UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
ESCOLA DE INFORMÁTICA APLICADA

ANÁLISE DA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS UNIVERSIDADES FEDERAIS DO ESTADO DO RIO DE JANEIRO

Paula Dias de Figueiredo

Orientador
Morganna Carmem Diniz

RIO DE JANEIRO, RJ – BRASIL
AGOSTO DE 2022

PAULA DIAS DE FIGUEIREDO

Análise da Implementação da Lei Geral de Proteção de Dados nas Universidades Federais do Estado do Rio de Janeiro

Trabalho de Conclusão de Curso de graduação, apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro, como requisito para obtenção do título de Bacharel em Sistemas de Informação.

Orientadora: Profa. Dra. Morganna Carmem Diniz

Rio de Janeiro, RJ - Brasil

Agosto de 2022

Catalogação informatizada pelo autor

Dias de Figueiredo, Paula
D475 Análise da implementação da Lei Geral de Proteção de Dados nas universidades federais do Estado do Rio de Janeiro / Paula Dias de Figueiredo. -- Rio de Janeiro, 2022.
70p

Orientadora: Morganna Carmem Diniz.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Sistemas de Informação, 2022.

1. LGPD. 2. proteção de dados. 3. segurança da informação. I. Carmem Diniz, Morganna, orient. II. Título.

ANÁLISE DA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS UNIVERSIDADES FEDERAIS DO ESTADO DO RIO DE JANEIRO

PAULA DIAS DE FIGUEIREDO

Projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) para obtenção do título de Bacharel em Sistemas de Informação.

Aprovado por:

_____

Profa. Dra. Morganna Carmem Diniz (Orientadora)
Universidade Federal do Estado do Rio de Janeiro – UNIRIO

_____

Prof. Dr. Asterio Kiyoshi Tanaka

_____

Profa. Dra. Simone Bacellar Leal Ferreira

Rio de Janeiro, RJ – Brasil
Agosto de 2022

Agradecimentos

Em primeiro lugar, agradeço a Deus por ter me dado força e perseverança para conquistar esse objetivo.

Agradeço à minha avó, Helena, que está olhando por mim; minha avó sempre será a minha maior inspiração.

Agradeço à minha mãe, Regina, ao meu pai, Luiz, e à minha tia, Mirian, que sempre apoiaram e incentivaram a minha educação de todas as formas.

Agradeço à minha irmã Mirella, que sempre esteve ao meu lado em todos os momentos, me ouvindo e sendo o meu apoio.

Agradeço ao meu namorado, Thiago, que sempre me deu suporte, apoio e compreensão, e esteve ao meu lado para tudo.

Aos meus amigos do coração que a UNIRIO me deu: Renata, Rodrigo e Bruna.

A todos os meus familiares e amigos queridos que torceram por mim e vibraram pelas minhas conquistas.

Aos meus professores por toda a vida e, em especial, à minha orientadora Morganna, que é uma inspiração para mim.

RESUMO

Os dados são itens de extrema importância para o cenário tecnológico atual e, por conta disso, a proteção dos dados é cada vez mais requerida. Devido a invasão de privacidade, incidentes de segurança e violação de dados dos cidadãos, surgiu a necessidade de uma regulamentação no país que objetivasse proteger as informações pessoais. Em 14 de Agosto de 2018, foi promulgada a Lei nº 13.709, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD regulamenta o uso dos dados pessoais e concede aos titulares o direito sobre os seus próprios dados. Ademais, a lei incentiva o incremento da segurança da informação e fomenta boas práticas de governança de dados. Através disso, é incentivada a inovação tecnológica e revisão de processos nas instituições, propiciando ambientes éticos e mais seguros para operações com dados pessoais. Neste trabalho, a LGPD é interpretada de modo a associá-la com cenários práticos de seu escopo. São apresentadas etapas para o processo de implementação da LGPD em uma organização. Por fim, é apresentada a análise realizada nos sítios eletrônicos de quatro Instituições Federais de Ensino Superior do Rio de Janeiro, a fim de identificar a postura de cada uma em relação à LGPD.

Palavras-chave: LGPD, proteção de dados, segurança da informação

ABSTRACT

Data management is extremely important in the current technology scenario, therefore, data protection is more required every day. Because of privacy invasion, security incidents and personal data violation, it has been identified the necessity to develop a regulation with the objective of protecting personal data. On August 14th of 2018, it was enacted the law nº 13.709, named "*Lei Geral de Proteção de Dados Pessoais (LGPD)*" (Personal Data Protection General Law). The LGPD regulates the use of personal data and grants to the holder the right to his own data. In addition, this law encourages the improvement of information security and promotes data governance good practices. Consequently, technology innovation and process review are encouraged at the institutions, resulting in ethical and safer environments for personal data operations. In this work, the LGPD is interpreted as a way to associate it with practical scenarios of its scope. The stages for the implementation of the LGPD in an organization are presented. Thereafter, it is presented an analysis completed at the websites of four Federal Educational Institutions of the State of Rio de Janeiro, with the purpose of identifying its situation related to the LGPD.

Keywords: LGPD, data protection, information security

Lista de Figuras

Lista de Tabelas

SUMÁRIO

1. Introdução

1.1 Motivação

Devido ao avanço exponencial da presença tecnológica na época atual, os dados se tornaram objeto de grande importância para as organizações contemporâneas. Pode-se dizer que, no atual momento, os dados são um dos principais ativos das empresas, pois a partir do processamento destes dados é possível gerar informação, possibilitando tomadas de decisões, construção de conhecimento e consequentemente lucro, inovação e crescimento.

Para os fins da Lei Geral de Proteção de Dados (LGPD), que é o objeto do presente estudo, dados pessoais são considerados como qualquer "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Pode-se interpretar dado pessoal como qualquer informação associada ao titular dos dados, seja ela capaz de identificar um indivíduo (como nome, CPF, telefone, e-mail, dentre outros) ou apenas descrever algum atributo (como idade, profissão, estado civil etc.). Muitas vezes, determinada ótica ou combinação de atributos permite identificar o titular dos dados, daí a denominação de pessoa natural identificável.

Os dados pessoais são de grande importância para as organizações públicas e privadas, pois a partir desse tipo de dados é possível mapear as pessoas, formular processos internos, elaborar estratégias, gerar campanhas de marketing, desenvolver pesquisas, dentre muitas outras atividades factíveis. Por conta disso muitas organizações passaram a coletar e utilizar dados pessoais de forma indiscriminada, acarretando riscos aos titulares devido a incidentes de segurança (SILVA; AROUCA, 2020).

Quando não há a devida importância à proteção dos dados pessoais por parte da organização, está é colocada em risco, abrindo possibilidades para que pessoas sejam prejudicadas por conta da ocorrência de acessos indevidos, utilização imprópria ou vazamento desses dados. Por exemplo, criminosos podem utilizar informações pessoais de um indivíduo para a criação de contas digitais ou solicitação de empréstimos utilizando-se do nome de terceiros. De acordo com a reportagem do jornal Valor, a empresa de cibersegurança PSafe identificou mais de 600 milhões de dados de cidadãos vazados no país no ano de 2021, 44,5 milhões de tentativas de golpes virtuais, e 41 milhões de bloqueios de arquivos maliciosos que buscam invadir redes de empresas. No relatório anual da PSafe, o ano de 2021 foi marcado por um recorde no número de crimes de cibersegurança (KUCK, 2022).

Observando por outro lado, em outra reportagem do jornal Valor, foi apresentado um estudo realizado pela empresa Cisco em 2021 que levantou informações de 2.800 profissionais de 13 países diferentes, a fim de avaliar os retornos positivos provenientes de investimentos em privacidade e proteção de dados pessoais. O estudo resultou em 70% das empresas relatando terem sido beneficiadas comercialmente por conta daqueles investimentos. Dentre as empresas que relataram benefícios decorrentes do investimento em proteção de dados pessoais, foram identificados 67% de diminuição de atraso em vendas; 71% de mitigação de perdas devido a violação de dados pessoais; 71% de melhoria em agilidade e inovação; 74% de aumento da confiança e fidelização de clientes; 73% a mais na atração de investimentos; e por fim, 72% de aumento na eficiência das operações de controles de dados pessoais. Esse mesmo estudo identificou que na média global, a cada US$1 que as empresas investem em privacidade e proteção de dados pessoais, o retorno desse investimento é de US$2,70, com variação dependendo do país. No Brasil, foi observado um retorno dos investimentos em proteção de dados bastante relevante, apresentando o coeficiente de 3,3 vezes o valor investido (MASTROPASQUA, 2022).

A proteção de dados pessoais é importante não somente por conta de exigências legais, mas também para a mitigação de riscos e para a segurança das organizações. Investir em segurança da informação e em políticas de privacidade possibilita o aumento da confiança por parte do usufruidor ou cliente, de entidades públicas ou privadas, além de resguardar os dados que atualmente representam objeto de grande valor para as instituições.

1.2 Objetivo

O objetivo deste trabalho é apresentar conceitos da Lei Geral de Proteção de Dados, correlacionando-os com atividades práticas para o processo de implementação da lei em uma organização. Para isso, foi realizado um estudo da legislação a fim de identificar e interpretar seus principais conceitos e definições. Através da revisão teórica são sugeridas as etapas para um projeto de adequação à lei, com base na revisão de processos, criação de políticas internas e monitoramento constante.

Foi realizado um estudo com base nos portais das quatro universidades federais do Estado do Rio de Janeiro. Neste estudo, foram analisadas as informações disponibilizadas por essas quatro instituições de ensino, para avaliar como elas estão agindo em relação a LGPD.

1.3 Organização do texto

A estrutura deste trabalho é apresentada em formato de capítulos, contendo as seguintes descrições:

- **Capítulo 2: Revisão Teórica** – É discutida a Legislação de Proteção de Dados e o seu contexto histórico.
- **Capítulo 3: O processo de implementação da LGPD** – São apresentadas as etapas para um processo eficiente de implementação da LGPD em uma organização, correlacionando essas etapas com as exigências e boas práticas existentes na lei.
- **Capítulo 4: Avaliação de Instituições de Ensino Superior** – É realizado um estudo nos materiais de LGPD disponibilizado por quatro Universidades Federais, e avaliadas as suas respectivas páginas eletrônicas destinadas a essa lei.
- **Capítulo 5: Conclusão** – São feitas as considerações finais deste trabalho e sugeridos temas de trabalhos futuros correlacionados ao presente estudo.

2. Revisão teórica

2.1 - A Lei Geral de Proteção de Dados (LGPD)

2.1.1 - Contexto histórico

No Brasil, a primeira norma jurídica relativa à proteção dos dados está na Constituição Federal Brasileira de 1988. No artigo 5º, inciso X é dito: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”, e no inciso XII do mesmo artigo é mencionado como “inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial (…)”. Pode-se afirmar que a Constituição Federal de 1988 reconhece a proteção à intimidade, vida privada e imagem dos cidadãos brasileiros (QUINTILIANO, 2021).

O Código de Defesa do Consumidor (CDC), aprovado em 1990, trouxe consigo algumas normas importantes para prover ao consumidor o direito de um maior controle sobre seus dados e informações pessoais, mesmo que de forma limitada às finalidades de suas normas. No artigo 43 do CDC é previsto o direito do consumidor acessar suas informações existentes em cadastros e fichas, e são também exigidas clareza, finalidade e acuracidade dos cadastros e registros de dados, assim como o descarte das informações armazenadas há mais de 5 anos. Ademais, é apresentada a exigência de que o consumidor seja comunicado imediatamente no caso de abertura de cadastro não solicitada por ele (NETO, 2020).

Em 2014, foi aprovado e sancionado o Marco Civil da Internet (MCI). Essa lei (Lei 12.965/2014) apresentou princípios e garantias para o uso da internet no Brasil. No MCI são estabelecidas regras a respeito da proteção dos dados pessoais e a privacidade dos indivíduos com uma abordagem principiológica, ou seja, sem estabelecer regras técnicas para que assim não fosse prejudicada a inovação tecnológica das redes de internet (NETO, 2020).

No ano de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), que passou a vigorar a partir de agosto de 2020. A LGPD tem como inspiração a resolução da União Europeia “General Data Protection Regulation" (GDPR), e visa garantir direitos fundamentais

de liberdade e de privacidade. A GDPR será brevemente abordada na seção 2.2 do presente trabalho.

No dia 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional 115, incluindo no artigo 5º da Constituição Federal, citado anteriormente, o inciso LXXIX que diz: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Por conta disso, se tornou ainda mais explícita a importância e a relevância da disciplina da proteção de dados, que agora é amparada também pela Constituição Federal (PINTO, 2022).

2.1.2 - Visão geral da LGPD

Em 14 de Agosto de 2018, foi promulgada a Lei Geral de Proteção de Dados, conhecida como LGPD, que possui como principal objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018). Para a realização deste objetivo, a lei tem como foco regular as atividades de tratamento de dados pessoais, tanto no meio digital quanto no meio físico. A LGPD possui um formato muito abrangente e, por conta disso, se aplica a organizações e empresas de todas as dimensões, e de quaisquer setores da economia.

O conceito de tratamento de dados pessoais pode ser definido como qualquer operação que utilize este tipo de dado ao ser executada. A lei define uma série de procedimentos que se enquadram como tratamento de dados, e na lista abaixo é possível visualizar a definição para cada um desses procedimentos, na ordem que são citados pela LGPD (SILVA; AROUCA, 2020):

- **Coleta** - Captar dados para finalidade específica ou não;
- **Produção** - Combinar e analisar dados para gerar informação;
- **Recepção** - Receber dados por uma transmissão;
- **Classificação** - Dispor dados de forma categorizada;
- **Utilização** - Ato ou efeito de usufruir dos dados;
- **Acesso** - Ato ou efeito de visualizar os dados;

- **Reprodução** - Ato ou efeito de copiar dados existentes;
- **Transmissão** - Mover dados entre dois pontos, por meio digital ou físico;
- **Distribuição** - Ato ou efeito de divulgar dados;
- **Processamento** - Executar série de atividades com os dados, com finalidade de gerar informação;
- **Arquivamento** - Catalogar dados;
- **Armazenamento** - Manter dados em um repositório;
- **Eliminação** - Remover dados de um repositório;
- **Avaliação ou controle da informação** - Moderar as ações sobre dados;
- **Modificação** - Alterar dados;
- **Comunicação** - Transmitir informações a respeito de determinados dados;
- **Transferência** - Mover os dados de um local a outro;
- **Difusão** - Disseminar os dados em questão;
- **Extração** - Obter ou duplicar dados do repositório de origem.

Devido a sua abrangência, a LGPD atua em qualquer operação de tratamento de dados realizada em território nacional, por pessoa natural ou jurídica, de direito público ou privado que possua como propósito "a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional" (BRASIL, 2018), e no caso desses dados pertencerem a um titular que se encontre no Brasil no momento da realização da coleta.

De acordo com o Art. 2º, a LGPD utiliza como base os fundamentos da disciplina da proteção de dados pessoais, que são:

> o respeito à privacidade; à autodeterminação informativa;
> a liberdade de expressão, de informação de comunicação e de opinião;
> a inviolabilidade da intimidade, da honra e da imagem;
> o desenvolvimento econômico e tecnológico e a inovação;

> a livre iniciativa, a livre concorrência e a defesa do consumidor;
> e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018)

Pode-se assim dizer que a LGPD possui como objetivo mitigar os riscos provenientes do tratamento inadequado, indevido ou abusivo dos dados, ao mesmo tempo que possibilita melhores condições para a inovação e o desenvolvimento tecnológico, em um ambiente seguro no âmbito jurídico (SILVA; AROUCA, 2020).

A LGPD concede ao titular dos dados pessoais o direito de adquirir informações precisas, claras e evidentes de como seus dados estão sendo utilizados nas operações de tratamento, que de acordo com a lei, engloba qualquer ação de: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais (BRASIL, 2018). Atribui também ao titular de dados o direito de consentir, ou não, com estas atividades de tratamento. O consentimento é definido pela lei como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018).

Ademais, a lei também apresenta outras reivindicações, tais como promover melhores práticas de segurança no uso e tratamento dos dados pessoais, reforçar a confiança dos cidadãos na coleta e uso de seus dados, e prover a eles um maior controle sobre informações que os identifiquem individualmente.

Com o aumento exponencial da tecnologia nos tempos modernos, muitas atividades foram criadas ou migradas para o meio digital. Por conta disso, é cada vez mais necessário o tratamento de dados pessoais por parte das empresas e organizações, para ser possível a entrega dos seus serviços e produtos, para a realização de estudos e campanhas de marketing, para o estreitamento do contato com os clientes, alavancar a inovação, dentre diversos outros objetivos. Neste contexto, o tratamento de dados realizado nestas atividades pode vir a apresentar grandes riscos para os seus titulares caso não haja regras, privacidade e segurança (SILVA; AROUCA, 2020).

