

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande

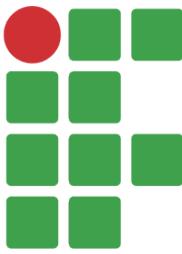
Coordenação do Curso Superior de Bacharelado em Engenharia
de Computação

LGPD Compliance: Aplicando *Cheklist* para Avaliação de Sistemas à Luz da Lei Geral de Proteção de Dados

Lucas Matheus Torres Costa
Moabe Barbosa Alves
Rafael Figueiredo Guimarães

Orientador: Prof. Danyllo Wagner Albuquerque, Msc.

Campina Grande, Agosto de 2022
②Lucas Matheus Torres Costa
②Moabe Barbosa Alves
②Rafael Figueiredo Guimarães



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande

Coordenação do Curso Superior de Bacharelado em Engenharia
de Computação

LGPD Compliance: Aplicando *Cheklist* para Avaliação de Sistemas à Luz da Lei Geral de Proteção de Dados

Lucas Matheus Torres Costa

Moabe Barbosa Alves

Rafael Figueiredo Guimarães

Monografia apresentada à Coordenação do
Curso Superior de Bacharelado em Enge-
nharia de Computação do IFPB - *Campus*
Campina Grande, como requisito parcial
para conclusão do curso de Bacharelado em
Engenharia de Computação.

Orientador: Prof. Danyollo Wagner Albuquerque, Msc.

Campina Grande, Agosto de 2022

LGPD Compliance: Aplicando *Cheklist* para Avaliação de Sistemas à Luz da Lei Geral de Proteção de Dados

Lucas Matheus Torres Costa

Moabe Barbosa Alves

Rafael Figueiredo Guimarães

Prof. Danyollo Wagner Albuquerque, MSc.

Orientador

Profa. Ana Cristina Alves de Oliveira Dantas, DSc.

Membro da Banca

Prof. Katyusco de Farias Santos, DSc.

Membro da Banca

Campina Grande, Paraíba, Brasil

Agosto/2022

"A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo".
(Albert Einstein)

"Tenho a impressão de ter sido uma criança brincando à beira-mar, divertindo-me em descobrir uma pedrinha mais lisa ou uma concha mais bonita que as outras, enquanto o imenso oceano da verdade continua misterioso diante de meus olhos".
(Isaac Newton)

"Ciência é uma equação diferencial. Religião é a condição de contorno".
(Alan Turing)

Agradecimentos

Agradecimentos Lucas Matheus Torres Costa

Agradecimentos Moabe Barbosa Alves

Agradecimentos Rafael Figueiredo Guimarães

Em primeiro lugar, agradeço a Deus, por ter permitido que eu tivesse saúde determinação para não desanimar durante a realização deste trabalho. A minha família, que me incentivou nos momentos difíceis e compreendeu a minha ausência enquanto eu me dedicava as minhas ocupações acadêmicas. Aos meus amigos Lucas Mateus e Moabe Barbosa, por suas contribuições sem as quais, a realização deste trabalho não seria possível. Ao professor Danyllo Albuquerque, por ter sido nosso orientador e ter desempenhado tal função com dedicação e companheirismo. A todos os professores, por todos os conselhos e ensinamentos que guiaram o meu aprendizado. Aos meus meus colegas de turma, por compartilharem comigo momentos de crescimento. Ao Instituto Federal de Educação Ciência e Tecnologia da Paraíba, essencial no meu processo de formação profissional por tudo o que aprendi ao longo dos 5 anos de curso.

Resumo

[Contexto] A Lei Geral de Proteção de Dados (LGPD) surgiu com a intenção de regulamentar a utilização e manipulação de dados por sistemas computacionais no Brasil. [Descrição do problema] Diversas empresas e profissionais enfrentavam dificuldades sobre o correto manuseio dos dados e como tornarem-se aderentes a LGPD. Contudo, a lei é composta basicamente por termos e definições jurídicos que não indicam ações e meios para adequação dos sistemas a essa lei. [Objetivo] Esta pesquisa, tem como foco projetar e desenvolver uma plataforma que ajude profissionais a obter conhecimento sobre a LGPD no intuito de adequação de seus projetos de software. [Método] Para isso, através do uso da técnica de *checklist*, foi construída uma plataforma web que disponibiliza um questionário para avaliação da adequabilidade de projetos de software a supracitada lei. [Resultados] Os autores desse trabalho mapearam e validaram os principais requisitos da plataforma e, com uso de tecnologias web, desenvolveram e disponibilizaram o LGPD Compliance, uma plataforma WEB, contendo um *checklist* de fácil acesso e sem custo para utilização. Mediante utilização de um *survey*, cerca de 20 respondentes avaliaram as funcionalidades e usabilidade da plataforma. [Conclusão] A aplicação do *checklist* mostrou-se adequada ao contexto da LGPD e contribui para avaliação dos projetos de software à luz da legislação vigente, além de prover dicas e ações práticas visando a conformidade destes projetos.

Palavras-chave: LGPD, Proteção de Dados, *Checklist*, *Feedbacks*, Plataforma WEB, Questionário.

Abstract

[Context] The General Data Protection Law (LGPD) was created with the intention of regulating the use and manipulation of data by software systems in Brazil. [Problem Statement] Several organizations and professionals faced difficulties regarding the correct handling of data and how to become adhering to the LGPD. However, the law is basically composed of legal terms and definitions that do not indicate actions and means for adapting systems to this law. [Objective] Our research focuses on designing and developing a platform that helps professionals gain knowledge about the LGPD in order to adapt their software projects. [Method] For this, through the use of the *checklist* technique, a web platform was built that provides a questionnaire to assess the suitability of software projects to the aforementioned law. [Results] The authors mapped and validated the main requirements of the platform and, using web technologies, developed and made available the LGPD Compliance - a WEB platform containing an easily accessible *checklist* at no cost to use. Using a survey, about 20 respondents evaluated the platform's functionality and usability. [Conclusion] The application of the *checklist* proved to be adequate to the LGPD context and contributes to the evaluation of software projects in light of current legislation, in addition to providing tips and practical actions aimed at the compliance of these software projects.

Keywords: LGPD, Data Protection, Checklist, Feedbacks, WEB Platform, Questionnaire.

Sumário

| | |
|---|-------------|
| Lista de Abreviaturas | xii |
| Lista de Figuras | xiii |
| Lista de Tabelas | xv |
| 1 Introdução | 1 |
| 1.1 Problemática | 2 |
| 1.2 Objetivos | 2 |
| 1.3 Metodologia | 3 |
| 1.4 Exemplo Motivador | 4 |
| 1.5 Justificativa e Relevância do Trabalho | 4 |
| 1.6 Estrutura do Trabalho | 5 |
| 2 Fundamentação Teórica | 6 |
| 2.1 LGPD - Lei Geral de Proteção de Dados | 6 |
| 2.1.1 Definições e comentários a LGPD | 9 |
| 2.2 <i>CheckList</i> na Computação | 10 |
| 2.3 Tecnologias Utilizadas | 11 |
| 2.3.1 <i>Backend</i> | 11 |
| 2.3.2 <i>Front-end</i> | 12 |
| 2.4 Processo de Desenvolvimento | 15 |
| 3 Trabalhos Relacionados | 18 |
| 4 Configuração de Estudo | 20 |
| 4.1 Análise e Definição de Requisitos | 20 |
| 4.2 Definição Arquitetural | 21 |
| 4.3 Desenvolvimento de Software | 22 |
| 4.3.1 Desenvolvimento do Módulo Database | 23 |
| 4.3.2 Desenvolvimento do Módulo <i>Backend</i> | 27 |
| 4.3.3 Desenvolvimento do Módulo <i>Frontend</i> | 28 |
| 4.4 Validação | 32 |

| | | |
|----------|--|-----------|
| 4.5 | Implantação | 33 |
| 5 | Resultados | 34 |
| 5.1 | A Plataforma LGPD <i>Compliance</i> | 34 |
| 5.1.1 | Funcionalidades Públicas | 34 |
| 5.1.2 | Mecanismo de Autenticação | 36 |
| 5.1.3 | Funcionalidades do Usuário Comum | 38 |
| 5.1.4 | Funcionalidades do Usuário administrador | 42 |
| 5.1.5 | Responsividade das telas | 44 |
| 5.2 | Validação da plataforma | 49 |
| 5.2.1 | Projeto do Questionário | 49 |
| 5.2.2 | Execução de Testes-piloto | 50 |
| 5.2.3 | Definição da Amostra e Coleta de Dados | 50 |
| 5.2.4 | Resultados da validação | 50 |
| 6 | Ameaças a Validade | 52 |
| 6.1 | Validade de conclusão | 52 |
| 6.2 | Validade interna | 52 |
| 6.3 | Validade de construção | 53 |
| 6.4 | Validade externa | 53 |
| 7 | Considerações Finais | 54 |
| | Referências Bibliográficas | 55 |

Listas de Abreviaturas

| | |
|-------|---|
| IFPB | Instituto Federal da Paraíba |
| LGPD | Lei Geral de Proteção de Dados |
| GDPR | <i>General Data Protection Regulation</i> (Regulamento Geral de Proteção de Dados) |
| DPO | <i>Data Protection Officer</i> (Diretor de Proteção de Dados) |
| IoT | <i>Internet Of Things</i> (Internet das Coisas) |
| MIT | <i>Massachusetts Institute Technology</i> |
| ORM | <i>Object-Relational Mapping</i> (Mapeamento objeto-relacional) |
| SDK | <i>Software Development Kit</i> (Kit de desenvolvimento de software) |
| HTML | <i>Hypertext Transfer Protocol</i> (Protocolo de Transferência de Hipertexto) |
| CSS | <i>Cascading Style Sheet</i> (Folha de Estilo em Cascatas) |
| HTTP | <i>Hyper Text Transfer Protocol</i> (Protocolo de Transferência de Hipertexto) |
| HTTPS | <i>Hypertext Transfer Protocol Secure</i> (Protocolo de Transferência de Hipertexto Seguro) |
| URL | <i>Uniform Resource Locator</i> (Localizador Uniforme de Recursos) |
| MVC | <i>Model View e Controller</i> (Modelo, Visão e Controle) |
| ORM | Object-Relational Mapping (Mapeamento Objeto-Relacional) |
| SQL | <i>Structured Query Language</i> (Linguagem de Consulta Estruturada) |
| URL | Uniform Resource Locator (Localizador Padrão de Recursos) |
| API | <i>Application Programming Interface</i> (Interface de Programação de Aplicação) |
| VPS | <i>Virtual Private Server</i> (Servidor Virtual Privado) |
| JSON | <i>JavaScript Object Notation</i> (Notação de Objeto JavaScript) |
| SMTP | <i>Simple Mail Transfer Protocol</i> (Protocolo Simples de Transferência de Correio) |

Listas de Figuras

| | | |
|---------------------|---|----|
| 1.1 | Etapas do processo de desenvolvimento | 3 |
| 2.1 | Linha do Tempo da LGPD ¹ | 8 |
| 2.2 | Contêiner do <i>docker</i> ² | 11 |
| 2.3 | Migrações e introspecção SQL ³ | 12 |
| 2.4 | Hierarquia de <i>Widgets</i> ⁴ | 13 |
| 2.5 | Arquitetura do Flutter Web ⁵ | 14 |
| 2.6 | Funcionamento do Scrum ⁶ | 16 |
| 4.1 | Arquitetura do Sistema LGPD | 22 |
| 4.2 | Quadro de tarefas baseado na metodologia Kanban | 23 |
| 4.3 | Diagrama de Entidade e Relacionamento <i>LGPD Compliance</i> | 25 |
| 26figure.caption.20 | | |
| 4.5 | Diagrama de Fluxo Dados do <i>Backend</i> | 27 |
| 4.6 | Diagrama Genérico do Módulo <i>Frontend</i> | 28 |
| 4.7 | Diagrama de classe simplificado do Submódulo de Autenticação | 29 |
| 4.8 | Diagrama de classe simplificado do Submódulo Plataforma LGPD | 31 |
| 4.9 | Diagrama de classe simplificado do Submódulo de Plataforma LGPD Admin | 32 |
| 5.1 | Tela Inicial. | 35 |
| 5.2 | Tela de Saiba Mais. | 35 |
| 5.3 | Tela de Entrar em Contato. | 36 |
| 5.4 | Tela de Entrar em Contato. | 36 |
| 5.5 | Tela de Cadastro. | 37 |
| 5.6 | Tela de Cadastro. | 37 |
| 5.7 | Aba do LGPD. | 38 |
| 5.8 | Aba do Perfil. | 39 |
| 5.9 | <i>Pop-up</i> para confirma solicitação de exclusão do usuário. | 39 |
| 5.10 | Aba da Etapa 1 do <i>Quiz</i> | 40 |
| 5.11 | Aba da Etapa 2 do <i>Quiz</i> | 40 |
| 5.12 | Aba da Etapa 3 do <i>Quiz</i> | 41 |
| 5.13 | Aba de Histórico | 41 |

| | |
|---|----|
| 5.14 Aba de Histórico: ver detalhes | 42 |
| 5.15 Aba LGPD do administrador | 43 |
| 5.16 Aba de lista de usuários | 43 |
| 5.17 Aba de lista de usuários | 44 |
| 5.18 Aba de lista de usuários | 44 |
| 5.19 Fluxo das funcionalidades públicas | 45 |
| 5.20 Fluxo de autenticação | 46 |
| 5.21 Fluxo de um usuário comum | 47 |
| 5.22 Fluxo de um usuário administrador | 48 |

Lista de Tabelas

| | | |
|-----|--|----|
| 4.1 | Lista Preliminar de Requisitos Funcionais - <i>LGPD Compliance</i> | 21 |
| 4.2 | Lista Preliminar Não Funcionais - <i>LGPD Compliance</i> | 21 |
| 5.1 | Seções do Questionário. | 49 |

Capítulo 1

Introdução

A internet é um termo relativamente recente em paralelo com outros elementos de nossa vida habitual. A partir da sua criação no final da década de 60 até os dias atuais, essa tecnologia impactou diretamente nas relações humanas, desde a comunicação até a forma de se realizar negócio. Nesse contexto, o normativo jurídico para regulamentação dos atos realizados em ambientes virtuais ainda carece de ajustes.

Exemplo disso, no panorama internacional, em meados de 2018 noticiou-se, nos principais meios de comunicação, o vazamento de dados ligado a rede social *Facebook*. Essa situação, envolveu a divulgação e a utilização inadequada de dados pessoais de milhões de usuários, informações que teriam sido utilizadas pela empresa britânica *Cambridge Analytica* para traçar perfis políticos, com o intuito de direcionar de forma mais eficaz as propagandas e divulgações da campanha presidencial de Donald Trump, candidato a presidência dos Estados Unidos neste período. Nesse incidente a *Federal Trade Commission* (FTC) - o órgão dos Estados Unidos que regula as relação entre consumidores e empresas - aplicou a a maior multa da história da agência a uma empresa de tecnologia, US\$ 5 bilhões, por conta deste uso indevido de dados.

