UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JHONY WESLEY MARQUES

ANÁLISE DO NÍVEL DE ADERÊNCIA À LGPD NO SETOR PÚBLICO

TOLEDO

2022

JHONY WESLEY MARQUES

ANÁLISE DO NÍVEL DE ADERÊNCIA À LGPD NO SETOR PÚBLICO

Analysis of the level of adherence to the LGPD in the public sector

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Sistemas para Internet do Curso de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Ivan Luiz Salvadori

TOLEDO

2022

JHONY WESLEY MARQUES

ANÁLISE DO NÍVEL DE ADERÊNCIA À LGPD NO SETOR PÚBLICO

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Sistemas para Internet do Curso de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 08 de dezembro de 2022

Prof. Dr. Ivan Luiz Salvadori
Orientador/Presidente
COTSI-TD/ UTFPR-TD

Prof. Dr. Fábio Engel de Camargo
Avaliador 1
COTSI-TD/ UTFPR-TD

Prof. Dr. Thiago Henrique Pereira Silva
Avaliador 2
COTSI-TD/ UTFPR-TD

TOLEDO

2022

RESUMO

No Brasil, com grande frequência vemos notícias sobre o desrespeito à proteção de dados e como as empresas privadas e públicas estão em passos lentos para implementar os controles previstos na Lei Geral de Proteção de Dados do Brasil(LGPD). Este trabalho apresenta uma análise técnica sobre o nível de adequação das organizações públicas para com a LGPD. A análise considera o relatório publicado pelo TCU em 2022, que contém uma pesquisa feita junto a 382 órgãos públicos. Os resultados demonstrados no relatório foram preocupantes, colocando o risco na segurança de dados em um nível alarmante. Este trabalho também apresenta uma relação de ferramentas que podem auxiliar o setor público a adequar-se à LGPD. Com base nas ferramentas selecionadas, traça-se um paralelo entre o relatório do TCU, as ferramentas e outras possíveis soluções que podem corrigir o panorama de proteção de dados nos órgãos públicos.

Palavras-chave: lgpd; gdpr; aderência; setor público; compliance.

ABSTRACT

In Brazil, we often see news about disrespect for data protection and how private and public companies are taking slow steps to implement the controls provided for in the General Data Protection Law of Brazil (LGPD). This work presents a technical analysis on the level of adequacy of public organizations towards the LGPD. The analysis considers the report published by TCU in 2022, which contains a survey carried out with 382 public bodies. The results demonstrated in the report were worrisome, putting the data security risk at an alarming level. This work also presents a list of tools that can help the public sector to adapt to the LGPD. Based on the selected tools, a parallel is drawn between the TCU report, the tools and other possible solutions that can correct the data protection scenario in public bodies.

Keywords: lgpd; gdpr; public sector; compliance; adherence.

LISTA DE FIGURAS

Figura 1 – Resposta para a Pergunta 2.2. Fonte: (UNIÃO, 2022) **27**
Figura 2 – Resposta para a Pergunta 3.1. Fonte: (UNIÃO, 2022) **28**
Figura 3 – Resposta para a Pergunta 3.2. Fonte: (UNIÃO, 2022) **29**
Figura 4 – Resposta para a Pergunta 3.5. Fonte: (UNIÃO, 2022) **30**
Figura 5 – Resposta para a Pergunta 4.1. Fonte: (UNIÃO, 2022) **30**
Figura 6 – Resposta para a Pergunta 4.2. Fonte: (UNIÃO, 2022) **31**
Figura 7 – Resposta para a Pergunta 5.2. Fonte: (UNIÃO, 2022) **32**
Figura 8 – Resposta para a Pergunta 6.1. Fonte: (UNIÃO, 2022) **32**
Figura 9 – Resposta para a Pergunta 6.3. Fonte: (UNIÃO, 2022) **33**
Figura 10 – Resposta para a Pergunta 6.4. Fonte: (UNIÃO, 2022) **34**
Figura 11 – Resposta para a Pergunta 7.1. Fonte: (UNIÃO, 2022) **34**
Figura 12 – Resposta para a Pergunta 7.2. Fonte: (UNIÃO, 2022) **35**
Figura 13 – Resposta para a Pergunta 9.1. Fonte: (UNIÃO, 2022) **36**
Figura 14 – Resposta para a Pergunta 9.2. Fonte: (UNIÃO, 2022) **37**
Figura 15 – Resposta para a Pergunta 9.4. Fonte: (UNIÃO, 2022) **37**

LISTA DE TABELAS

Tabela 1 – Principais Diferenças entre GDPR e LGPD 13

Tabela 2 – Tabela de ferramentas e seus suportes para cada ponto 38

SUMÁRIO

1 INTRODUÇÃO 7
1.1 Considerações iniciais 7
1.2 Motivação e Justificativa 7
1.3 Contribuições 8
1.4 Objetivos 8
1.4.1 Objetivo geral 8
1.4.2 Objetivos específicos 8
1.5 Estrutura do trabalho 8
2 REFERENCIAL TEÓRICO 10
2.1 LGPD 10
2.2 GDPR 10
2.3 Principais diferenças 11
2.4 Classificação dos dados 14
2.5 Princípios 14
2.6 Fiscalização 15
2.7 Orientação e Prevenção 16
2.8 Sanções 17
3 REVISÃO DA LITERATURA 18
4 FERRAMENTAS PARA SUPORTE À LGPD 20
4.1 Privacytool 20
4.2 Ecomply 21
4.3 GestaoXLGPD 22
4.4 dpomax 24
4.5 Onetrust 25
5 ANÁLISE DA ADERÊNCIA DA LGPD NO SETOR PÚBLICO 27
5.1 Principais pontos que foram analisados 27
5.2 Comparação das ferramentas 37
6 CONCLUSÃO 40
REFERÊNCIAS 41

1 INTRODUÇÃO

1.1 Considerações iniciais

A Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018), criada em 2018, alterou a forma com que empresas brasileiras e estrangeiras coletam e processam dados no território brasileiro. Em vigor a partir de setembro de 2020, obriga todas as empresas a investirem em segurança da informação, pois para se adequarem a lei várias medidas técnicas e administrativas devem ser tomadas para garantir a proteção de dados pessoais. Este é um processo difícil de ser rapidamente implementado, visto que não se trata apenas de aumentar a segurança, deve-se mudar toda a cultura e paradigma da empresa e seus funcionários no que diz respeito à proteção de dados.

1.2 Motivação e Justificativa

De acordo com relatório do Banco Mundial (DENNER *et al.*, 2021), o Brasil tornou-se o 7º país mais digitalizado no mundo, na frente dos Estados Unidos da América e Canadá sendo o país mais digitalizado das Américas. Diante disso, a grande circulação na internet de dados pessoais pode atrair crimes cibernéticos, fazendo com que as medidas técnicas de segurança sejam aumentadas. Segundo o relatório The Global Risks Report (MCLENNAN; GROUP; GROUP, 2021) apresentado todo ano no Fórum Econômico Mundial, apontou o aumento de ataques cibernéticos como o principal risco para os próximos anos. A circulação de dados na Web está em crescimento. Os crimes cibernéticos acompanham este crescimento, especialmente o sequestro de dados.

Na pandemia(COVID19), tanto no Brasil quanto em vários outros países tiveram um grande aumento do trabalho à distância e na circulação dos dados pessoais online sem a necessidade do comparecimento da pessoa física com documentos. Atraindo pessoas mal intencionadas que buscam explorar as vulnerabilidades encontradas na proteção dos dados podendo alterar, vender ou fazer fraudes de dados. Para solucionar esse e outros casos que a LGPD colabora exigindo a adoção/melhorias dos mecanismos de segurança de dados pelas empresas. Mesmo com o fim de pandemia(COVID19), diversas empresas privadas e públicas ainda estão com altas demandas para se adequar a LGPD. Diversos setores ficaram com as suas demandas com dificuldades de serem supridas o que gerou uma quantidade grande de empresas que ainda estão irregulares e isso se agrava no setor público onde 76,7% de 382 órgãos federais não adotam a LGPD e 24% não têm sequer uma política de segurança da informação.

De acordo com o relatório (UNIÃO (2022)) auditado e realizada pelo Tribunal de Contas da União((TCU, 2022)), comandada pela Secretaria de Fiscalização de TI (Sefti). Foi enviado no primeiro trimestre de 2021 para 382 órgãos federais utilizando um questionário de 60 perguntas,

com os temas de: “preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção”.

Diante do diagnóstico exposto sobre o alto risco à privacidade de dados pessoais coletados pelo governo, o TCU decidiu cobrar o Gabinete de Segurança Institucional da Presidência da República (GSI) para que sejam tomadas providências sobre esses problemas. No dia 15 de junho de 2022 o TCU publicou o Acórdão Nº 1384/2022, no qual traz um longo discurso para que o governo federal procure sanar a situação.(NARDES, 2022)

1.3 Contribuições

Este trabalho busca contribuir com o aumento na proteção de dados e adequação à LGPD para com o setor público. Apresenta uma análise técnica sobre o relatório disponibilizado pelo TCU(UNIÃO, 2022), sob a perspectiva técnica do ponto de vista de gestão de informações e projetos.

1.4 Objetivos

1.4.1 Objetivo geral

O principal objetivo deste trabalho é identificar o grau de adequação da LGPD no setor público, mostrando o perigo que as organizações estão gerando para os titulares de dados, junto a soluções e ferramentas que podem ajudar a solucionar o problema de proteção de dados no Brasil.

1.4.2 Objetivos específicos

Realizar uma análise do relatório disponibilizado pelo TCU, identificando os principais pontos críticos, apontando a importância da adequação, junto das possíveis metodologias e ferramentas para a adequação à LGPD. Identificar ferramentas de software que podem ser utilizadas no auxílio das organizações no setor para adequação a LGPD a partir de pontos selecionados no relatório do TCU que é objeto deste estudo.

1.5 Estrutura do trabalho

Este trabalho está organizado da seguinte forma:

- Capítulo 1 - Introdução: apresenta a contextualização e descreve o problema abordado pelo trabalho, além de apresentar a motivação e justificativa.
- Capítulo 2 - Referencial Teórico: Apresenta os conceitos fundamentais para o entendimento deste trabalho.
- Capítulo 3 - Revisão da Literatura: descreve os trabalhos relacionados relevantes à pesquisa.
- Capítulo 4 - Ferramentas para suporte à LGPD: Apresenta ferramentas que auxiliam na adequação para com a LGPD.
- Capítulo 5 - Análise da aderência da LGPD no setor público: Apresenta a análise proposta.
- Capítulo 6 - Conclusão: apresenta as conclusões, contribuições, limitações e trabalhos futuros.