Através da LGPD foi declarada a criação da Autoridade Nacional de Proteção de Dados (ANPD), que é um órgão da administração pública federal cuja principal função é fiscalizar, nos termos da legislação, a execução geral da proteção dos dados pessoais. Além disso, também compete à ANPD a criação de procedimentos e normas para a Política Nacional de Proteção

de Dados Pessoais e da Privacidade, a fiscalização e aplicação de sanções em situações de descumprimento à legislação ao tratar dados pessoais, dentre outras funções discriminadas no Artigo 55-J da LGPD. O *website* da ANPD pode ser encontrado no endereço <https://www.gov.br/anpd/pt-br>.

A LGPD definiu três importantes agentes de tratamento de dados: o controlador, o operador e o encarregado.

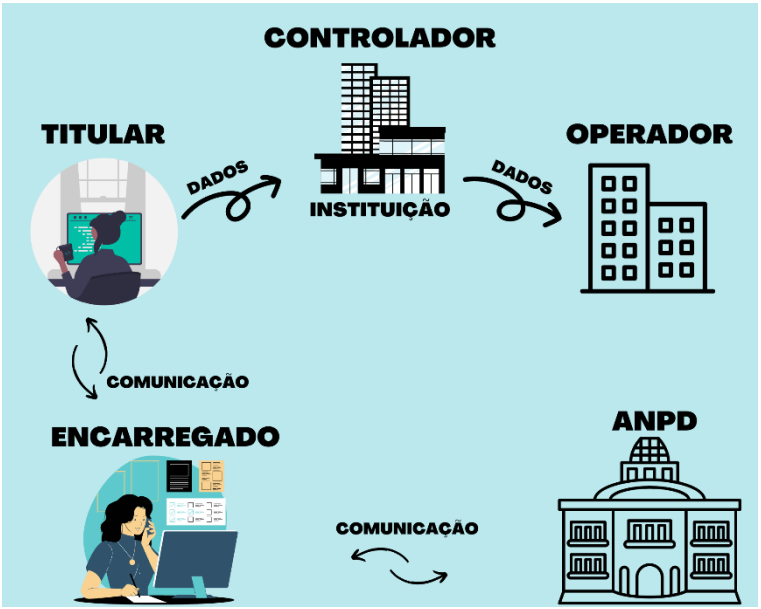
O controlador corresponde à "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018). Isto significa que o controlador é a entidade que realiza a coleta dos dados pessoais e toma decisões referentes aos processos de tratamento e ao ciclo de vida dos dados que se encontram sob sua gestão.

O operador é qualquer instituição que "realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018). Pode-se exemplificar como uma empresa prestadora de serviço que efetua operações de tratamento com os dados pessoais sob o domínio do controlador.

O encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados" (BRASIL, 2018). O encarregado tem como principal objetivo ser uma ponte de comunicação entre os titulares dos dados, a ANPD, e o controlador. Tem o papel de receber quaisquer reclamações e comunicações dos titulares, prover os esclarecimentos pertinentes e tomar as providências necessárias. Deve também trabalhar como um canal com a ANPD, caso haja o recebimento de comunicações da autoridade nacional. A lei determina que a identidade e informações de contato do encarregado devem ser publicamente divulgadas, preferencialmente no site eletrônico do controlador.

A Figura 1 ilustra os papéis dos agentes de tratamento de dados, segundo a LGPD.

Figura 1 - Gráfico dos agentes de tratamento de dados



Fonte: Autoria própria

As instituições que descumprirem as normas previstas pela lei poderão sofrer sanções administrativas por parte da ANPD, de acordo com o nível da infração cometida. Essas sanções podem ser desde uma advertência, até multas que podem chegar a 2% do faturamento da pessoa jurídica de direito privado, com limite de 50 milhões de reais. Além disso, a ANPD pode exigir o bloqueio ou eliminação dos dados pessoais a que se refere a infração, e no caso extremo, a proibição parcial ou total das atividades de tratamento de dados por parte da empresa.

Além das sanções oficiais, um impacto negativo também pode ocorrer à imagem de uma instituição, pública ou privada, caso haja um episódio de vazamento de dados ou caso dados pessoais sejam operados de forma incorreta. De tal forma, a instituição pode perder a confiança por parte de seus clientes e usuários, que em um ambiente competitivo, possui extrema importância. Com isso, as instituições passaram a ter maiores responsabilidades no âmbito do tratamento de dados pessoais, necessitando de um sistema de proteção e segurança, visando a prevenção de incidentes e a prestação de contas.

2.1.3 - Princípios do tratamento de Dados Pessoais

A LGPD determina regras, princípios e fundamentos para o tratamento de dados pessoais. É importante ressaltar que esta lei não se aplica a operações de tratamento executadas por pessoal natural, para fins estritamente particulares e não econômicos. E também não se aplica

nas situações em que o tratamento de dados é feito para fins exclusivamente jornalísticos e artísticos, acadêmicos, de segurança pública, do Estado e de defesa nacional, ou atividades de investigação e repressão de infrações penais (BRASIL, 2018).

Conforme é explicitado no artigo 6º da LGPD, quaisquer atividades de tratamento devem seguir a boa-fé e os princípios de:

- **Finalidade** – Propósitos legítimos e específicos, não sendo possível o tratamento posterior caso não se mantenha esta finalidade, e que, ademais, precisa ter sido informada previamente ao titular, de forma explícita;
- **Adequação** – O tratamento precisa ser compatível com a finalidade acima, e com o que foi informado ao titular;
- **Livre acesso** – Deve ser possível que o titular realize consulta de forma simples e gratuita sobre informações a respeito do tratamento e integridade dos seus dados;
- **Qualidade dos dados** – Deve ser garantido aos titulares a integridade de seus dados, e a possibilidade de atualizá-los de acordo com a necessidade para o cumprimento do tratamento em questão;
- **Transparência** – Informações de forma acessível aos titulares, sobre a realização do tratamento de seus dados e os agentes de tratamento envolvidos, mantendo os segredos comerciais e industriais;
- **Segurança** – Medidas técnicas e administrativas capacitadas a proteger os dados pessoais contra acessos indevidos e situações acidentais ou ilícitas, como por exemplo, invasão, roubo ou vazamento, alteração, ou difusão destes dados;
- **Prevenção** – Medidas de mitigação de riscos nas operações de tratamento de dados pessoais;
- **Não discriminação** – Proibição de procedimentos de tratamento que tenham fins discriminatórios, ilícitos ou abusivos.
- **Responsabilização e prestação de contas –** Os agentes de tratamento devem demonstrar e comprovar salvaguardas e medidas eficazes tomadas para o cumprimento das normas de proteção de dados pessoais.

A LGPD possui uma alta rigorosidade quando o assunto são dados pessoais sensíveis, e dados de crianças e adolescentes.

Dados pessoais sensíveis são todos os tipos de informações que podem expor um indivíduo a situações que o prejudique moralmente, ou o faça sofrer qualquer tipo de

discriminação. A LGPD define nessa categoria, os dados relativos a: “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018). O tratamento dessa categoria de dados só poderá ser realizado caso haja o consentimento do titular, de forma específica e destacada, para finalidades específicas, ou em casos de força maior como, por exemplo, caso seja indispensável para cumprimento de obrigação legal ou regulatória, ou para a proteção da vida do titular.

No caso de dados de crianças e adolescentes, a autorização específica para tal deverá ser fornecida por pelo menos um dos pais ou responsável legal. Caso ocorram danos devido ao tratamento irregular dessas duas categorias citadas, as sanções sofridas pela instituição em questão poderão ser mais severas.

Conforme é apresentado no Capítulo IV da LGPD, nas situações em que o tratamento de dados for exercido por pessoas jurídicas de direito público, ele deverá seguir regras e boas práticas específicas para este grupo. Só poderá ser efetuado para atender a sua finalidade pública, com o objetivo de executar competências legais e para cumprir atribuições legais do serviço público. A ANPD terá o poder de solicitar informações a respeito do tratamento de dados aos órgãos e entidades do poder público, e, além disso, emitir parecer técnico para garantir o cumprimento da lei. Ademais, poderá solicitar a publicação de relatórios de impacto à proteção de dados pessoais, e sugerir adoção de padrões e boas práticas a essas instituições. Caso ocorra qualquer infração, a ANPD poderá enviar informe com medidas cabíveis.

A LGPD determina regras específicas para a transferência internacional de dados. De acordo com o Capítulo V, essa atividade poderá ser realizada caso o país destino proporcione grau de proteção de dados pessoais adequado à lei brasileira, ou em casos em que o controlador possa garantir o cumprimento dos princípios, dos direitos do titular, e obedeça ao regime de proteção de dados previstos pela LGPD. Essa comprovação deverá ser feita por meio de cláusulas contratuais, cláusulas para a transferência dos dados, normas corporativas e certificados regularmente emitidos. Além disso, a transferência internacional de dados é permitida em situações de necessidade do cumprimento de obrigação legal ou regulatória, e para cooperação jurídica internacional entre órgãos públicos de inteligência. A entidade responsável por avaliar circunstâncias especiais, e o nível da proteção de dados do país ou da organização internacional, será a Autoridade Nacional de Proteção de Dados (ANPD).

O término do tratamento de dados pessoais deverá ocorrer caso sua finalidade seja atingida, caso esses dados não sejam mais necessários, ou alcance o fim do período de

tratamento, e também nos casos em que o titular solicitar o término do acordo através do seu direito de revogação do consentimento, que será apresentado na seção 2.2.6 deste trabalho. A ANPD também poderá intervir solicitando o término do tratamento em situações que ocorra violação à LGPD, como forma de sanção e zelo pela proteção de dados. Após ser determinado o fim do tratamento de dados, eles deverão ser eliminados de acordo com os limites técnicos das atividades, e poderá ser mantido no caso da necessidade de cumprimento legal pelo controlador, ou caso seja utilizado por órgão de pesquisa.

2.1.4 - Hipóteses para o tratamento de Dados Pessoais

A LGPD determina no artigo 7º em quais hipóteses é permitido realizar o tratamento dos dados pessoais por parte das empresas e instituições. Dentre os incisos deste artigo, estão listadas diversas hipóteses, o primeiro inciso diz respeito ao cenário em que o titular fornece o seu consentimento, concordando com o tratamento dos seus dados.

Logo após, é apresentada a hipótese do controlador necessitar realizar o tratamento dos dados para o cumprimento de obrigações legais ou regulatórias. Em terceiro, existe a hipótese de quando há a necessidade do tratamento para a execução de políticas públicas previstas em leis e regulamentos; ou quando o tratamento dos dados se torna necessário para execução de contrato do qual o titular faça parte, conforme é apresentado no inciso VI.

Dentre outras hipóteses que também são apresentadas no artigo 7º, podem ser citados o tratamento de dados para a proteção da vida, ou tutela da saúde, e a realização de estudos por órgão de pesquisa.

De acordo com o artigo 8º, o consentimento que é citado no inciso I das hipóteses apresentadas acima, deve ser fornecido por escrito, ou de outra forma que seja demonstrada a decisão do titular em consentir com o tratamento de seus dados, de forma inequívoca. Ademais, é obrigação do controlador poder provar que este consentimento foi adquirido de forma idônea, de acordo com o que é disposto na LGPD. E, inclusive, tornando possível a revogação do consentimento por parte do titular, através de procedimento gratuito e facilitado (BRASIL, 2018).

2.1.5 - Os direitos dos titulares dos Dados

Devido a legislações como a LGPD, se tornou possível ao titular obter um maior domínio sobre os seus dados, e maior controle sobre a forma como são utilizados, consequentemente ampliando a preservação da sua privacidade. A LGPD estabelece padrões de segurança e sigilo das informações, e estimula boas práticas de proteção de dados por parte das empresas e instituições, e como efeito disso surgem ambientes mais controlados e seguros, em que os tratamentos de dados pessoais são realizados de forma correta, respeitando os direitos do titular.

Os direitos do titular são citados no Capítulo III da LGPD, onde é assegurado a toda pessoa natural a titularidade dos seus dados pessoais, e garantido os direitos de liberdade, intimidade e privacidade nos termos da Lei. De forma sintetizada, o titular tem direito a obter do controlador informações referentes à existência de tratamento, ter acesso aos seus dados, corrigir informações incompletas ou incorretas, e solicitar a eliminação dos dados tratados, salvo impossibilidade por motivos regulatórios. Também é garantido ao titular o direito de solicitar informações ao controlador, sobre o uso compartilhado dos seus dados pessoais com outras entidades, sejam elas públicas ou privadas.

O artigo 19 define que, mediante solicitação do titular, a confirmação de existência ou o acesso aos seus dados, devem ser providenciados em formato simplificado, no prazo de até quinze dias a partir da data da solicitação. Em seguida, o artigo 20 garante ao titular o direito de solicitar revisão de qualquer decisão que lhe diga respeito, caso esta tenha sido tomada por um tratamento automatizado das suas informações individuais (BRASIL, 2018).

2.2 - Leis de proteção de dados internacionais

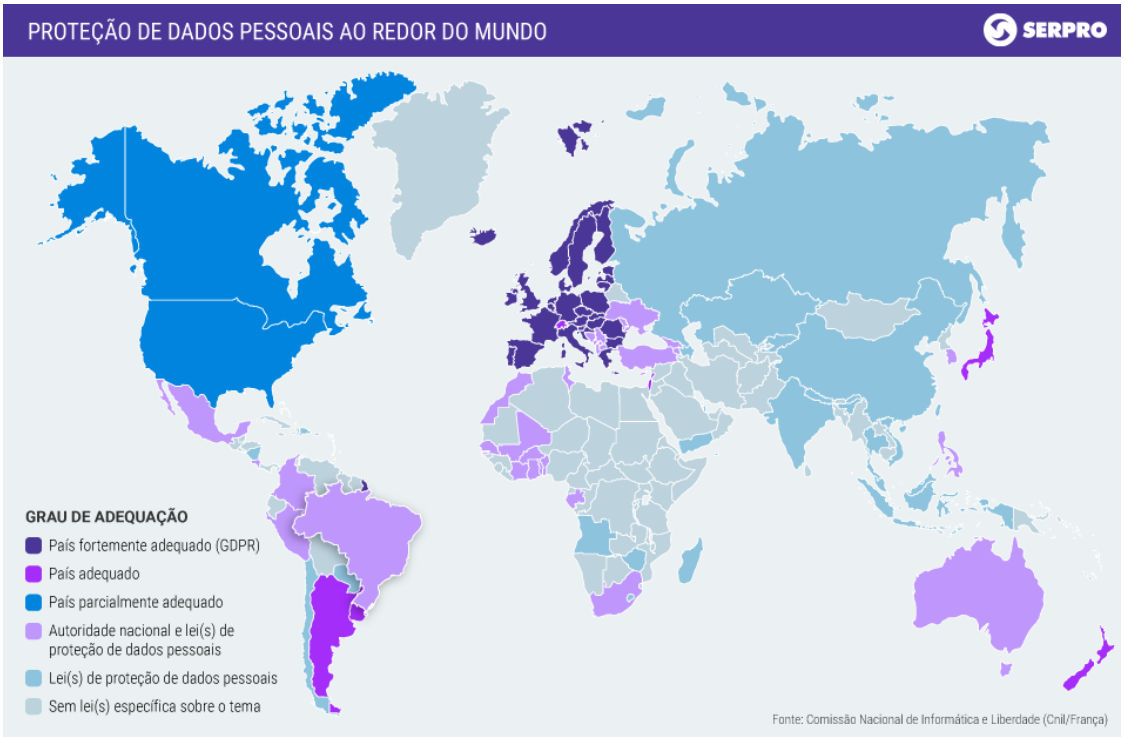
No dia 25 de maio de 2018 entrou em vigor na União Europeia o Regulamento Geral de Proteção de Dados (GDPR em inglês - *"General Data Protection Regulation"*), dois anos antes de entrar em vigor a lei de proteção de dados brasileira. A GDPR estabelece regras estritas para a transferência e tratamento de dados pessoais provenientes da União Europeia, sendo permitido somente no caso do país ou organização de destino possuir um nível adequado de proteção.

A LGPD foi fortemente inspirada na GDPR, e a lei europeia é vista como o modelo regulatório mais abrangente e completo no âmbito da proteção de dados. Por conta disso, algumas das leis de proteção de dados ao redor do mundo sofreram influência da regulação da União Europeia nas suas redações. Pode-se ressaltar que os principais objetivos das leis nacionais de proteção de dados são reconhecer os poderes dos cidadãos quanto ao controle dos seus dados pessoais, através da imposição de obrigações aos agentes de tratamento de dados, provendo mais transparência sobre o uso e fluxo dos dados, e garantindo os direitos de seus titulares (CIEB, 2020).

É notório um movimento global na criação de leis e regulamentos modernos que possuem como fim a proteção dos dados pessoais. Pode ser citada a Lei de Privacidade do Consumidor da Califórnia, do inglês *California Consumer Privacy Act* (CCPA), que entrou em vigor no dia 1º de janeiro de 2020. A CCPA concede aos residentes da Califórnia alguns direitos sobre seus dados pessoais, e também foi inspirada na GDPR.

A Figura 2 apresenta um mapa de adequação dos países à GDPR.

