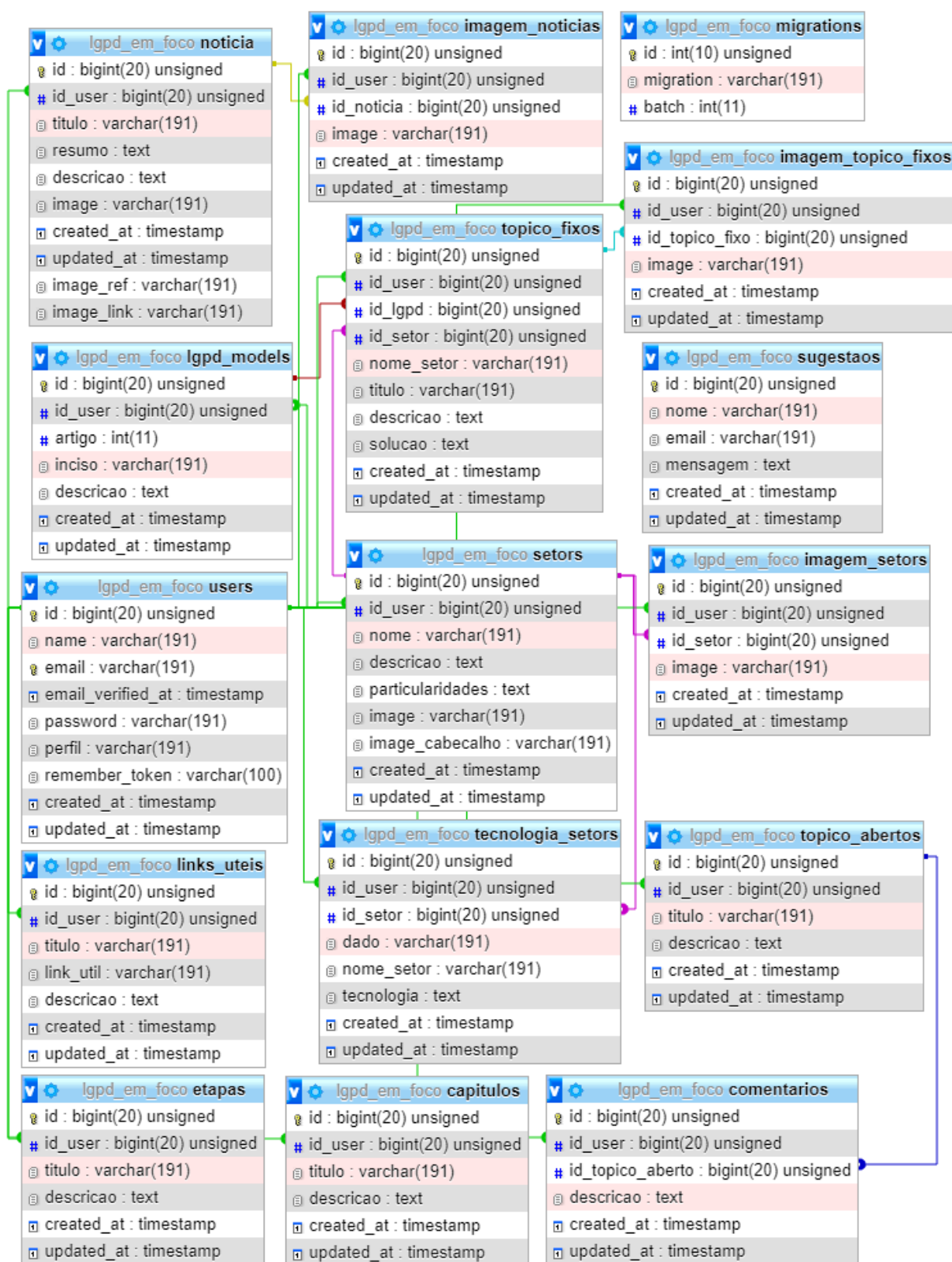
Além disso, destaca-se também o fato de que a grande maioria das tabelas do sistema apresentam relação com a tabela **“users”**, com exceção da tabela **“sugestaos”**, a qual corresponde a tabela onde ficarão registrados os dados de sugestões e comentários dos usuário do sistema e a tabela **“migrations”**, a qual é especificamente criada pelo Laravel, e tem a função de manter um registro ativo de todas as tabelas já criadas por meio do Laravel, de forma que quando executado o comando para criação de tabelas no framework, não sejam sobrescritas tabelas já criadas anteriormente.

Para uma melhor compreensão do diagrama, será adicionada uma legenda dos relacionamentos entre as tabelas, conforme as cores retratadas na imagem. No que tange ao relacionamento das demais tabelas com a tabela **“users”**, o objetivo é manter um histórico dos cadastros do sistema, e identificar claramente responsável pelas inserções de informações para fins tanto de auditorias, como de comprovação em questões judiciais que envolvam os dados presentes no site. Em relação a legenda de relacionamento das tabelas, a distribuição segue conforme listagem abaixo:

- Relacionamentos Tabela **users** (Verde);
- Relacionamento Tabela **lgpd\_models** (Vermelho);
- Relacionamento Tabela **noticia** (Amarelo);
- Relacionamento Tabela **setores** (Roxo);
- Relacionamento Tabela **topico\_abertos** (Azul);

- Relacionamento Tabela **topico\_fixos** (Azul Claro).