Diante desse cenário, diversos países do mundo buscaram ajustar sua regulamentação a respeito de uso e manipulação de dados. Por exemplo, com objetivo de proteger a privacidade dos dados referentes ao usuários europeus, em maio de 2018, entrou em vigor a *General Data Protection Regulation* (GDPR). Este é um conjunto de normas para regulamentar a coleta e o uso de dados pessoais de usuários que se encontram na União Europeia.

Por consequência do incidente do escândalo da *Cambridge Analytica* bem como da elaboração e sanção da GDPR, diversas entidades brasileiras precisaram se adequar para esta nova realidade. Isso culminou com a propositura e aprovação da Lei Geral de Proteção de Dados (LGPD) em meados de agosto de 2020. Esta lei tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como alvo a criação de um contexto na segurança jurídica, com a padronização de regulamentos e costumes para promover a

proteção aos dados pessoais de todo cidadão que esteja no Brasil. Resumidamente, esta lei foi criada para adequar as práticas de empresas brasileiras a esses novos padrões e ao cenário global, inserindo o Brasil no rol dos mais de 120 países que contam com uma lei específica para tratar de proteção de dados.

1.1 Problemática

A partir da criação da LGPD, há uma mudança de paradigma na gestão dos dados pessoais nas organizações, evidenciando a necessidade de adequações internas para a construção de uma política de manipulação e salvaguarda de dados. De acordo com a nova legislação, toda operação realizada com dados pessoais, no que diz respeito a coleta, produção, extração entre outros devem ser realizados por meio de bases legais. Consequentemente, qualquer empresa que realizar essas operações sem a devida conformidade poderá sofrer multas e outras penalidades.

Do ponto de vista dessas organizações que devem se adequar a nova realidade, essa tarefa pode representar um desafio levando em consideração a aplicabilidade prática da LGPD em suas atividades. Cabe a ressalva de que a supracitada lei é composta basicamente de conceitos e terminologias, sem a indicação prática de ações e meios necessários para adequação dos sistemas. Tal situação pode desencorajar organizações e profissionais a realizarem as ações necessárias a salvaguarda e manipulação de dados por parte dos sistemas. Como consequência, usuários podem estar sujeito a utilização de sistemas sem a devida regulamentação a respeito do uso de seus dados pessoais.

1.2 Objetivos

O objetivo desta pesquisa consiste na implementação de uma plataforma que auxiliem organizações e profissionais obter conhecimento sobre a LGPD no intuito de adequação de seus projetos de software a este normativo jurídico. A plataforma LGPD Compliance irá utilizar a técnica de *checklist* para o desenvolvimento de um questionário composto por questões alusivas a diversos segmentos da LGPD. Com a resolução do questionário, um score de adequabilidade será gerado juntamente com as melhores recomendações para se aplicar no projeto pretendido.

A fim de que os objetivos gerais sejam atendidos, é necessário a observação dos seguintes objetivos específicos:

- Identificar um conjunto de requisitos para criação do LGPD Compliance;
- Validação dos requisitos do LGPD Compliance com especialistas;
- Desenvolvimento de um protótipo de baixa fidelidade para constituição dos principais fluxos do LGPD Compliance;

- Catalogar e identificar tecnologias necessárias ao desenvolvimento do LGPD Compliance;
- Projetar uma arquitetura aderente as necessidades do LGPD Compliance;
- Desenvolver a plataforma LGPD compliance como uma aplicação mobile e web responsiva;
- Realizar testes de usabilidade para sanar possíveis inconsistências; e
- Publicar a plataforma em ambiente de computação em nuvem.

1.3 Metodologia

Este trabalho tem como finalidade construir uma plataforma que estabelece métricas de conformidade baseadas na LGPD. Para que essas questões sejam atendidas, a configuração desse trabalho será dividido nas etapas, conforme descrito na Figura 1.1.

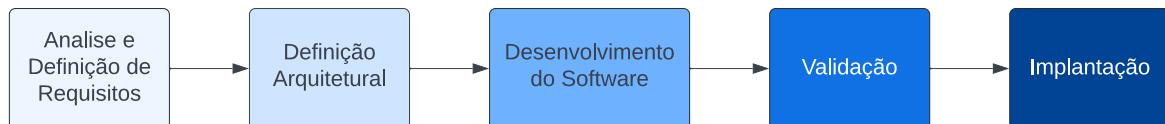


Figura 1.1: Etapas do processo de desenvolvimento

A **primeira etapa** do desenvolvimento consiste na análise e definição de requisitos do sistema. Os requisitos definem o que o sistema deve fazer em termos de funcionalidades e estabelecem como o sistema se comportar e suas restrições. Nessa etapa também será estudado a fundo o domínio do problema.

A **segunda etapa** consiste na definição da arquitetura do sistema. Desse modo, nessa etapa serão projetados em alto nível as definições dos módulos do sistema, bem como suas respectivas interações e os principais modelos de dados.

A **terceira etapa** consiste no desenvolvimento da aplicação, essa etapa envolve criação de banco de dados, criação de modelos, classes, funções, estruturas relacionadas ao *Backend* e *Frontend* entre outros. Além disso, A metodologia a ser utilizada no desenvolvimento é uma decisão importante uma vez que procuram estabelecer um processo disciplinado, com o objetivo de tornar mais previsível e eficiente possível as atividades(Awad, 2005).

A **quarta etapa** abrange verificar e documentar o sistema e o meio no qual ele atua com a intenção estabelecer maior garantia ao que já foi desenvolvido atendendo aos requisitos

já definidos (Conexorama, 2018). Inicialmente, será realizada uma validação dos requisitos do sistema, verificando se de fato as funcionalidades do sistema cumprem com o que foi planejado em sua definição (Conexorama, 2018).

A **quinta etapa** foi definida como implantação, segundo (FOKUS Mercury Computer Systems, 2003), o processo de implantação de *software* é iniciado quando o *software* já está desenvolvido, empacotado e é transferido para o servidor que proporcionará o acesso aos demais serviços oferecidos.

1.4 Exemplo Motivador

Nesta seção será apresentado um exemplo motivador que evidencie a necessidade de desenvolvimento do presente sistema. Nosso exemplo inicia com José, um desenvolvedor web que mantém um sistema de gestão empresarial de uma rede de supermercados. Recentemente, José sentiu a necessidade de reestruturar a forma de coleta e manipulação de dados sensíveis dos clientes, visando a adequabilidade a legislação vigente.

Nesse sentido, José buscou a LGPD para leitura e compreensão desta lei. Após uma leitura detalhada da lei, José sentiu-se inseguro a respeito de quais ações deveria tomar a respeito da manipulação e salvaguarda de dados. José arguiu que a lei apresentava muitas terminologias e conceitos não-nativos à profissionais da área de informática bem como carecer de expor ações práticas para adequação dos sistemas de software. Finalmente, diante de tal contexto, José sentiu-se desencorajado a aplicar alterações em seu sistema em relação aos dados dos clientes.

Assim, com o uso da LGPD Compliance, José realizou o preenchimento do questionário a respeito dos segmentos (i) governança, (ii) conformidade legal e (iii) transparência e direitos do titular. Após o preenchimento, João recebeu um score de 52%, denotando que seu sistema necessita de implementação de melhorias em relação a esses segmentos da LGPD. Concomitantemente, José recebeu um *feedback* em forma de um relatório, indicando precisamente ações que deveriam ser aplicadas visando a elevação do score e, consequentemente, a adequação do sistema em relação a LGPD.

1.5 Justificativa e Relevância do Trabalho

A adequação à lei geral de proteção de dados faz-se necessária por todas organizações e profissionais que, de algum modo, manipulam e armazenam dados de usuários. A necessidade de regulamentação à LGPD ganhou mais notoriedade com a globalização e a internacionalização dos dados (Pinheiro, 2020), evidenciando a necessidade de uma padronização de procedimentos frente à questão. De acordo com a pesquisa (RDStation, 2021), 93% das empresas conhecem ou pelo menos já ouviram falar da LGPD, mas apenas 15% se mostram minimamente aderentes a tal legislação. Além disso, outro recente estudo global

(Ponemom, 2018), apontou que 54% das empresas consideram que a principal ameaça sobre a confidencialidade dos dados está na falha de processos e de pessoas. Enquanto 23% têm preocupação com a ação de colaboradores temporários.

De acordo com o artigo 7º da lei Nº 13.709, de 14 De Agosto de 2018 (Brasil, 2018), no tratamento de dados de uma pessoa, no caso, o titular, é necessária a permissão do mesmo para utilização dos seus dados. No artigo 9 da mesma lei, é exigida a identificação do controlador dos dados e a finalidade específica do tratamento que será realizado. Com isso, fica evidente que a adequação a LGPD, além de ser importante para a padronização de procedimentos, é algo que precisa ser seguido para que sejam evitadas possíveis sanções legais cabíveis em caso de descumprimento.

Ademais, uma pesquisa recente desenvolvida por pesquisadores do *Massachusetts Institute of Technology (MIT)* (Neto et al., 2021) indicou que os vazamentos de dados aumentaram cerca de 49% no Brasil entre 2018 e 2019. Dessa forma, justifica-se a criação de uma plataforma para auxiliar na adequação da LGPD. Espera-se que, a partir da utilização da plataforma, organizações e profissionais elevem seu conhecimento desta legislação e obtenha indicações de ações práticas para adequabilidade dos seus sistemas frente ao armazenamento e manipulação de dados de forma geral.

1.6 Estrutura do Trabalho

Os capítulos restantes que compõem este documento estão organizados da seguinte forma:

- **Capítulo 2: Fundamentação Teórica.** Apresentam-se definições gerais dos temas abordados neste documento.
- **Capítulo 3: Trabalhos Relacionados.** Discutem-se os principais trabalhos relacionados ao presente estudo.
- **Capítulo 4: Configuração de Estudo.** Apresenta a configuração metodológica bem como os passos realizados para a construção desse estudo.
- **Capítulo 5: Resultados.** Apresenta-se os resultados obtidos ao final do processo metodológico.
- **Capítulo 6: Ameaças à validade.** Apresentam-se as principais ameaças associadas a esse estudo.
- **Capítulo 7: Considerações Finais.** Apresentam-se as principais conclusões e desdobramentos com a realização deste estudo.

Capítulo 2

Fundamentação Teórica

Neste capítulo serão introduzidos os principais conceitos necessários ao entendimento desse trabalho de conclusão de curso. Inicialmente, descreve-se assuntos relacionados a Lei geral de Proteção de Dados (Seção 2.1). Em seguida, será apresentado conceito de *checklist* em computação (Seção 2.2). Por último, serão comentadas as tecnologias utilizadas (Seção 2.3) bem como o processo de desenvolvimento empregado para construção da plataforma LGPD Compliance (Seção 2.4).

2.1 LGPD - Lei Geral de Proteção de Dados

A privacidade é algo que permeia os diferentes setores da sociedade e ao longo do tempo foi algo que foi bastante associado ao meio físico. Nos últimos anos, a privacidade no meio digital tem ganhado muita atenção, visto que as relações humanas tiveram um crescimento bem acentuado no meio digital, através de ligações por videochamadas, uso de transportes por meio de *smartphones*, entre outros (Garcia et al., 2020).

Para que tudo isso aconteça de forma satisfatória e que diversos problemas sejam evitados, é importante que exista uma regulamentação para garantir o bem estar de cada indivíduo com relação aos seus dados pessoais. Contudo, vale destacar que o conceito de privacidade não é o mesmo que o conceito de proteção de dados. A privacidade de dados está preocupada com o controle de acesso à dados privados, enquanto que a proteção de dados, atua tanto no controle de dados privados como também de dados públicos. Em vista disso, a LGPD foi criada para proporcionar uma estrutura legal para a proteção dos dados (Garcia et al., 2020).

A LGPD está aplicada aos diversos setores da sociedade que utilizam e precisam de dados para os seus processos. Desde 2018, quando a lei foi aprovada, organizações e profissionais, devido à necessidade de adequação aos parâmetros instituídos na lei, tiveram um aumento no seu custo operacional (Pinheiro, 2021). Por exemplo, as organizações vem adicionando em seu quadro de funcionários a nomeação de um Encarregado pela salvaguarda de dados (a.k.a., DPO(*Data Protection Officer*)). Este perfil profissional é responsável legal-

mente pelo gerenciamento de dados da empresa e tem como principais atribuições:

- Supervisionar, administrar e auditar o cumprimento da LGPD pela empresa;
- Orientar e fiscalizar os funcionários da empresa quando a lei; e
- Ser mediador entre os titulares dos dados e a empresa, dando o suporte necessário a receber reclamações, prestar esclarecimento e adotar as providências.

Para garantir o cumprimento das normas da LGPD, a Autoridade Nacional de Dados é o órgão que fiscaliza os processos privados e proteção de dados realizados pelas empresas, podendo exigir a qualquer momento relatórios de riscos de privacidade. Cabe ao órgão também a aplicação de multas em caso de descumprimento da lei. Em virtude da atuação desse órgão, as organizações devem estar prontas para apresentar termos de uso claros ao usuário, que explicitem quais dados pessoais serão tratados e para qual finalidade. Além disso, elas devem se preparar para atender às solicitações de correção e exclusão de dados, estruturando uma equipe qualificada para realizar esses procedimentos, checagens manuais e o atendimento ao usuário, quando necessário.

Após alguns adiamentos, a LGPD entrou oficialmente em vigor em Agosto de 2020 e por conta das consequências da pandemia da Covid-19, foi então acordado que as penalizações passam a ser aplicadas a partir de agosto de 2021, como podemos observar na linha do tempo descrita na Figura 2.1.



Figura 2.1: Linha do Tempo da LGPD¹

¹Disponível em: <https://guialgpd.com.br/o-que-e-a-lgpd/>

2.1.1 Definições e comentários a LGPD

Em seu primeiro artigo, a LGPD especifica que a regulamentação dispõe sobre tratamento de dados pessoais, inclusive nos meios digitais por pessoa natural ou jurídica de direito público e privado. O regimento tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Por fim é definido que as regras mencionadas valem em todo o território nacional e devem ser respeitadas em toda União, Estados, Distrito Federal e Municípios.