Figura 2 - Mapa da Proteção de dados pessoais ao redor do mundo



Fonte: Mapa da proteção de dados, Serpro.[1]

[1] Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais>. Acesso em: 20 mai. 2022.

3. O processo de implementação da LGPD

3.1 - Gestão de projeto e fase preliminar

De acordo com o Guia PMBOK®, o livro de maior referência na área de gerenciamento de projetos, projeto é definido como "um esforço temporário empreendido para criar um produto, serviço ou resultado único" (apud MONTES, 2017, p. 10). Entende-se por temporário, o fato de existir uma data de início, e uma previsão para o fim. Faz-se importante a estruturação de um projeto para a implementação da LGPD, por se tratar de um escopo que envolve uma instituição inteira. Ao fazer uso de práticas de gerenciamento de projetos é possível utilizar o conhecimento, a equipe, metodologias e ferramentas, dentre outros ativos, para se tornar possível alcançar os objetivos do projeto em questão, e cumprir os seus requisitos (MONTES, 2017).

Inicialmente, em uma instituição pública ou privada, é importante que seja realizada a formação inicial de um Grupo de Trabalho, que se trata de um grupo de profissionais da própria instituição, ou terceirizados, que terá a designação de elaborar os relatórios, e realizar o gerenciamento do projeto para a implementação da LGPD. Esse Grupo de Trabalho precisará concluir treinamentos de capacitação sobre a lei, a fim de se instruírem para todas as próximas etapas.

Dentre as fases iniciais do planejamento, é necessária a realização de um levantamento de informações sobre a referida organização. Através disso é possível obter uma noção inicial dos riscos presentes no âmbito da proteção de dados da instituição, tornando-se possível minimizar estes riscos antes mesmo de concluir a adequação por completo. Ademais, este levantamento também tem como objetivo estruturar quais serão as próximas ações, pois elas dependerão do modelo de cada organização (SILVA; AROUCA, 2020). É possível salientar algumas informações importantes para o primeiro momento de análise:

- A natureza jurídica da instituição, o segmento de atuação e sua dimensão;
- Tipo de governança, e organograma da estrutura administrativa;
- Atos normativos internos, e legislações próprias que afetam diretamente a instituição;
- Controles já existentes (segurança da informação, políticas internas, etc);
- Identificar os terceiros/parceiros da instituição;

- Políticas públicas ou projetos sociais em que a instituição está inserida;
- Verificação das análises de risco e programas de integridades já existentes.

Através da reunião dessas informações iniciais, se obtém um parâmetro para uma pré-avaliação de qual estado a instituição se encontra perante as exigências da Lei. Com isso, é possível formular um plano de ação e definir o escopo do trabalho para todas as áreas que realizam o tratamento de dados pessoais, mantendo como prioridade as áreas que apresentam um maior risco de exposição.

Devido ao fato da LGPD já estar em vigor, é exigido que a organização possua a figura do Encarregado de Proteção de Dados, que de acordo com a lei terá como função receber reclamações e comunicações dos titulares, provendo quaisquer esclarecimentos, e adotando providências caso necessário; ser a ponte de comunicação com a ANPD; e, orientar os funcionários a respeito de práticas de proteção de dados pessoais. Portanto, é necessário a instituição qualificar algum de seus colaboradores para determinada função ou realizar a contratação de um Encarregado de Proteção de Dados terceirizado. Este profissional é de extrema importância, e precisará ter conhecimentos a respeito da execução da proteção de dados pessoais, das regras e das regulamentações.

Durante a fase preliminar da implementação da LGPD é importante a realização de um *Gap Analysis* (em português, análise de lacunas), que se trata de um procedimento para medir a diferença entre o nível de conformidade em que a organização se encontra, em relação ao objetivo, que nesta situação é a adequação à LGPD. Para tal atividade o Grupo de Trabalho precisa elaborar um questionário e aplicá-lo para cada departamento da instituição (SILVA; AROUCA, 2020).

O questionário deve conter perguntas relativas aos processos internos: se há existência de tratamento de dados pessoais no departamento, sendo estes sensíveis ou não; se é realizado o tratamento de dados de crianças ou adolescentes; se é obtido o consentimento dos titulares ou responsáveis ao se realizar coleta de dados pessoais; qual a finalidade dos tratamentos de dados realizados na área em questão; se há o compartilhamento desses dados com outras áreas ou entidades terceiras; dentre várias outras perguntas relevantes, que devem ser formuladas de acordo com as exigências da lei, dentro da realidade de cada organização. As respostas serão utilizadas para aferir o grau de maturidade da organização, e determinar quais são as necessidades para adequação, e os riscos presentes em cada departamento.

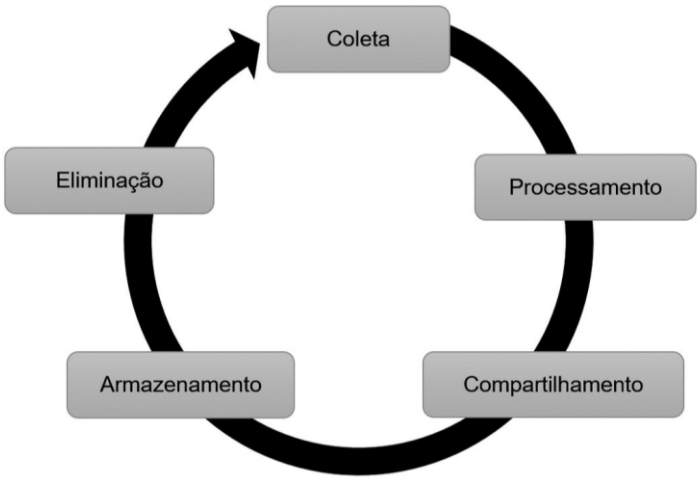
Por fim, na fase preliminar, é importante a aplicação de treinamentos sobre privacidade e proteção de dados para os colaboradores, e também cursos sobre a LGPD em específico,

principalmente nos casos dos departamentos que realizam tratamentos de dados pessoais. Através do treinamento é possível gerar clareza aos colaboradores, dos porquês das adaptações e mudanças que estão por vir, além de denotar a importância da proteção de dados pessoais.

3.2 - Mapeamento dos dados pessoais

Realizar o mapeamento dos dados pessoais, também conhecido como inventário de dados pessoais, pode ser uma excelente forma de otimizar a criação de políticas de segurança e proteção de dados pessoais. Quando os dados são mapeados e inventariados, se obtém o panorama completo de como funciona o fluxo do ciclo de vida dos dados na instituição, ou seja, de onde eles são recebidos, para onde são enviados, e qual a finalidade do uso, se tornando assim mais simples a adequação às bases legais da lei. O ciclo de vida dos dados envolve coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, dentre outras operações possíveis. Através da figura abaixo, pode-se visualizar um modelo simplificado do ciclo de vida dos dados.

Figura 3 - Ciclo de vida dos dados



Fonte: (DONDA, 2020)

Portanto, no processo de implementação da LGPD, é importante a realização das seguintes etapas quando se trata de compreender o fluxo dos dados: realizar um levantamento das

informações pessoais; utilizar um diagrama de fluxo de dados para visualização; gerar o mapeamento de dados; e, elaborar o registro das operações de tratamento de dados pessoais. Ademais, também é interessante aproveitar este momento para realizar análises de segurança na proteção dessas informações, ou seja, avaliar como são feitos os tratamentos dos dados, quais são os controles de segurança utilizados, se somente as pessoas corretas possuem acessos, e se o ambiente se encontra em conformidade (DONDA, 2020).

Na primeira etapa, é preciso que o Grupo de Trabalho realize um levantamento de todos os dados pessoais que transitam pela instituição, podendo este ser feito através de uma abordagem de processos em cada departamento, área ou setor da organização. É estratégica a aplicação de questionários, entrevistas ou análises documentais em cada área separadamente. Segue abaixo um exemplo de questionário simples para o levantamento dos dados pessoais, construída com base no Anexo do Guia de Elaboração do Inventário de Dados pessoais da Coordenação-Geral de Segurança da Informação do Ministério da Economia:

Categoria dos dados	Descrição	É realizado tratamento?	Fonte dos dados
Dados de Identificação Pessoal	Nome, endereço residencial, número celular pessoal, e-mail pessoal, CPF, RG, endereços IP, etc.		
Dados Financeiros	Números de identificação, números de contas bancárias, renda, investimento, dívidas sobre ativos, benefícios, bonificações, etc.		

Características pessoais	Idade, sexo, data de nascimento, situação militar, altura, peso, características distintivas, etc.		
Dados profissionais	Empregador, descrição do cargo e função, data de recrutamento, avaliação de desempenho, etc.		
Outros dados	(Especificar)		

Tabela 1: Questionário para levantamento de dados pessoais

A partir da coleta dessas informações, é possível obter noções sobre quais áreas precisam de prioridade, quais tipos de dados são tratados em cada setor da instituição e quais foram os pontos de entrada na coleta dessas informações. Os dados podem ter como origem cadastros online, sistemas informatizados, formulários escritos, outros departamentos, recebimento por meio de terceiros, dentre outros meios. E, independentemente do método, todos devem respeitar as bases legais da LGPD para sofrerem qualquer tipo de tratamento (SILVA; AROUCA, 2020).

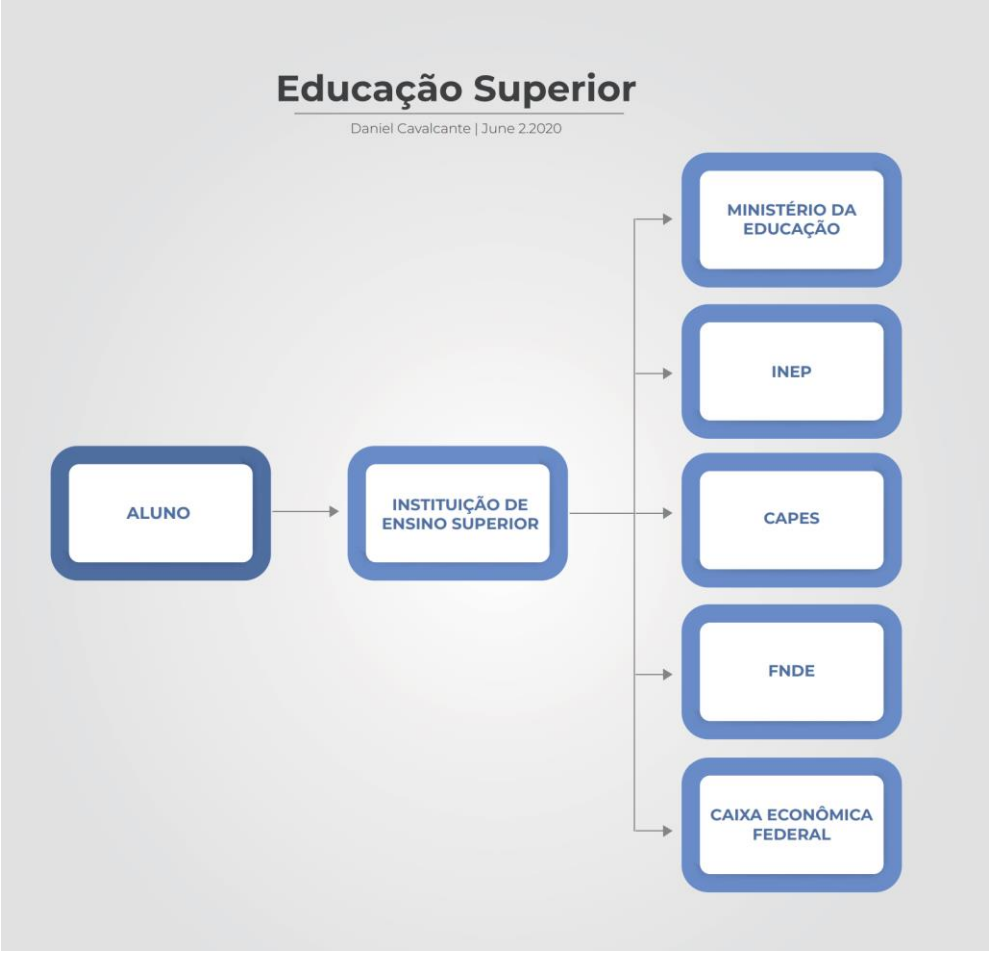
Após coletadas as informações iniciais, é importante o uso de ferramentas de representações gráficas dos fluxos de dados por parte do Grupo de Trabalho. Por meio da exibição visual deste mapeamento, é possível compreender processos e sistemas, e obter informações a respeito dos riscos envolvidos nos diferentes momentos do ciclo de vida dos dados.

A utilização de Diagrama de Fluxo de Dados (Data Flow Diagrams ou DFD) é indicado como uma boa prática pela norma ISO/IEC 27701, que é uma extensão de privacidade à ISO/IEC 27001 - norma de referência mundial para Sistemas de Gestão de Segurança da Informação (SILVA; AROUCA, 2020). O DFD representa um fluxo de trabalho ou de etapas dentro de um processo, mantendo seu foco no fluxo e na transformação dos dados. Ele pode

ser criado no nível de processo de negócios ou de sistemas, podendo ser usado para retratar aplicações, databases e arquivos (HATHAWAY,T.; HATHAWAY,A., 2016).

Abaixo é possível visualizar o exemplo de um Diagrama de Fluxo de Dados de uma visão macro sobre como os dados transitam do aluno para uma instituição de ensino superior, e da instituição para terceiros. Neste cenário, as regras e recomendações da LGPD objetivam manter os dados do aluno íntegros durante todo esse fluxo de informações.

Figura 4 - Diagrama de fluxo de dados da Educação Superior



Fonte: (SILVA; AROUCA, 2020)

A realização do mapeamento de dados é de extrema complexidade. É uma etapa que exige uma exploração minuciosa pelos processos de cada área de uma instituição. A fim de cumprir essa etapa é preciso compreender a fundo quais são as operações realizadas dentro de cada setor, para se tornar possível mapear quais dados são mantidos ou coletados, quais operações de tratamento são feitas a partir destes dados, e em quais momentos estes dados são

compartilhados com terceiros. Toda essa análise precisa ser feita a fim de responder questionamentos importantes que são necessários para a adequação à lei, como por exemplo:

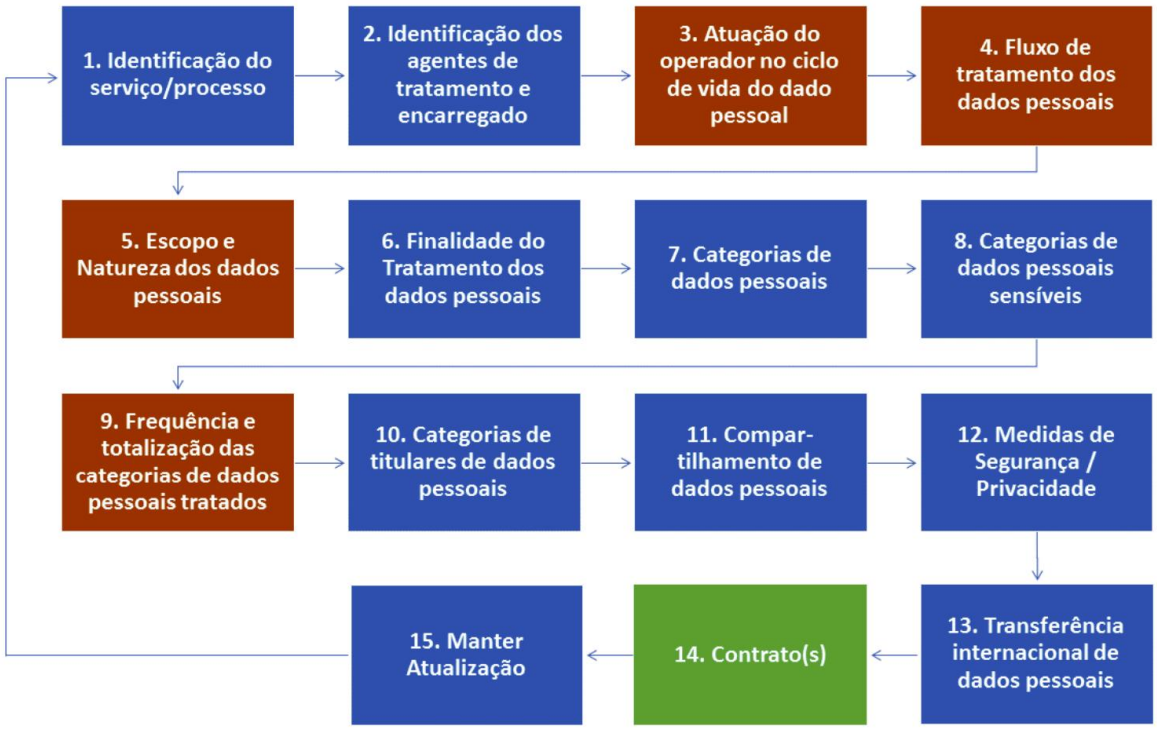
- Quais são os dados pessoais tratados?
- Quais são os dados pessoais sensíveis tratados?
- É feito o tratamento dos dados de menores de idade?
- Qual é a fonte de origem destes dados?
- Qual a finalidade das operações que envolvem tratamento de dados?
- Qual o fundamento legal para a coleta destes dados?
- Qual a base legal para o tratamento destes dados?
- Se for necessário o consentimento do titular, este foi obtido?
- Se for necessário o consentimento dos responsáveis, foi obtido?
- Existe a necessidade da retenção destes dados? Se sim, por qual período?
- Qual o local de armazenamento destes dados?
- Por quais sistemas (digitais ou físicos) estes dados fluem, ou são armazenados?
- É realizada transferência dos dados? Se sim, é feito para entidades terceiras?