Figura 8 — Imagem do Diagrama do Banco de Dados



Fonte: O autor (2021)

## 4.7 PÁGINAS DESENVOLVIDAS

Após todo o planejamento realizado nos demais itens deste Capítulo, seguimos com o desenvolvimento do site, conforme as melhores práticas de interface de usuário e regulamentações impostas pela LGPD, culminando com as páginas representadas pelas figuras abaixo, seguidas de uma breve descrição.

Figura 9 — Página Home



Fonte: O autor (2021)



A primeira página construída foi a página home, a qual foi dividida em seções, de forma a concentrar o conteúdo disponível a todos os usuários, como os Setores de Serviço, Notícias e Tópicos Fixos, além de possibilitar que o usuário de sua contribuição, com sugestões e avaliações, objetivando a melhoria continua de site.

Especificamente nas sugestões, são registrados alguns dados como e-mail e nome da pessoa que disponibilizou sua mensagem, sendo informado o destino de seus dados em mensagem anterior aos campos, e ao lado, as últimas sugestões com apenas parte do e-mail visualizável para garantir a identificação do titular.

Figura 10 — Página de Registro

**LGPD EM FOCO**

LGPD ▾ Setores de Serviço ▾ Notícias ▾ Fórum ▾ Links Úteis ▾ Sobre ▾ Eduardo Mariano Dolovitsch ▾

## FAÇA SEU REGISTRO

**Edição da Usuário**

**OBS:** A senha não será preenchida para evitar que seja usado algum recurso para obter a mesma.

Preencha as informações abaixo para efetuar seu registro no Site.

Seu registro irá possibilitar seu acesso a recursos mais avançados como o Fórum de Discussão e irá propiciar uma utilização mais personalizada do site.

**Nome**

**E-Mail**

**Senha**

**Repita a Senha**

**Editar** **Cancelar**



**Eduardo Mariano Dolovitsch**

Desenvolvedor do Web Site LGPD em Foco, formado em Ciência da Computação pela UNIJUÍ. Desenvolveu o presente web site visando alguns objetivos, como expostos abaixo:

- Divulgar a LGPD
- Auxiliar os Profissionais de Compliance
- Integrar a Comunidade em torno da LGPD

**Desejas baixar nossa política de Segurança?**

**Clique aqui**

Fonte: O autor (2021)

A próxima página desenvolvida visa o registro do usuário no site, com a inserção do mínimo de informações necessárias e uso de criptografia na inserção dos dados no banco de dados, além de apresentar uma sessão com informações do desenvolvedor e responsável pelo site, e a possibilidade de acesso a política de privacidade e segurança do site. Essas definições foram implementadas, para estarem de acordo com as solicitações da LGPD.

Figura 11 — Página de Capítulos Comentados da LGPD



Fonte: O autor (2021)

Página desenvolvida com o intuito de transmitir informações dos capítulos da LGPD de forma comentada e mais acessível a qualquer usuário.

Figura 12 — Página de Etapas de Implantação da LGPD



Fonte: O autor (2021)

Semelhantemente a página da Figura 11, retrata de forma comentada as etapas para implantação da LGPD de forma geral. Destaco que ambas as páginas da Figura 11 e 12, representam conteúdo resultante deste estudo, presente nos capítulos Fundamentos e Conceitos da LGPD e Adequação e Implantação da LGPD.

Figura 13 — Página de Setores de Serviço


LGPD • Setores de Serviço • Notícias • Fórum • Links Úteis • Sobre •
Convidado •

## SETOR SERVIÇO



### Saúde



#### Descrição

Setor relacionado as definições da área de saúde, que pode amparar tanto hospitais e clínicas, quanto setores de empresas responsáveis pela manutenção da sanidade das pessoas ou colaboradores da empresa.

#### Documentações Relacionadas


#### Particularidades

Isto ressalta a atenção que deve ser dada na adequação a LGPD dos processos que envolvam esses dados, pois embora boa parte deles dispense de consentimento do titular, por se enquadrarem em base legal, tutela de saúde, proteção a vida ou cumprimento de obrigação legal, isto apenas afeta a etapa de coleta dos dados, sendo que as demais operações com os mesmos deverão observar os princípios de segurança da informação e da LGPD.

#### Dados e Tecnologias

Dado	Tecnologia
<b>Tipo</b> <b>Sanguíneo</b>	Podem ser usadas tecnologias de criptografia para impedir a identificação, por se tratar de dados sensível.
<b>Receita</b> <b>Física</b>	Indica-se que o presente dados seja digitalizado e após isso, eliminada, sendo que a parte digitalizada deve ser guardada criptografada, com acesso restrito.