Logo depois em seu artigo segundo, estabelece os fundamentos a disciplina da proteção de dados pessoais, tal como: o respeito à privacidade, a liberdade de expressão, os direitos humanos, a inviolabilidade da intimidade, da honra e da imagem entre outros. Nos artigos seguintes o regimento determina os domínios de atuação e estabelece que a norma aplica-se a qualquer operação de tratamento de dados, realizada por pessoa natural, ou pessoa jurídica de direito público ou privado desde que a operação de tratamento seja realizada ou coletadas em território nacional. Essa regulamentação estabelece um conjunto de definições relativos ao entendimento da lei, que incluem mas não estão limitados a:

- *dado pessoal*: informação relacionada a pessoa natural identificada ou identificável;
- *dado pessoal sensível*: dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- *dado anonimizado*: dado relativo a titular que não possa ser identificado;
- *banco de dados*: conjunto estruturado de dados pessoais;
- *titular*: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; e
- *controlador*: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Em seu artigo sexto, a LGPD também especifica princípios que devem ser observados no tratamento de dados, dentre os quais estão:

- *Finalidade*: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular;
- *Adequação*: compatibilidade do tratamento com as finalidades informadas ao titular;
- *Necessidade*: limitação do tratamento ao mínimo necessário para a realização de suas finalidades;

- *Livre acesso*: garantia, aos titulares, de consulta facilitada, integral e gratuita sobre a forma e a duração do tratamento de seus dados pessoais;
- *Qualidade dos dados*: refere-se garantia de exatidão, clareza, relevância e atualização dos dados;
- *Transparéncia*: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis;
- *Segurança*: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais;
- *Prevenção*: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e
- *Não discriminação*: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

A LGPD entende por “dados pessoais” qualquer informação capaz de identificar ou tornar identificável. Supondo que uma empresa não possui o *e-mail* ou nome do usuário, contudo, possui dados de navegação (*cookies* por exemplo) o usuário poderá ser encontrado através de publicidade direta. A LGPD também estabelece bases legais que são hipóteses que autorizam o tratamento de dados pessoais. Na prática, a partir do momento em que a LGPD entrou em vigor, empresas que utilizarem dados pessoais sem uma base legal adequada, estarão tratando dados de forma ilegal.

2.2 *CheckList* na Computação

Uma forma de inspecionar os artefatos dos sistemas computacionais é através do uso de técnicas baseadas em *checklists*. Essas técnicas consistem em um conjunto de perguntas criadas a partir da enumeração de itens necessários para execução de uma determinada atividade. Nesse contexto, de acordo com o artigo (Zat, 2016) ao aplicar um *checklist*, um avaliador revisa um artefato, com o objetivo de receber dicas e recomendações sobre o que avaliar através das perguntas, com o intuito de evitar futuros erros com mais facilidade.

Uma das características mais lembradas desse método de controle das atividades é a sua simplicidade e capacidade de adaptação para diferentes contextos, sejam eles no mundo digital ou mesmo real. Por exemplo, no contexto da aviação o uso de *checklists* é bastante amplo, indo desde a verificação das condições de segurança da aeronave até a avaliação da rota e suas condições meteorológicas. Dessa forma, o *checklist* é uma ferramenta que traz inúmeros benefícios. Afinal, possibilita mais organização nas atividades, minimizando falhas e esquecimentos e dando mais segurança aos processos, acelerando a produtividade e as realização das tarefas promovendo uma eficiência operacional.

2.3 Tecnologias Utilizadas

Nesta seção serão apresentadas as principais tecnologias empregadas na construção das regras de negócio da plataforma (Seção 2.3.1) bem como aquelas aplicadas na construção das diversas interfaces para interação com usuários (Seção 2.3.2).

2.3.1 *Backend*

O backend é a estrutura que possibilita a operação do sistema. Em resumo, o desenvolvimento *backend* cuida das engrenagens de uma aplicação, criando estruturas de códigos para que as funções do sistema sejam executadas (Mardan, 2018). No que segue, iremos descrever de modo sucinto as principais tecnologias e ferramentas empregadas no presente estudo.

Node js. É definido como uma plataforma que foi construída com o uso do tempo de execução do *Javascript* e foi criado em 2009 (CANTELON MARC HARTER, 2014). A estratégia utilizada no *nodejs* é bem interessante, pois permite que as aplicações sejam implementadas de forma mais rápida, como também a possibilidade de ter uma aplicação escalável torna-se muito viável (CANTELON MARC HARTER, 2014). Por fim, no *NodeJS* foi adicionado, recentemente, o *TypeScript*, o qual traz uma grande ajuda para que as suas implementações recebam uma melhor tipagem.

Docker. Funciona através de um contêiner de código aberto e permite a construção, envio e execução de aplicações que funcionam de forma distribuída (Bui, 2014). Diversas empresas e órgãos usufruem dos recursos que o *docker* oferece para trazer mais agilidade para as diversas rotinas do dia a dia. Com isso, erros tornam-se mais escassos, o que resultará numa melhor performance dos processos.

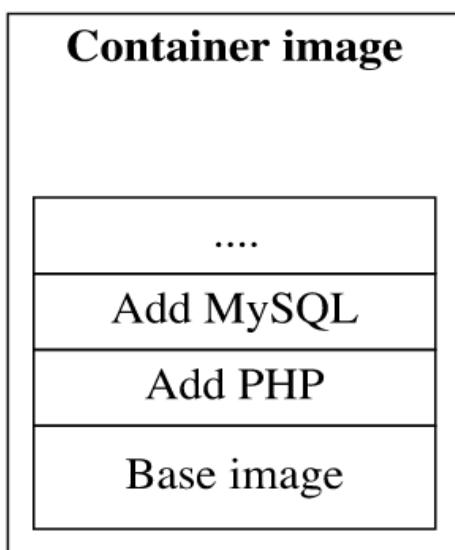


Figura 2.2: Contêiner do docker²

Prisma. É uma ferramenta de código aberto e funciona como um ORM de próxima geração (Prisma, 2022). Ele pode ser dividido em algumas partes que são:

- Prisma *Client*: Constrói as consultas de forma automática e tem segurança de tipo para *NodeJS* e *TypeScript*.
- Prisma *Migrate*: Realiza as migrações do banco de dados.
- Prisma *Studio*: Interface para editar e ver os dados do banco de dados.

Abaixo, temos uma representação do fluxo de geração do prisma:

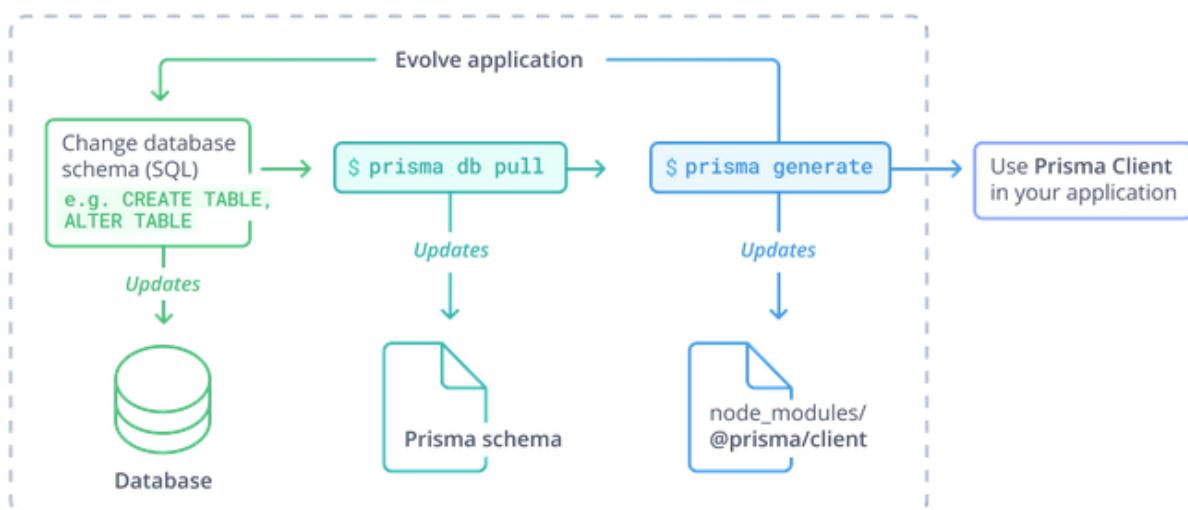


Figura 2.3: Migrações e introspecção SQL³

2.3.2 *Front-end*

O *front-end* pode ser definido como o componente de um sistema que cuida da apresentação de suas interfaces gráficas (Mardan, 2018). Ou seja, cuida das partes visuais e da interação entre usuários e a tela, gerenciando a usabilidade, o design e a experiência do usuário. No que segue, iremos descrever de modo sucinto as principais tecnologias e ferramentas empregadas no presente estudo.

Flutter. É o *SDK* de código aberto do *Google* que permite o desenvolvimento de aplicações que executam em multiplataformas a partir de uma única base de código seja na plataforma *Mobile*(*IOS* e *Android*), *Desktop* (*Windows*, *Linux* e *MAC*) ou *Web*. Seu objetivo é permitir que os desenvolvedores criem aplicativos de alta performance com uma experiência nativa em todas as plataformas.

Seu fluxo de desenvolvimento é orientado ao design e os *widgets* são os blocos básicos da interface de usuário de um aplicativo Flutter. Assim, existem *widgets* para definir elementos estruturais (e.g., botões e menus), elementos de estilo (e.g., fontes e cores), aspectos de layouts (e.g., margens e espaçamentos). Além disso, o Flutter foi projetado para facilitar a criação de novos *widgets* e a personalização dos existentes.

Durante a fase de construção, o Flutter traduz os *widgets* expressos em código numa árvore de elementos correspondente, com um elemento para cada *widget*. Cada elemento representa uma instância específica de um *widget* em um determinado local da hierarquia da árvore, como mostrado na Figura 2.4.

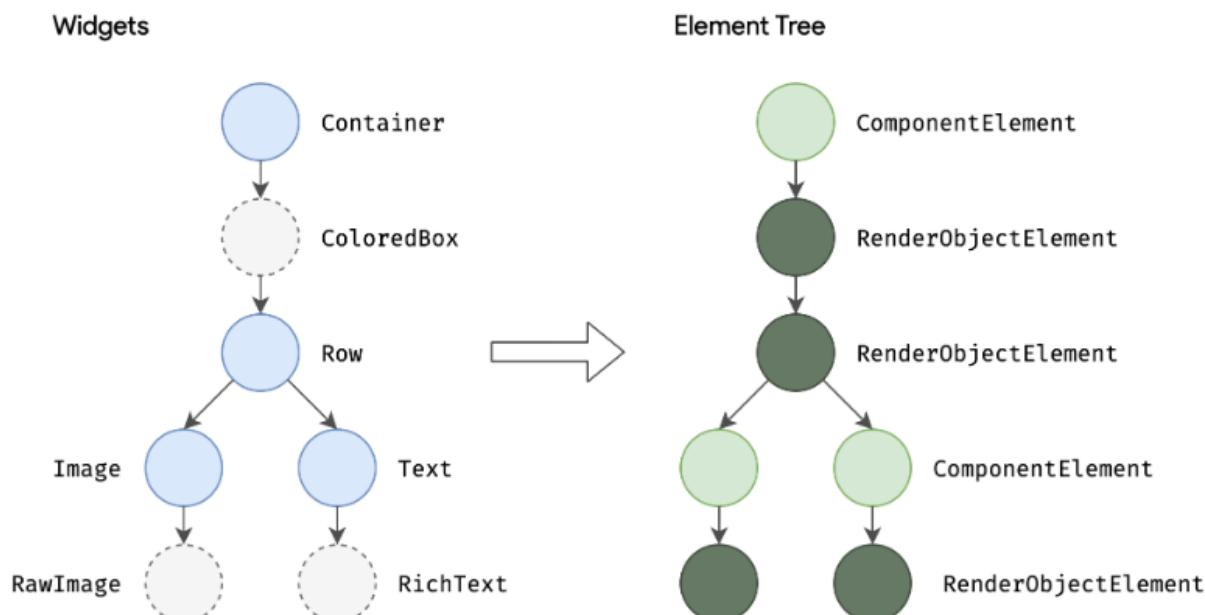


Figura 2.4: Hierarquia de Widgets⁴

Na Figura 2.5, é representado a arquitetura do Flutter WEB, que é composta pela camada *Framework*, que consiste nos principais blocos de construção/renderização do Flutter, cuja implementação é feita em *Dart*, uma linguagem de programação moderna, concisa e fortemente tipada e orientada a objetos. E a camada *Browser*, construídas em códigos *JavaScript/C++*.

⁴Disponível em: <https://docs.flutter.dev/resources/architectural-overview>

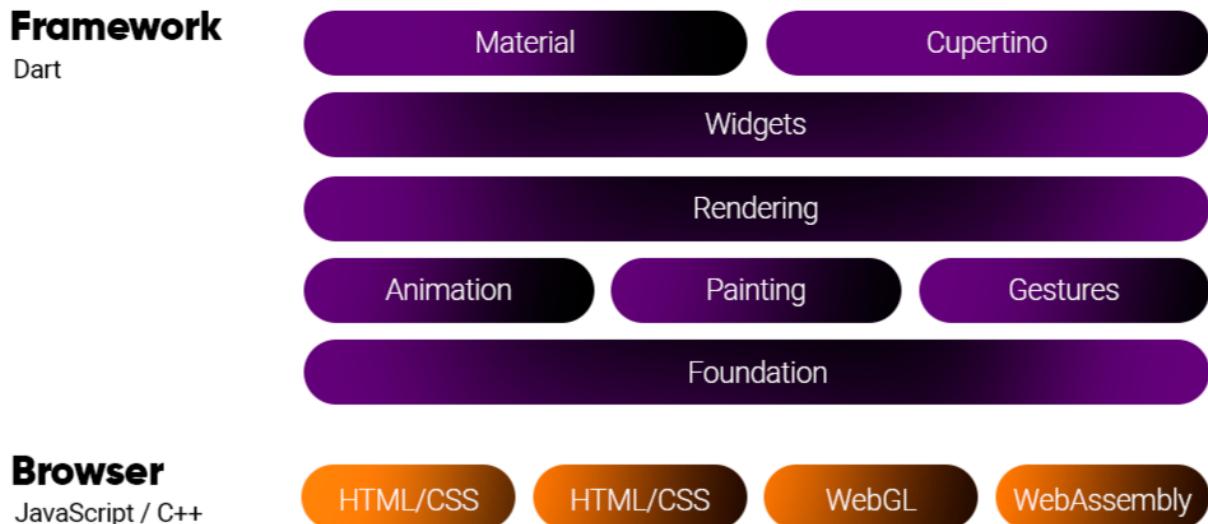


Figura 2.5: Arquitetura do *Flutter Web*⁵

Tecnologias Cliente. São as tecnologias que são executadas no lado do cliente (i.e., navegador) em uma aplicação web. Quando construímos aplicação com uso do *Flutter*, a renderização junto ao cliente é feita através de *Web Renderers*. Estes, por sua vez, utilizam uma combinação de elementos das linguagens *HTML*, *CSS* e *JavaScript* para renderizar um aplicativo *Flutter* na Web. Nos itens a seguir iremos descrever minimamente cada uma dessas linguagens.

HTML é a linguagem de marcação padrão usada para criar páginas da Web e aplicativos Web (Enterprise, 2018). Seus elementos formam os blocos de construção de páginas, representando o texto formatado, imagens, entradas de formulário e outras estruturas. Quando um navegador faz uma solicitação para uma URL, independentemente se ele está buscando uma página ou um aplicativo, a primeira coisa retornada é um documento *HTML*. Esse documento *HTML* pode referenciar ou incluir informações adicionais sobre sua aparência e o layout na forma de *CSS* ou sobre seu comportamento na forma de *JavaScript*.