Sintetizando, o mapeamento dos dados pessoais, se trata de uma documentação que mantém as informações e registros sobre como são feitos os tratamentos dos dados pessoais na instituição. Nessa documentação, é feito um balanço de quais dados pessoais são tratados, onde eles estão alocados, em quais operações eles são utilizados, e quais as bases legais para o tratamento destes dados (XAVIER, 2022).

Na imagem abaixo, é possível visualizar uma sugestão de fluxo de etapas para elaboração do inventário de dados pessoais (IDP). Este gráfico foi retirado do Guia de Elaboração de Inventário de Dados Pessoais criado pela Secretaria de Governo Digital do Ministério da Economia, disponível através do link <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf>.

As fases destacadas em azul representam elementos mínimos para a criação do IDP; as fases em laranja correspondem a levantamento complementar que podem auxiliar na construção do Relatório de Impacto de Proteção de Dados Pessoais, que será explicado posteriormente; e a fase destacada em verde corresponde à análise de adequação contratual.

Figura 5 - Fluxo de etapas para o inventário de dados pessoais



Fonte: Guia de Elaboração de Inventário de Dados Pessoais[2]

A partir do mapeamento dos dados, é possível construir o registro das operações de tratamento de dados pessoais, que é exigido ao controlador e operador no artigo 37 da LGPD. Com os dados pessoais devidamente mapeados, se tornam executáveis processos de controles para manter o registro dessas operações de tratamento, através da atualização dos sistemas de informação, da revisão dos processos, ou até mesmo através da implantação de sistemas automatizados para auditoria. Mas para isso é preciso que os dados tenham sido inventariados, que as operações de tratamento de dados de cada área tenham sido identificadas, e que as respostas para os questionamentos acima estejam documentadas.

A LGPD determina em seu artigo 38 que "a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados(...)" (BRASIL, 2018). Ademais, este mesmo relatório é mencionado anteriormente no artigo 32 do capítulo IV da LGPD, que é destinado ao tratamento de dados pelo Poder Público, mencionando que "a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de

[2] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf>. Acesso em: 20 mai. 2022

dados pessoais e sugerir a adoção de padrões e boas práticas para o tratamento de dados pessoais pelo Poder Público" (BRASIL, 2018).

É explicitado no Art. 38 que o RIPD (Relatório de Impacto à Proteção de Dados) precisará conter em sua documentação a descrição dos tipos dos dados coletados, qual metodologia utilizada para a coleta e para a segurança das informações, além das medidas para mitigação de riscos que foram adotadas. Para a elaboração desse relatório, também será de grande utilidade o prévio mapeamento dos dados pessoais.

O consentimento do titular não precisa ser obtido em todas as situações, como por exemplo nos casos em que o tratamento dos dados é realizado para cumprimento de obrigação legal, mas, de qualquer forma, é exigido que a instituição siga as medidas determinadas pela lei, principalmente no quesito da segurança. Por conta disso, é de extrema importância que as operações de tratamento, os propósitos, finalidades e hipóteses para o uso desses dados, estejam devidamente documentados.

3.3 - Políticas de Segurança da Informação e Proteção de dados

A LGPD trouxe consigo a obrigação legal de responsabilidades relacionadas à segurança da informação. Certas práticas que antes eram vistas como boas condutas, agora são normas registradas na legislação. Devido às leis que visam proteger os dados pessoais, a segurança da informação se tornou algo imprescindível para as organizações, e hoje necessita que sua implementação esteja alinhada à privacidade.

O Capítulo VII da LGPD é dedicado à segurança e boas práticas. A Seção I é destinada a Segurança e Sigilo de Dados, e é iniciada pelo artigo 46 e 47, que determinam:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (BRASIL, 2018).

É altamente recomendado que no quesito segurança dos dados, a organização siga as recomendações da Norma Técnica ABNT NBR ISO/IEC 27002, que se trata de um código de

práticas reconhecidas mundialmente sobre o tema de controles de segurança da informação. De acordo com a norma ABNT NBR ISO/IEC 27002:

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

Os princípios fundamentais da segurança da informação são a confidencialidade, a integridade e a disponibilidade das informações, e as medidas técnicas e organizacionais devem ser implementadas de modo a suprir cada um destes princípios (D'AVILA; SILVA; ARAUJO, 2021). Pode-se dizer que as leis de privacidade objetivam disciplinar estes princípios para obter a garantia da proteção dos dados pessoais. Segue abaixo o significado de cada um destes fundamentos.

Confidencialidade: Este pilar irá prover a garantia de que somente as pessoas com a permissão correta, terão acesso aos dados e informações. Ele é sustentado por meio de controles e padrões técnicos, como por exemplo: a configuração de permissões de acesso ao banco de dados; controle das permissões de compartilhamento; criptografia dos arquivos e dados.

Integridade: Pilar que irá assegurar que os dados e informações permanecerão íntegros e corretos, que não serão manipulados nem modificados de forma errônea, acidental ou mal intencionada. A integridade é sustentada com apoio de medidas técnicas como por exemplo: os logs dos sistemas, a segurança das informações armazenadas ou em trânsito, e os mecanismos de proteção.

Disponibilidade: Para garantir que os dados e informações estejam disponíveis e acessíveis a todo momento que seja necessário, para o correto funcionamento da organização. Este pilar é construído por meio de planos de recuperação de desastres, de continuidade de negócios, *e* realização contínua do *backup* dos dados.

A política de segurança da informação trata de documentações que estabelecem as diretrizes da organização a respeito da proteção da informação, e sua instauração se faz necessária para a garantia de que a instituição aja de acordo com as regulamentações e leis. A política pode ser criada com base nas recomendações da norma ABNT NBR ISO/IEC 27002, que orienta que haja o alinhamento aos requisitos de negócio, e às legislações do contexto da organização. Após ser definido, deve ser aprovado pela direção, publicado e comunicado a todas as partes relevantes.

A norma ABNT NBR ISO/IEC 27002 recomenda que contenha o documento contenha declarações a respeito da definição de segurança da informação, seus objetivos e princípios; a atribuição de responsabilidades; e informações sobre os processos que irão tratar possíveis desvios e exceções. A norma apresenta uma listagem de possíveis tópicos a serem abordados de forma mais específica na política de segurança da informação. Pode-se observar 3 exemplos abaixo, retirados da ABNT NBR ISO/IEC 27002:

(a) controle de acesso: tópico que objetiva limitar o acesso à informação e aos seus recursos.

(b) classificação e tratamento da informação: assegura que a informação receba um nível adequado de proteção, de acordo com sua importância.

(c) segurança física e do ambiente: objetiva a prevenção contra o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações.

Também é importante que no conteúdo da política de segurança da informação sejam apresentadas as consequências para violações das normas, e contenha orientações a respeito de itens como: uso dos ativos de TI, controle de senha, utilização dos e-mails e da internet, antivírus, trabalho por acesso remoto, *backup*, descarte de ativos, retenção de dados, dentre outros tópicos (SILVA; AROUCA, 2020).

Ressalta-se que a ANPD poderá solicitar a adoção de padrões técnicos mínimos a fim de garantir a segurança dos dados. De acordo com o artigo 49, os sistemas que realizam tratamento de dados pessoais devem ser desenvolvidos de forma que atendam aos requisitos de segurança, padrões de boas práticas, e aos princípios gerais previstos na LGPD. E de acordo com o artigo 51, a ANPD poderá também incentivar adoção de certos padrões técnicos que facilitem aos titulares a realização do controle de seus dados pessoais (BRASIL, 2018).

A Seção II do Capítulo VII da LGPD é destinada às Boas Práticas e de Governança, e se inicia com o Art. 50, que diz:

> "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais"
>
> (BRASIL, 2018).

É encorajado que as organizações implementem programas de governança em privacidade que representam o engajamento do controlador em cumprir boas práticas relacionadas à proteção de dados pessoais. Estes programas devem ser criados de acordo com a estrutura da organização, o volume das operações e a sensibilidade dos dados tratados. Lembrando que essas políticas de segurança e privacidade servirão como defesa para a organização em possíveis casos de infrações ou vazamento de dados, podendo contribuir para uma maior leveza das sanções de acordo com o artigo 52 da LGPD, da seção de Sanções Administrativas (BRASIL, 2018).

A LGPD, inspirada pela GDPR, incentiva técnicas de *Privacy by Design*, que em português tem o significado de 'Privacidade desde a concepção'. Este conceito foi criado pela Dra. Ann Cavoukian, e aparece no parágrafo 2º do art. 46 da lei brasileira, onde é citado que as medidas de privacidade e proteção de dados "devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018). O *Privacy by Design* trata-se de uma metodologia que prega que a privacidade e proteção de dados devem ser considerados como fatores cruciais em todo o ciclo de vida de um projeto, sistema, serviço ou processo (XAVIER, 2022).

É importante a criação de uma Política de Privacidade, que se trata de um documento cujo principal objetivo é dar ênfase ao tratamento de dados pessoais em um determinado serviço, demonstrando adequação às exigências da LGPD. Deve ser abordado no documento quais os tratamentos de dados que serão realizados e de quais formas procederão. Também é importante indicar se haverá compartilhamento dos dados do titular, para quais partes e a referida finalidade. Dentre outras informações pertinentes que devem ser apresentadas neste documento, a fim de atender às exigências e orientações da LGPD no que diz respeito às informações que devem ser comunicadas ao titular, e aos consentimentos que devem ser solicitados a ele. No caso de serviços online, também deve ser inserido nesta política, ou em separado, informações transparentes a respeito da utilização de *cookies*, que são mecanismos utilizados na internet para coletar os dados de navegação dos usuários, retratando quais são os *cookies* utilizados e a finalidade da coleta. Através da norma ABNT ISO/IEC 27701:2019 é possível obter recomendações e boas práticas para gestão de privacidade nas organizações.

A partir do momento que a organização segue bons padrões técnicos de segurança, boas práticas de proteção de dados e privacidade e transparência e respeito aos titulares dos dados pessoais, ela se torna muito mais protegida e resguardada para quaisquer situações de adversidade referentes a incidentes relacionados a dados.

3.4 - O papel dos Profissionais de Sistemas de Informação na LGPD

A participação de profissionais da área de Tecnologia da Informação em todo o processo de adequação à LGPD é de extrema importância. No mundo contemporâneo a tecnologia se encontra fortemente inserida no cotidiano da população como um todo. Diversas atividades dependem diretamente dos sistemas de informação e ambientes digitais, além de outros processos que são amplamente suportados e apoiados por estes mesmos recursos tecnológicos.

A LGPD menciona explicitamente que as suas regras são válidas tanto no meio físico quanto no digital, e para se tornar possível as devidas adequações tecnológicas e sistêmicas, é necessário o envolvimento de especialistas da área de Sistemas de Informação em todo o processo de adequação à lei. Principalmente nos contextos em que os dados pessoais são armazenados e tratados nos meios digitais.

É possível ressaltar, na legislação, conceitos que estão fortemente ligados ao desenvolvimento tecnológico como, por exemplo, o *Privacy by Design*, citado anteriormente neste trabalho. Este conceito apresenta a idealização de que a disciplina da proteção de dados pessoais deve ser aplicada em todo o ciclo de desenvolvimento de um serviço ou produto, com o acompanhamento de tecnologias que possibilitem o devido controle, privacidade e proteção das informações pessoais. Pode-se apresentar como exemplo de tecnologias que favorecem *Privacy by Design*: a criptografia para garantia da confidencialidade; a anonimização dos dados pessoais para evitar a identificação de um indivíduo através de um dado; e mecanismos de navegação anônima que irão impossibilitar o rastreamento de determinado usuário; dentre outros possíveis recursos. Tendo em consideração estes exemplos, observa-se que a arquitetura dos Sistemas de Informação é um meio de extrema eficiência para exercer a proteção dos dados pessoais dos titulares (BIONI, 2021).

Os recursos informatizados também auxiliam na execução do mapeamento e inventário de dados, possibilitando que através dos sistemas de informação seja estudado, compreendido e visualizado o fluxo de tratamento e o ciclo de vida dos dados pessoais por todo o meio digital de uma organização, para que através disso sejam revisados, alterados e corrigidos quaisquer sejam os pontos necessários.

Além dos recursos tecnológicos intrínsecos à sociedade da informação, podem ser ressaltadas múltiplas áreas da tecnologia da informação que precisam considerar a privacidade e a proteção dos dados pessoais. São exemplos que podem ser citados:o *Big Data* e mineração

de dados; a Inteligência Artificial; a Internet das Coisas (*IoT*); e a comunicação e o Marketing Digital. Para que sejam executadas de forma ética e dentro da lei, essas tecnologias não podem ignorar áreas como a segurança da informação, a governança de dados e a proteção de dados pessoais.

3.5 - Implementação dos direitos dos titulares

O capítulo III da LGPD é destinado à garantia dos direitos dos titulares, que é iniciado pelo artigo 17, que diz: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta lei". (BRASIL, 2018) Em seguida, são enumerados os direitos do titular em relação a obtenção de informações referentes ao tratamento de dados por parte do controlador.

O titular dos dados tem direito de obter informações a respeito da confirmação da existência de tratamento, ter acesso aos dados sob domínio do controlador, a poder corrigir e atualizar dados incompletos ou incorretos. Ademais, o titular também tem o direito de solicitar a exclusão de dados desnecessários, de revogar o seu consentimento em determinadas situações, obter informações sobre quais entidades o controlador realizou compartilhamento dos dados. Portanto, se tornou de extrema importância que as instituições sejam transparentes com os titulares nos casos em que são efetuados tratamentos de dados.

É eficiente a criação de uma política interna para organizar o processo de requisição dos titulares de dados, pois envolverá o recebimento da solicitação, o processamento e a resposta à requisição (SILVA; AROUCA, 2020). É necessário definir quem são os responsáveis por este processo, e qual será o seu fluxo de acordo com as exigências da LGPD, tornando-se necessário a adaptação de sistemas e banco de dados para tal. O artigo 19 da lei diz que a confirmação de existência ou acesso aos dados pessoais devem ser providenciados ao titular em formato simplificado, de forma imediata ou no prazo de até 15 (quinze) dias após o requerimento ter sido feito. Lembrando que o contato do Encarregado de Proteção de Dados deve ser disponibilizado em fácil acesso no *website* da organização.

De acordo com o cenário da organização, devem ser implementados mecanismos que proporcionem aos titulares dos dados formas de exercerem seus direitos de forma facilitada. Como por exemplo, no website de uma empresa pode ser implementado um portal de privacidade em que o usuário consiga gerenciar seus dados compartilhados com a organização,

tendo a possibilidade de acessá-los, salvá-los, atualizá-los ou até de revogar seu consentimento para determinadas operações de tratamento. Tal funcionalidade proporciona tanto a adequação à lei, quanto uma melhor experiência para o usuário, no que tange a privacidade.

3.6 - Gerenciamento de Risco e de Violação de dados

A LGPD determina regras para situações em que ocorram incidentes de segurança que possam danificar ou expor dados pessoais. De acordo com o artigo 48, é exigido do controlador que efetue a comunicação à ANPD e ao titular em prazo razoável, descrevendo a natureza dos dados pessoais afetados, as informações do titular envolvido, medidas técnicas e de segurança referente a proteção, os riscos relativos ao incidente e as medidas que foram adotadas para reverter ou mitigar os efeitos do incidente (BRASIL, 2018).

Conforme citado anteriormente, existem diversos níveis de sanções administrativas relativas a infrações cometidas, podendo ser uma advertência com prazo para medidas corretivas, multa de até 2% (dois por cento) do faturamento no caso de organização privada, e em situações mais severas pode ocorrer suspensão ou proibição do exercício da atividade de tratamento de dados pessoais, dentre outras sanções possíveis.

Conforme o § 1º do artigo 52, diversos critérios são considerados no momento em que for aplicada a sanção. Serão considerados fatores como por exemplo: a gravidade do incidente, a boa-fé do infrator, sua condição econômica, a reincidência, o grau do dano, dentre outros. No inciso VIII desse mesmo parágrafo, é citado como um dos critérios “a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados (...)”, e no inciso X é citada “a pronta adoção de medidas corretivas” (BRASIL, 2018). Dito isto, é possível comprovar a importância da realização do gerenciamento de riscos e violação de dados por parte dos agentes de tratamento. É esperado da organização que sejam formulados planos de resposta a incidentes e remediação, conforme é mencionado no artigo 50 da seção de boas práticas e governança.