2 REFERENCIAL TEÓRICO

2.1 LGPD

No Brasil existem várias normas legais federais que de múltiplas formas se cruzam criando assim uma estrutura legal que lida com a proteção de dados e privacidade, entretanto essas leis trabalham setorialmente regulamentando de forma específica cada setor como bancos, direitos do consumidor entre outros.

Já a LGPD que está em vigor desde 2020, traz a regulamentação de como os dados pessoais devem ser coletados e tradados no Brasil visando integrar os inúmeros cenários regulatórios abrangendo tudo nesta lei referente a proteção de dados. Todavia a LGDP não substituirá as outras leis em casos específicos em que a LGPD não contempla o caso na totalidade. As outras leis ainda devem ser utilizadas, como, por exemplo, no caso do MCI (Marco Civil da Internet) que abrange outras áreas como a garantia da liberdade de expressão e liberdade na rede.(REPúBLICA, 2014)

Assim como outras leis, o MCI anda lado a lado à LGPD, e elas sofrem mudanças conjuntas para não existirem lacunas umas com as outras que possam ser utilizadas por pessoas para colocar em risco a segurança dos dados. Como a lei visa proteger os dados das pessoas naturais/físicas, todo e qualquer pessoa que detém os dados de outras estão sujeitos a LGDP.

Em fevereiro de 2022 a Proposta de Emenda Constitucional Nº 17 (PEC-17) foi aprovada e transformada na Emenda Constitucional 115/2022, inserindo a proteção de dados na constituição federal, e por isso a LGPD passa a ser regida pelo governo federal, podendo ser julgada na Suprema Corte Federal (STF) pois agora o descumprimento da LGDP passa a ser inconstitucional. Como resultado, a lei agora possui superioridade em comparação às leis municipais, estaduais ou gerais referente ao tema.(BRASIL, 2022)

2.2 GDPR

Quando a LGPD foi idealizada, ela teve uma grande influência na *General Data Protection Regulation* (GDPR), sendo a lei de regulamentação de dados europeus que pertence à Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Os europeus foram um dos pioneiros na idealização de uma lei de proteção de dados e a GDPR é uma das mais completas em termos legais e estruturais sobre privacidade virtual. A GDPR tem como base o respeito à individualidade dos usuários e a inviolabilidade dos dados, garantindo ao titular direito de ceder consentimento total e inequívoco, que precisa ser claro e explícito antes da coleta e uso de seus dados, podendo ser revogado a qualquer momento.

O Brasil já iniciou o processo para a entrada na OCDE que é formada por países desenvolvidos que favorecem o comércio entre si, o que pode trazer muitos benefícios econômicos

para o Brasil caso consiga entrar. Entretanto, um dos requisitos é ter uma lei de proteção de dados pessoais operante, pois as quando o país se tornar integrante a OCDE novas pessoas passariam a ter seus dados coletados e processador pelo governo ou empresas brasileiras. Obviamente os países pertencentes à OCDE já tem leis para garantir a privacidade dos dados e para o Brasil fazer parte da OCDE também deve garantir a segurança dos dados.

Entendendo que para a GDPR, dados pessoais são definidos como qualquer dado que se relaciona a uma pessoa física identificada ou identificável, logo qualquer informação que possa ser usada para identificar uma pessoa direta ou indiretamente é um dado pessoal.

2.3 Principais diferenças

A LGPD por ser baseada na GDPR tem muita similaridade, entretanto por ser uma lei criada para ser aplicada de forma regional no Brasil existem algumas diferenças Monteiro Odélio Porto Junior (2018),Parliament (2016). As diferenças entre a LGPD e a GDPR podem ser melhor explicitadas como demonstrado na Tabela 1.

Diferenças		
Assunto	**GDPR**	**LGPD**
Dados pessoais	Especifica que a lei se aplica independentemente de sua nacionalidade e residência.	Não especifica explicitamente que se aplica a pessoas independente de sua nacionalidade e residência.
Territorial	Nesse setor a lei se aplica até a empresas que mesmo residindo em outro país, mas esteja de alguma forma monitorando comportamentos de indivíduos da UE.	No setor extraterritorial a LGPD não se aplica a atividades que de alguma forma monitoram o comportamento dos indivíduos do Brasil, apenas na coleta e processamento de dados do indivíduo que no momento da coleta estejam dentro do território brasileiro.
Dados	Ela se aplica a dados se eles fazem parte de algum sistema de arquivamento. Ela não trata especifica quando dados anônimos são utilizados para criação um perfil pessoal.	Se aplica a qualquer tipo de processamento de dados. Os dados anônimos quando utilizados para formular um perfil que identifica uma pessoa individual, pode ser considerado dado pessoal.

Anonimização ou Pseudonimização	Trata-se como dado pessoal se a anonimização ou pseudoanonimização de alguma forma pode-se identificar o usuário através de dados adicionais.	Prevê que em estudos relacionados a saúde pública as entidades responsáveis possam ter acesso aos dados pessoais, contando que seja estritamente para realizar estudos e pesquisas em ambientes controlados e seguros. Se possível com anonimização ou pseudoanonimização dos dados. As instituições devem ser órgãos ou pessoas jurídicas da administração pública ligada direta, ou indiretamente a uma pessoa jurídica sem fins lucrativos que legalmente esteja de acordo com a lei, sediada e com jurisdição no Brasil. Que tenha como objetivo a pesquisa básica ou aplicada, histórica, tecnológica, científica ou estatística.
Controladores e processadores	Deve haver um contrato/ato jurídico vinculando o controlador ao processador, onde se define todos os aspectos de processamento, os direitos e obrigações do controlador.	Na LGPD é mais simples, pois determina apenas que o processador deve realizar o processo conforme as instruções do controlador que posteriormente verifica as conformidades do processo, não havendo nenhum contrato ou ato legal sobre o processo.
Crianças	Especifica que o consentimento da criança apenas se aplica em casos de serviços da sociedade da informação, por exemplo, em casos de marketing, ou na criação de usuários de perfis. A idade mínima estipulada é de 16 anos, entretanto alguns países podem diminuir essa idade até no mínimo 13 anos.	Estipula a idade minima de 13 anos. Em casos específicos como para a proteção da criança ou para contato com os pais e representantes, é possível coletar os dados, sem o armazenamento ou compartilhamento dos dados. Em casos de jogos, aplicativos ou atividades mediante a fornecimento de dados de crianças deve ser condicionado a dados estritamente necessários para a atividade.

Pesquisa	O processamento para fins de arquivo de interesse público, científico ou fins de pesquisa deve-se cumprir um propósito, e que não deve infringir os direitos de privacidade dos indivíduos o prejudicando.	Os dados podem ser processados apenas para pesquisas científicas sem fins lucrativos, apenas por "órgãos de pesquisa". Deve ser um órgão ou pessoa jurídica da administração pública ligada direta ou indiretamente, e pessoa jurídica sem fins lucrativos que legalmente esteja de acordo com a lei. Deve ser sediada e com jurisdição no Brasil que tenha como missão ou objetivo pesquisa básica ou aplicada de forma histórica, tecnológica, científica ou estatística. E conforme a LGPD titulares de dados não podem revogar quando o processamento for para fins de pesquisa.
Base legal	(1) Em procedimentos legítimos realizados por uma fundação, associação ou órgão sem fins lucrativos com objetivo político, religioso, sindical ou filosófico, sob a condição que o processamento se refere exclusivamente aos membros, ex-membros ou pessoas com contato regular do órgão consoante com seus propósitos, e que os dados não sejam divulgados para fora desse órgão sem consentimentos dos titulares dos dados.(2) Tratamento de dados pessoais, que são tornados públicos pelo titular dos dados.	(1) Para realizar investigações.(2) Para o exercício de processos judiciais e administrativos.(3) Para os profissionais da saúde ou entidades.(4) Quando necessário para proteção de crédito, com o intuito de evitar fraudes, tanto na utilização dos dados de uma pessoa quanto para a instituição evitar a fraude.
Direitos dos indivíduos	Estipulam um prazo de 1 a 2 meses para resolver a qualquer requisição feita por um titular de dados.	A requisição de um titular de dados deve ser respondida imediatamente, se não for possível imediatamente deve-se informar para o titular o motivo e o tempo para a resolução.
Compensação por danos	Especifica como que os danos devem ser compensados.	Não especifica como os danos devem ser compensados, permitindo que seja utilizado o Código Civil Brasileiro que não estabelece limite ou metodologia, baseando-se apenas na jurisprudência.

Tabela 1 – Principais Diferenças entre GDPR e LGPD

2.4 Classificação dos dados

No contexto da LGPD os dados são classificados da seguinte forma:

- **Dados pessoais:** São os dados que possibilitam a identificação direta ou indireta da pessoa natural como CPF, renda, IP, e-mail, foto, etc.
- **Dados sensíveis:** São dados de menores de idade ou dados que revelam etnia, religiões, opiniões políticas ou filosóficas. Esses dados tem que ter um tratamento mais severo, podendo apenas ter acesso mediante ao consentimento explícito junto a um fim bem definido, pois o vazamento desses dados pode gerar consequências mais graves.
- **Dados públicos:** Estes dados tem como finalidade considerar a boa-fé e o interesse público que justificaram a sua disponibilização. Os dados também podem tratados novamente sem o consentimento do usuário, pois já foi concedido posteriormente e sendo necessário um novo consentimento apenas em casos de compartilhamento de dados entre organizações.
- **Dados Anonimizados:** Utilizando uma técnica de processamento de dados consegue-se remover ou modificar os dados de forma que não se possa identificar a pessoa e nesse caso a LGPD não se aplica.

2.5 Princípios

A LGPD possui inúmeros princípios nos quais devem-se fundamentar a realização de tratamento dos dados pessoais, são eles:

- **Finalidade:** Os processos de coleta e tratamento dos dados devem-se ser legítimos, específicos e explicitados em seus propósitos para que o titular dos dados possa consentir o todo o processo.
- **Adequação:** Esse princípio refere-se ao contexto do tratamento dos dados para a finalidade sob o qual foi consentido pelo titular.
- **Necessidade:** O tratamento deve-se limitar a sua finalidade utilizando apenas os dados pertinentes e proporcionais exigidos pela finalidade acordada.
- **Acesso livre:** Garantia de acesso livre, gratuito e facilitado aos dados do titular junto a forma e a duração do tratamento dos seus dados.
- **Qualidade dos dados:** Garantia de exatidão, clareza, relevância e atualização dos dados de acordo com a finalidade e necessidade para o tratamento dos dados.