O *CSS* (folhas de estilos em cascata) é usado para controlar a aparência e o layout de elementos *HTML* (Silva, 2008). Os estilos *CSS* podem ser aplicados diretamente a um elemento *HTML*, definidos separadamente na mesma página ou definidos em um arquivo separado e referenciados pela página. Os estilos são aplicados em cascata de acordo com a forma como são usados para selecionar determinado elemento *HTML*. Por exemplo, um estilo pode se aplicar a um documento inteiro, mas ser substituído por um estilo aplicado a um elemento específico.

O *JavaScript* é uma linguagem de programação dinâmica e interpretada que foi padronizada na especificação da linguagem ECMAScript (Silva, 2010). É a linguagem de programação da Web. Assim como o *CSS*, o *JavaScript* pode ser definido como atributos em

⁵Disponível em: <https://medium.com/ioasys-voices/flutter-do-mobile-à-web-7f81fd5d7f35>

elementos *HTML*, como blocos de script em uma página ou em arquivos separados. Ao trabalhar com o *JavaScript* no aplicativo Web, há algumas tarefas que você geralmente precisará executar: (i) Selecionar um elemento *HTML* e recuperar e/ou atualizar seu valor; (ii) Consultar dados em uma API Web; (iii) Enviando um comando para uma API Web (e respondendo a um retorno de chamada com seu resultado); e (iv) Executando a validação.

2.4 Processo de Desenvolvimento

O processo de desenvolvimento é o conjunto de atividades e de resultados associados, necessários para construir aplicações de alta qualidade. Ele forma a base para o controle gerencial do projeto, estabelecendo o contexto no qual os métodos técnicos são aplicados, os produtos de trabalho produzidos e os marcos estabelecidos; então, a qualidade é assegurada e as modificações são adequadamente geradas (Pressman, 2006).

Existem duas metodologias principais para gestão das atividades do desenvolvimento de *software*: cascata e ágil (Pressman, 2006). O modelo cascata é uma abordagem linear que conta com uma sequência de eventos (e.g., análise de requisitos, definição de arquitetura, desenvolvimento entre outros) para obtenção de resultados. Em um projeto onde o Modelo Cascata é usado, cada evento representa um estágio distinto de desenvolvimento de *software*, e cada estágio geralmente termina antes que o próximo possa começar (Pressman, 2006). Uma área que quase sempre fica aquém nesse modelo tradicional de trabalho é a eficácia dos requisitos. Reunir e documentar requisitos de uma forma significativa para um cliente é, muitas vezes, a parte mais difícil do desenvolvimento de *software*. Outra possível desvantagem do desenvolvimento no modelo Cascata é a possibilidade de o cliente ficar insatisfeito com o *software* entregue. Como todos os produtos são baseados em requisitos documentados, um cliente pode não ver o que será entregue até que esteja quase concluído. Nesse momento, as mudanças podem ser difíceis (e caras) de implementar.

Por outro lado, o modelo Ágil é uma abordagem iterativa que enfatiza a entrega rápida de uma aplicação em componentes funcionais completos (Sutherland, 2014). Em vez de criar tarefas e programações, todo o tempo é dividido em fases chamadas “*sprints*”. Cada *sprint* tem uma duração definida (geralmente em semanas) com uma lista de entregas planejada em seu início (Schwaber; Sutherland, 2011). Entregas são priorizadas pelo valor do negócio, conforme determinado pelo cliente. Se todo o esforço planejado para o *sprint* não puder ser concluído, o trabalho é redimensionado e as informações são usadas para o planejamento futuro. À medida que o trabalho é concluído, ele pode ser revisado e avaliado pela equipe do projeto e pelo cliente, por meio de compilações diárias e demonstrações de final de *sprint*. A metodologia Ágil depende de um nível bastante alto de envolvimento do cliente durante todo o projeto, mas especialmente durante as revisões (Schwaber; Sutherland, 2011).

Para gestão ágil do processo de desenvolvimento, um *framework* relevante e mundialmente difundido é o *Scrum* (Bhavsar; Shah; Gopalan, 2020). Este arcabouço representa um

conjunto de boas práticas empregado no gerenciamento de projetos. Focado nos membros da equipe, o *Scrum* torna os processos mais simples e claros, pois mantém registros visíveis sobre o andamento de todas as etapas. Assim, os participantes sabem em que fase o projeto está, o que já foi concluído e o que falta ser feito para a sua entrega. A metodologia também possibilita que produtos sejam apresentados em menor tempo, sem deixar de lado a qualidade.

O processo dessa metodologia começa com a definição do responsável pelo projeto, chamado *Product Owner*. Ele é encarregado pela equipe e pela supervisão das etapas (Schwaber; Sutherland, 2011). Ele desenvolverá uma lista de objetivos chamada *Product Backlog*, cujos itens serão distribuídos entre os integrantes para sua realização. Com as demandas delegadas, cria-se uma nova lista chamada *Sprint Backlog*, que baseará as *Sprints*. Antes de iniciar a realização das tarefas, ocorre a *Sprint Planning*, reunião na qual se decidem os prazos das *sprints*. Após a definição da estratégia e da previsão de entrega, devem acontecer as *Daily Scrums*, reuniões diárias que colocam todos a par do que já aconteceu, o que tem sido desenvolvido e quais serão os próximos passos (Schwaber; Sutherland, 2011). Com a conclusão das etapas, há a última reunião chamada de *Sprint Retrospective*. Nela, se analisam os pontos positivos e negativos do projeto e o resultado final para validação. Uma vez finalizado, tem início o planejamento da próxima *Sprint*. Todo esse processo é exemplificado na Figura 2.6 abaixo.

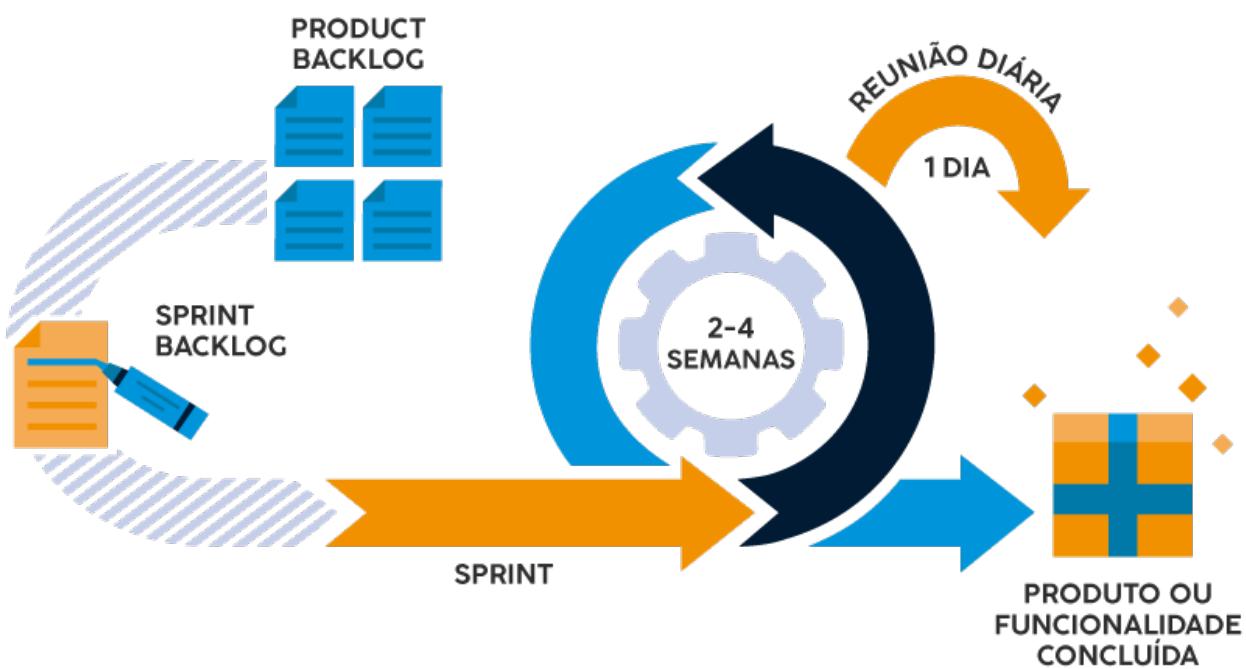


Figura 2.6: Funcionamento do Scrum⁶

Outra metodologia ágil bastante utilizada é o *Kanban*. Ela se baseia em um quadro que divide as tarefas em colunas *TO DO*(à fazer), *IN PROGRESS*(fazendo) e *DONE*(concluído). Todos os requisitos são colocados na primeira coluna do quadro e cada membro da equipe fica responsável por implementá-los e entregá-los. Cada tarefa tem sua descrição, prioridade e seu prazo de entrega. Assim como no *Scrum*, as tarefas prioritárias devem ser executadas primeiro. A ideia central do *Kanban* é o foco na produtividade. Cada membro não pode executar mais de uma tarefa por vez. Seu método é tão simples que pode ser personalizado de inúmeras maneiras para atender as demandas de uma empresa.

⁶Disponível em: <https://www.tecnicon.com.br/upload/public/Blog/post-scrum.png>

Capítulo 3

Trabalhos Relacionados

Neste capítulo são apresentados os trabalhos relacionados a presente pesquisa. Inicialmente, Raposo e colegas (Rapôso et al., 2019) realizaram uma revisão bibliográfica com objetivo de reunir, de forma sistemática em um período de cinco anos, artigos que englobam a LGPD, envolvendo tecnologia da informação. Como resultado a partir de um estudo de 438 artigos, 12 tinham relação direta com o tema. O autor conclui que existem poucos artigos relacionando a temática desta legislação com tecnologia da informação, demonstrando existe uma necessidade de novas produções sobre a aplicabilidade do tema principalmente para as empresas. Em seguida, De Carvalho e colegas (Carvalho; Freitag,) desenvolveram um estudo com objetivo de identificar por meio de uma revisão sistemática da literatura baseada no protocolo PRISMA os aspectos que devem ser considerados por uma organização para se adequar à LGPD. Como resultado o autor defende que as empresas devem revisar suas políticas de segurança da informação baseando-se na LGPD, reavaliando processos, bem como verificar a necessidade de adequação tecnológica com o objetivo de suportar o aumento do volume de dados.

É importante mencionar que na *Lei Geral de Proteção de Dados (LGPD): Guia de implantação* (Garcia et al., 2020) é definida uma metodologia para implementar a transformação da LGPD de forma sustentável, eficiente e à longo prazo, em um programa transformador e multidisciplinar, com controles, métricas e evidências claras de que o direito está sendo respeitado. Com base nisso, no trabalho de Spadaccini e Viola (Teffé; Viola, 2020) foi feita uma análise das bases legais da *Lei Geral de Proteção de Dados* para o tratamento de dados diante da necessidade de enquadrar todo o tratamento de dados em uma base legal determinada, prevista pelos artigos 7º e 11º da Lei. Como resultado destacou o caráter preventivo dessas bases legais visando a proteção de dados. Similarmente, o trabalho desenvolvido por Roque (Roque, 2019) se propõe a analisar os principais aspectos processuais relacionados à tutela coletiva na Lei n.º 13.709/2018 no que tange as categorias dos direitos coletivos e decisões estruturantes da LGPD. Como resultado, evidencia que a legislação vigente demandará razoável esforço dos agentes de tratamento para que atuem de acordo com as suas determinações.

Com relação a aplicação da LGPD, De Oliveira e colegas (Oliveira et al., 2019) abordaram a temática de segurança da informação sob os aspectos da lei brasileira que trata da proteção de dados dos usuários aplicada a *IoT*, enfatizando aspectos como coleta e transmissão de dados bem como o armazenamento de dados sigilosos visando a discussão sobre os principais conceitos requeridos pela LGPD. Os autores destacam que são grandes os desafios do tema proposto devido a complexabilidade de aplicar requisitos de segurança a sistemas com capacidade de processamento e memória limitadas.

Por sua vez, o trabalho de Fernandes e colegas (Fernandes, 2018) apresenta uma metodologia usando engenharia de requisitos baseada em modelos para elaborar um catálogo reutilizável de dados pessoais e requisito de proteção alinhados com a *GDPR*. Seguindo uma abordagem de separação de interesses, o catálogo pode servir ao propósito de construir sistemas de informação capazes de se comunicar com aqueles que processam dados pessoais de indivíduos para materializar a proteção regulatória de dados.

Finalmente, Sánchez e colegas (Sánchez; Viejo; Batet, 2021) apresentaram um sistema que avalia automaticamente as políticas de privacidade. A proposta quantifica o grau de conformidade da política com relação às metas de proteção de dados declaradas pela *GPDR*; e apresenta pontuações de privacidade claras e intuitivas para o usuário.

De um modo geral, observa-se que há um crescente e recente interesse da comunidade científica em explorar a temática de proteção de dados. Notamos que existe alguns estudos secundários tentando mapear a pesquisa realizada na área. Adicionalmente, notamos a existência de outros estudos avaliando a aplicação de técnicas para verificar a adequabilidade de sistemas de determinadas contextos a normas como LGPD e *GDPR*. Assim, este estudo promove avanço no estado da arte pois realiza a aplicação de *checklist* para auxiliar organizações e profissionais na obtenção de conhecimento sobre a LGPD no intuito de adequação de seus projetos de software. Dessa forma, na medida do nosso conhecimento, o presente estudo é pioneiro na utilização da técnica de *checklist* para avaliação específica no contexto da LGPD.

Capítulo 4

Configuração de Estudo

Neste capítulo serão descritas todas as etapas metodológicas do presente estudo. Inicialmente, iremos descrever o processo de análise e definição de requisitos (Seção 4.1). Em seguida, exibiremos os detalhes para definição arquitetural (Seção 4.2) e o processo empregado para o desenvolvimento da plataforma *LGPD Compliance* (Seção 4.3). Por fim, discutiremos as etapas de validação (Seção 4.4) e implantação (Seção 4.5) da plataforma.

4.1 Análise e Definição de Requisitos

O propósito desta etapa é guiar o desenvolvimento para produzir o *software* de acordo com o que foi solicitado nos requisitos (Camoglu; Kandemir, 2019). Se os requisitos não forem alcançados corretamente, existe uma probabilidade elevada de falha no projeto, mesmo que as demais etapas de projeto sejam realizadas de modo correto (B; Wiegers; Ebert, 2001).

Em vista disso, foram estabelecidos dois conjuntos de requisitos. Primeiramente, buscou-se definir os requisitos *funcionais* da plataforma que definem essencialmente as necessidades que devem ser atendidas. Em seguida, buscou-se elencar os requisitos *não-funcionais* que consistem nas restrições de operação da plataforma bem como os atributos de qualidade pretendidos. Exemplos típicos deste tipo de requisitos envolvem desempenho, usabilidade, confiabilidade, segurança, disponibilidade, manutenibilidade bem como restrições ligadas às tecnologias envolvidas.