A norma ABNT NBR ISO/IEC 27005 provê diretrizes sobre gestão de riscos de segurança da informação em uma organização. A gestão de riscos irá atuar com o objetivo de avaliar os riscos presentes e o impacto que eles iriam causar, para então ser definido um plano de tratamento dos riscos, além do estabelecimento de políticas para mitigá-los. Nesta norma

são determinados como critérios para avaliação de riscos o valor estratégico, a importância da informação em questão, a atenção necessária a determinada operação e negócios, e as expectativas das partes interessadas.

Exemplos de ameaças que podem significar riscos para a proteção dos dados pessoais são o roubo de informação, perda de dispositivos eletrônicos que contenham dados pessoais, acesso indevido por usuário não autorizado, vazamento de dados por questões acidentais ou intencionais, dentre outros possíveis incidentes.

Interpreta-se que o plano de resposta a incidentes e remediação citado na lei, funcione como ações a serem executadas assim que ocorrer um incidente. Portanto, é viável de ser estruturado em formato de procedimentos, com tarefas para serem atuadas desde a identificação do incidente até a mitigação dos danos (SILVA; AROUCA, 2020). Deve conter operações de investigação interna e também o processo de comunicação às partes impactadas pelo incidente, que nesse caso inclui-se o titular dos dados e a ANPD. Lembrando que é de extrema importância fornecer aos colaboradores treinamentos relacionados a este plano. Através destas atividades, se torna possível que a organização responda em tempo razoável a um incidente de segurança, limitando os danos e realizando as devidas comunicações que são previstas por lei.

3.7 - Encerramento do Projeto

Na fase final do projeto é necessário avaliar a maturidade obtida pela organização no que tange a LGPD. É estratégico uma nova realização do *Gap Analysis* (análise de lacunas) para identificar se os pontos faltantes foram completos, e revisar quais processos ainda podem ser melhorados ou implementados (SILVA; AROUCA, 2020).

A manutenção da LGPD se trata de um processo contínuo, que necessita de constante monitoramento e avaliação. Cada fase precisa ser revisitada periodicamente, a fim de atualizar e rever processos e operações. Existem recomendações técnicas que ainda serão futuramente fornecidas pela ANPD, e devido ao fato da tecnologia estar sempre em evolução, as políticas de segurança e medidas técnicas precisam ser atualizadas regularmente.

A LGPD trouxe consigo regras para o estabelecimento de uma nova cultura para a proteção de dados e segurança da informação, então tornou-se necessário que estas práticas e fundamentos estejam intrínsecos à estrutura da organização. Lembrando que é de extrema

importância que sejam ministrados treinamentos e cursos relacionados a LGPD, pois cada colaborador de uma instituição será essencial para o funcionamento dessa nova cultura.

4. Avaliação de Instituições de Ensino Superior

4.1 - Estudo de caso nos sites institucionais das Universidades Federais do RJ

Diversas exigências e boas práticas apresentadas pela LGPD e por outras legislações de proteção de dados pessoais, têm como fundamento a transparência das empresas e organizações com os seus clientes e usufruidores. Não basta somente empregar altos níveis de segurança da informação, também é necessário demonstrar e comprovar as práticas corretas de privacidade e proteção de dados, além de uma comunicação eficiente com os titulares dos dados.

No atual capítulo, será apresentado um estudo de campo tendo como base os *websites* das quatro instituições federais de ensino superior do Estado do Rio de Janeiro: a UNIRIO (Universidade Federal do Estado do RJ), UFRJ (Universidade Federal do RJ), UFF (Universidade Federal Fluminense) e UFRRJ (Universidade Federal Rural do RJ). Os recursos informativos destinados à proteção de dados pessoais em seus *websites* institucionais serão analisados com base em critérios retirados da LGPD, mediante interpretação própria.

Para cada item avaliado, foi designado um peso para a pontuação final, o peso 3 corresponde a itens de práticas previstas e exigidas pela LGPD, o peso 2 corresponde a itens de boas práticas apontadas pela LGPD, e o peso 1 corresponde a práticas complementares às duas citadas anteriormente. Para os sete itens destacados para a realização deste estudo, totalizam-se 12 pontos no caso de todos os critérios terem sido atendidos.

Seguem abaixo os itens a serem avaliados e seus respectivos pesos:

1- Existência de página destinada a apresentar informações referentes à proteção de dados pessoais (peso 2).

Este item pode ser relacionado ao artigo 23 do capítulo IV, que é destinado ao tratamento de dados pessoais pelo poder público, visto que as instituições analisadas são órgãos da Administração Pública Federal. No inciso I deste artigo, é recomendado que sejam

divulgadas informações claras a respeito do tratamento de dados pessoais, preferencialmente no próprio *website* institucional do agente de tratamento.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. (BRASIL, 2018)

2- A página citada no item 1 possui fácil acesso e localização no site da instituição (peso 1).

Critério considerado a fim de avaliar a viabilidade do acesso à página por parte do usuário, pois através desta página que se tornarão disponíveis as informações que devem ser fornecidas publicamente.

3- O website disponibiliza publicamente a identidade e informações de contato do Encarregado de Proteção de Dados da instituição. De forma clara e de fácil acesso (peso 3).

O item em questão é amparado pelo artigo 41 no Capítulo VI, que diz respeito às obrigações dos agentes de tratamento de dados pessoais. É informado que a identidade e contato do encarregado devem ser disponibilizadas preferencialmente no *website* do controlador.

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
>
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. (BRASIL, 2018)

4- O website apresenta orientação de como requisitar a confirmação de existência ou o acesso aos dados pessoais do titular (peso 3).

É interessante que este item seja implementado a fim de atender ao artigo 18 do capítulo III da LGPD, que é destinado aos direitos do titular dos dados pessoais. Neste artigo, é explicitado o direito do titular a solicitar informações referentes aos dados que possam estar sob o domínio do controlador. A legislação exige que a resposta seja providenciada ao titular em formato simplificado e no prazo de até quinze dias a partir da data do requerimento, portanto é de extrema importância que este processo seja bem definido dentro da instituição. Deduz-se a necessidade de disponibilizar aos titulares informações de como este requerimento pode ser feito, preferencialmente na própria página destinada à LGPD.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I - confirmação da existência de tratamento;
>
> II - acesso aos dados;
>
> III - correção de dados incompletos, inexatos ou desatualizados;
>
> (...)
>
> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
>
> I - em formato simplificado, imediatamente; ou
>
> II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. (BRASIL, 2018)

5- A página em questão disponibiliza materiais informativos a respeito da LGPD e dos direitos do titular (peso 1).

É fortemente encorajado a transparência e a disponibilidade de informações claras aos titulares por parte dos agentes de tratamento, portanto, o item 5 foi apontado como uma boa prática complementar, por se tratar do ato de disponibilizar conteúdos informativos para as partes interessadas, de forma a ser publicamente compartilhado no website institucional da Universidade.

6- O *website* informa a política de privacidade da instituição (peso 1).

Mediante o conteúdo legislativo que foi visualizado e estudado ao longo deste trabalho, é possível determinar a importância de uma instituição possuir e disponibilizar uma declaração de privacidade que esteja alinhada a esfera da organização. Nesta declaração, é possível contemplar informações sobre quais dados pessoais são coletados e qual a finalidade, quais as operações de tratamento realizadas, se há transferência ou compartilhamento destes dados e para quem, dentre outras informações pertinentes (DONDA, 2020). Devido à relevância da comunicação com os titulares dos dados, torna-se uma boa prática disponibilizar ao público a política de privacidade da instituição.

7- A página em questão adverte ao usuário a respeito do uso e política de *cookies* do *website* (peso 1).

Os *cookies* são mecanismos utilizados na internet para coletar os dados de navegação dos usuários ao utilizarem um *site* ou aplicação *web*. Eles são dados armazenados no navegador podendo ser tratados para se extrair informação deles para múltiplas finalidades, como por exemplo, salvar registro do endereço IP do acesso, salvar as preferências da navegação do usuário, restaurar os dados de login e senha utilizados, e sugerir publicidades de acordo com as interpretações de consumo do indivíduo em específico (CARDOSO, 2021).

Devido ao fato da LGPD trazer a necessidade do consentimento do titular dos dados, os *websites* passaram a informar aos usuários sobre a utilização e coleta dos *cookies*, pois cabe ao titular concordar em fornecer o seu consentimento para o tratamento de dados, ou não. Portanto, foi levantada como uma boa prática, que a página da instituição informe ao usuário a respeito da política de cookies adotada pelo website.

4.2 Universidade Federal Fluminense

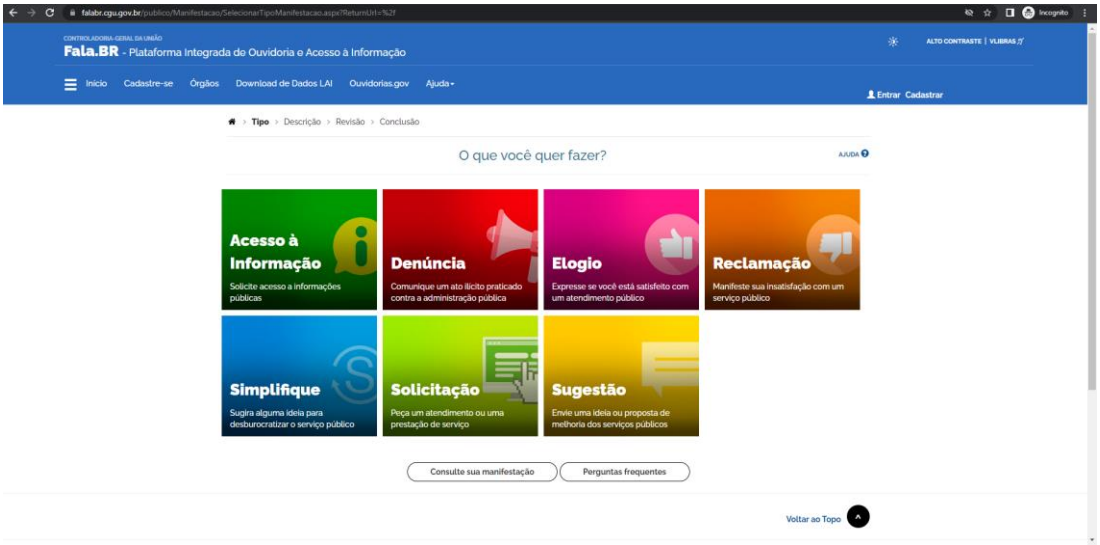
A página de LGPD da UFF (https://www.uff.br/lgpd) atendeu a todos os itens de peso 3 destacados neste estudo, também disponibilizando informações adicionais, como por exemplo, uma seção de perguntas frequentes e links para capacitações em LGPD. Na página é possível ter acesso ao contato do Encarregado de Proteção de Dados da instituição e ao canal de atendimento às demandas da LGPD.

Figura 6 - Página de LGPD da UFF

Fonte: Página de LGPD da UFF[3]

O canal de atendimento às requisições dos titulares disponibilizado pela UFF é a página do Fala.BR (https://falabr.cgu.gov.br/), que se trata de uma plataforma da Controladoria-geral da União para fins de ouvidoria e acesso à informação. Através do Fala.BR é possível realizar solicitações de acesso a informações públicas, denúncias, reclamações a respeito de um serviço público, sugestões, dentre outros tipos de requisições.

Figura 7 - Página do Fala.BR



Fonte: Site Fala.br[4]

[3] Disponível em: <https://www.uff.br/lgpd>. Acesso em: 20 jun. 2022.
[4] Disponível em: <https://falabr.cgu.gov.br/>. Acesso em: 20 jun. 2022.

É disponibilizado inicialmente na página, um texto resumindo informações referentes à LGPD e como ela se aplica às Instituições de Ensino Superior, e mais especificamente como se aplica à própria UFF. É citado que em muitos processos existentes em uma instituição são realizados tratamentos de dados pessoais, como por exemplo, na efetivação de matrículas, no histórico escolar do aluno, na coleta de dados de servidores, técnicos administrativos e professores, dentre outras situações possíveis.

Neste texto, além de serem apresentadas definições da legislação, também é mencionado como a LGPD trouxe novas demandas de desenvolvimento aos setores de tecnologia e segurança da informação devido ao fato de serem um dos principais atores na revisão dos meios de tratamento dos dados pessoais. Eles também citam a necessidade do acompanhamento jurídico e a necessidade da UFF definir um plano de adequação, para que sejam realizados projetos e implementadas ações que possibilitem que a Instituição esteja em conformidade com a LGPD. É mencionada a importância do papel dos servidores na adequação à lei, pois eles precisarão estar alinhados à política interna de proteção de dados, por meio da realização de cursos, treinamentos e solicitações.

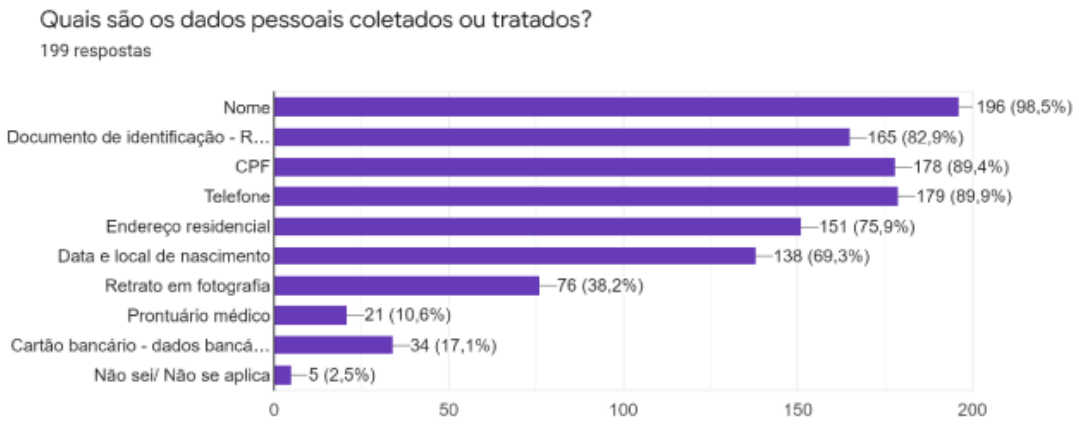
Na página, também foi disponibilizado o relatório final do Grupo de Trabalho de LGPD da instituição, onde são esclarecidas as diversas ações tomadas na instituição. Seu plano de implementação da LGPD foi dividido em quatro etapas, que eles denominaram de objetivos. O relatório da implementação pode ser encontrado no link <https://www.uff.br/sites/default/files/relatorio_final_gt_lgpd_-_marco_de_2022.pdf> e será resumido abaixo.

A primeira etapa de adequação da UFF consistiu na divulgação de informações sobre a LGPD para a instituição, onde é citada a criação da própria página de LGPD da UFF <https://www.uff.br/lgpd>. Ademais, para o cumprimento deste mesmo objetivo foram realizadas diversas reuniões com o Comitê de Governança, Integridade, Riscos e Controles, com o Comitê de Apoio à Governança e com os servidores indicados como pontos focais para o programa de adequação da LGPD na UFF. Por fim, neste primeiro momento, compartilharam boletins sobre práticas da LGPD com os seus servidores.

A segunda etapa da implementação da legislação foi denominada como “Avaliação da realidade atual sobre o tratamento de dados pessoais na UFF”. É descrito no relatório que nesta etapa foi aplicada uma enquete por meio do *Google Forms*, referente aos processos de tratamento de dados na oferta dos serviços públicos da UFF. Através das respostas dos servidores, técnicos administrativos e docentes, foi consolidada a apuração da enquete no documento de Diagnóstico da Cultura Organizacional, observando-se a necessidade de se

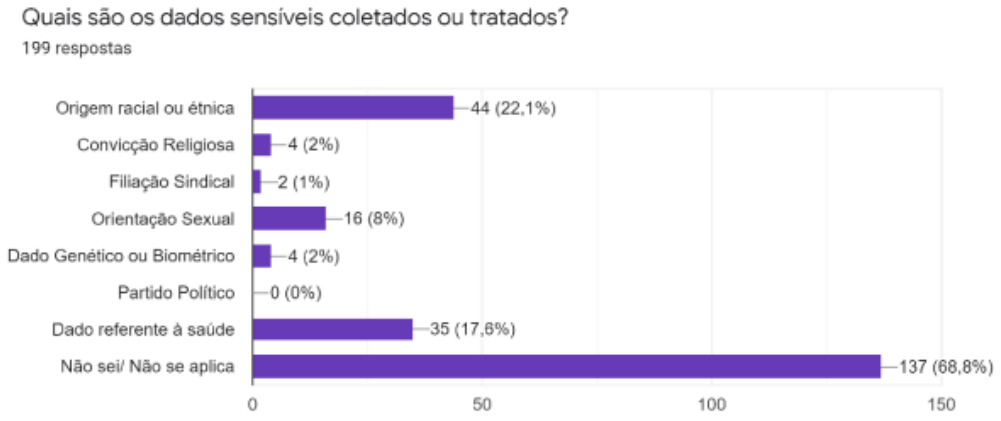
ampliar a divulgação de informações sobre a LGPD, efetuar a avaliação dos tratamentos de dados pessoais realizados pela UFF e a definição de uma estrutura de governança da LGPD na instituição. Segue abaixo um exemplo de pergunta realizada neste questionário.