- **Transparência:** Garantia que os titulares terão informações claras, precisas e facilmente acessíveis sobre os tratamentos e responsáveis.
- **Segurança:** Exigência de que medidas técnicas e administrativas de seguranças serão aplicadas para proteger os dados pessoais para não serem indevidamente acessados.
- **Prevenção:** Adoção de medidas de prevenção a danos causados pelo tratamento dos dados.
- **Não discriminação:** Não permite que o tratamento dos dados seja utilizado para fins discriminatórios, ilícitos ou abusivos.
- **Responsabilização e prestação de contas:** Deve-se demonstrar pelos controladores ou operados que todas as medidas eficazes para garantir a proteção dos dados foram cumpridas com comprovação do comprimento da lei.

Logo, garantir a segurança e a proteção de dados é o que deve ser feito pelos detentores de dados. Utilizando as boas práticas junto ao levantamento dos requisitos exigidos pela LGPD deve-se conseguir se encaixar na lei. Entretanto, não é fácil conseguir seguir todas as regras, uma vez que isso é necessário contratar empresas especializadas ou fazer um treinamento junto a um especialista para modificar todo o sistema da empresa e adaptá-lo à lei. Esse é um dos desafios para conseguir se adequar à lei, visto que muitas empresas são pequenas e não possuem recursos para esta destinação.

2.6 Fiscalização

Em 29 de outubro de 2021 foi publicada a Resolução CD/ANPD Nº 1/2021 no Diário Oficial da União, onde aprovava o regulamento para o processo de fiscalização e sancionatório no âmbito de competência da Autoridade Nacional de Proteção de Dados Pessoais(ANPD (2020)).(BRASIL, 2021).

O regulamento tem como objetivo estabelecer os procedimentos a serem seguidos no processo de fiscalização e regras a serem contempladas no processo administrativo sancionador da ANPD. A fiscalização compreende o monitoramento, orientação, atuação preventiva e repressiva à LGPD. No artº 4 traz o conceito de atuação, denúncia e petição titular, que devem ser comunicadas à ANPD por qualquer pessoa natural ou jurídica sobre suposta infração ou conduta de obstrução de atividade de fiscalização.

O artº 4 também estabelece os "agentes regulados"esses agentes são responsáveis por tratar os dados ou integrantes do processo de tratamento de dados pessoais. Além disso tem como dever fornecer cópia de documentos, dados e informações relevantes para a avaliação das atividades de tratamento de dados no prazo, local, formato e demais condições estabelecidas pela ANPD. O agente deve permitir o acesso às instalações e sistemas de toda a empresa ou

de terceiros que estejam em seu poder e que foram utilizados no processo de tratamento dos dados junto aos prazos e datas.

As empresas devem manter todas as informações sobre a coleta e tratamento de dados durante os prazos estabelecidos na lei. Essas informações devem ser disponibilizadas sempre que for requisitado junto a representantes aptos para oferecer suporte à atuação da ANPD. Os prazos de procedimentos administrativos ou comunicados serão contabilizados em dias úteis, começando a ser contados a partir do conhecimento oficial do agente de tratamento, sendo também comunicado aos titulares de dados todo o processo e como podem ser afetados.

Deve-se submeter a auditorias realizadas ou determinadas pela ANPD, podendo o agente de tratamento de dados pessoas acompanhar a auditoria resguardado os casos em que não é avisado da auditória ou não seja possível o acompanhamento. Em caso de todos os deveres previstos na resolução não forem cumpridos, poderá acarretar uma obstrução da fiscalização com agravamento nas sanções.

Importante dizer que a ANPD, na competência fiscalizatória, poderá atuar não apenas de ofício mediante a denúncias, mas também em ocorrências periódicas de fiscalização, podendo ser de forma coordenada com órgãos e entidades públicas ou autoridades de proteção de dados internacional ou transnacional.

No artº 24, a ANPD estabelecerá e divulgará os meios para recebimento dos requerimentos. A admissibilidade será realizada pela Coordenação-Geral de Fiscalização que vai aferir os pontos elencados no artº 25 se fazem presentes, lembrando que denúncias anônimas caso seja verificada a verossimilhança das alegações podem ser recebidas e processadas.

2.7 Orientação e Prevenção

Visando orientar e prevenir na resolução Brasil (2021), o artº29 prevê que a ANPD promoverá a elaboração e disponibilização de guias para boas práticas e modelos de documentos para serem utilizados. São previstas também a realização de treinamentos e cursos, elaboração de ferramentas de autoavaliação de conformidade e riscos para serem utilizados pelos agentes de tratamento, reconhecimento e divulgações de padrões técnicos e regras de boas práticas e governacia.

No que tange a prevenção, a ANPD poderá tomar medidas em divulgar informações relevantes e dados setoriais, avisos ou solicitação de regularização, junto a informações suficientes, medidas preventivas e resolução de problemas para o agente de tratamento possa identificar e regularizar em prazos determinados ou determinar que seja elaborado um plano de conformidade.

2.8 Sanções

Se instaurado um processo administrativo o agente de tratamento será intimado e deverá apresentar a defesa no prazo de até 10 dias úteis. Compete ao autuado provar culpa ou não dos fatos que foram alegados contra ele. Caso o processo seja deferido as sanções serão impostas pela ANPD tendo em acordo com o art. 52. As sanções podem ser a advertência indicando um prazo para adequação de medidas corretivas. Multa simples ou diária de até 2 por cento do faturamento anual limitando-se ao total de R$ 50.000.000,00 por infração.

Pode também haver outras punições como bloqueio dos dados pessoais até a sua regularização, eliminação dos dados pessoais, suspensão parcial do funcionamento do banco de dados ou suspensão total do banco de dados. Outra ação que ser tomada pela ANPD é a publicização da infração após feito devida apuração e confirmação da sua ocorrência, que acarretaria em perda de confiança pela população com a empresa, tendo em vista que se for divulgado quem iria confiar em uma empresa que não está de acordo com a lei.

As sanções impostas serão consideradas de "boa-fé"ou "má-fé"da empresa. Em casos em que a empresa fez tudo o que podia para evitar o vazamento, será levantado se as ações da empresa foram corretas ou não para pesar no agravamento ou não nas sanções impostas:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas;

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Como a lei abrange todo e qualquer pessoa que detém dados de terceiros, logo os órgãos e as entidades públicas sofrerão punições previstas na LGPD salvo as sanções monetárias.

3 REVISÃO DA LITERATURA

Botelho (2022) aborda de forma jurídica a LGDP como norma protetiva dos direitos dos dados da pessoa natural, bem como as responsabilidades tanto do setor privado como também o público que devem respeitar os princípios previstos na LGPD integralmente e cumprir os requisitos e solicitações de dados da pessoa natural apenas em casos que a finalidade pública e o interesse público estejam presentes, até mesmo nos casos de banco de dados seja de acesso público.

Celidonio, Neves e Doná (2020) aborda procedimentos metodológicos baseando-se na ISO/IEC 27701/2019 que contém orientações e mapeamentos para a implementar os requisitos e controles necessários na LGPD. Nele também sugere itens adicionais como outros padrões para implementações que mapeiam requisitos de privacidade. Juntando as normas de boas práticas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013, ISO 27018 e ISO 29100, foi elaborada uma metodologia que contem 3 fases, cada uma com 2 etapas a serem executadas. O resultado mostrou que dos 325 pontos analisados a metodologia atendou 117 pontos de forma plena, 67 de forma parcial e em 141 não atendeu os requisitos determinados pela LGPD. O trabalho mostra que mesmo aplicando a metodologia baseada em algumas normas de boas práticas que já existem no mercado os resultados não são satisfatórios. Pois em 43% dos pontos analisados ainda seguem desprotegidos ou desprovidos de mecanismos de defesa.

De acordo com Ferreira *et al.* (2022) existem inúmeras vantagens na utilização de ferramentas e métodos no auxílio da organização e visualização de conceitos que devem ser seguidos para que os requerimentos da LGPD sejam cumpridos. No artigo foi proposto a necessidade de criar um método mais visual apontando os principais pontos a serem seguidos, foi escolhido o framework canvas como ferramenta para criação do modelo e utilizando como base o Business Model Canvas criado por Alex Osterwalder e Yves Pigneur junto a 470 praticantes de todo o mundo que oferece uma tela simples e visual a ser seguido para projetar e inovar em um modelo de negócio. Seguindo assim a proposta de utilizar o framework canvas e o modelo de Alex Osterwalder, os autores propõem um modelo para LGPD no canvas com nove processos, que devem ser executados para que alcançar o nível de segurança exigido pela LGPD. Os processos são: (1) Dados pessoais; (2) Origem; (3) Cronograma; (4) Objetivo; (5) Base legal; (6) Direitos; (7) Transferência, (8) Armazenamento; e (9) Segurança.

Ferreira *et al.* (2022) faz também uma pesquisa com 216 profissionais de todas as regiões do país com um questionário de 10 perguntas abordando os processos de implantação da LGPD nas empresas. Foram analisadas e confrontadas com a teoria estudada e o resultado foi que 66,2% das empresas já estão em processo de adequação com a LGPD. Entretanto apenas 60,2% acredita que o framework canvas criado ajudaria na adequação do projeto, e o mais preocupante é que apenas 9% acredita que a empresa tem um alto nível de maturidade quando se trata de proteção de dados, pois isso se reflete na cultura interna da empresa. Uma vez

que apenas 53,7% das pessoas receberam treinamento sobre a LGPD mostrando que ainda estamos em passos iniciais nos projetos de adaptação da LGDP.

Magacho e Trento (2021) responde a algumas questões sobre em *compliance*(Estar em conformidades com a lei) na administração pública no Brasil, que como todos sabemos no tocante à administração não pode ser levado como referência. As políticas de boa governança tem como foco o fortalecimento da confiança dos cidadãos com a gestão estatal. Também busca uma melhor gerência e o aprimoramento gerencial para o estabelecimento de uma segurança mínima pela governança publica. Entretanto, temos um grande desgaste da sociedade com as instituições públicas, geradas por vários escândalos de má gestão que descredibiliza as instituições.