#### Tópicos Fixados

**LGPD nos Prontuários Eletrônicos**  
 Postado em 17/06/21 10:06:32  
[Continuar Lendo](#)

**LGPD e a Privacidade dos Paciente**  
 Postado em 18/06/21 12:06:02  
[Continuar Lendo](#)

**A LGPD na vida dos Pacientes dos Hospitais**  
 Postado em 17/06/21 12:06:03  
[Continuar Lendo](#)

**O momento atual e a privacidade no âmbito de hospitais e clínicas no Brasil**  
 Postado em 18/06/21 12:06:06  
[Continuar Lendo](#)

Fonte: O autor (2021)



Nesta página o foco foi adicionar informações para implantação e adequação a LGPD, dentro de cada setor de serviço, ressaltando particularidades, documentações, dados e tópicos de conhecimento específicos do setor.

Figura 14 — Página de Listagem de Notícias



Fonte: O autor (2021)

Tratando das mais diversas notícias relacionadas a LGPD, esta página lista as últimas 3 (três) notícias cadastradas no site, com a possibilidade de utilizar o recurso de paginação para acessar as demais notícias do site. Além disso, abaixo das imagens fica disponível a referência da notícia original ou da imagem utilizada, bem com o link da mesma.

Figura 15 — Página de Exibição das Notícias



LGPD ▾ Setores de Serviço ▾ Notícias ▾ Fórum ▾ Links Úteis ▾ Sobre ▾

Eduardo Mariano Dolovitsch ▾



**Qualicorp é acusada de ferir LGPD e abre discussão sobre o dono do cliente**

As marcas pesquisadas foram CGA, Leader, Renner, Riachuelo, além das farmácias Pacheco, DrogaRaia e Venâncio. A sensação é de que, no ambiente digital, as empresas já começaram a dar os primeiros passos no sentido de adequação. No entanto, quando há canal específico para essa finalidade, o processo é burocrático, com a possibilidade de requisitar uma informação por vez, e as respostas são vagas. No mundo físico, a situação é bem pior: colaboradores desconhecem a lei, negam armazenamento de dados ou, ainda, dão respostas completamente erradas. Você pode conferir a experiência em cada marca na arte abaixo.

Quem nunca foi fazer uma compra e foi perguntado do CPF à data de nascimento? Essa prática vai desde a compra de um simples remédio de dor de cabeça até a de itens mais caros, como roupas, eletrônicos e bens duráveis. Porém, o hábito de lojistas brasileiros colecionarem informações sensíveis de clientes sem maiores cuidados ou objetivo claro está com os dias contados. A Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde o segundo semestre do ano passado, empodera o cidadão para dar consentimento ou não para uso de suas informações pessoais. Sendo assim, ele pode perguntar às empresas quais dados ela armazena, por quanto tempo, para qual finalidade e com quem os compartilha. Como as punições para o desrespeito às normas só começam a valer em agosto, muita empresa que ainda não se adequou. Para conferir como está sendo o cumprimento da lei na prática, o EXTRA fez um teste: no papel de consumidor, requisitamos pela internet e em lojas físicas esclarecimentos sobre o tratamento de dados.

— As empresas estão demorando a entender que já passou da hora de começar a implementação dessa lei. Estão esperando o início das multas, que podem chegar a R\$ 50 milhões, para ver como vai ser a fiscalização. Mas a adequação não se faz da noite para o dia, é algo que leva meses — comenta a especialista em Direito Digital da Russell Bedford, Vitória Bernardi.

De acordo com o sócio do escritório Prado Vidigal na área de Proteção de Dados e Direito Digital, Luis Fernando Prado, além das sanções administrativas, as empresas que violarem as regras estão sujeitas a responder a ações judiciais, com pedido de indenização pelo vazamento de dados, e à publicização da ocorrência, com danos à reputação e, consequentemente, prejuízos ainda maiores.

[Compartilhar](#)

**Quer saber mais sobre outras Notícias?**

**Clique aqui**

Fonte: O autor (2021)



Após acessada a listagem das notícias, é possível visualizar todas as informações das mesmas, como a descrição da notícia, imagens que a ilustrem melhor, bem como compartilhar a mesma no *Facebook*.