O projeto *LGPD Compliance* é definido como uma plataforma de adequação da LGPD. Consequentemente, necessitará de (i) um ambiente privado para os usuários bem como (ii) um *checklist* que será disponibilizado através de um *quiz*. Baseado nessa definição inicial, estabeleceu-se uma lista preliminar de requisitos funcionais conforme descrição na Tabela 4.1.

| ID | REQUISITOS FUNCIONAIS |
|------|--|
| RF01 | <i>Checklist</i> de adequação LGPD em formato de <i>quiz</i> |
| RF02 | Seção de resultados, baseado nos dados recebidos no <i>quiz</i> |
| RF03 | Score (sistema de pontuação relativo ao <i>quiz</i>) |
| RF04 | Seção de sugestões de adequação a LGPD (baseado no <i>quiz</i>) |
| RF05 | Seção para visualizar histórico de respostas ao <i>quiz</i> |
| RF06 | Ambiente para usuário administrador |
| RF07 | Administrador: Consulta de Usuários |
| RF08 | Administrador: Ambiente para análise estatística |

Tabela 4.1: *Lista Preliminar de Requisitos Funcionais - LGPD Compliance*

Em seguida, buscou-se a definição de uma lista preliminar de requisitos *não-funcionais* considerados prioritários no desenvolvimento da plataforma. Baseado no crescimento de sistemas web e na facilidade de acesso nos dias atuais os seguintes requisitos não funcionais foram estabelecidos e disponibilizados na Tabela 4.2.

| ID | REQUISITOS NÃO FUNCIONAIS |
|-------|---|
| RNF01 | Sistema deve ser criado em plataforma Web responsivo |
| RNF02 | Todo acesso deve ser realizado de forma online |
| RNF03 | A aplicação deve ser de fácil compreensão e usabilidade |
| RNF04 | A arquitetura do sistema deve ser escalável |
| RNF05 | Hospedagem dos serviços em servidor online |
| RNF06 | Seção para visualizar histórico de respostas ao <i>quiz</i> |
| RNF07 | Ambiente para usuário administrador |
| RNF08 | O sistema deve ser seguro |

Tabela 4.2: *Lista Preliminar Não Funcionais - LGPD Compliance*

Cabe ressalva de que a lista final de requisitos *funcionais* e *não-funcionais* emergiram de um processo iterativo entre os autores deste estudo e especialistas externos (i.e., um profissional de desenvolvimento de software e dois profissionais da área de direito). Mediante processo colaborativo, os requisitos foram refinados e validados visando a organização das funcionalidades do *LGPD Compliance*.

4.2 Definição Arquitetural

A arquitetura do sistema *LGPD Compliance* mencionada acima é baseada na arquitetura MVC (*Model, View, Controller*). Dessa forma, temos o *Model* que serve para armazenar e persistir os dados (Módulo Database), a *View* que servirá apenas para exibir as informações enviadas pelo *Controller* ao (Módulo Frontend) e o *Controller* que é responsável por

fazer o intermédio entre o *Model* e a *View* e também responsável por toda a lógica do sistema(Módulo *Backend*).

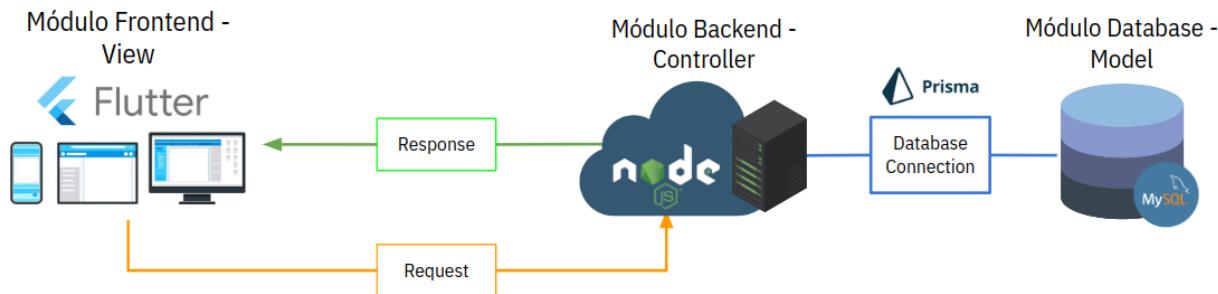


Figura 4.1: Arquitetura do Sistema LGPD

Conforme descrição da Figura 4.1, a arquitetura do sistema consiste em três principais módulos: *Database*, *Backend* e *Frontend*.

- O primeiro módulo definido como *Database* e implementado em *MySQL*, é responsável por armazenar todos os dados da aplicação de forma estruturada, utilizando-se de modelos que são mapeados diretamente para as regras do negócio.
- O segundo módulo, chamado de *Backend* desenvolvido em *NodeJs*, tem como principal finalidade de receber, processar e responder às solicitações oriundas do *Frontend*. Essa comunicação é realizada através do protocolo *http* utilizando como método de comunicação *request-response* ou *request-reply*. Além disso, para realizar seu papel de forma adequada o backend precisa se comunicar com o *Database* por meio de operações de leitura e escrita.
- O terceiro módulo, *Frontend* foi desenvolvido utilizando a tecnologia *Flutter*, destinado a plataforma WEB de forma responsiva. Esse módulo tem como principal responsabilidade, abrigar a interface para utilização do Sistema LGPD por parte do usuário, funcionalidades estas que em partes usam o Módulo de *Backend*.

4.3 Desenvolvimento de Software

Para gestão das atividades do processo de desenvolvimento da plataforma *LGPD Compliance* foram aplicadas duas metodologia ágeis: *Scrum* e *Kanban*. Tais metodologias foram escolhidas em virtude de serem amplamente utilizadas para o desenvolvimento de sistemas de software onde os requisitos tendem a alterar ao longo do processo, como é o caso da plataforma *LGPD Compliance*. Utilizou-se de práticas ágeis como *Sprint Planning* para

planejamento e execução de reuniões para a criação do *Product Backlog* com vistas a: (i) distribuir tarefas para cada integrante do time desenvolvimento e (ii) estimar o tempo requerido para conclusão destas tarefas. Adicionalmente, utilizou-se da prática de *Dailies Scrum* que eram reuniões diárias com objetivo de acompanhar o andamento das atividades do projeto bem como identificar algum impedimento para conclusão de alguma tarefa.

Além disso, aplicamos a ideia do Quadro Kanban (Figura 4.2) no qual, renomeamos e criamos as seguintes colunas: *Backlog* (lista de tarefas pendentes), *In Progress* (lista de tarefas em andamento), *Review* (lista de tarefas para revisão), *Master* (lista de tarefas já revisadas, mas não foram realizadas a implantação delas), *Stable* (lista de tarefas que já foram realizadas a implantação). Dessa forma, foram desenvolvidos os módulos que serão apresentados a seguir.

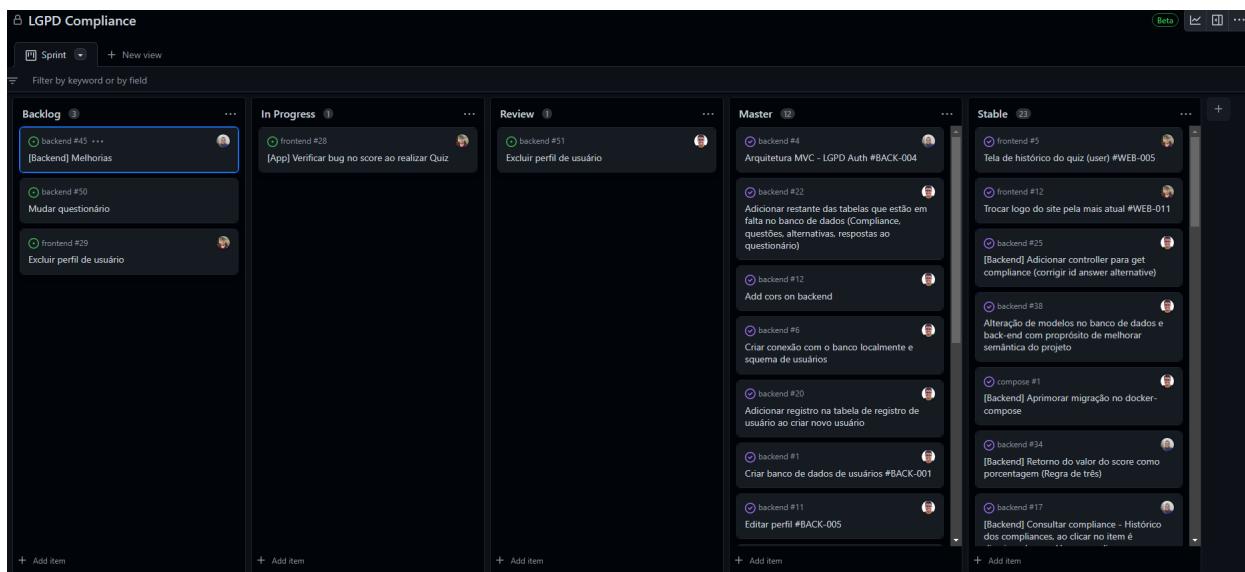


Figura 4.2: Quadro de tarefas baseado na metodologia Kanban

4.3.1 Desenvolvimento do Módulo Database

O módulo *Database* ou traduzindo *Banco de dados* pode ser definido como um repositório sistemático de informações. A principal finalidade do Banco de Dados é armazenar os dados de forma segura, organizada e estruturada. Existem diversos tipos de banco de dados atualmente. No projeto *LGPD Compliance* foi estimado o uso de um *banco de dados relacional*. Esse tipo de banco de dados tem como vantagens a organização de informações relacionadas e armazenadas em tabelas. Um banco de dados relacional pode ser considerado onde há necessidade de informações na qual os dados se relacionam entre si e devem ser gerenciados de maneira segura e consistente, com base em restrições e princípios.

Visando suportar a documentação do sistema bem como guiar as atividades de desenvolvimento, criou-se um modelo do banco de dados. Para tanto, foi utilizada a técnica

de *Diagrama de Entidade Relacionamento* para estruturar o banco de dados e visualizar de forma diagramada o projeto da camada de dados da plataforma. Neste modelo estão definidos alguns conceitos conforme o que segue:

- **Entidades:** São representações de objetos do "mundo real".
- **Atributos:** São as características específicas de uma entidade.
- **Relacionamentos:** Um relacionamento consiste em uma associação entre entidades.

Na Figura 4.3 é mostrado o diagrama de entidade relacionamento do projeto *LGPD Compliance*. A seguir será definido o papel de cada entidade e os seus respectivos relacionamentos.

- *User*: Nessa entidade é representado o usuário do sistema e suas principais informações como Nome, *e-mail*, tipo, etc.
- *User Register*: Nessa entidade é feito o registro do usuário, essa tabela possui relação direta com usuário e a tabela de autenticação. Essa entidade serve essencialmente para armazenar a data de criação do usuário e o status da conta do mesmo. Por meio desta entidade é possível desativar ou deletar todos os dados relativos a um usuário (incluindo suas respostas à um quiz).
- *Authentications*: Essa tabela armazena dados de autenticação do usuário como *e-mail* e senha criptografada.
- *Quiz Answer*: Nessa entidade são persistidas a resposta ao um questionário específico do *LGPD Compliance*, essa entidade tem um papel fundamental no projeto, porque possui relação direta com o usuário e todas as outras entidades do modelo de forma direta ou indireta. Essa entidade possui relação direta com a entidade *Question Answer*, visto que a resposta a um questionário consiste de um conjunto de respostas à questões de um questionário.
- *Question Answer*: Essa entidade representa a resposta a uma questão específica de um quiz. Está diretamente relacionada com a entidade *Question* e *Alternative*.
- *Quiz*: Essa entidade representa um questionário do *LGPD Compliance*. Possui relação direta com a entidade *Question* uma vez que, um questionário é formado por um conjunto de questões.
- *Section*: Essa entidade é utilizada para estruturar o quiz em segmentos da LGPD. Por esse motivo, a entidade possui relação com de 1 para muitos com a entidade *Question* e de semelhante modo com a entidade *Feedback*.

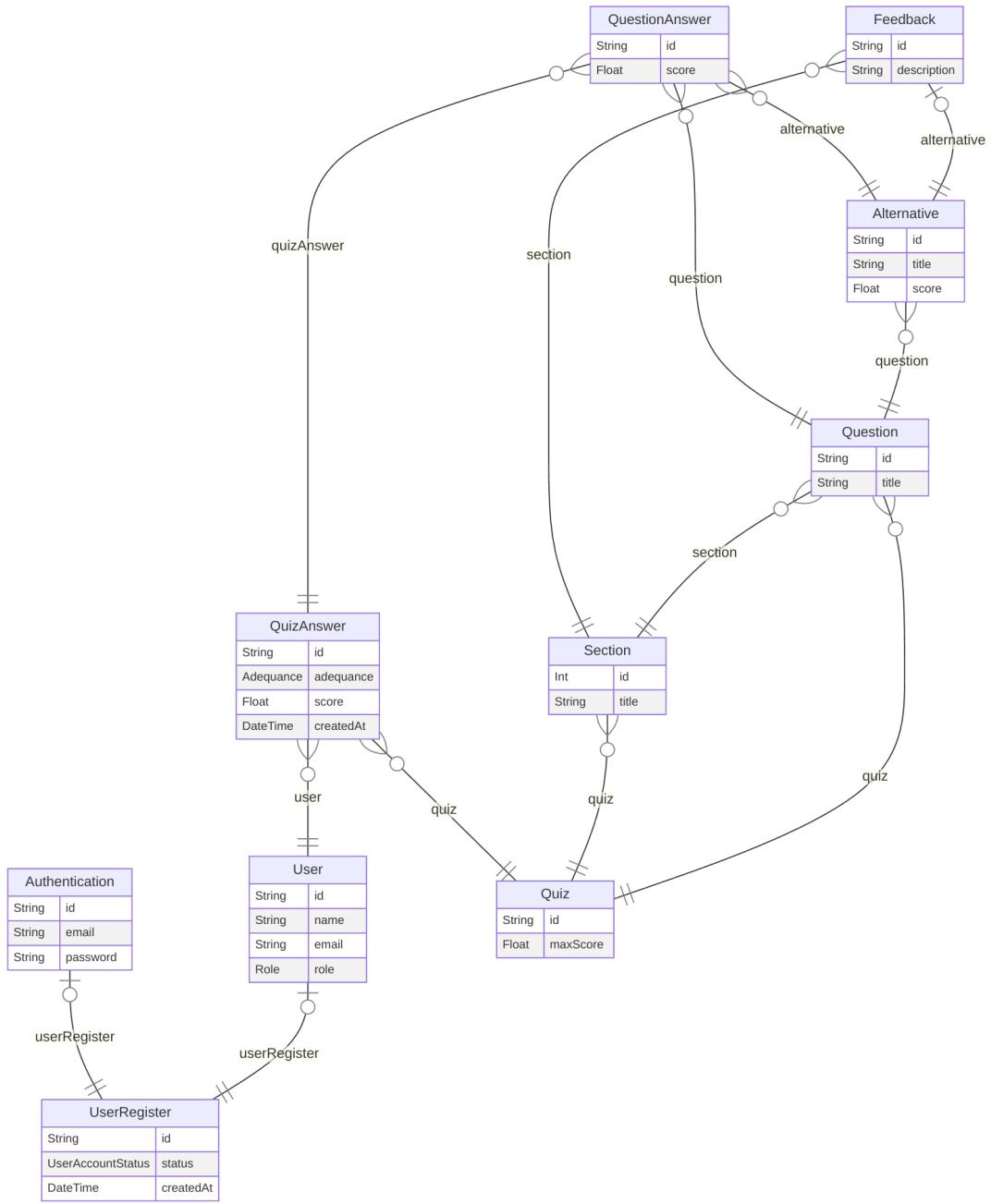


Figura 4.3: Diagrama de Entidade e Relacionamento LGPD Compliance

- *Question*: Essa entidade representa uma questão objetiva no modelo de dados e possui relação direta com a tabela *Alternative*. Cada questão tem um conjunto de alternativas associadas para que o usuário possa marcar sua resposta.
- *Alternative*: Como mencionado anteriormente essa entidade representa a alternativa de uma questão. Quando o usuário marca uma alternativa como correta, seu identificador único é adicionado no conjunto de respostas, tornando as respostas do usuário estruturadas facilitando o acesso e representação dos dados.
- *Feedback*: Essa entidade possui relação direta com a entidade *Alternative* e serve para guardar as sugestões de adequação quando o usuário marca uma alternativa que não está adequada com a LGPD.