Magacho e Trento (2021) propõem que primeiro de tudo, deve haver um comprometimento maior do setor público mudando a cultura e o cenário de boa governança. Um dos passos apontados é procurar capacitar as pessoas para atuarem como encarregadas reformulando assim a forma de como armazenamos dados no setor público. O setor publico coletam muitos dados sensíveis, em alguns casos os bancos de dados estão sobrecarregados, portando é recomendado que sejam reanalisados e se necessário descartá-los ou atualizá-los cumprindo as normas da LGDP.

Além disso, adotando o *compliance* é necessário fazer manutenções de rotina e avaliações para informar possíveis problemas e impactos, planejando ações para prevenir ou mesmo corrigir futuros problemas e vazamentos. Apesar do o *compliance* ser mais utilizado em empresar privadas, ela pode ser facilmente empregada no setor público, visto que a LGPD deve ser cumprida por todos e seria ideal que o setor público desse o exemplo.

O problema é que apenas a LGDP e o compliance não garantem a proteção dos dados do usuário. É essencial o evolvimento e comprometimento dos agentes públicos, junto ao monitoramento e criação de parâmetros de controle dos dados como exigidos na lei. Caso a lei seja infringida deve-se responsabilizar os operadores e controladores do tratamento de dados.

4 FERRAMENTAS PARA SUPORTE À LGPD

4.1 Privacytool

PrivacyTech é uma empresa brasileira que fornece uma plataforma chamada Privacy tool que faz o gerenciamento da privacidade de forma modular. A ferramenta é pensada para diversos setores do mercado cumprindo as obrigações das legislações LGPD e GDPR.

A ferramenta apresenta o seguinte conjunto de módulos:

- Data Mapping
    1. Pode criar e gerenciar o ciclo de vida dos dados.
    2. Bases legais.
    3. Mapeamento dos riscos dos seus fornecedores.
    4. Modelos prontos para aplicar diagnósticos como ISO27001, NIST, em transferências de dados para terceiros.
    5. Crie e edite modelos para emissão de análises de impacto.
    6. API com autenticação OAuth2 para desenvolvedores automatizarem o data mapping.
    7. Organize e gerencie as atividades da sua equipe.
- Gestão de Incidentes - Avisos automatizados em casos de violação às leis, com identificação da violação e relatorio.
- Data discovery - automatização na busca e classificação dos dados pessoais com mapeamento de dados.
- Open Finance - Gestor de consentimento dos titulares para o compartilhamento de dados pessoais.
- Gestão de Auditoria - Funcionalidade para passar por uma auditoria através de conformidades escolhidas baseada em modelos de normas e controles.
- Gestão de cookies - Gestão de Cookies da Privacy Tools para manter o website em conformidade.
- Gestão de Políticas - Esse gestor tem o foco na criação de um modelo de políticas e normas para personalizar e integrar ao seu site ou software.
- Gestão de Consentimento - Gestor para gerenciar, registar ou renovar os consentimentos dos titulares de dados.

- Pedidos dos titulares - Funcionalidade de gestão de atendimento especializada nos direitos do titular dos dados.
- Portal da Privacidade - Permite criar um espaço para comunicação e exibição dos dados coletados e consentimento conferidos.

Os planos e valores são apresentados, ou disponibilizados, apenas mediante a cadastro/consultoria. A empresa permite teste gratuito da ferramenta por 5 dias. Empresas que utilizam a ferramenta:

- SICOOB
- BoaVista SCPC
- Grupo RBS
- Banco RCI

Mais detalhes sobre esta ferramenta podem ser obtidos no site do desenvolvedor: https://privacytools.com.br/

4.2 Ecomply

Ecomply é uma empresa alemã que fornece uma ferramente web de gerenciamento de proteção de dados que auxilia na construção e operação de uma empresa, cumprindo as legislações GDPR, LGPD e NDPR no tocante de proteção de dados. Os dados são armazenados de forma segura, no pacote padrão os dados são em armazenados em um data center com certificação ISO27001 com backups redundantes e precisos em Frankfurt, Alemanha. Nos pacotes de nível mais avançados é possível contratar outros data centers e backups personalizados.

Funcionalidades:

- LogBook - Rastreio automático de todas as alterações feitas no sistema.
- Registro de Atividades de Tratamento - Podendo ser compartilhado e de fácil acesso, com filtros e buscas eficientes.
- Controle de processos - Possibilidade de administrar contratos e fornecedores.
- Gestão de Incidentes - Registro de ocorrências de incidentes e documentação de como foram resolvidos.
- Gestão de Requisições - Processa requisições de titulares de dados de forma profissional.

- Gestão de Medidas Técnicas e Organizacionais - Documentação de Medidas Técnicas e Organizacionais envolvendo as pessoas corretas.
- Assistente de Auditorias - Relatórios de auditoria são salvos, com emissão de relatório automático.
- Colaboração - Funcionalidade para trabalho em equipe com atribuição de tarefas, discussões, comentários e lembretes.
- Dashboard - Para o gerenciamento de clientes de forma efetiva.
- Branding - Funcionalidade para customização/inclusão da sua marca e identidade no software e relatórios.

O plano mais básico oferece todas as funcionalidades descritas acima. O que muda de um plano para o outro é a escalabilidade das funcionalidades, tendo em vista que empresas grandes com muitos funcionários necessitam de maior número de funções como, por exemplo, limite de quantos funcionários pode utilizar o sistema, número de impressões de relatórios, utilização de APIs, etc. O valor aumenta para cada customização adicionada.

1. Pequenas empresas - R$ 4500/ano.
2. Médias empresas - R$ 8750/ano
3. Corporação - valor deve ser consultado, pois varia diante as necessidades.
4. Parceiro / Grupo - valor deve ser consultado, pois varia diante as necessidades.

Empresas que utilizam a ferramenta:

- Technical University of Munich
- Otovo
- Ultrax Aerospace
- I-Sec

Mais detalhes sobre esta ferramenta podem ser obtidos no site do desenvolvedor: https://www.ecomply.io/brasil/home

4.3 GestaoXLGPD

GestaoXLGPD é um software desenvolvido pela empresa Brasileira EMX Tecnologia que oferece todas as funcionalidades necessárias para entrar em conformidade com a LGPD. Conjunto de ferramentas:

- Gerenciamento completo do projeto à adequação.
    1. Gerenciamento de riscos.
    2. Gerenciamento do consentimento do titular.
    3. Gerenciamento de incidentes de violação de dados pessoais.
    4. Gerenciamento dos termos de entrega e aceite de documentos.
    5. Gerenciamento de contratos em observância à LGPD.
    6. Gerenciamento eletrônico de documentos obrigatórios exigidos pela lei.
- Registro e Auditorias
    1. Mapeamento das atividades de tratamento.
    2. Suporte para auditorias de conformidade com a LGPD e a ISO 27001.
    3. Portal da privacidade do titular e gestão de notificações – autoridade, titular, controlador e operador.
- Relatórios e Dashboards.
    1. Avaliação de impactos à proteção de dados.
    2. Boas práticas de governança.
    3. Dashboards.
    4. Relatórios gerenciais e analíticos para controle e manutenção da conformidade.
- Tem opção de terceirização do DPO(encarregado pelo tratamento de dados) pela EMX.

Os planos disponíveis são: GestãoX-LGPD básico: R$99,00 para micro e pequenas empresas. GestãoX-LGPD Completo valor informado apenas por meio de Consulta.

Empresas que utilizam a ferramenta:

- Rodan Serviços Ltda
- Labtest Diagnóstica S.A

Mais detalhes sobre esta ferramenta podem ser obtidos no site do desenvolvedor: https://emxtecnologia.com.br/gestao-x-lgpd/

4.4 dpomax

DPOMAX White Label é um software desenvolvido pela empresa Brasileira DPO MAX, que permite a gestão personalizada customizável para adequação de sua empresa à LGPD. Ele é todo organizado para percorrer a toda a jornada de adequação em cada um desses pontos: diagnósticos, controles de segurança e privacidade, inventário de dados, gestão de risco, relatório de impacto, trilha de auditoria e metodologia certificada. A empresa garante celeridade, competitividade, valor, reputação, segurança da informação e compliance para sua empresa.

Funcionalidades:

- Evidências e rastreabilidade.
- Diagnóstico LGPD.
- Varredura passiva de sites com relatório e orçamento para correção.
- Módulo de mapeamento de dados para todas as fases propostas pela ANPD.
- Módulo RIPD/DPIA para atribuição de responsáveis para cada função.
- Gestão de riscos e BI(processo de coleta e transformação de dados em informação clara e valiosa) visando resultados.
- Implementação ISO/IEC 27.701 para a adequação do sistema de gerenciamento de informação e privacidade.
- Sistema customizável.
- Disponibiliza os requisitos para registro das operações que envolvam dados pessoais, para controladores e operadores.
- Comunicação de Incidentes de Segurança.
- Cláusulas completas da LGPD para leitura.
- *STATUS SERVER* para monitoramento de falta de serviço.
- Assinaturas eletrônicas e digitais.
- Disponibilizamos assinaturas digitais com validade jurídica.
- Gestão de incidentes de segurança.
- Gestão de projetos de LGPD.
- Estruturação de contratos.
- Gestão de tarefas Kanban.

- Gestão de *Tickets* para suporte.
- Painel de controle com os principais gráficos com fácil entendimento.
- Planos de assinatura eletrônica/digital.
- Apontamento de contratos e pagamentos.
- Biblioteca para disponibilizar módulos de conhecimento.
- Segurança da informação.
- Log de usuários/auditoria.
- *Tracking* das ações.
- Suporte avançado.
- Integrações de sistemas (API).

A variação dos preços de cada pacote muda pelo tamanho da empresa.

1. BASIC - R$ 1.099,00 empresa com até 3 cnpj, 50 funcionários e 5 usuarios do software.
2. PRO - R$ 1.967,00 empresa com até 6 cnpj, 100 funcionários e 5 usuarios do software.
3. PREMIUM - R$ 2.967,00 empresa com até 10 cnpj, 500 funcionários e 10 usuarios do software.
4. GOLD - R$ 4.967,00 empresa com até 20 cnpj, 1000 funcionários e 30 usuarios do software.