Figura 16 — Página do Fórum

**LGPD em Foco**

LGPD ▾ Setores de Serviço ▾ Notícias ▾ Fórum ▾ Links Úteis ▾ Sobre ▾ Eduardo Mariano Dolovitsch ▾

## FÓRUM

**Setores**



**Tópicos Abertos**

**Lgpd aplicado ao Ramo Financeiro**  
Tenho uma consultoria financeira, e com a pandemia meu atendimento ficou em boa parte de forma on-line. Quais cuidados devo tomar para garantir a segurança de meus clientes.  
Postado em 18/06/21 01:06:32  
Comentar Comentários 4

**Retorno sobre o site LGPD em Foco**  
Gostaria por favor que todas as pessoas que estejam fazendo uso deste web site, dessem seu retorno para que possamos melhorar cada vez mais.  
Postado em 18/06/21 12:06:12  
Comentar Comentários 2

[Acessar demais tópicos abertos](#)

**Tópicos Fixados**

**LGPD e a Privacidade dos Paciente**  
Postado em 18/06/21 12:06:02  
[Continuar Lendo](#)

**O momento atual e a privacidade no âmbito de hospitais e clínicas no Brasil**  
Postado em 18/06/21 12:06:06  
[Continuar Lendo](#)

**LGPD nos Prontuários Eletrônicos**  
Postado em 17/06/21 10:06:32  
[Continuar Lendo](#)

[Acessar demais tópicos fixos](#)

**Seus Tópicos**

**Título**

**Descrição**

[Abrir](#)

**LGPD na Saúde e sua Implicações**  
Postado em 18/06/21 12:06:56  
[Comentar](#)

**LGPD nas Escolas**  
Postado em 18/06/21 12:06:58  
[Comentar](#)

Fonte: O autor (2021)

Com o intuito de possibilitar uma maior interação e incentivar o desenvolvimento de uma comunidade de conhecimento em torno da LGPD, foi criada uma página de Fórum, onde os usuário podem visualizar os últimos tópicos abertos, fixados, filtrar os mesmos pelo setores, e ainda criar seu próprio tópico, gerando uma imensa gama de conhecimento sobre o assunto da LGPD.

Vale destacar que as opções de fórum serão acessíveis apenas aos usuários registrados no sistema, pois para questão de registro e segurança do site, todos os tópicos e comentário adicionados ficam relacionados internamente ao usuário logado no site, de forma que caso os mesmos tenham algum cunho irregular, o respectivo usuário possa ser responsabilizado.

Figura 17 — Página de Comentários



The screenshot displays the 'COMENTÁRIOS' (Comments) section of the 'LGPD EM FOCO' website. At the top, there is a navigation bar with links: LGPD, Setores de Serviço, Notícias, Fórum, Links Úteis, and Sobre. The user 'Eduardo Mariano Dolovitsch' is logged in. The main heading 'COMENTÁRIOS' is in large green letters. Below it, a dark grey box contains a comment: 'Tenho uma consultoria financeira, e com a pandemia meu atendimento ficou em boa parte de forma on-line. Quais cuidados devo tomar para garantir a segurança de meus clientes.' This is followed by a red bar with the word 'Comentários'. The page then shows three comments in a light green box, each with its text and posting time (18/06/21 02:06:45, 18/06/21 02:06:14, and 18/06/21 02:06:39). A pagination bar shows '1' and '2'. At the bottom, there is a 'Comentário' form with a text area and a green 'Comentar' button.

Fonte: O autor (2021)



Ao acessar um tópico aberto, será disponibilizada uma página contendo os comentários adicionados ao mesmo, ocultando o usuário que fez o comentário, para garantir a privacidade do mesmo, e possibilidade de que o usuário que acessou a mesma contribua também com seus comentários e opiniões.

Figura 18 — Página de Tópico Fixo



LGPD ▾ Setores de Serviço ▾ Notícias ▾ Fórum ▾ Links Úteis ▾ Sobre ▾

Eduardo Mariano Dolovitsch ▾

# TÓPICO FIXO

LGPD nos Prontuários Eletrônicos



## Descrição

Gostaria de verificar o que posso exigir em relação aos prontuário eletrônicos no hospital, para garantir que fiquem em segurança e de acordo com as novas solicitação indicadas pela LGPD.

## Solução

A melhor opção corresponde com a utilização de prontuários eletrônicos, onde as políticas de segurança sejam devidamente disponibilizadas aos cliente da forma mais clara e acessível possível. Assim podemos verificar se esta tudo ocorrendo da melhor maneira possível e o resto estou escrevendo apenas para garantir que tenha bastante texto para poder prosseguir com os dados que eu preciso.