A manipulação do banco de dados da plataforma *LGPD Compliance* foi realizada por meio do Prisma ORM (do inglês, *Object-Relational Mapping*). Através dessa ferramenta foi desenvolvido um esquema que representa todos os modelos ou classes que serão utilizadas no projeto. O prisma interpreta esse arquivo gerando uma migração para a linguagem *MySQL*. A partir disso, todas as tabelas e relacionamentos são criados no banco de dados como mostrado na Figura 4.4.

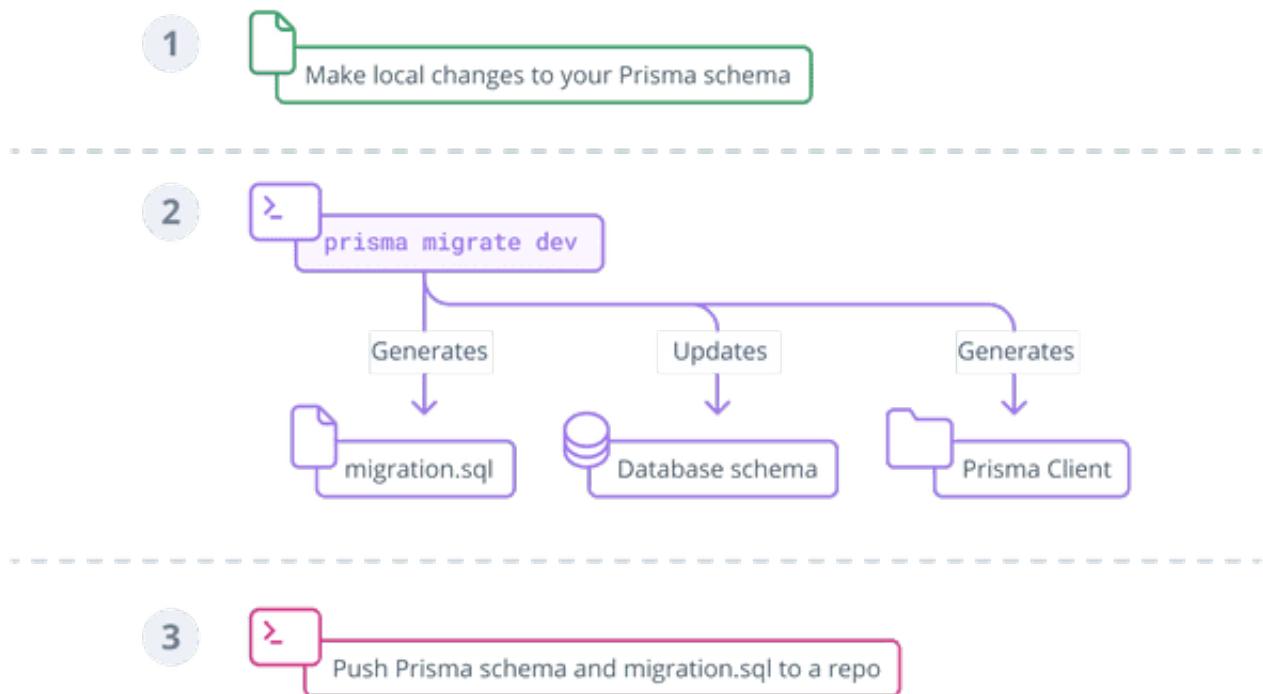


Figura 4.4: Fluxo de criação do Banco de dados usando Prisma.¹

¹Disponível em: <https://www.prisma.io/docs/concepts/overview/what-is-prisma>

4.3.2 Desenvolvimento do Módulo *Backend*

Conforme discussão apresentada na seção 4.2, o módulo *frontend* se comunica com o módulo *backend* por meio de requisições. Na Figura 4.5 é apresentado o caminho das requisições através de camadas internas do *backend*. A seguir, a finalidade de cada camada será detalhada com o objetivo demonstrar em alto nível como o *backend* processa e responde requisições.

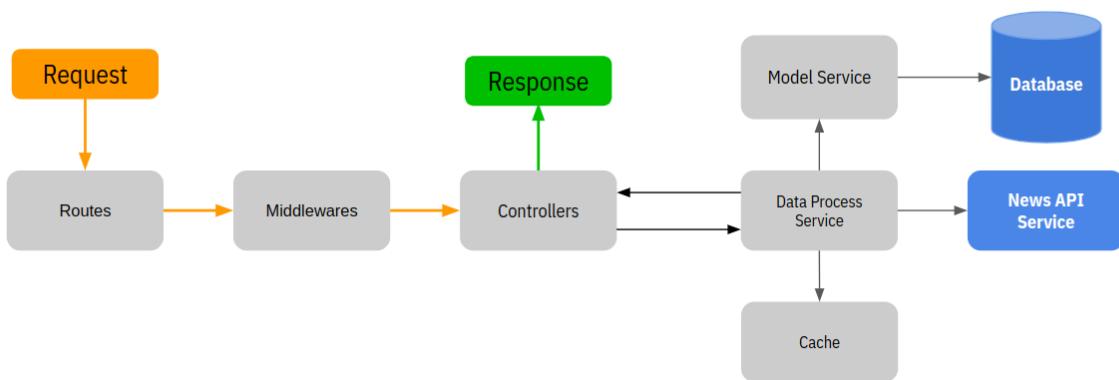


Figura 4.5: Diagrama de Fluxo Dados do Backend

- **Routes.** Refere-se a determinar como a aplicação responde a uma requisição do frontend por meio de uma *URL* (inglês *Uniform Resource Locator*) e um método *HTTP* específico (e.g., *GET*, *POST*, *PUT* entre outros). Todas as requisições passam por essa camada antes de serem processadas.
- **Middlewares.** São funções que podem executar alguma tarefa antes da requisição chegar no *controller*. No *backend*, os validadores e métodos que verificam se o usuário está autenticado ficam localizados nessa camada.
- **Controllers.** Nessa camada são processadas as requisições e definidas as respostas que serão enviadas para o módulo *frontend*. Antes de enviar uma resposta normalmente o *controller* se comunica com o banco de dados ou serviços externos antes enviar a resposta para o *frontend*.
- **Data process service.** Nessa camada os dados da requisição são processados e retornados para o *controller* em formato json. Durante o processamento é possível que esse serviço se comunique com a Cache, *Model service* ou *API's* externas.

- **Model service.** Essa camada é responsável por criar uma interface entre o banco de dados e o controller. Por meio dela são realizadas queries de leitura e escrita no banco de dados.
- **Cache.** É um serviço dentro do *backend* utilizado para minimizar as requisições em serviços externos e reduzir a latência de resposta entre o *frontend* e *backend*. O *LGPD Compliance* possui uma pagina de Notícias sobre a LGPD oriunda de um serviço externo. Diante disso, serviço de cache memoriza os dados da requisição de uma API externa, de modo que se outra requisição do mesmo tipo for realizada em um curto intervalo de tempo, os dados estarão disponíveis sem a necessidade de uma nova requisição.

4.3.3 Desenvolvimento do Módulo *Frontend*

Para uma melhor organização o módulo *frontend* foi dividido em submódulos que serão citados e explicados no que segue. Todos esses submódulos seguem o mesmo padrão e encontram-se estruturados conforme descrição da Figura 4.6.

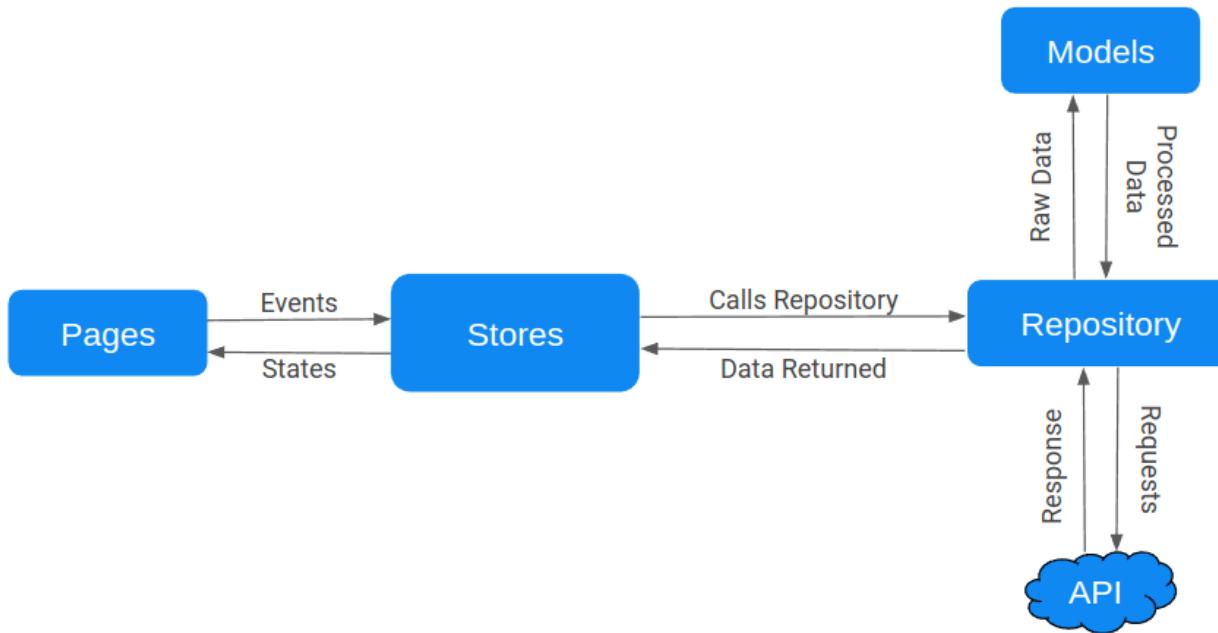


Figura 4.6: Digrama Genérico do Módulo *Frontend*

- *Pages*: É onde contém os *Widgets* e a tela com a qual o usuário interage. Cada interação como um clique de botão, uma rolagem, etc, pode ser mapeada para um *Event* e passada para a *Store*.
- *Stores*: Uma *Store* pega o *State* atual e o *Event*, e o mapeia para um estado diferente usando a lógica de negócios necessária. Também é responsável por interagir com o *Repository* para quaisquer dados necessários.

- *Repository*: Atua como uma interface entre uma *Store* e a API. Na medida que uma *Store* requer alguma informação, o *Repository* faz a requisição na API, após a resposta, o dado é tratado no *Models* e retornado para *Store*.
- *Models*: Recebe os dados vindo da API e faz o tratamento e processamentos desses dados.

Submódulo Autenticação

Nesse submódulo fica toda a parte de realização do cadastro e login na plataforma. Aprofundando um pouco sobre o funcionamento da parte de cadastro, *AuthStore* possui um método chamado *signUp* responsável por reunir todas as informações inseridas pelo usuário na parte da *SignUpPage* e passa-los para o *AuthRepository*, que possui um método com a finalidade de fazer uma requisição POST com a API para realização do cadastro. Essa requisição sempre haverá uma mensagem de resposta (i.e., sucesso ou falha) exibida oportunamente ao usuário.

De forma semelhante, acontece quando um usuário realiza o login na plataforma. O *AuthStore* possui um método chamado *signIn* que é responsável por agrupar todas as informações de login inseridas pelo usuário em *SignInPage* e passa-las para o método também chamado de *signIn* dentro de *AuthRepository*. Este é encarregado de fazer uma requisição POST com a API onde, em caso de sucesso, é retornado todos os dados desse usuário em forma de JSON. Estes dados formatados serão tratados pelo *UserModel* e, posteriormente devolvido para o *AuthStore* em forma de objeto.

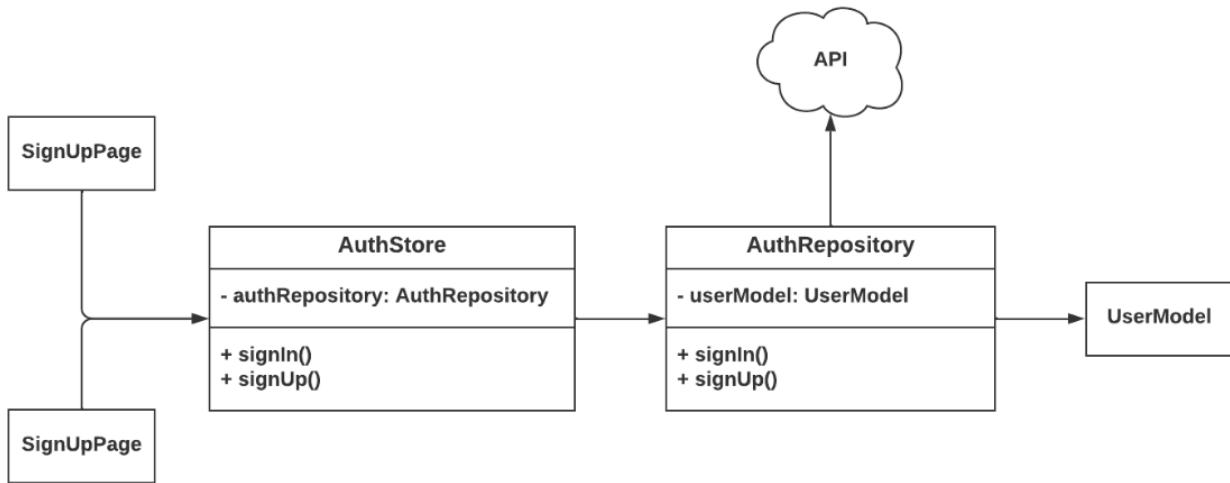


Figura 4.7: Diagrama de classe simplificado do Submódulo de Autenticação

Finalmente, após realizar o login, existe uma *flag* retornada da API no qual é possível identificar se o usuário é do tipo comum ou administrador. Baseado nisso, ele é redirecionado

para o Submódulo Plataforma Comum ou Submódulo Plataforma Administrador, descritos no que segue.