Mais detalhes sobre esta ferramenta podem ser obtidos no site do desenvolvedor: https://dpomax.com.br

4.5 Onetrust

Onetrust é uma empresa do Reino Unido e conta com um software que auxilia na automatização da sua organização para com a LGPD. Desde a recolha de consentimento válido até à recepção e cumprimento dos pedidos de direitos dos titulares de dados. A automatização citata é feita por uma inteligência artificial(IA) que em alguns pontos ajuda na organização, identificação, mapeamento de dados, etc.

Funcionalidades:

- Simplificação das solicitações de titulares de dados e automatização todas as fases do processo, incluindo registro, verificação de identidade, descoberta de dados, exclusão e resposta segura.

- Gerenciamento de consentimento com banco de dados.
- Configuração e incorporamento facilitado aos centros de preferências voltados para o usuário.
- Gerenciamento, criação e distribuição das políticas e avisos voltadas para o publico ou para os funcionários da empresa.
- Busca e classificação os dados em dados estruturado ou não estruturados na nuvem, local ou sistemas.
- Vinculação de dados aos usuários identificados.
- Mapeamento dos inventários de dados para documentação do fluxo de dados internos e transferências para terceiros.
- Gerenciamento de risco interno e do fornecedor de dados.
- Modelos de autoavaliação com relatórios de risco automatizado.
- Com PIAs, PbD e avaliações de fornecedores voltadas ao seu mapa de dados para obter visibilidade total dos fluxos de dados e riscos associados.
- Rastreamento, gerenciamento e relatórios de incidentes.
- Vinculação de incidentes com o mapa de dados para entender melhor o risco e a gravidade do incidente.
- Funcionalidade de acompanhamento sobre a maturidade em relação aos requisitos da LGPD e outras leis e estruturas globais de privacidade e segurança.
- Funcionalidade de comparação da sua organização com outras semelhante por tamanho, setor e região.

Os planos e valores apenas mediante a cadastro/consultoria.
Empresas que utilizam a ferramenta:

- Oracle
- Reclameaqui
- Unimed
- Electrolux

Mais detalhes sobre esta ferramenta podem ser obtidos no site do desenvolvedor: https://www.onetrust.com/solutions/brazil-lgpd-compliance/

5 ANÁLISE DA ADERÊNCIA DA LGPD NO SETOR PÚBLICO

5.1 Principais pontos que foram analisados

O relatório analisado faz parte de uma auditoria realizada pelo TCU previamente avisado com três meses de antecedência no primeiro trimestre de 2021. Foram feitas 60 perguntas que foram respondidas por 382 organizações públicas federais, trilhando o caminho para o *compliance* foram selecionados alguns pontos de extrema importância para garantir a segurança dos dados.

- **Ponto 1**

  Pergunta: A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?

  Análise: A organização é de extrema importância na elaboração de um projeto. Para iniciar o processo de adaptação da LGPD, recomenda-se um planejamento prévio, logo a organização deve documentar as informações inerentes a aplitação da lei, como: o que será feito, quais recursos serão utilizados, quem serão os responsáveis por cada etapa, quando será iniciado e concluído, etc.

  No gráfico apresentado pela Figura 1, fica demonstrado que apenas 51% das organizações iniciaram algum processo de adequação da lei e produziram algum tipo de artefato. Planos de ação e planos de projeto já fazem parte do cotidiano de desenvolvedores e projetistas de software, não deveria ser nenhuma novidade para funcionários e responsáveis em proteger os dados dos titulares. Entretando, metade das organizações nem mesmo elaboraram um plano de projeto mostrando o grande risco que os titulares de dados estão correndo.

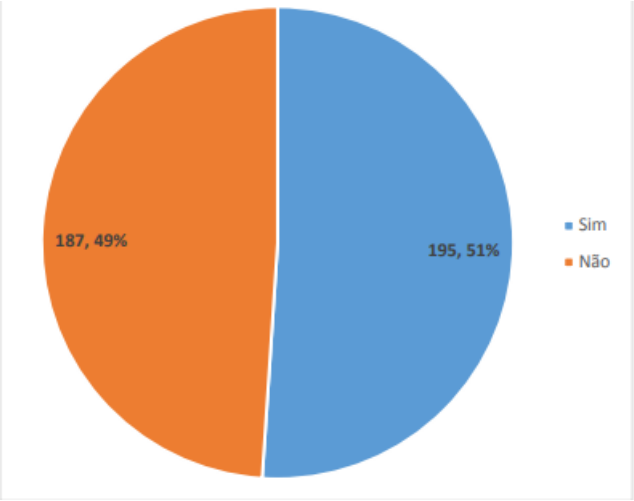

Figura 1 – Resposta para a Pergunta 2.2. Fonte: (UNIÃO, 2022)

- **Ponto 2**

  Pergunta: A organização conduziu iniciativa para identificar outros normativos, além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?

  Análise: Quando se está almejando um *complience* deve-se ter conhecimento de todas as leis relacionadas ao tratamento de dados pessoais e não apenas a LGPD que é uma entre muitas, portanto deve-se estar ciente de outros fatores que possam influenciar os aspectos de proteção de dados: como leis federais, leis trabalhistas, código de defesa do consumidor, etc, essas leis todas têm relação ao tratamento de dados pessoais e devem ser cumpridas pelas organizações.

  No gráfico da Figura 2, demonstra que a maioria das organizações, 76%, conduziu iniciativas para identificar esses normativos. Percebe-se então que as organizações mesmo se estiverem de acordo com a LGPD poderão infringir as outras leis vigentes no país. Do ponto de vista da privacidade/proteção de dados, pode presentar perigo aos titulares de dados, recomenda-se que sejam identificados os normativos correlatos e que sejam aplicados junto as normas estabelecidas na LGPD.

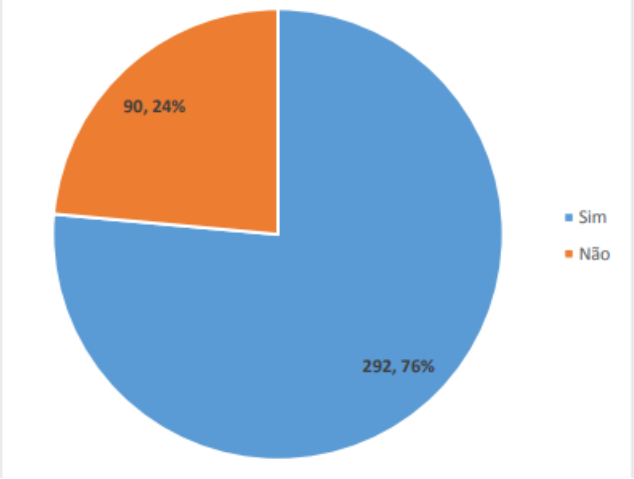

Figura 2 – Resposta para a Pergunta 3.1. Fonte: (UNIÃO, 2022)

- **Ponto 3**

  Pergunta: A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?

  Análise: Quando se está fazendo o tratamento de dados, eles estão relacionados a um titular que é uma pessoa natural, entretanto existem diversas categorias para esses titulares, como: cidadão, cliente, servidor público, representante de fornecedor e terceirizado.

  No gráfico apresentado pela Figura 3, constatou que 77% das organizações não identificaram todas as categorias dos titulares de dados com quais eles mantêm relacio-

namento. Quando se está tratando dados devemos categorizá-los para que cada um receba o devido tratamento especificado, como citado na LGDP. Pois essa identificação é importante para auxiliar no planejamento dos controles de cada categoria, uma vez que cada uma delas deve ter um tratamento diferente. Por exemplo dados de crianças e adolescentes que contém controles mais rigorosos no tratamento destes dados.

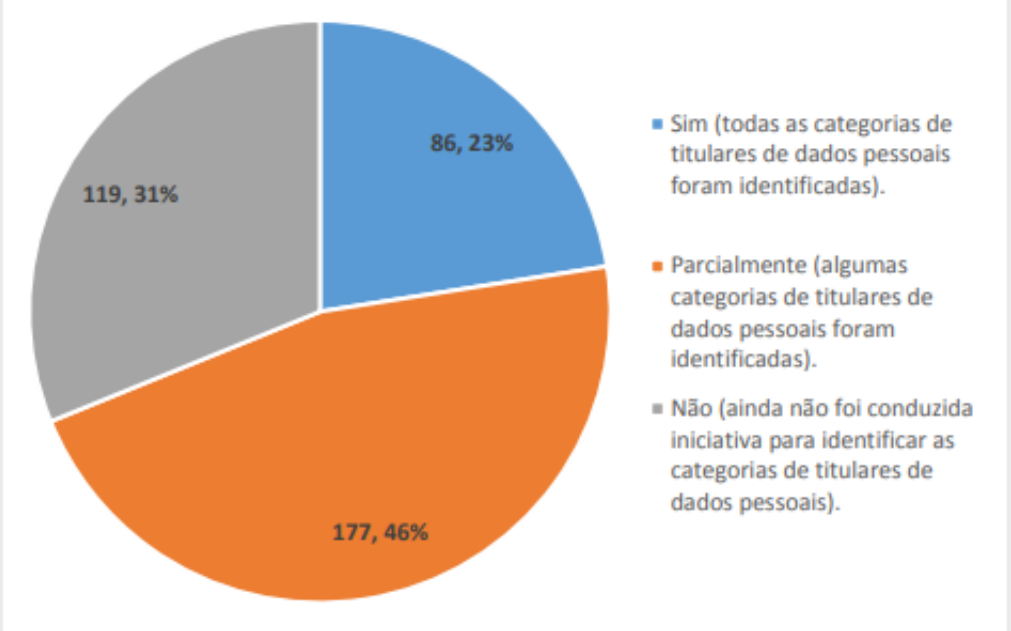

Figura 3 – Resposta para a Pergunta 3.2. Fonte: (UNIÃO, 2022)

- **Ponto 4**

  Pergunta: A organização identificou os processos de negócio que realizam tratamento de dados pessoais?

  Análise: Quando se está realizando o tratamento de dados pessoais, varias operações podem estar acontecendo, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. A LGPD é aplicável a todo tratamento de dados pessoais que deve-se manter registro.

  No gráfico apresentado pela Figura 4, constatou que 17% das organizações identificaram todos os processos que realizam tratamento de dados pessoais. Logo é de suma importância a identificação dos processos, pois a partir dela que é possível avaliar os riscos de cada processo e identificar informações relevantes como: o propósito do tratamento, a base legal que justifica esse tratamento e as categorias de titulares de dados envolvidas.