Figura 8 - Gráfico do tratamento de dados pessoais na UFF



Fonte: Relatório Final GT-LGPD UFF

Figura 9 - Gráfico do tratamento de dados pessoais sensíveis na UFF



Fonte: Relatório Final GT-LGPD UFF

Além disso, na segunda etapa foi realizado o diagnóstico de maturidade da UFF, através do questionário disponibilizado pela Secretaria de Governo Digital no endereço

<https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-privacidade-lgpd>. Através deste questionário é possível avaliar o grau da maturidade em privacidade por parte das entidades públicas, no que tange a LGPD, e por meio dos resultados podem ser definidas as ações necessárias para se adequar a lei. No caso da UFF, eles citam que irão utilizar a análise deste diagnóstico a fim de apoiar a modelagem do Inventário de Dados Pessoais (IDP), e posteriormente para desenvolver o Relatório de Impacto à Proteção de Dados (RIPD), sendo este exigido pela lei.

Como terceira etapa, a UFF realizou um levantamento dos contratos a fim de identificar os que possuem relação com dados pessoais, para futuramente esta informação auxiliar na composição das cláusulas de segurança nos diversos contratos efetuados na UFF. É mencionado que, através das informações disponibilizadas pelo Inventário de Dados Pessoais, eles poderão adequar os termos dos contratos de acordo com as operações de tratamento de dados pessoais realizadas, como por exemplo, coleta, transferência e processamento.

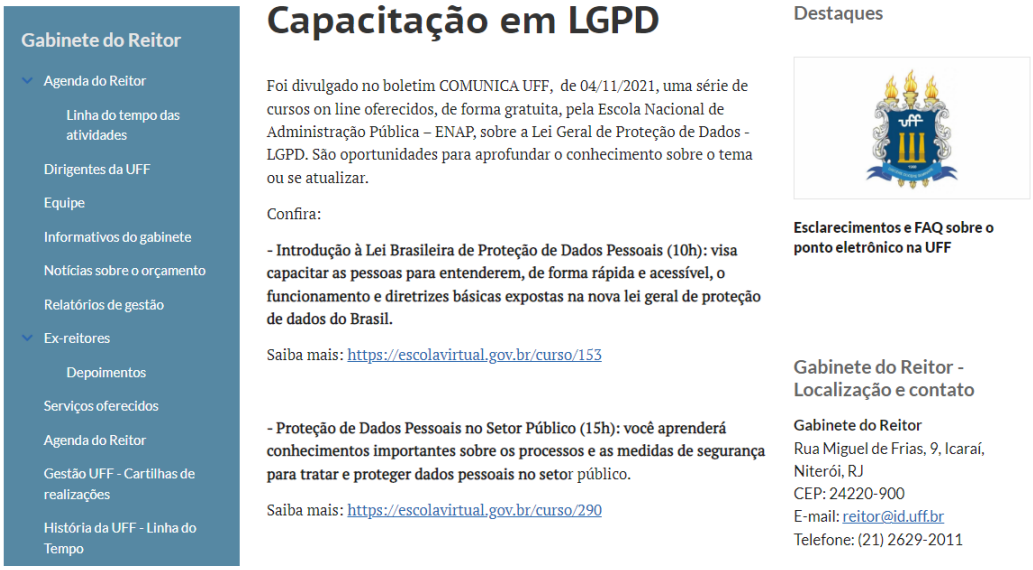
Em sua quarta etapa no plano de adequação, o Grupo de Trabalho da UFF identificou a necessidade de implantar um Programa de Governança em Privacidade (PGP) para estruturar a governança da LGPD na UFF. É mencionado o guia de Elaboração de Programa de Governança em Privacidade que é disponibilizado pelo Ministério da Economia no link <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf>. Este guia é destinado aos órgãos e entidades da Administração Pública Federal, e apresenta a intenção de se manter alinhado às orientações e diretrizes determinadas pela Autoridade Nacional de Dados Pessoais (ANPD). O guia objetiva orientar as ações a serem tomadas a nível de estrutura organizacional a fim de que os dados pessoais sejam devidamente gerenciados, assim como a segurança e os riscos. Ademais, para que sejam asseguradas a existência e o cumprimento de normas e políticas internas relativas à proteção dos dados pessoais e de seu uso correto perante a lei.

Ainda na quarta e última etapa do relatório, é apresentada como sugestão pelo Grupo de Trabalho, a criação de um Escritório de Governança de Dados que seja composto por representantes das áreas de Comunicação Social, Documentação, Planejamento e Tecnologia da Informação, de forma a suportar as atividades do Encarregado de Proteção de Dados da UFF, e atuar juntamente ao Comitê de Governança Digital da Instituição.

Na página de LGPD da UFF, é disponibilizado um link para outra página do *website* institucional que contém diversos cursos online para capacitação em LGPD ofertados na Escola Virtual do governo (<https://www.escolavirtual.gov.br/>). Assim, a UFF colabora com a comunidade ao divulgar conteúdos e conhecimentos da área de proteção de dados, que além de

serem conhecimentos necessários devido a legislação, é também uma área de grande crescimento devido ao enorme avanço tecnológico global. Além disso, a UFF também disponibilizou em sua página o Guia de Boas Práticas para Implementação da LGPD na administração pública federal, do gov.br (<https://www.uff.br/sites/default/files/guia_lgpd_-_agosto2020.pdf>).

Figura 10 - Página de capacitação em LGPD da UFF

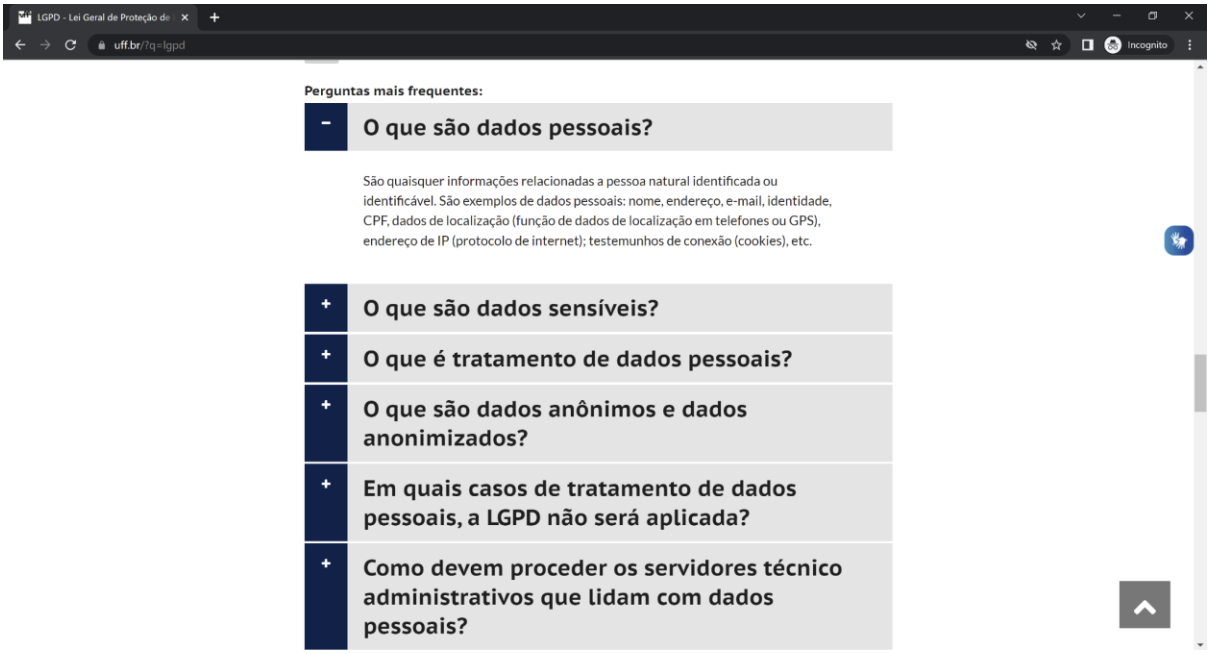


Fonte: Página Capacitação em LGPD UFF[5]

Como último tópico na página de LGPD da UFF, é disponibilizada uma seção de perguntas mais frequentes (FAQ), com tópicos gerais e específicos para a administração pública. Nesta FAQ, são apresentadas perguntas referentes a LGPD em geral e como os servidores federais devem proceder ao lidar com dados pessoais.

[5] Disponível em: <https://www.uff.br/?q=capacitacao-em-lgpd>. Acesso em: 20 jun. 2022.

Figura 11 - Perguntas mais frequentes da página de LGPD da UFF

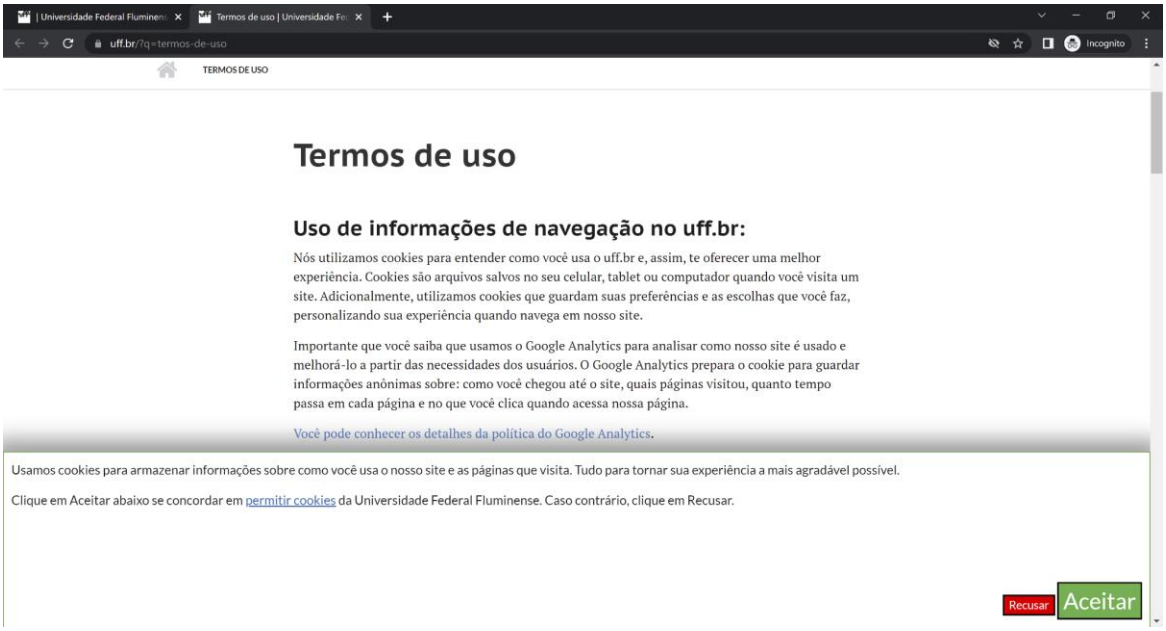


Fonte: Página de LGPD da UFF[6]

Por fim, o website institucional da UFF é o único, entre os quatro avaliados neste estudo, que informa ao usuário a política de *cookies* (arquivos utilizados para salvar as preferências e escolhas do usuário em um site eletrônico). Devido ao fato desses arquivos gravarem informações relativas à navegação de um usuário em um *website*, os *cookies* possibilitam associar e distinguir indivíduos facilitando, assim, a coleta de dados pessoais.

[6] Disponível em: <https://www.uff.br/lgpd>. Acesso em: 20 jun. 2022.

Figura 12 - Solicitação de permissão para uso de Cookies no uff.br



Fonte: Política de cookies da UFF[7]

Através da análise do portal de LGPD da UFF, é possível observar que a instituição está engajada nas atividades de proteção de dados pessoais e no processo de adequação à LGPD. É de extrema importância o trabalho feito no compartilhamento de informações, através da indicação de cursos, do conteúdo disposto na página e da cartilha de LGPD construída pela UFF. A instituição está sendo transparente em relação a todo o processo de implementação da proteção de dados, demonstrando atitudes práticas e não omitindo os pontos a serem melhorados pela instituição.

4.3 Universidade Federal do Rio de Janeiro

A página da UFRJ (https://ufrj.br/acesso-a-informacao/lgpd/) exibe inicialmente um texto informativo sobre a LGPD e como ela se aplica nas universidades. A seguir, eles mencionam que, na UFRJ, as atividades relacionadas a LGPD estão sob amparo do Comitê de Governança Digital. Este órgão atua nas políticas gerais de governança digital, tecnologia da informação e comunicação, almejando a eficiência e a estruturação da governança de T.I, de forma a manter esta área alinhada aos objetivos da instituição.

[7] Disponível em: <https://www.uff.br/?q=termos-de-uso>. Acesso em: 20 jun. 2022.

Figura 13 - Página de LGPD da UFRJ

Fonte: Página de LGPD da UFRJ[8]

Como próximo tópico apresentado na página, é compartilhado publicamente a identificação do Encarregado de Proteção de Dados da instituição, e o seu contato, conforme é exigido pela lei. A página também disponibiliza as informações a respeito das obrigações do Encarregado, que são: aceitar as reclamações e requisições dos titulares; fornecer esclarecimentos e agir nas devidas providências; e atuar como um ponto focal de orientações a respeito da LGPD para os servidores e contratados da Universidade. Como ferramenta para as requisições dos titulares de dados é indicada a página do Fala.BR, assim como no portal da UFF.

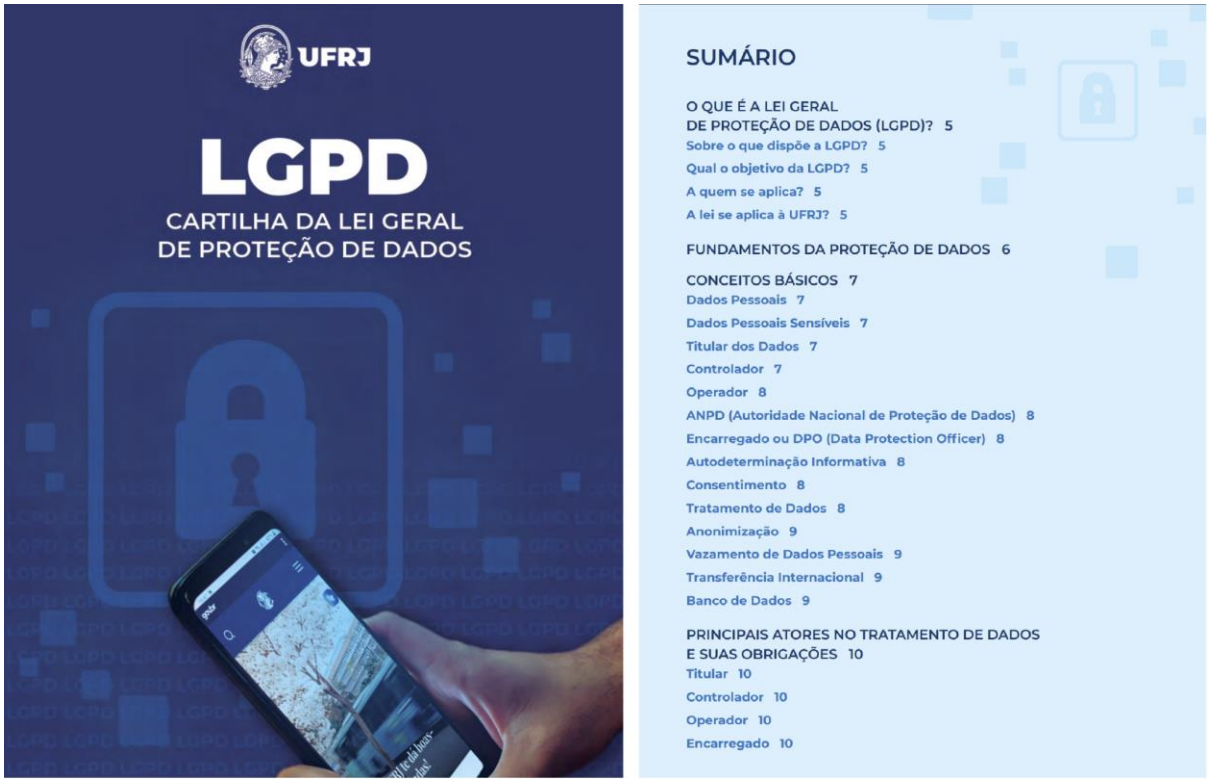
A página da UFRJ menciona a criação de um Grupo de Trabalho multidisciplinar para atuar no desenvolvimento e implementação de um Plano de Adequação à LGPD com prazo de dia 31 de dezembro de 2021 para a entrega do relatório final. Porém não há informações adicionais a respeito do relatório em questão.