Submódulo Comum da Plataforma LGPD

Este submódulo é responsável pela Home, Edição do Cadastro, Quiz e Histórico. Cada uma dessas funcionalidades tem suas respectivas classes de *Pages*, que são encarregadas de exibir a parte visual e as classes *Stores* (i.e., *HomeStore*, *ProfileStore*, *QuizStore*, *HistoricStore*) que são atribuídos métodos para interagir com *ComplianceRepository* com a função de requisitar dados da API. O *ComplianceRepository* possui os seguintes métodos:

- *getNewsLGPD*. Realiza uma requisição GET para API e é retornado um JSON no qual é transformado em um objeto do tipo *NewsModel*, contendo notícias relacionadas a LGPD.
- *updateUser*. Efetua uma requisição PUT, onde é passado no *body* as alterações realizadas pelo usuário de e-mail ou nome. E como resposta, é retornado um JSON com os dados do usuário atualizado que posteriormente é transformado em um objeto do tipo *UserModel*.
- *getCompliance*. Realiza uma requisição GET para API e é retornado um JSON onde, é convertido em um objeto do tipo *ComplianceModel*, contendo as perguntas do quiz.
- *submitQuizCompliance*. Responsável por realizar uma requisição POST, onde é passado no body as alternativas referentes ao que o usuário marcou no quiz. Por fim, a resposta dessa requisição é devolvida em formato JSON, sendo transformado em um objeto do tipo *FeedbackModel*. É digno mencionar que este objeto contém os *feedbacks* e o *score* de acordo com as respostas do usuário.
- *getQuizHistoric*. Possui a função de efetuar uma requisição GET para API, no qual é retornado um JSON, que por sua vez é convertido em um objeto do tipo *HistoricModel*. Este objeto contém uma lista de todos os *quizzes* realizados pelo usuário.

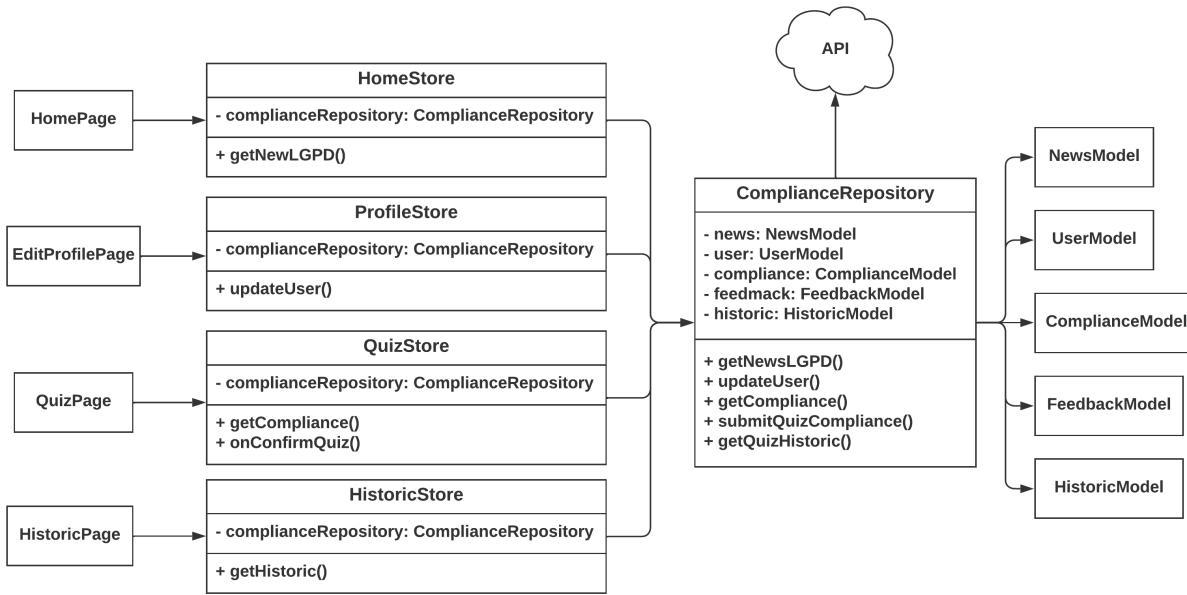


Figura 4.8: Diagrama de classe simplificado do Submódulo Plataforma LGPD

Submódulo Administrador da Plataforma LGPD

Este submódulo é encarregado das opções de *Home Admin* e *Lista de Usuários*. Essas duas opções tem suas respectivas classes de *Pages* responsáveis pela visualização por parte do usuário. Há também a classe *AdminStore* que interage diretamente com *AdminRepository*. Este, por sua vez, possui os métodos *getInfoGraphic* e *getInfoUsers* que serão chamadas a medida que necessitará requisitar informações.

O método *getInfoGraphic* é responsável por realizar uma requisição do tipo GET. Onde, é retornado um JSON contendo informações gerais sobre as ações realizadas pelos usuários comuns, por exemplo, quantidade de quiz respondidos durante a semana e por fim, convertido em um objeto do tipo *GraphicModel*. Por outro lado, o método *getInfoUsers* é atribuído a função de requisitar da API via GET, informações dos usuários cadastrados, como, o histórico dos *quizzes* respondidos de cada usuário com seus respectivos scores e *feedbacks*.

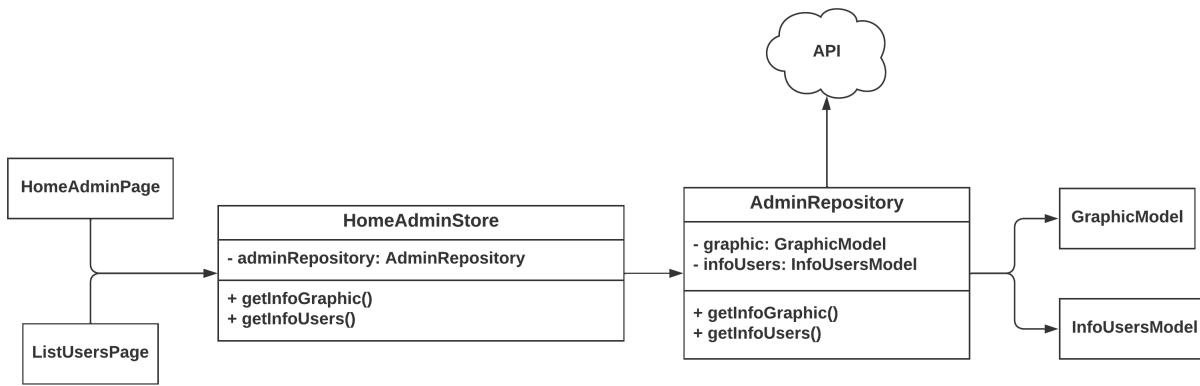


Figura 4.9: Diagrama de classe simplificado do Submódulo de Plataforma LGPD Admin

4.4 Validação

A etapa de validação de um sistema de *software* é de extrema importância pois nele é possível (i) a identificação de cenários que não foram mapeados anteriormente durante o desenvolvimento e a (ii) a comprovação da eficácia do *software* em cenários já mapeados. Novos cenários proporcionam ao *software* uma aderência às expectativas dos usuários uma vez que são identificadas lacunas não observadas na etapa de definição arquitetural e na etapa de desenvolvimento. Isso proporciona ao sistema uma maior robustez quanto ao seu resultado que será encaminhado para a implantação posteriormente.

Para validar a eficácia do processo de desenvolvimento alguns testes de usabilidade foram realizados. Os testes usabilidade proporcionam ao *software* um maior nível de qualidade, pois nele as funcionalidades são testadas com um olhar mais crítico, visando evitar que surjam problemas quando a aplicação estiver disponível para os usuários finais. Vale destacar também que no processo de validação, é de suma importância a opinião dos usuários do sistema relativo ao uso da ferramenta até o momento, se de fato as soluções são viáveis, quais foram suas principais dificuldades durante o uso e sugestões de melhoria (Lima et al., 2020).

Validações do módulo *Frontend*. Para validação deste módulo, testes de usabilidade foram utilizados com o objetivo de provar a consistência e a solidez da interface ao colocá-la para o uso em situações comuns. Dessa forma, o *LGPD Compliance* foi compartilhado com um pequeno grupo de usuários com o objetivo de receber *feedbacks* para identificação de falhas ou oportunidades de melhoria da plataforma de modo geral.

Validação do módulo *Backend*. Para validação deste módulo foram realizadas validações nos principais métodos utilizados na aplicação, como: login, cadastro de usuários, notícias sobre a LGPD e envio dos dados do *quiz*, já com as respostas preenchidas. Esse processo também contou com a participação de um especialista na área de engenharia de software externo ao time de desenvolvimento.

Validação do módulo *Database*. As validações deste módulo foram realizadas através da análise dos desenvolvedores aos dados gerados pelo ORM no banco de dados. Dois componentes do time de desenvolvimento revisaram os artefatos de software bem como os resultados gerados por estes com intuito de garantir o correto funcionamento.

4.5 Implantação

A etapa de implantação do *software* é de extrema relevância pois após sua realização o sistema ficará disponível para acesso por parte dos usuários finais. É necessário atenção, pois qualquer erro nas atividades desta etapa pode ocasionar resultados diferentes do esperado e, como consequência, gerando insatisfação por parte dos futuros utilizadores do *software*.

Para a implantação do sistema, utilizou-se os serviços de computação em nuvem da *Hostinger*. Esta plataforma foi escolhida em virtude de ser um provedor de serviços de computação em nuvem de relevância em diversos países. Adicionalmente, identificamos que sua base de serviços possuía excelente custo benefício se considerados os requisitos da plataforma *LGPD Compliance*. Ademais, esta plataforma foi hospedada no seguinte domínio: <https://www.lgpdcompliance.com>.

Implantação do *Frontend*. Para implantação do *frontend* utilizamos o serviço de hospedagem compartilhada, que é um tipo de hospedagem que permite a divisão de um mesmo servidor para diversos sites, da *Hostinger* para disponibilização do sistema para os usuários. O processo foi realizado através de uma ferramenta, chamada de *Filezilla*, que permitiu o envio dos arquivos para o servidor da *Hostinger*. Todo o processo de execução do *software* ficou sob a responsabilidade do serviço de hospedagem.

Implantação do *Backend*. A implantação do *backend*, utilizamos um servidor VPS (do inglês, *Virtual Private Server*). Este servidor permite que o *software* seja implantado com uma maior autonomia para o uso de dependências externas, necessárias ao *software*, como também, o VPS pode possuir um melhor poder de processamento, para a execução do *backend*, em comparação com uma hospedagem compartilhada.

Implantação do *Database*. A implantação do banco de dados foi realizada também através do *Hostinger* que permitiu o acesso ao *host* que a instância do banco está sendo executada. O processo de construção das tabelas no banco de dados foi realizado pelo *prisma*, um ORM, utilizado junto ao *NodeJS*.

É importante destacar que após o término do processo de implantação da plataforma, buscou-se monitorar diversos indicadores disponibilizados através da infraestrutura *Hostinger*. Dados como tempo de resposta, latência de banco de dados, tempo entre requisições foram identificados e monitorados afim de assegurar a correta operação da plataforma *LGPD Compliance*. Ademais, um mecanismo de *log* foi acoplado aos módulos da plataforma (i.e., database, frontend e backend) visando o correto mapeamento de possíveis erros e falhas no sistema.

Capítulo 5

Resultados

Este capítulo descreve os principais resultados obtidos a partir da realização do presente estudo. Inicialmente, iremos descrever as principais funcionalidades da plataforma LGPD *Compliance* de acordo com todas as atividades do processo de desenvolvimento (Seção 5.1). Em seguida, iremos exibir o modo de validação preliminar da plataforma em termo de suas funcionalidades bem como sua usabilidade (Seção 5.2).

5.1 A Plataforma LGPD *Compliance*

Esta seção tem por objetivo demonstrar os principais artefatos de software desenvolvidos de acordo com a metodologia descrita no capítulo 4. Para tal, em cada seção a seguir descreve-se os fluxos principais da plataforma LGPD *Compliance* focando principalmente na camada de *frontend* com objetivo de ilustrar ao leitor a forma de operação bem como as principais interações que o usuário poderá realizar. Assim, descreve-se as principais funcionalidades públicas da plataforma (5.1.1), o mecanismo de autenticação (Seção 5.1.2), as funcionalidades do usuário comum (5.1.3) bem como aquelas do usuário administrador da plataforma (5.1.4). Por fim, exibe-se alguns detalhes associados a responsividade das interfaces com o usuário (Seção 5.1.5) com objetivo de denotar o uso dessa plataforma a partir de dispositivos móveis.

5.1.1 Funcionalidades Públicas

No que segue, iremos apresentar as principais seções da página de entrada da plataforma LGPD *Compliance*. Ao entrar no sistema, é mostrado a tela inicial (Figura 5.1) contendo a logo principal do projeto e mais abaixo dois botões.



Figura 5.1: Tela Inicial.

A partir do botão "Entrar", o usuário é redirecionado para a parte de autenticação, no qual, será possível realizar o cadastro e login na plataforma. Com uso do botão "Saiba mais", o usuário obtém informações gerais associadas a LGPD (Figura 5.2).

O que é a LGPD?

A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709, de 14 de agosto de 2018) foi aprovada em 2018. Em vigor desde 18 de setembro de 2020, pode ser considerada a resposta brasileira ao GDPR (Regulamento Geral sobre a Proteção de Dados) da União Europeia - com muitos alinhamentos da lei brasileira em relação à europeia, mas também com algumas diferenças. A intenção da lei é substituir ou complementar o atual panorama jurídico bastante disperso, que conta com mais de 40 especificações federais para o setor, e criar um marco regulatório.

Quem precisa se adaptar a LGPD?

Todas as empresas que captam e processam informações pessoais devem se submeter à nova legislação. Isso inclui o recolhimento de dados online e offline!

O que são “dados pessoais” na LGPD?

É simples. Se uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP (Protocolo da Internet) e cookies, entre outros.

O que pode acontecer se a empresa não cumprir com algum dos requisitos?

- Multas aplicadas pela lei podem chegar a R\$ 50 milhões;
- Empresas sofrem impactos na reputação, credibilidade e imagem junto a clientes e ao mercado;
- Nos casos de cibercrimes que violam a privacidade e roubam dados, os prejuízos financeiros são gigantescos;

A quais locais a LGPD se aplica?

Assim como o GDPR, a LGPD aplica-se a um escopo territorial que vai além do Brasil. Isso significa que é preciso estar em conformidade com ela mesmo que você ou seu negócio não esteja localizado no Brasil. Na prática, a LGPD é aplicável se:

- Suas atividades de tratamento de dados são realizadas no Brasil (e.g. você usa servidores localizados no Brasil);
- Você oferece ou fornece bens ou serviços a pessoas localizadas no Brasil, independentemente da nacionalidade delas;
- Você processa dados provenientes de pessoas localizadas no Brasil (mesmo no caso em que a pessoa está no país apenas no momento da coleta de dados e depois mude de localidade).