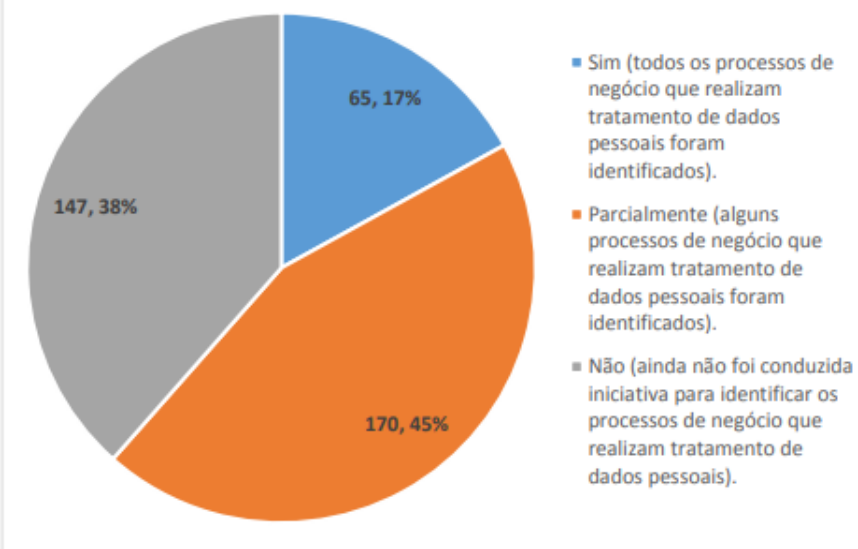

Figura 4 – Resposta para a Pergunta 3.5. Fonte: (UNIÃO, 2022)

- **Ponto 5**

  Pergunta: A organização possui Política de Segurança da Informação ou instrumento similar?

  Análise: A Segurança da informação é um das bases que possibilita a proteção de dados pessoais, logo é de suma importância que as organizações estabeleçam a sua política de segurança para poderem utilizá-las para gerenciar os objetivos de segurança de informações acordado com as leis de segurança.

  No gráfico apresentado pela Figura 5, podemos observar que 24% das organizações não possuem Política de Segurança da Informação ou instrumento similar. O resultado é preocupante, pois a política de segurança é um dos pilares que sustenta a proteção de dados pessoais, como apontado na NBR ISO/IEC 27002 que pode ser utilizada como referência para as organizações na hora de escrever sua política de segurança.

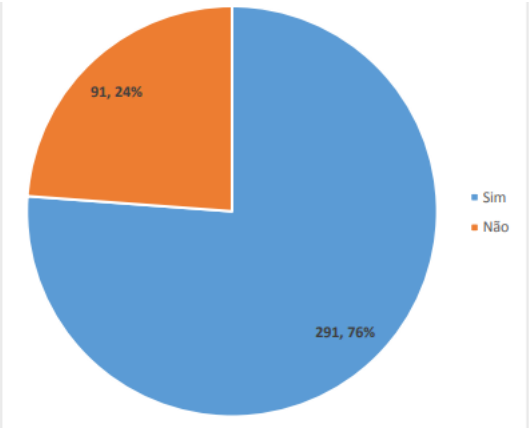

Figura 5 – Resposta para a Pergunta 4.1. Fonte: (UNIÃO, 2022)

- **Ponto 6**

  Pergunta: A organização possui Política de Classificação da Informação ou instrumento similar?

  Análise: A classificação da informação é importante para a proteção de dados pessoais, portanto viabiliza que estes sejam identificados e tratados adequadamente. Cada tipo de dado tem cuidados específicos em seu tratamento, pois dados sensíveis como origem racial, religião, opinião política, entre outros devem ser tratados de forma mais firmes quando vinculados a uma pessoa natural.

  O gráfico apresentado pela Figura 6 mostra que 35% das organizações possuem política de classificação da informação. Como apontado no gráfico a classificação deve ser contemplada pela organização. Dados sensíveis podem acabar gerando graves danos aos titulares dos dados, trazendo uma exposição maior ao titular podendo acarretar em danos na vida social e profissional.

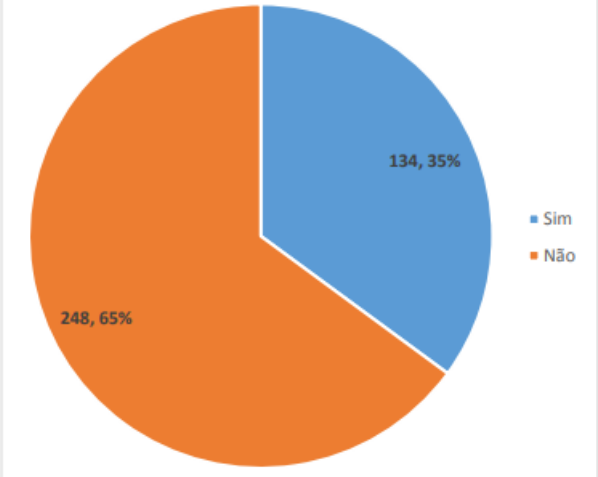

Figura 6 – Resposta para a Pergunta 4.2. Fonte: (UNIÃO, 2022)

- **Ponto 7**

  Pergunta: Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?

  Análise: Responsáveis que estão diretamente envolvidos a atividades que realizam o tratamento de dados não necessitam obrigatoriamente ter treinamento sobre a LGDP em específico, apenas treinamento para a função que ele atua que seria proteção e tratamento de dados.

  No gráfico apresentado pela Figura 7, é possível observar que apenas 10% das organizações treinou os colaboradores que estão diretamente envolvidos em atividades de tratamento de dados pessoais. Infelizmente esse numero é preocupante, dessa forma mesmo que o funcionário tenha conhecimento na área de proteção de dados isso não

seria o bastante visto que a LGPD é uma lei brasileira com diretrizes específicas que devem ser respeitadas e como os responsáveis vão fazer isso sem o conhecimento da mesma.

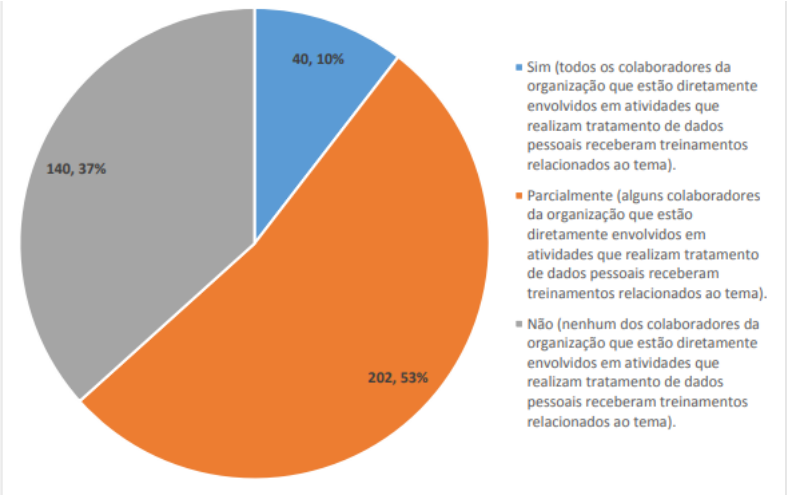

Figura 7 – Resposta para a Pergunta 5.2. Fonte: (UNIÃO, 2022)

- **Ponto 8**

  Pergunta: A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?

  Análise: No gráfico apresentado pela Figura 8, podemos observar que apenas 11% das organizações identificaram e documentaram todas as finalidades das atividades de tratamento de dados pessoais. Para que dados não sejam coletados de forma indevida ou tratados para finalidades erradas deve-se documentar e identificar as finalidades para qual aquele dado foi coletado e como ele vai ser utilizado, como o *complience* exige.

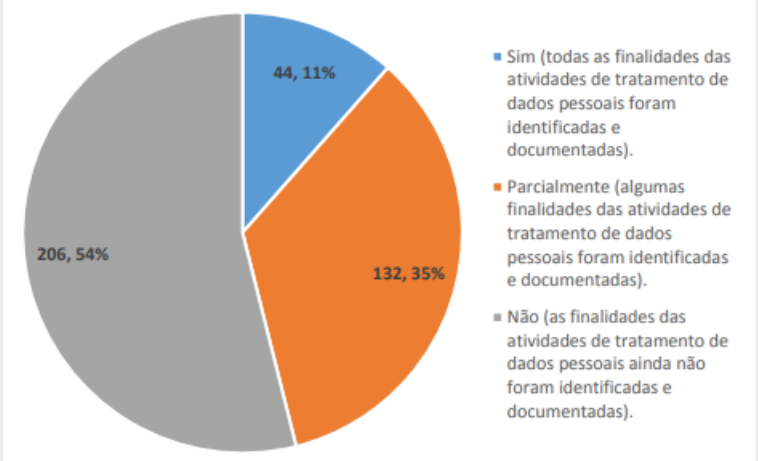

Figura 8 – Resposta para a Pergunta 6.1. Fonte: (UNIÃO, 2022)

- **Ponto 9**

  Pergunta: Há um registro instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?

  Análise: Quando falamos do controlador e o operador, eles são os responsáveis em manter registro das operações de tratamento de dados pessoais que realizam. Na LGPD é bem claro que deve-se manter registros de todas as operações feitas para posteriormente, se necessário, serem relatadas ou informadas para determinada finalidade.

  O gráfico apresentado pela Figura 9, mostra que 82% das organizações não possuem um registro instituído das informações relacionadas às características das atividades de tratamento de dados pessoais. Os registros são muito importantes, pois impactam em uma investigação apontando os responsáveis pela infração da lei.

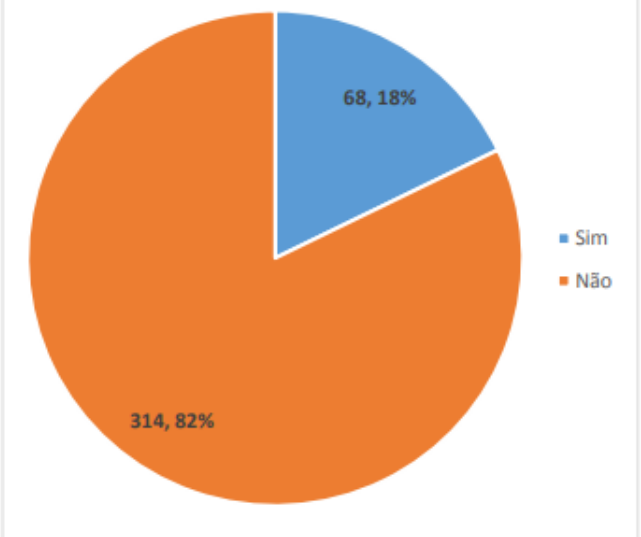

Figura 9 – Resposta para a Pergunta 6.3. Fonte: (UNIÃO, 2022)

- **Ponto 10**

  Pergunta: A organização elaborou relatório de impacto à proteção de dados pessoais?