## Legislação

**Art. 1 - V**  
órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

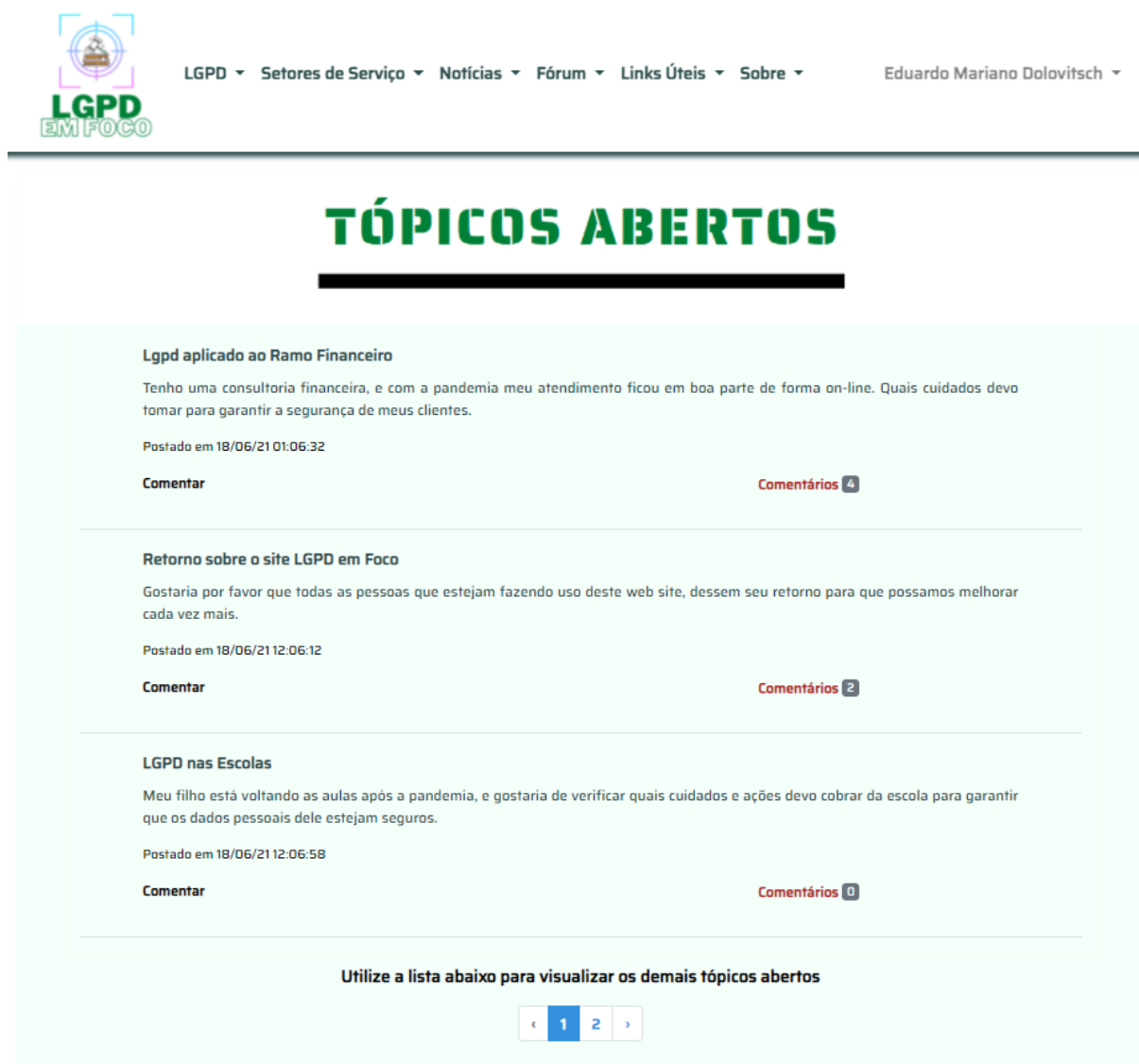
Imagens





Além do acesso aos tópicos abertos, você pode acessar os tópicos fixos, os quais serão inseridos por usuário com perfil de administrador, que tenham conhecimento ilibado sobre o assunto. Estes usuários irão analisar os tópicos abertos e comentários, para gerar um tópico fixo, contendo a solução ao tópico aberto, amparada por imagens e pelas legislações da LGPD relacionadas ao assunto do tópico.

Figura 19 — Página de Listagem de Tópicos Abertos



Fonte: O autor (2021)

Destacando nos tópicos abertos a informação do número de comentários existentes, relacionados ao respectivo tópico, possibilitando ao usuário verificar se o tópico já foi ou está sendo abordado por uma grande gama de usuários.