Uma cartilha é disponibilizada pela UFRJ para *download* (<https://ufrj.br/wp-content/uploads/2022/06/lgpd-cartilha-ufrj-21-06-22.pdf>). Nesta cartilha, são apresentadas diversas informações importantes sobre LGPD, proteção de dados e como esses assuntos se

[8] Disponível em: <https://ufrj.br/acesso-a-informacao/lgpd/>. Acesso em: 20 jun. 2022.

aplicam à UFRJ. Foram cobertos todos os assuntos da LGPD, sendo este um material informativo claro e completo para a comunidade.

Figura 14 - Cartilha de LGPD da UFRJ



Fonte: Cartilha de LGPD da UFRJ[9]

É importante observar que a página de LGPD da UFRJ compartilha informações a respeito de como a instituição está lidando com o processo de adequação à lei, ou sobre quais foram as medidas adotadas e quais os próximos passos a serem tomados.

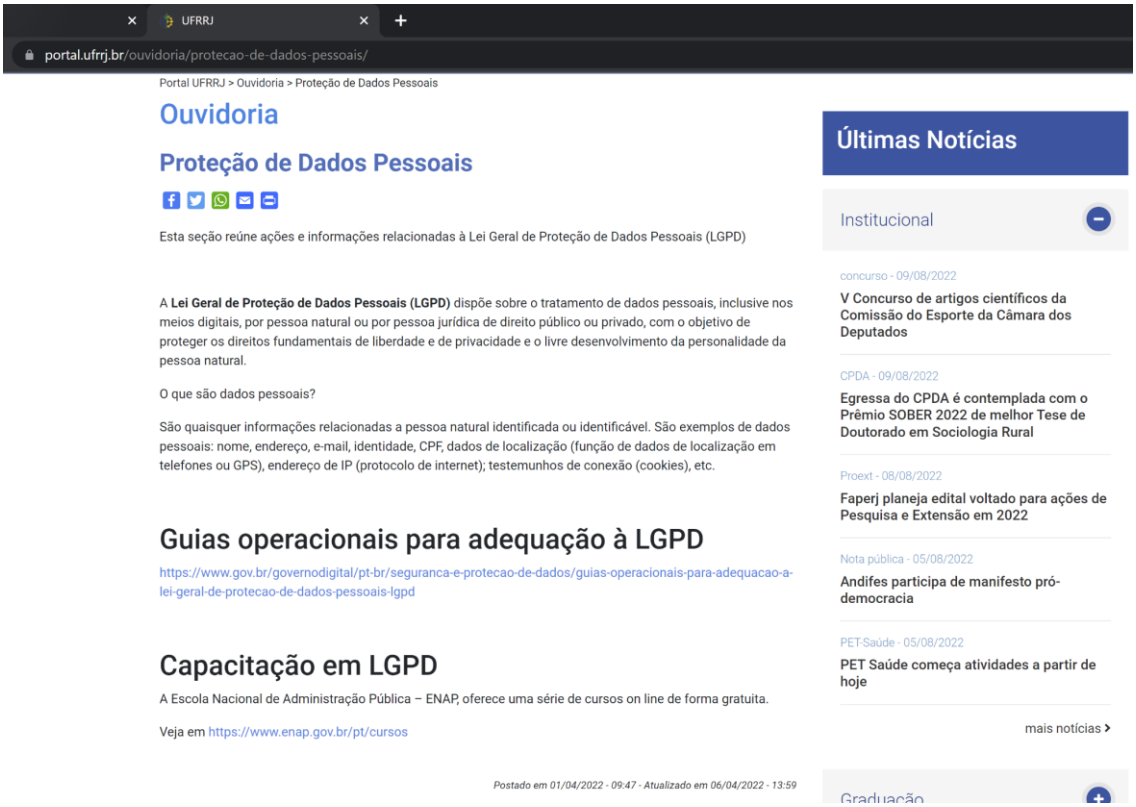
4.4 Universidade Federal Rural do Rio de Janeiro

A página da UFRRJ (https://portal.ufrrj.br/ouvidoria/protecao-de-dados-pessoais/) apresenta informações sucintas do que é a LGPD, e disponibiliza o endereço para uma página

[9] Disponível em: <https://ufrj.br/wp-content/uploads/2022/06/lgpd-cartilha-ufrj-21-06-22.pdf>. Acesso em: 20 jun. 2022.

do governo que contém um guia de adequação. A página da UFRRJ não atendeu aos itens 3 e 4 que são considerados como práticas previstas pela LGPD.

Figura 15 - Página de LGPD da UFRRJ



Fonte: Página de LGPD da UFRRJ[10]

Devido à falta de informações referentes à LGPD no *website* institucional da UFRRJ, não foi possível realizar uma avaliação a respeito da postura da universidade perante a proteção de dados pessoais. Por ser uma universidade federal, seria esperado um maior avanço nas atividades de conformidade com a LGPD em seu meio de comunicação digital. Não foram compartilhadas informações importantes para a legislação em questão, e não foram mencionadas atividades realizadas para adequação da instituição à LGPD.

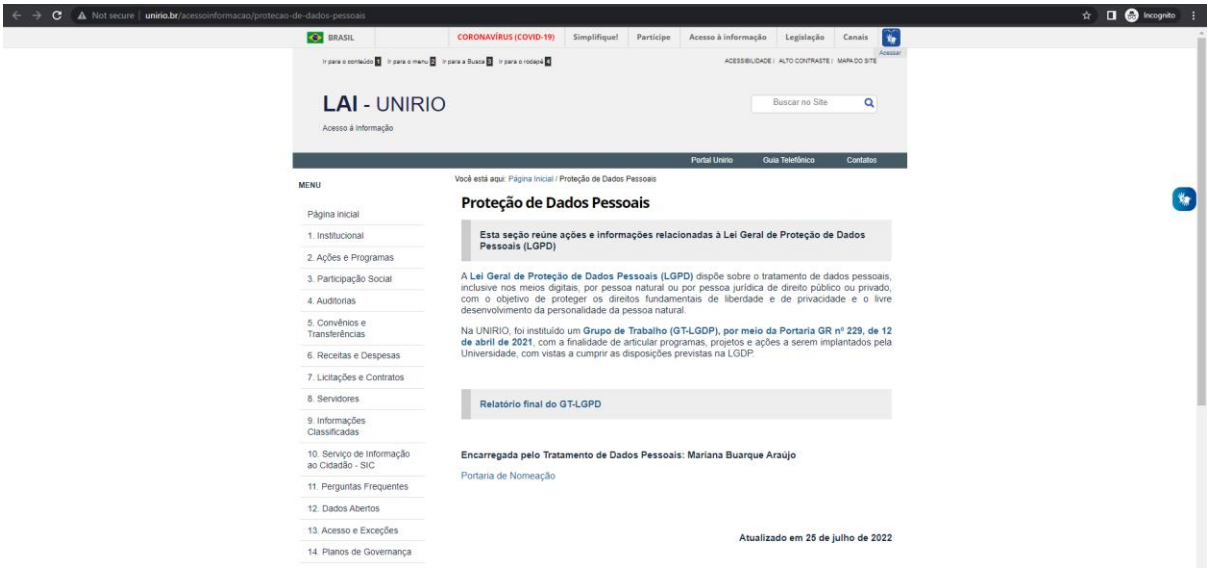
[10] Disponível em: <https://portal.ufrrj.br/ouvidoria/protecao-de-dados-pessoais/>. Acesso em: 20 jun. 2022.

4.5 Universidade Federal do Estado do Rio de Janeiro

No portal da UNIRIO (http://www.unirio.br/acessoinformacao/protecao-de-dados-pessoais) alguns critérios não foram atendidos. Por exemplo, apesar de o nome do Encarregado de Proteção de Dados ter sido publicado na página no dia 25 de julho de 2022, as informações de contato não foram fornecidas. Não foi localizada orientação para os requerimentos do usuário destacado no item 4 da análise.

A página apresenta materiais informativos da LGPD com explicações bem reduzidas: informa apenas o que é LGPD. Nenhum outro conceito da lei é discutido.

Figura 16 - Página de LGPD da UNIRIO



Fonte: Página de LGPD da UNIRIO[11]

Na UNIRIO, também foi criado um Grupo de Trabalho (GT) para realizar ações relacionadas à LGPD. Este grupo tinha formato multidisciplinar, sendo composto por servidores de diversas áreas: ensino, gestão de pessoas, tecnologia da informação, gestão de documentos, comunicação e acesso à informação. O GT-LGPD da UNIRIO elaborou um relatório que está disponibilizado para visualização na página de LGPD da referida instituição de ensino, através do link <http://www.unirio.br/acessoinformacao/arquivos/RelatrioFinalGTLGPD.docx.pdf>.

[11] Disponível em: <http://www.unirio.br/acessoinformacao/protecao-de-dados-pessoais>. Acesso em: 26 jul. 2022.

O Relatório Final do GT-LGPD foi aprovado no dia 16 de julho de 2021 e apresenta três tópicos: informações, alcance e plano de adequação.

O primeiro tópico apresenta informações gerais sobre a LGPD, e sobre a pesquisa realizada nos departamentos da instituição. Como diagnóstico, é mencionado que a maioria das unidades realizam tratamento de dados pessoais e dados pessoais sensíveis, porém, até aquele momento, ainda não seguiam as regras estabelecidas pela LGPD. O relatório apresenta o resultado da pesquisa de tratamento de dados na UNIRIO: o levantamento de informações das catorze unidades da instituição. Abaixo, é apresentada a síntese de algumas perguntas e respostas da pesquisa.

Unidade	Tratamento de dados pessoais	Sistemas em que dados pessoais estão armazenados	Compartilhamento de dados pessoais	Com quem é feito o compartilhamento
Reitoria	Sim	Google Drive, Google Forms, Excel	Sim	Servidores, Terceirizados, Site da unidade, universidades parceiras
Vice-Reitoria	Não	Google Drive	Sim	Servidores
PROGRAD	Sim	SIE	Sim	Servidores
PROPGPI	Sim	SIE, Sucupira	Não há certeza	Capes, MEC
PRAE	Sim	Google Drive, Google Forms, Excel	Sim	Servidores, Terceirizados, Site da unidade
PROPLAN	Sim	SIE, LDAP, GLPI, Google Drive	Sim	Servidores, empresas contratadas
PROAD	Sim	e-mail, Google Drive	Sim	Servidores, Terceirizados, empresas contratadas
PROGEPE	Sim	SIE, SIAPENET,	Sim	Servidores, Terceirizados,

		planilhas		Site da unidade
CCET	Sim	e-mail institucional, Google Drive institucional, SIE, portal de pesquisa e de extensão	Sim	Servidores
Arquivo Central	Sim	armazenamento local, Google Drive, excel	Sim	Servidores, Terceirizados
Biblioteca Central	Sim	RI Hórus, SophiA	Não	Não aplicável
Auditoria	Sim	armazenamento local, Google Drive, email	Sim	Servidores
CCJP	Sim	armazenamento local	Sim	Servidores
Ouvidoria	Sim	Fala.BR, e-mail institucional	Sim	Servidores

Tabela 2: Levantamento de informações na UNIRIO sintetizado pelo autor[12]

Através das respostas desta pesquisa, observa-se a necessidade de um alinhamento entre as unidades da instituição a respeito das medidas de proteção de dados. No questionário, é feita a pergunta se há procedimento estabelecido para mitigação de riscos nos tratamentos de dados pessoais, e cada unidade respondeu de forma distinta. Além disso, algumas respostas não pareceram claras, como por exemplo em relação ao entendimento de como e quando deve ser feita a solicitação de consentimento aos titulares, o que demonstra a necessidade de mais capacitação na área da LGPD e proteção de dados. Observa-se a resposta da Vice-reitoria que mencionou não haver o tratamento de dados pessoais, porém responderam aos outros itens sobre operações de tratamento, o que não deixou claro se a unidade lida com dados pessoais,

[12] Documento original disponível em: <https://docs.google.com/spreadsheets/d/1qLHl7lCxJ084DkssK0HSne-toQXI2DYc6hkUTwvIkVs/edit#gid=2127979727>. Acesso em: 26 jul. 2022.

ou somente com outros tipos de dados. Lembrando que o acesso e armazenamento são considerados pela LGPD como tratamento de dados pessoais.

Através da análise desta pesquisa, é percebida a necessidade da realização de um mapeamento do fluxo de dados na instituição e da instauração de um gerenciamento de riscos: aproximadamente 93% das unidades realizam o tratamento de dados pessoais, e aproximadamente 42% das unidades responderam que não existe ou que desconhecem procedimento para mitigação de riscos no tratamento destes dados.

Como segundo tópico do relatório do GT-LGPD, é apresentada a definição dos papéis de todos os atores envolvidos na LGPD, tais como os titulares de dados, os agentes de tratamento, o Encarregado de Proteção de Dados e a ANPD. Foi entendido que a UNIRIO realiza tratamento de dados pessoais dos seguintes papéis:

1. Alunos
2. Servidores
3. Terceirizados
4. Parceiros
5. Comunidade

A UNIRIO se enquadra como controladora, e o papel do operador pode ser composto por fornecedores, terceiros e/ou parceiros que possuam algum tipo de vínculo com a instituição e tenham acesso aos dados dos usuários.

Como terceiro tópico, são apresentados os objetivos do plano de adequação da instituição, sendo citado: a adequação dos procedimentos, processos ou tecnologias para a devida conformidade com a lei; e a capacitação dos colaboradores a fim de estarem aptos a garantir a privacidade dos dados. Também é mencionada neste tópico a intenção de prover transparência sobre o uso dos dados, proporcionar segurança jurídica em relação aos dados pessoais e uma maior consistência e qualidade destes dados. No relatório, foi considerado como importante para o processo de adequação da UNIRIO: a participação da alta gestão; o envolvimento das unidades; a qualidade da comunicação; a cultura organizacional da UNIRIO; a segurança da informação; e a implementação de uma gestão para riscos e incidentes.

Por fim, no quarto tópico foram apresentadas as considerações finais, concluindo que as ações a serem tomadas e a instauração do plano de adequação serão articulados após a designação e início do exercício do Encarregado de Proteção de Dados. Também foi sugerido a criação de um Comitê Permanente multidisciplinar para trabalhar juntamente a este Encarregado de Dados, a fim de elaborar, aplicar e monitorar o Plano de Adequação da LGPD na UNIRIO.

Perante a análise feita, é evidente a necessidade de melhorias na página destinada a LGPD no *website* da UNIRIO. O nome do Encarregado de Dados da instituição foi determinado de forma tardia considerando que a lei entrou em vigor no ano de 2020, e as informações de contato da mesma ainda não foram disponibilizadas. Ademais, não foi disposto ao público orientações de como realizar requisições que são amparadas pela LGPD nos direitos dos titulares. Ações relativamente simples de divulgação de informação poderiam incrementar a seção do *site* destinada aos assuntos de Proteção de Dados Pessoais.

4.6 Avaliação Final e sugestões para o website da UNIRIO

O resultado das análises realizadas nas páginas de LGPD nos *websites* das quatro Instituições de Ensino Superior Federais pode ser visualizado no quadro abaixo.

Item	Peso	**UFF**	**UFRJ**	**UFRRJ**	**UNIRIO**
1- Página destinada à LGPD	2	Sim	Sim	Sim	Sim
2- Página localizada em fácil acesso	1	Sim	Não	Não	Não
3- Informações do Encarregado de Proteção de dados	3	Sim	Sim	Não	Sim
4- Orientação para requerimento dos titulares de dados	3	Sim	Sim	Não	Não
5- Materiais informativos sobre a LGPD e direitos dos titulares	1	Sim	Sim	Sim	Sim
6- Política de privacidade na página de LGPD	1	Não	Não	Não	Não
7- Informação sobre a política de cookies	1	Sim	Não	Não	Não
Total avaliado*:	12	11	9	3	6

Total de critérios atendidos em porcentagem aproximada:	100%	92%	75%	25%	50%

Tabela 3: Avaliação final das instituições federais

*Acesso às páginas realizado no dia 20 de junho de 2022.

A partir das análises feitas nos meios de comunicação digital das quatro universidades, é possível observar que para uma instituição se adequar a LGPD, é imprescindível que haja meios de troca de informação entre os agentes de tratamento e os titulares dos dados. Além da adequação dos processos e da segurança da informação, é de suma importância a transparência por parte da instituição, e a demonstração das ações relacionadas à proteção dos dados pessoais. Afinal, é de responsabilidade do controlador a comprovação de que os direitos dos titulares estão sendo atendidos dentro da organização. Pelo conteúdo analisado foi percebido também a necessidade de um maior investimento na área de tecnologia das instituições, mais precisamente em Segurança da Informação.

A fim de solucionar os problemas identificados no portal de LGPD da UNIRIO, é proposto neste trabalho uma seção no site institucional que contemple os itens avaliados neste capítulo. É possível visualizar abaixo uma sugestão de interface para um Portal de LGPD da UNIRIO, que seria um importante recurso para a instituição, para a comunidade acadêmica e para o público externo.