  Análise: Como mostra o gráfico da Figura 10, foi demonstrado que somente 2% das organizações elaboram RIPD que abrange todos os processos de tratamento de dados pessoais que podem gerar riscos aos titulares. Seguindo boas práticas de segurança e proteção de dados como a NBR ISO/IEC 27701 é recomendado que seja criado um relatório de impacto contendo riscos gerados pelo tratamento dos dados, avaliando os principais pontos críticos como tipos de dados pessoais tratados, local de armazenamento desses dados e para onde os dados podem ser transferidos, para poder ser utilizado como base no desenvolvimento de medidas de segurança.

- **Ponto 11**

  Pergunta: A organização possui Política de Privacidade?

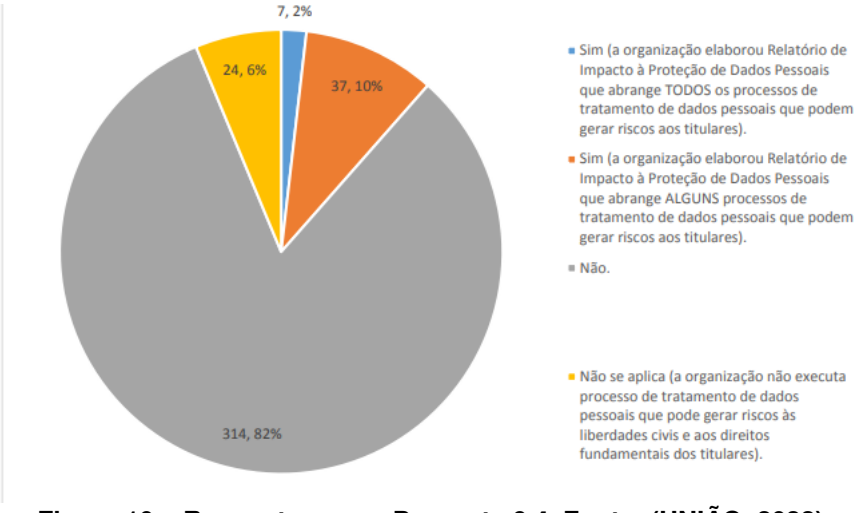

Figura 10 – Resposta para a Pergunta 6.4. Fonte: (UNIÃO, 2022)

Análise: No gráfico apresentado pela Figura 11, vemos que 75% das organizações ainda não elaboraram o artefato demonstrando que não é dada a devida transparência ao titular de como os seus dados pessoais são tratados. Quando falamos de transparência é recomendado que a organização determine, documente e forneça aos titulares de dados pessoais, de forma clara e facilmente acessível, informações que identifiquem o controlador de dados pessoais e que descrevam o tratamento de seus dados pessoais. Também é mencionado que as informações devem ser fornecidas em tempo hábil e de forma concisa, completa, transparente, inteligível e facilmente acessível, usando uma linguagem curta e clara, apropriada ao público-alvo. Convém que essas informações sejam reunidas em um documento que deverá ser endereçado aos usuários de seus serviços e sistemas. Em concordância com a LGPD, a política de privacidade deve estar disponível em veículos de fácil acesso.

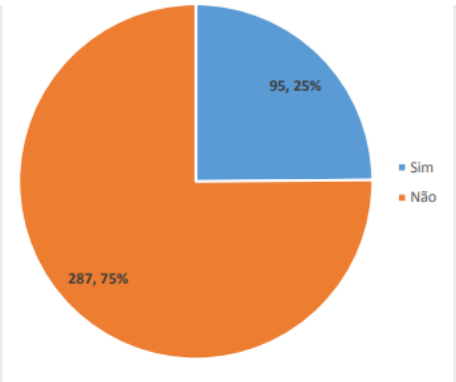

Figura 11 – Resposta para a Pergunta 7.1. Fonte: (UNIÃO, 2022)

- **Ponto 12**

  Pergunta: Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?

Análise: A organização deve assegurar que os titulares de dados tenham acesso às informações sobre o tratamento de seus dados, cumprindo os nove direitos dos titulares estabelecidos no art. 18 da LGPD.

No gráfico apresentado pela Figura 12, podemos ver que somente 14% das organizações implementaram os mecanismos para o acesso dos titulares. Levando em conta que muitas empresas não tem os mecanismos, elas podem considerar as diretrizes da NBR ISO/IEC 27701 e desenvolver, disponibilizar um local onde os titulares de dados podem verificar todas as devidas informações previstas em lei sobre seus dados.

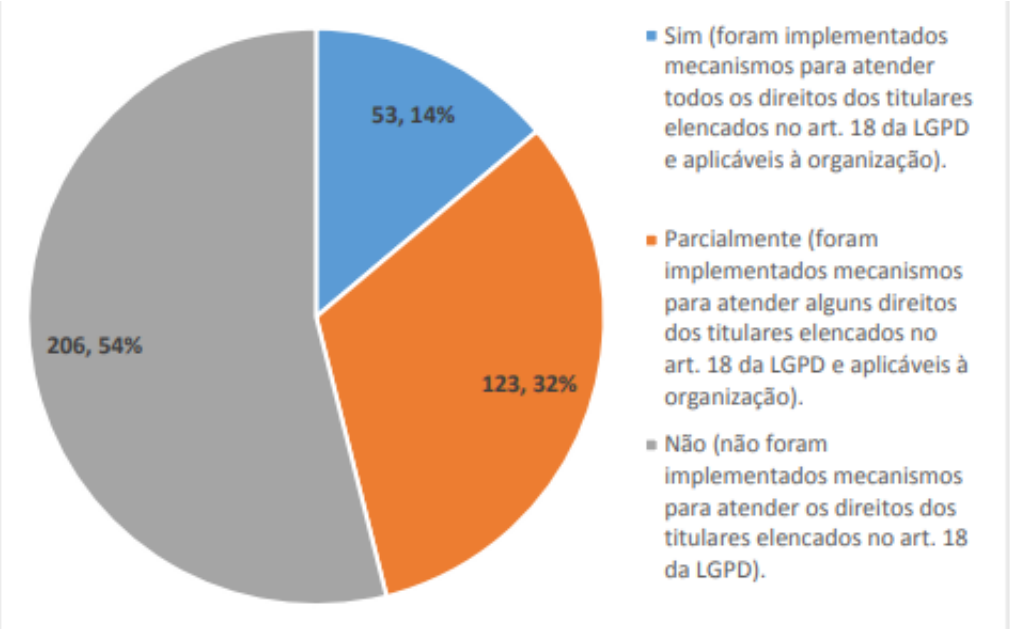

Figura 12 – Resposta para a Pergunta 7.2. Fonte: (UNIÃO, 2022)

- **Ponto 13**

  Pergunta: A organização possui plano de resposta a incidentes que abrange o tratamento de incidentes que envolvem violação de dados pessoais?

  Análise: Segundo a LGPD toda a organização que trata os dados é a responsável em casos de incidentes envolvendo a violação de dados pessoais, logo recomenda-se que seja organizado um plano de resposta contra incidentes para ter uma resposta rápida e eficiente mostrando que a organização fez de todo o possível para corrigi-la. No momento de aplicação de uma punição pela ANPD, é analisado e considerado o comprometimento da empresa em corrigir casos de violação. Portanto se for identificado que a empresa não fez todo o possível para evitar ou corrigir os incidentes poderão levar uma punição mais severa.

  No gráfico apresentado pela Figura 13, foi mostrado que 84% das organizações não possuem plano de reposta a incidentes. É fundamental que uma organização possa identificar e responder aos incidentes de segurança, uma vez que ninguém está 100%

seguro. Um plano de resposta é importante, visto que com ele a empresa tera uma forma mais rápida e eficiente de lidar com violações minimizando os prejuízos causados.

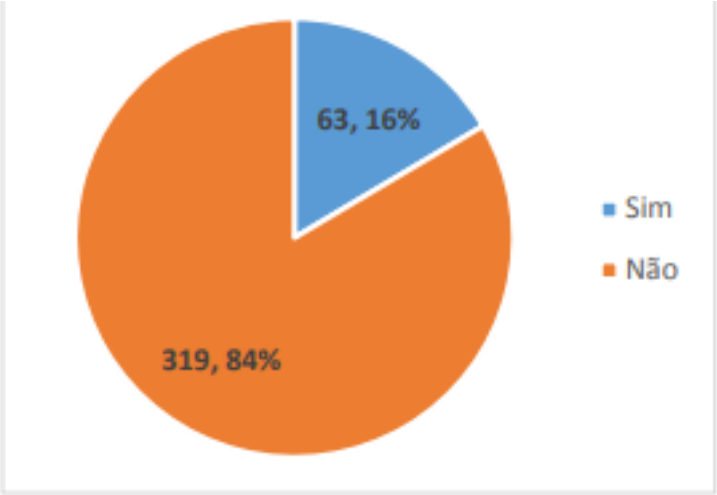

Figura 13 – Resposta para a Pergunta 9.1. Fonte: (UNIÃO, 2022)

- **Ponto 14**

  Pergunta: A organização possui um sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?

  Análise: A LGPD prevê que as organizações devem possuir registros de incidentes de segurança envolvendo violação de dados com informação abrangente, estabelecendo se possível responsabilidades e procedimentos de identificação, registro e tratamento dado na violação de dados.

  O gráfico apresentado pela Figura 14, mostra que 72% das organizações não possuem sistema para registro de incidentes.

  É importante aprender com os erros, um sistema que contenha um histórico de incidentes pode ser utilizado para aprendizagem. Isto pode reduzir o risco de ocorrências futuras, pois, o registro de um incidente, junto de todos os passos tomados, pode ser utilizados para traçar mecanismos mais efetivos ou mesmo a correção de violações futuras.

- **Ponto 15**

  Pergunta: A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?

  Análise: Para que sejam identificadas violações de dados pessoais rapidamente, recomenda-se que tenha o monitoramento de eventos para serem analisados. Devem ser registrados também se são ou não violações de dados pessoais para que sejam adotadas respostas adequadas.