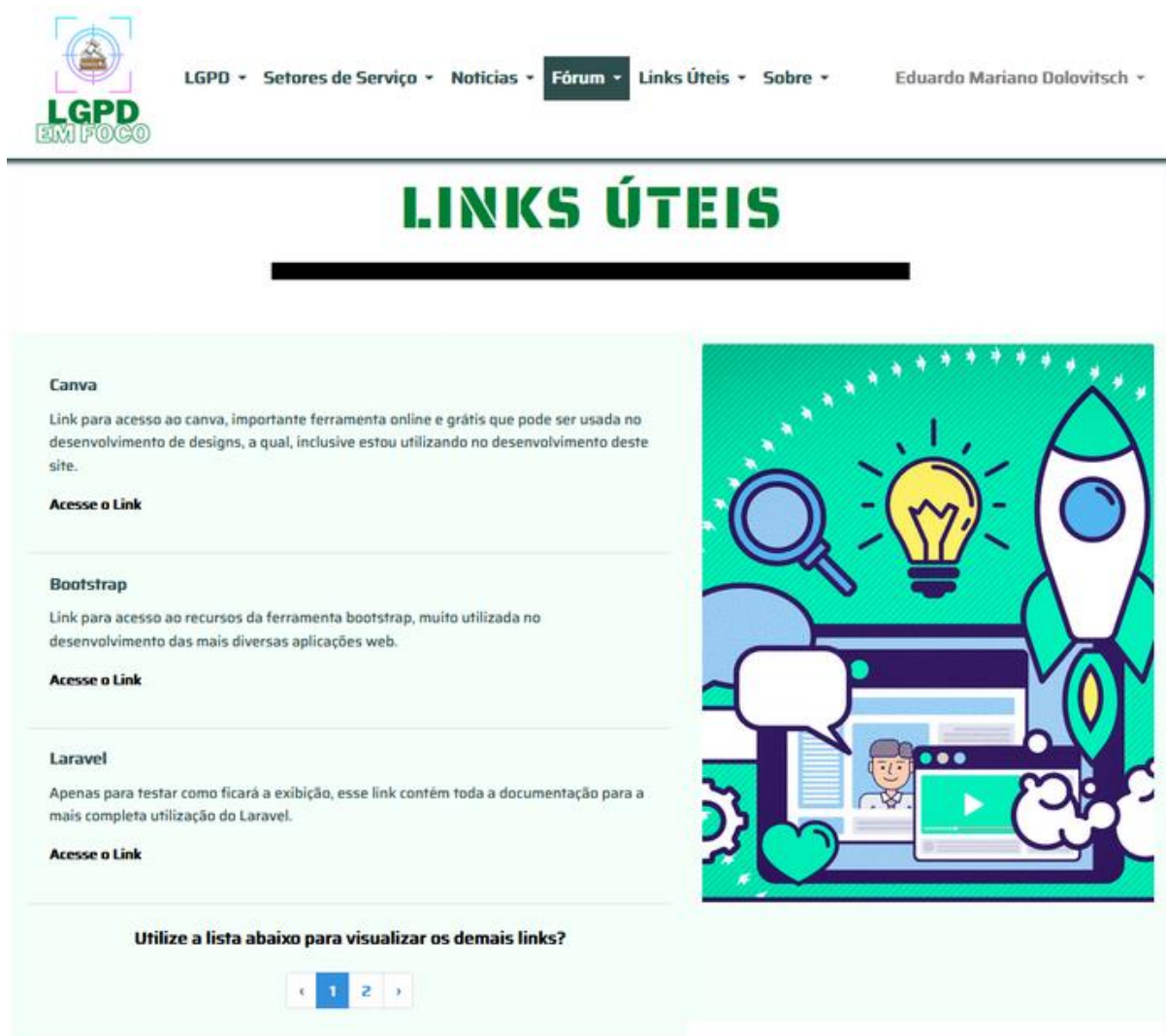
Figura 20 — Página de Listagem de Tópicos Fixos



Fonte: O autor (2021)

Complementando a página do Fórum, foram criadas duas páginas, que serão representadas pelas Figura 19 e 20, para disponibilizar a listagem completa de tópicos abertos e fixos aos usuários.

Figura 21 — Página de Listagem de Links Úteis



Fonte: O autor (2021)

Outra página criada foi a de Links Úteis, com a intenção de disponibilizar aos usuários links dos mais diversos assuntos como leis, regulamentações, guias, tecnologias, dentre outros recursos que tratem da LGPD e possam auxiliar os usuários.

Figura 22 — Página Sobre




Fonte: O autor (2021)

Finalizando as opções do menu, temos a página sobre a qual corresponde apenas a uma descrição da página desenvolvida, com sua razão e finalidade de desenvolvimento.



Figura 23 — Página de Cadastro Interna



Usuários ▾ LGPD ▾ Setores de Serviço ▾ Notícias ▾ Tópicos ▾ Links Úteis ▾ Sobre ▾ Sugestões ▾ Eduardo Mariano Dolovitsch ▾

Segue abaixo as listagens contendo os últimos 3 (três) registros feitos em cada sessão de cadastro.

Lista de Usuários			Lista de Setores de Serviço	
Nome	E-mail	Data	Nome	Data
teste	teste@hotmail.com	16/06/2021	Educação	19/06/2021
teste2	teste@gmail.com	13/06/2021	Saúde	17/06/2021
Eduardo Mariano Dolovitsch	eduwalkerbr@gmail.com	13/06/2021		

Lista de Notícias		Lista de Sugestões	
Título	Data	E-Mail	Data
LGPD garante proteção de dados íntimos de pessoas físicas	26/06/2021	carlos@hotmail.com	19/06/2021
Qualicorp é acusada de ferir LGPD e abre discussão sobre o dono do cliente	26/06/2021	eduwalkerbr@gmail.com	19/06/2021
Curso gratuito online com certificação discute LGPD; veja como se inscrever	26/06/2021		

Fonte: O autor (2021)

Por fim, a página de acesso restrito a usuários com perfil de Administrador, onde são realizados o cadastro da maior parte das informações disponibilizadas aos usuários do site. Destaco que o usuário que faça um registro na página representada pela Figura 10, tem definido seu perfil como Usuário, de forma que apenas administradores podem alterar o mesmo, e possibilitar aos usuários acessar a página de Cadastro Interna. Além disso, na página inicial ficam disponíveis para visualização os último 3 (três) registro feitos em cada sessão de cadastro, para acompanhamento do usuário administrador.