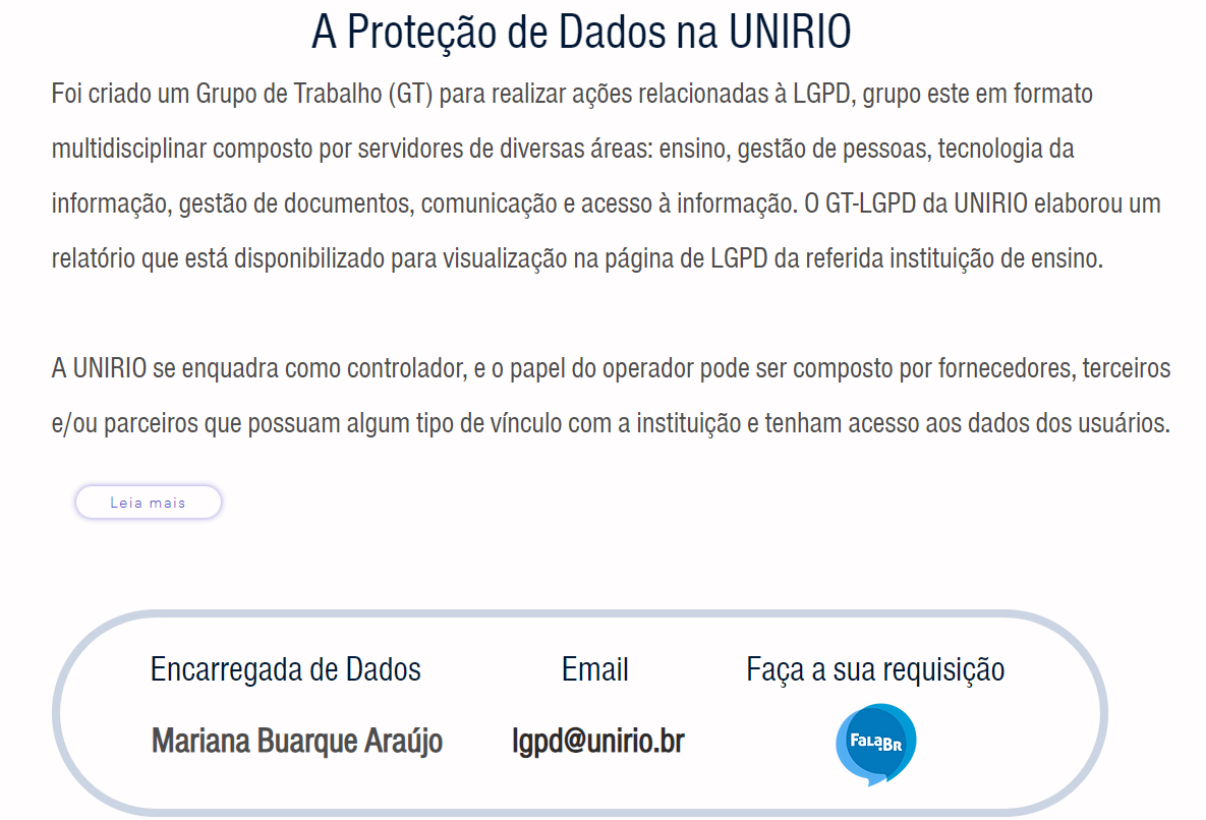
O *website* contemplaria os itens abordados neste capítulo de modo a proporcionar conteúdos informativos à comunidade, e atender aos critérios de exigência da LGPD. A iniciar com uma breve explicação a respeito desta lei, encaminhando para uma página com informações mais completas, incluindo sobre os direitos dos titulares.

Figura 17 - Protótipo para página de LGPD da UNIRIO

Fonte: Autoria própria

A seguir, é importante a divulgação de ações da própria instituição em relação à proteção de dados pessoais, disponibilizando informações de como está o andamento no processo de adequação à LGPD, e como a universidade se porta perante a disciplina de proteção de dados. Importante disponibilizar o contato do Encarregado de Proteção de Dados da instituição, e indicar por qual caminho os titulares podem fazer requisições e consultas em relação aos seus dados.

Figura 18 - Protótipo para divulgação de ações da UNIRIO



Fonte: Autoria própria

É uma excelente prática que o portal de LGPD disponibilize as normas e regras de privacidade de dados da instituição, e também a política de privacidade da mesma, pois estes conteúdos serão levados em consideração de forma positiva pela ANPD no caso de eventuais incidentes com os dados. Compartilhar conteúdos de capacitação, guias e cursos para a LGPD e proteção de dados é uma excelente atitude de serventia à comunidade, principalmente no âmbito de uma Universidade Federal. Ademais, por se tratar de uma Instituição de Ensino

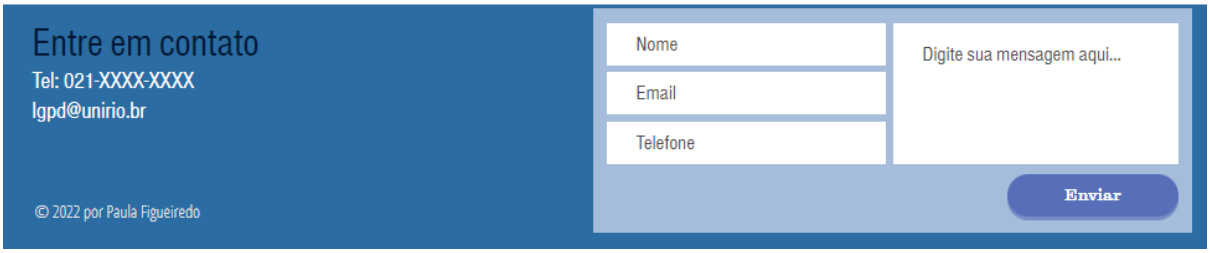
Superior, é muito útil que haja uma seção para a publicação de notícias, trabalhos e pesquisas na área da LGPD, proteção de dados e segurança da informação, que são assuntos muito discutidos e necessários na atualidade.

Figura 19 - Menu de conteúdos sobre a LGPD

Fonte: Autoria própria

Por fim, no rodapé, é sugerida uma área que contenha informações de contato dos administradores da página, ou do departamento designado.

Figura 20 - Rodapé da página de LGPD



Fonte: Autoria própria

Através da criação de um *website* semelhante, a UNIRIO manteria um portal destinado à LGPD, com informações transparentes da instituição, disponibilidade de educação e conhecimento à comunidade acadêmica e externa, e estaria em conformidade com alguns dos critérios e boas práticas existentes na legislação.

5. Conclusão

5.1 Considerações finais

Observa-se cada vez mais a aplicação multidisciplinar de conhecimentos do currículo da formação superior em Sistemas de Informação. Por conta dos recursos tecnológicos, a computação está sendo cada vez mais utilizada para o desenvolvimento e modernização de diversas áreas como a da saúde, da publicidade, financeira, dentre diversas outras. Devido a isso observa-se a integração da Tecnologia da Informação com outras áreas que em épocas passadas eram tratadas de forma totalmente separadas, e como consequência, esse fato ocasiona na necessidade da especialização multidisciplinar de muitos profissionais.

Neste trabalho, foi abordada a correlação entre as áreas do Direito e de Sistemas de Informação, que ganhou força nos últimos anos por conta do surgimento de legislações específicas que abordam o direito à proteção dos dados pessoais, como a GDPR na Europa e a LGPD aqui no Brasil. Apesar de um crescimento tecnológico exponencial, muitas organizações negligenciaram o âmbito da segurança e proteção de dados, resultando na necessidade de intervenção legislativa determinando regras para o uso dos dados pessoais da população. Este movimento regulatório possibilitou discussões que envolvem principalmente dois mundos, do direito e da T.I, trazendo consigo o surgimento de papéis que hoje são obrigatórios nas empresas.

Foram observados pontos de atenção de extrema importância para a adequação orgânica à LGPD: o mapeamento dos dados, a segurança da informação, o gerenciamento de riscos e a comunicação com os titulares dos dados pessoais. Para atuar em cada um desses pontos, é necessário o envolvimento de profissionais de múltiplas áreas e especializações, podendo então deduzir que, para se adequar corretamente à Legislação de Proteção de Dados, é importante o envolvimento da organização como um todo.

Para adequar os processos realizados com os dados pessoais, se torna necessária a visualização de como os dados transitam pela organização. Devido a isso, deduz-se a enorme importância de realizar o mapeamento dos dados pessoais, também conhecido como inventário de dados, no processo de adequação à lei. Entender como funciona a arquitetura dos bancos de dados, quais tipos de operações os sistemas possibilitam, além de quais são as transações manuais realizadas, é essencial para um eficiente processo de adequação à LGPD.

Pode-se dizer que a Segurança da Informação é um dos principais pilares da LGPD. Com as legislações de proteção de dados pelo mundo, houve um aumento da pressão nas empresas para se estar devidamente protegido. A lei de proteção de dados brasileira trouxe consigo obrigatoriedades no tema segurança da informação, as organizações necessitam aplicar bons padrões técnicos de segurança, além de demonstrar boas práticas de proteção de dados e privacidade, pois caso ocorra violação de dados as sanções e multas podem chegar a patamares altos.

Para uma organização estar devidamente protegida também é de extrema importância haver o gerenciamento de risco. Por mais que sejam feitos investimentos em tecnologia de ponta para a Segurança da Informação, ainda assim pode ocorrer violação ou vazamento de dados. Com isso, surge a necessidade de se estar preparado para incidentes de segurança, sendo encorajado o desenvolvimento de um plano de resposta a incidentes, contendo ações de remediação, investigação e comunicação às partes impactadas e a Autoridade Nacional de Proteção de Dados.

Para uma discussão mais aprofundada nos temas de governança e segurança de dados, é possível ressaltar o Trabalho de Conclusão de Curso de duas colegas da UNIRIO, Juliana Gonçalves e Sabrina Lapa, onde foi realizada uma análise dos impactos da LGPD sobre a governança e segurança de dados (SANTOS; SILVA, 2020).[13]

O uso correto do compartilhamento de informação sobre proteção de dados com os usuários de um produto ou serviço pode trazer benefícios no que condiz com a conformidade com a lei. Através do estudo realizado nos *websites* institucionais de quatro Universidades Federais, foi possível perceber a importância da comunicação apropriada nos meios digitais de uma instituição. O ato de disponibilizar certas informações pode ser visto como essencial para alguns aspectos da LGPD, sendo assim possível observar a importância da transparência por parte das organizações. Em termos gerais, os sistemas que de alguma forma executam qualquer tratamento de dados pessoais não poderão mais ser tratados como caixas pretas perante os seus usuários.

Através do estudo realizado ao longo do capítulo 4, foi possível dar destaque a duas das quatro instituições de ensino superior analisadas, são essas a UFF e a UFRJ. As duas demonstraram estar exercendo atitudes efetivas em relação à LGPD, em especial a UFF, que atendeu a 92% dos critérios selecionados.

[13] Disponível em: <https://bsi.uniriotec.br/publicacoes-de-tcc/>. Acesso: 16 ago. 2022.

A UFF, através de sua página de LGPD e de seu relatório geral, compartilhou muitas das informações exigidas e incentivadas pela lei. Ademais, a instituição está realizando um excelente trabalho de divulgação de informação, servindo à comunidade acadêmica conteúdos relevantes a respeito da proteção de dados pessoais.

A UFRJ, que apresentou os conteúdos de forma mais sucinta, atendeu a 75% dos critérios em sua página de LGPD demonstrando engajamento em relação ao tema.

A UFRRJ apresentou uma porcentagem baixa nos itens avaliados, o que levanta pontos de atenção em relação à LGPD por parte desta insituição federal. Algumas ações em seu portal eletrônico faria a instituição demonstrar um melhor processo de adequação à LGPD, tais como informações a respeito do Encarregado Proteção de Dados e orientações para requerimento dos titulares.

A UNIRIO atendeu a 50% dos critérios levantados neste estudo, mostrando espaços para melhoria. Ações de atualização em seu portal fará com que a instituição demonstre um maior engajamento em relação à LGPD, como por exemplo, orientações para solicitações dos titulares de dados. Conforme ressaltado neste trabalho, para a correta adequação é de extrema importância uma comunicação clara e efetiva entre a organização e o público.

5.2 Trabalhos futuros

Para trabalhos futuros existem diversas áreas de Sistemas de Informação que podem ser correlacionadas com o tema Proteção de Dados Pessoais e LGPD. É possível aprofundar este tema em praticamente qualquer área relacionada a dados e segurança da informação. Diversas tecnologias são dependentes de grandes volumes de dados para funcionarem ou serem desenvolvidas como por exemplo Big Data, Machine Learning, Inteligência Artificial. Ademais, é possível realizar estudos e pesquisas sobre como a Internet das Coisas está cada vez mais inserida no cotidiano das pessoas, e sobre como isso implica na proteção de dados. A LGPD trouxe consigo a proibição de discriminação por tratamento automático de dados pessoais, o que possibilita uma relação com debates e estudos sobre viés na Inteligência Artificial. Também é sugerida a realização de um estudo sobre a aplicação da LGPD nas principais redes sociais.

Como ideia de desenvolvimento de tecnologias, é possível a criação de um sistema para anonimização de dados pessoais, a criação de uma plataforma para empresas que viabilize ao

titular o controle dos seus dados pessoais, ou um estudo sobre a integração de práticas de *Privacy by Design* com modelos ágeis de desenvolvimento de *software*, dentre outras possibilidades existentes para estudo e desenvolvimento.

Além disso, é sugerido para trabalhos futuros o desenvolvimento de uma ferramenta que realize testes de LGPD em sites e aplicações, podendo ser criada uma avaliação própria para a ferramenta a partir de questionários com especialistas da área.

Referncias Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação, Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27701: Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Rio de Janeiro, 2019.

BIONI, B.R. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. 3ª edição. Rio de Janeiro: Forense, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 de outubro de 2021.

CARDOSO, O.V. A Proteção de Dados na Prática [livro eletrônico]. 1º edição. Volume 1. Xangri-Lá: Edição do Autor, 2021.

CIEB. CENTRO DE INOVAÇÃO PARA A EDUCAÇÃO BRASILEIRA. Manual de Proteção de Dados para Gestores e Gestoras Públicas Educacionais. São Paulo: CIEB, 2020. E-book.

D'AVILA, A.V.G.; SILVA, B.F.; ARAUJO, T.V. LGPD: muito além da Lei : Uma análise do direito em conjunto com a segurança da informação. Gvtech Soluções em Tecnologia da Informação Ltda. 2021.

DONDA, D. Guia prático de implementação da LGPD: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

GT LGPD UFF. Relatório Final GT-LGPD UFF. Portaria nº 68.038/2021. Disponível em <https://www.uff.br/sites/default/files/relatorio_final_gt_lgpd_-_marco_de_2022.pdf>. Acesso em 20 de Junho de 2022.

GT LGPD UNIRIO. Relatório Final GT-LGPD UNIRIO. Portaria nº 441. Disponível em <http://www.unirio.br/acessoinformacao/arquivos/RelatrioFinalGTLGPD.docx.pdf>. Acesso em 20 de Junho de 2022.

HATHAWAY, T.; HATHAWAY, A. Data Flow Diagrams - Simply Put!: Process Modeling Techniques for Requirements Elicitation and Workflow Analysis (Advanced Business Analysis Topics Book 5) (p. 23). BA-EXPERTS. 2016.

KUCK, D. Ano marcado por ciberataques eleva verba de proteção. Disponível em: <https://valor.globo.com/empresas/noticia/2021/12/22/ano-marcado-por-ciberataques-eleva-verba-de-protecao.ghtml>. Acesso em: 04 de Abril de 2022.

MASTROPASQUA, R. LGPD: empresas já veem retorno do investimento. Disponível em: <https://valor.globo.com/legislacao/coluna/lgpd-empresas-ja-veem-retorno-do-investimento.ghtml>. Acesso em: 21 de Janeiro de 2022.

MONTES, E. Introdução ao Gerenciamento de Projetos: Como gerenciar projetos pode fazer a diferença na sua vida. 1ª Edição, 2017. Publicado por Kindle Direct Publishing.

NETO, J.L.S. A proteção de dados pessoais na era da informação: 2020.

PINTO, D.G. A proteção de dados alçada a direito fundamental na Constituição brasileira. Disponível em: <https://www.conjur.com.br/2022-fev-17/douglas-pinto-protecao-dados-alcada-direito-fundamental>. Acesso em: 03 de maio de 2022.

QUINTILIANO, L. Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 04 de maio de 2022.

SANTOS, J.G.; SILVA, S.L.C. Análise dos impactos da Lei Geral de Proteção de Dados Pessoais sobre a governança e segurança de dados. Rio de Janeiro, 2020.

SILVA, D.C.; AROUCA, A.C. Manual da Lei Geral de Proteção de Dados para Instituições de Ensino [livro eletrônico]. 1ª edição. Brasília: 2020. PDF.

XAVIER, F.C. LGPD no setor público: Boas práticas para a jornada de adequação. 2022.