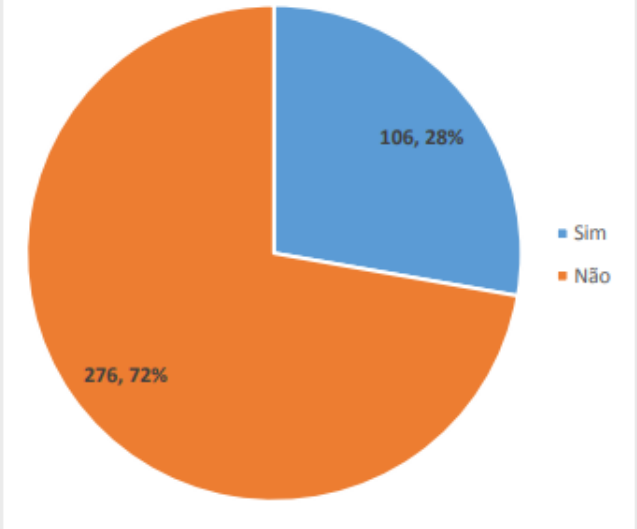

Figura 14 – Resposta para a Pergunta 9.2. Fonte: (UNIÃO, 2022)

No gráfico apresentado pela Figura 15, é mostrado que 66% das organizações não monitoram proativamente a ocorrência de eventos associados à violação de dados pessoais. Esse caso apresenta alto risco, visto que mesmo se a empresa tenha um sistema de monitoramento para identificar os eventos adotando rapidamente medidas de segurança de forma mais rápida e efetiva, ainda temos o problema de identificação de violações.

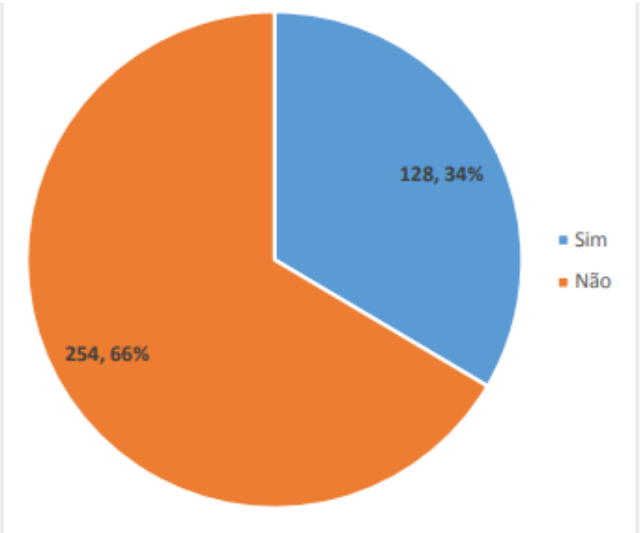

Figura 15 – Resposta para a Pergunta 9.4. Fonte: (UNIÃO, 2022)

5.2 Comparação das ferramentas

Os dados de cada ferramentas foram recolhidos dos seus respectivos sites e elencados todas as suas características, o resultado foi apresentado no capítulo 4.

Ferramentas					
Ponto	**Privacytool**	**Ecomply**	**GestaoX**	**DPOMAX**	**Onetrust**
Ponto 1	X	X	X	X	X
Ponto 2					
Ponto 3	X			X	X
Ponto 4	X	X	X	X	X
Ponto 5	X	X	X	X	X
Ponto 6	X	X	X	X	X
Ponto 7	X	X	X	X	X
Ponto 8	X	X	X	X	X
Ponto 9	X	X	X	X	X
Ponto 10	X	X	X	X	X
Ponto 11	X		X	X	X
Ponto 12	X	X	X	X	X
Ponto 13	X		X	X	X
Ponto 14	X	X	X	X	X
Ponto 15	X				X

Tabela 2 – Tabela de ferramentas e seus suportes para cada ponto

A tabela 2 permite construir uma visão mais compreensível de quais pontos abordados na análise os softwares se comprometem em resolver. Pode-se observar que a ferramenta com menor cobertura dos pontos analisados é a Ecomply, deixando pontos que outras ferramentas contemplam de lado, como no auxílio da criação de uma política de privacidade e o da criação de um plano de resposta a incidentes de violação de dados. Percebe-se também que as ferramentas Privacytool e Onetrust abragem a maior cobertura de funcionalidades quanto aos pontos elencados.

Entretanto, um diferencial deve ser citado quanto ao conhecimento necessário para a utilização da ferramenta. Onetrust é a única ferramenta de software que não necessita de co-

nhecimento em nível de um DPO. Esta ferramenta tem a proposta de identificar e classificar os dados via inteligencia artificial, não tendo a necessidade de um DPO operando a ferramenta.

Apesar das ferramentas serem capazes de cobrir vários pontos críticos sobre a adequação LGPD, nenhuma ferramenta informou funcionalidade de auxiliar a organização. O ponto específico **contemplar outras leis nacionais relacionadas a proteção de dados pessoais**, não possui cobertura por nenhuma das ferramentas analisadas. A cobertura deste ponto é importante, pois no Brasil existem outras leis complementares além da LGPD.

6 CONCLUSÃO

A LGPD tem no artigo primeiro, o direito fundamental de liberdade, privacidade e livre desenvolvimento da pessoa natural. Desde 2022 ela também foi incluída como um direito fundamental na constituição federal, seguindo outros países desenvolvidos que já possuem leis de proteção de dados. O Brasil é um dos países mais digitalizados do mundo com um alto tráfego de dados, entretanto ainda está longe de ser um país digitalmente seguro. Mesmo a LGPD estando em vigor há três anos a maioria das empreses não estão de acordo com a lei, o que significa que os dados e seus titulares não estão seguros e isso pode gerar graves danos financeiros e sociais.

Este trabalho buscou identificar o grau de adequação da LGPD no setor público. Foi realizada uma análise do relatório disponibilizado pelo TCU e foram identificados os principais pontos críticos. Em seguida, foi mostrado a importância da adequação, juntamente a ferramentas e metodologias que auxiliam as organizações a se adequarem a LGPD. Esta análise apontou a necessidade de aumento na segurança de dados é muito importante. Visto que a sua importância vai além do cumprimento da LGPD, pois, a falta de segurança nas organizações afetam diretamente os titulares de dados.

Trabalhos futuros incluem uma análise mais profunda e precisa sobre as ferramentas elencadas neste presente trabalho. Podendo ser realizado uma avaliação experimental, não apenas valendo-se das informações descritas pelos desenvolvedores. Podendo também participar de uma consultoria com as empresas apontando o que pode estar faltando, falhas e melhorias.

Uma medida que pode acelerar a adoção á LGPD, consiste em exigir que a ANPD realize um trabalho de fiscalização e conscientização sobre as instituições públicas no Brasil, junto a punições mais rigorosas. Uma boa notícia é que a LGPD e outras leis estão trazendo grandes inovações no setor de proteção de dados. A cada dia aparece no mercado novos softwares que prometem auxiliar a adaptação das organizações para com a LGDP. Mesmo o cenário de proteção de dados em organização pública estando muito longe do ideal, uma maior rigorosidade por parte da ADNP e também a adoção de novas tecnologias, pode tornar o Brasil uma referência no que diz respeito à proteção de dados.

REFERÊNCIAS

ANPD. **Autoridade Nacional de Proteção de Dados**. 2020. Disponível em: https://www.gov.br/anpd/pt-br.

BOTELHO, E. P. d. A. C. M. C. O tratamento de dados pessoais pelo poder público na lgpd. **REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)**, 2022. Disponível em: https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1034/pdf.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: [*s.n.*], 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Brasília: [*s.n.*], 2022. Disponível em: https://in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387.

BRASIL, A. N. d. P. d. D. ResoluÇÃo cd/anpd nº 1. **Diário oficial da união**, Brasília, v. 205, n. 1, p. 6, 10 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513.

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (lei geral de proteção de dados do brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - um estudo de caso / methodology for mapping and adequacy of the requirements listed in LGPD (brazil data protection general law number 13 709/18) in a financial institution - a case study. **Brazilian Journal of Business**, Brazilian Journal of Business, v. 2, n. 4, p. 3626–3648, 2020. Disponível em: https://doi.org/10.34140/bjbv2n4-012.

DENNER, C. *et al.* Govtech maturity index : The state of public sector digital transformation. **World Bank. © World Bank**, Washington, DC, 09 2021. Disponível em: https://openknowledge.worldbank.org/handle/10986/36233.

FERREIRA, L. *et al.* A panorama of the implementation of the general law for the protection of personal data (lgpd) in brazil: an exploratory survey. *In*: **2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)**. [*S.l.*: *s.n.*], 2022. p. 0723–0729.

MAGACHO, B. T. P.; TRENTO, M. LGPD e compliance na administração pública: O brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? é possível mensurar os impactos das adequações necessárias no setor público? ... **Revista Brasileira de Pesquisas Jurídicas (Brazilian Journal of Law Research)**, Revista Brasileira de Pesquisas Juridicas, v. 2, n. 2, p. 7–26, maio 2021. Disponível em: https://doi.org/10.51284/rbpj.02.trento.

MCLENNAN, M.; GROUP, S.; GROUP, Z. I. The global risks report 2021 16th edition. Geneva (Switzerland), p. 96, 2021. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

MONTEIRO ODéLIO PORTO JUNIOR, G. M. R. L. Comparing privacy laws: Gdpr v. lgpd. DataGuidance, 2018. Disponível em: https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf.

NARDES, M. A. Acordão nº 1384/2022. **Diário oficial da união**, Brasília, 06 2022. Disponível em: https://www.trt7.jus.br/files/acesso_informacao/transparencia/acoes_de_controle/TCU/Acordao_1384-2022-TCU-Plenario.pdf.

PARLIAMENT, C. o. t. E. U. E. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). **Official Journal of the European Union**, European Union, abril 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

REPúBLICA, P. da. Lei que estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. **Secretaria-Geral,Subchefia para Assuntos Jurídicos**, Brasília, abril 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm.

TCU. **Tribunal de contas da união**. 2022. Disponível em: https://portal.tcu.gov.br/inicio/.

UNIÃO, T. D. C. D. Auditoria. diagnóstico do grau de implementação da lei geral de proteção de dados na administraçãoo pública federal. **TCU**, Brasil, junho 2022. Disponível em: https://capitaldigital.com.br/wp-content/uploads/2022/06/038.172-2019-4-AN-auditoria_Lei-Geral-de-Protecao-de-Dados.pdf.