## 5 CONCLUSÃO

A evolução da sociedade como um todo, traz com ela sempre muitas mudanças, principalmente no que tange as relações sociais e econômicas. Caracterizando este fato, verificamos nos últimos anos a ascendência da informação, como artigo de extremo valor, seja qual for o panorama da sociedade abordado, destacando-se no âmbito econômico e tecnológico.

Objetivando deixar mais claro este fato, temos a balança comercial de recursos obtidos pelas empresas, onde os dados obtidos de seus clientes, quando da aquisição de seus serviços, geram mais valor à empresa do que a de seu produto por si só. Destacando que esses valores vão desde a abordagem, que corresponde ao valor econômico, como aos recursos de marketing, que propiciam a empresa estender sua imagem e influência frente a toda sociedade.

Este fato por sua vez, nos leva a um dilema, onde de um lado temos a implementação por parte da empresa, de ações que visem o incentivo ao compartilhamento de dados de seus clientes, e do outro, o fato de que os dados dizem respeito a informações pessoais, que podem afetar a integridade psicológica e física de seus titulares, caso sejam utilizadas de forma irresponsável ou descuidada.

Com a finalidade de garantir uma relação equilibrada entre as instituições e seus clientes, surge a Lei Geral de Proteção de Dados Pessoais (LGPD), no ano de 2018, visando gerenciar qualquer atividade que envolva a obtenção, tratamento e compartilhamento de dados pessoais.

Mas como nem tudo são flores, a lei trouxe grande contribuição, sendo um marco legal brasileiro, porém, essas contribuições estão pautadas em uma legislação que se apresenta, até certo ponto, complexa, não apenas por seus conceitos jurídicos, mas também por abordar diversas situações interpretativas, principalmente no que tange as possibilidades para obtenção dos dados.

Neste cenário, aliar os recursos de um mundo “on-line”, ou seja, onde todas as pessoas encontram-se quase que permanentemente conectadas a internet, a uma linguagem mais simples, clara e interativa, foram os fatos que pautaram esse estudo, voltado ao desenvolvimento de um site, contendo conhecimento sobre a LGPD, desde sua retratação, passando por sua análise, recursos, tecnologias e recomendações para sua compreensão e melhor utilização possível.

O Site tem como objetivo auxiliar cada vez mais na divulgação da LGPD, tornando a mesma conhecida entre todas as pessoas, e além de conhecida, também compreendida por meio da linguagem escrita e gráfica adotada no site. Além de conhecimento bruto sobre a LGPD, o site também é voltado a interação, com seções voltadas a geração de tópicos que retratem situações reais, onde as soluções são baseadas na contribuição da comunidade, e que após devidamente avaliadas e pautadas em dados sólidos, como artigos da lei, permanecem como fonte de conhecimento no site.

O estudo realizado e retratado se baseou nas questões e finalidades acima citadas, focado inicialmente em um estudo, artigo por artigo, da LGPD, fazendo uso não apenas da descrição da lei, mas de diversas análises de autores diferente. Isto resultou em uma descrição da LGPD, fracionada nos capítulos da mesma e comentada com o uso de uma linguagem mais simples e compreensível a qualquer pessoa.

De posse deste conhecimento, o próximo passo foi dispor ao leitor de um guia simplificado, e genérico, contendo as etapas a serem executadas para proceder a implantação e adequação da lei em qualquer instituição. Aqui além de ressaltar orientações dispostas pela lei e sugestões de diversos autores, estão presentes também análises do próprio autor, bem como tecnologias e conhecimentos adquiridos no transcorrer dos estudos e da experiência técnica que o mesmo dispõe.

Culminando com todas informações entorno da LGPD, foram utilizados recursos atuais de desenvolvimento web, seguindo as etapas retratadas no Capítulo Desenvolvimento do Web Site, que resultaram no site LGPD em Foco, contendo



grande gama de informações da LGPD, tanto de forma genérica, como de forma particionada por setores de serviço.

Descrevendo superficialmente o site, o mesmo apresenta seções para transmitir conteúdo a respeito da LGPD, destacando-se a lei comentada, as etapas de implantação genérica, e uma seção específica para tratar das particularidades e dados específicos de setores de serviço.

Além do aspecto informativo, foi abordado também a interação com os usuários, com o desenvolvimento de uma área de fórum, onde a principal finalidade é a formação de uma comunidade. Esta comunidade será pautada na diversidade, com a interação entre instituições, responsáveis técnicos, usuários e pessoas em geral, e também na colaboração para a constituição de uma grande gama de conhecimento, disponível publicamente e sem custos.

Destaco que ao iniciar o estudo, o principal objetivo era aprofundar-se sobre o assunto da LGPD, e partindo disso, criar um caminho sólido, atrativo e que permitisse a outras pessoas se aventurarem de forma segura e integra nesse mundo da LGPD, cujo ecossistema contempla tanto o mundo do direito, como de tecnologia da informação.

Isto fica bem evidenciado, pela abordagem e questionamento adotado, que consiste em como contribuir na divulgação da Lei Geral de Proteção de Dados (LGPD), tanto no que tange a divulgação dos direitos dos usuários, como nos aspectos a serem observados para adequação de empresas e instituições nos ramos de atividade comercial e de prestação de serviço a esta nova realidade?

E ao finalizar o estudo, considero que os objetivos foram amplamente alcançados, com a extensa gama de conhecimentos disponibilizada no site, amparada na facilidade de acesso e compreensão. Pode-se dizer que o caminho foi devidamente pavimentado, e que alguns recursos adicionais que surgiram com o andar do projeto, como o fórum, permitirão que demais pessoas possam melhorar

esse caminho e criar novas estradas secundárias, dando acesso a novos conhecimentos da LGPD ou que estejam relacionados a mesma.

Além disso, seguindo com esta analogia entre o estudo e as estradas de conhecimento, as estradas possuem a característica de serem continuas, ou seja, possibilitarem sua continuidade levando a novos caminhos e destinos. Neste ponto, deve-se deixar aqui, algumas sugestões para a continuidade do estudo, começando pela complementação do site, com a inserção de mais recursos em relação a LGPD, como questionários para avaliação e adequação da mesma, vídeos relacionados sobre o assunto, partindo de pessoas especializadas.

Outra funcionalidade interessante seria um calendário de eventos em relação a LGPD, um histórico de toda a evolução da Lei, e mais especificamente em relação ao fórum, o ideal seria realizar um acordo de cooperação com mais pessoas renomadas e especializadas no assunto, de forma que os tópicos levantados, possam ser devidamente avaliados, gerando uma imensa gama de conhecimento disponível a toda comunidade.

Complementado esses direcionamentos futuros de estudo, seria interessante abordar o público geral em detrimento ao público técnico, com a criação guias interativos, no modelo de workshops, de forma a esclarecer os direitos garantido pela LGPD, bem como estimular um maior interesse por parte das pessoas em geral, quanto as legislações existentes em nosso país. Afinal, como pessoas deve-se ter conhecimento de nossos direitos, e assim contribuir para que eles sejam respeitados, aprimorados e valorizados.

## REFERÊNCIAS

- BRASIL. Congresso Nacional. Lei n. 13.709, de 14 de agosto de 2018. **Diário Oficial da União**. Brasília, 14 de agosto de 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 16 dez. 2020.
- CORREIA, Thiago Martins. Cibercrimes: aspectos panorâmicos dos crimes informáticos mais praticados e as condutas de prevenção. **E-Civitas**, Belo Horizonte, v. 13, p. 119-135, jul 2020.
- DATA DILIGENCE CONSULTORIA E ACESSORIA EMPRESARIAL LTDA. **Guia de Boas Práticas: Implementando a LGPD**. 1. ed. Brasil: Publicação Independente, 2020. 59 p.
- DE ANDRADE, Ana Paula. **O que é laravel**. **Treinaweb**. São Paulo, 2020. Disponível em: <https://www.treinaweb.com.br/blog/o-que-e-laravel/>. Acesso em: 26 abr. 2021.
- DONDA, Daniel. **Guia prático de implementação da LGPD**. Editora Labrador, v. 3, f. 72, 2020. 144 p.
- FORRESTER. **A Ascensão do Executivo de Segurança alinhado ao Negócio. tenable**. 2020. Disponível em: <https://pt-br.tenable.com/analyst-research/forrester-cyber-risk-report-2020>. Acesso em: 30 out. 2021.
- GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, v. 3, f. 64, 2020. 128 p.
- LARAVEL. **The Php Framework for Web Artisans**. **Laravel**. 2021. Disponível em: <https://laravel.com/>. Acesso em: 27 abr. 2021.
- NETTO, ALVIM ANTONIO OLIVEIRA. **IHC - Modelagem e Gerência de Interfaces com Usuário**. VisualBooks Editora, f. 60. 120 p.
- PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD**. Saraiva Educação S.A., v. 3, 2020.
- POHLMANN, Sérgio Antônio. **LGPD Ninja: Entendendo e implementando a Lei Geral de Proteção de Dados na Empresa**. Editora Fross, v. 3, f. 154, 2019. 308 p.
- PRESSMAN, Roger; MAXIM, Bruce. **Engenharia de Software - 8ª Edição**. McGraw Hill Brasil, f. 484, 2015. 968 p.

SANTI, Leandro. **Lei nº 13.709/2018: análise à lei geral de proteção de dados pessoais (LGPD)**. Tubarão, 2020. 60 p. Monografia (Direito) - Universidade do Sul de Santa Catarina, Tubarão, 2020.