Figura 5.2: Tela de Saiba Mais.

Em seguida, é exibido um pequeno formulário para contato (Figura 5.3) contendo os campos de "Nome", "Email", "Assunto" e "Mensagem" que, ao ser preenchido corretamente pelo usuário, realiza o envio de uma mensagem de *e-mail* através de serviço SMTP.

The screenshot shows a contact form titled "Entre em contato". It includes fields for "Nome" (Name), "Email", "Assunto" (Subject), and "Mensagem" (Message). Below the message field is a "Enviar mensagem" (Send message) button. At the bottom center is the "LGPD compliance" logo.

Figura 5.3: Tela de Entrar em Contato.

5.1.2 Mecanismo de Autenticação

Na tela de login (Figura 5.4), o usuário precisar digitar suas credenciais contendo um e-mail válido e uma senha. Caso o usuário ainda não tenha uma conta cadastrada, ele pode acessar a tela de cadastro clicando no texto "Não tem conta? Cadastre-se" que está na parte inferior da tela. Dessa forma, o usuário é redirecionado para tela de cadastro mostrado na Figura 5.5.

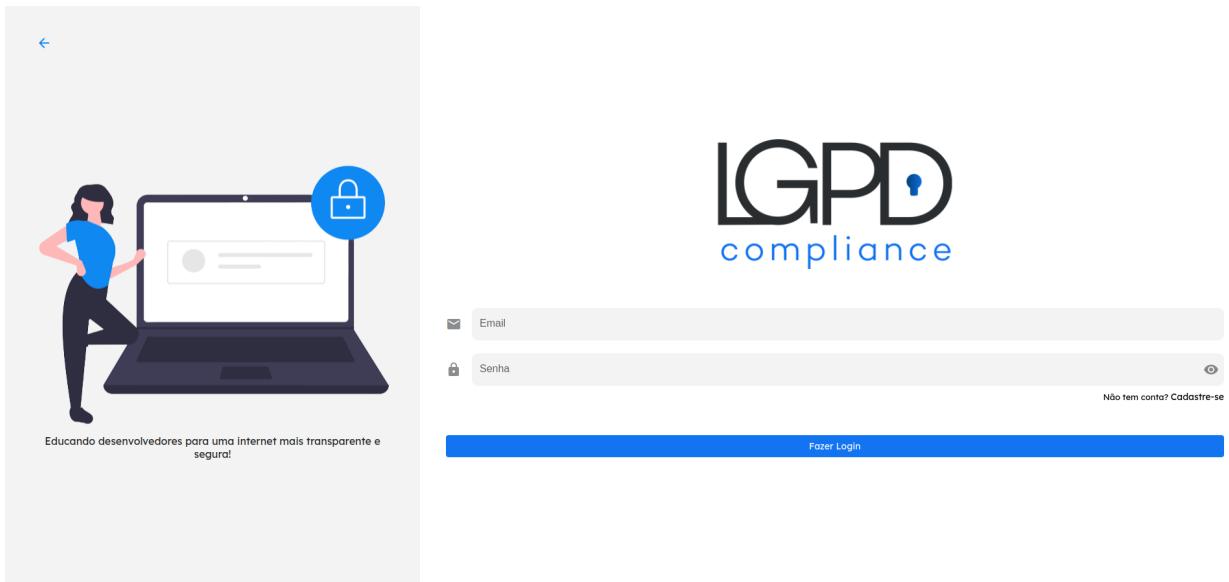


Figura 5.4: Tela de Entrar em Contato.

Na tela de cadastro (Figura 5.5), o usuário precisa fornecer seu nome completo, e-mail válido e uma senha para se cadastrar no banco de dados se estiver de acordo com os termos e condições de uso do site.

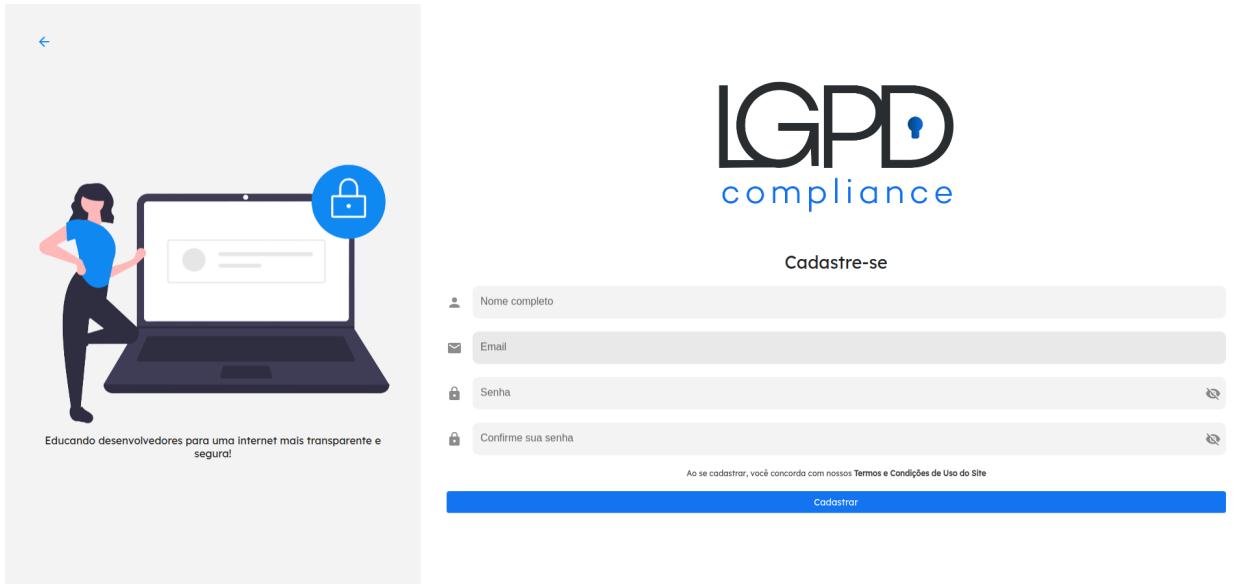


Figura 5.5: Tela de Cadastro.

Para visualização dos termos e condições do *LGPD Compliance* (Figura 5.6), basta clicar no texto acima do botão de cadastrar.

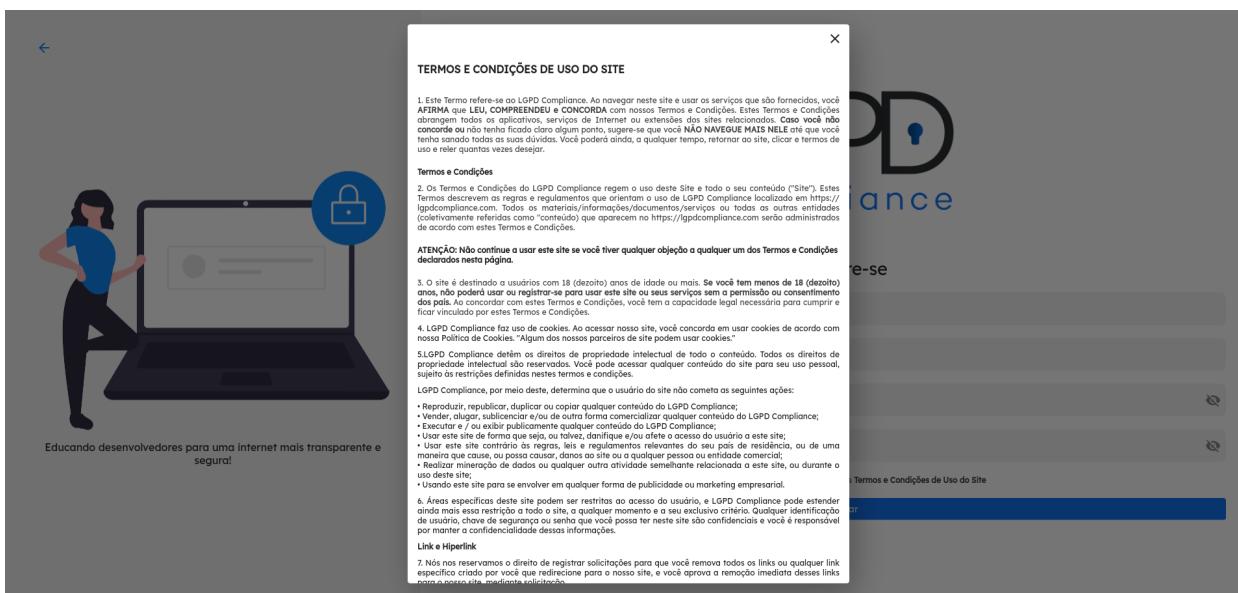


Figura 5.6: Tela de Cadastro.

Após realizar o login no sistema é detectado se as permissões do usuário é do tipo administrador ou comum. Se o usuário possuir permissões de administrador, será mostrado uma tela com apenas as abas de "LGPD" e "Usuários" (Vide Seção 5.1.4). Caso o usuário for de perfil comum, é exibido uma tela contendo menu lateral com as abas de "LGPD", "Perfil", "Quiz" e "Histórico" que será mais especificado a seguir.

5.1.3 Funcionalidades do Usuário Comum

Para usuários comuns, ao realizar o login, será exibido a aba de "LGPD" (Figura 5.4) que contém diversas notícias de vários autores e portais relacionadas ao tema da LGPD no Brasil. Essas notícias são exibidas de forma simplificada apenas com o título, um breve contexto, data da publicação e um link que redirecionará o usuário para sua origem.

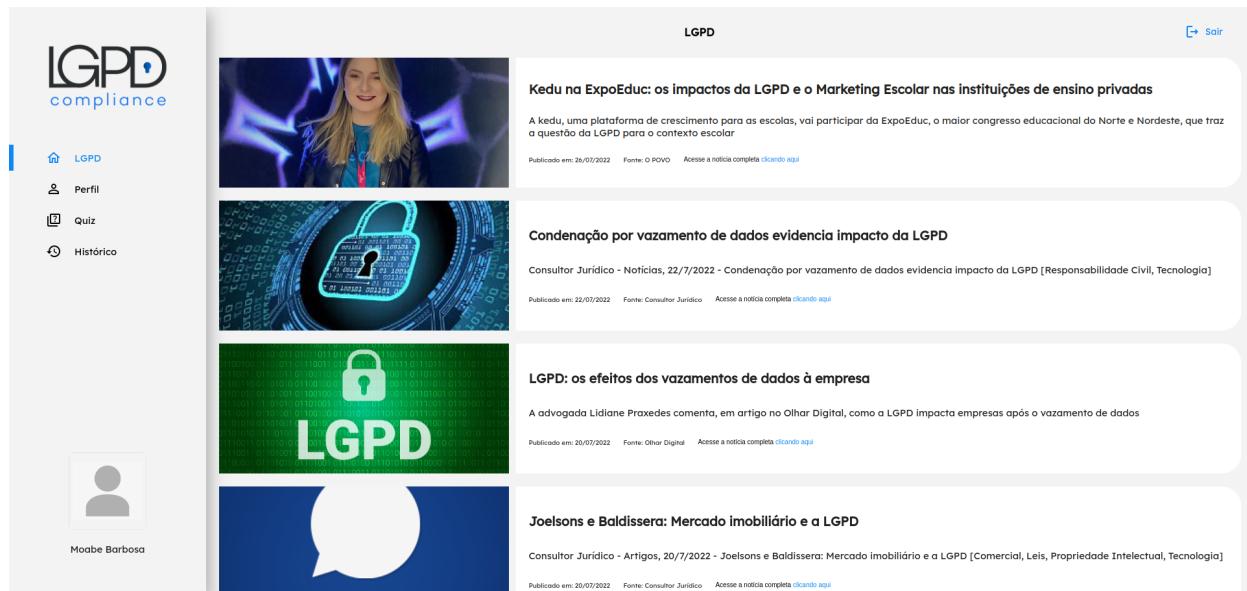


Figura 5.7: Aba do LGPD.

Na aba de "Perfil" mostrado na Figura 5.8, o usuário consegue alterar seus dados de cadastro (i.e., nome completo e o *e-mail*). Inicialmente, são exibidos os valores atuais desses campos e, caso o usuário deseja alterar algum dado, é necessário editar o campo e clicar no botão de salvar.

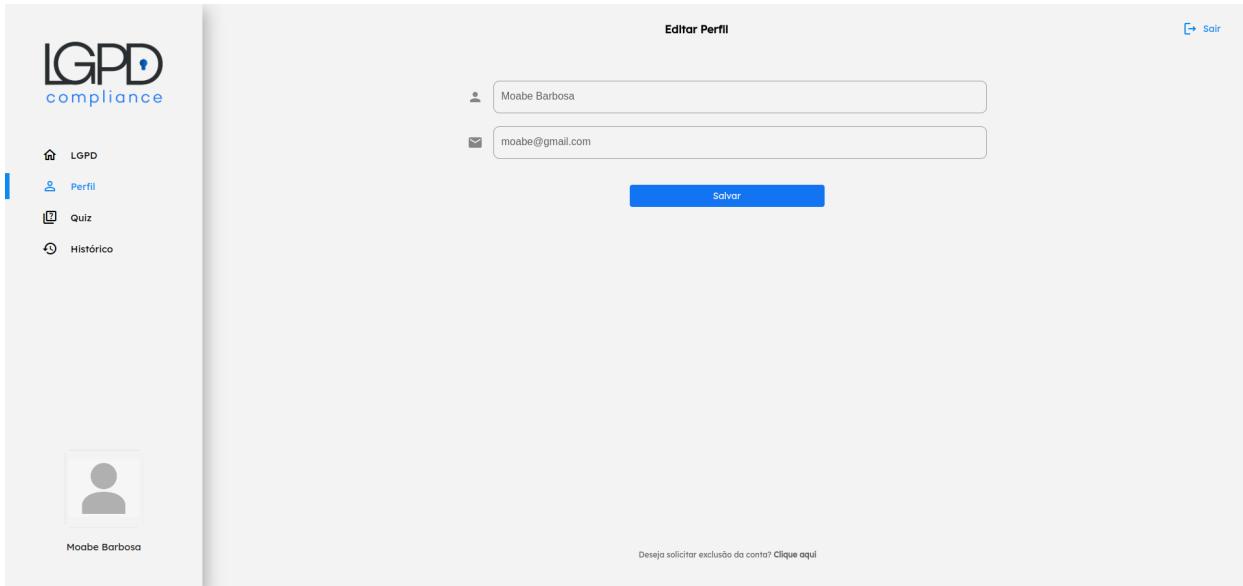


Figura 5.8: *Aba do Perfil.*

Na parte inferior, temos a frase "Deseja solicitar exclusão da conta? Clique aqui", que ao clicar, será exibido um *pop-up*(Figura ??) informando como será o processo de exclusão.

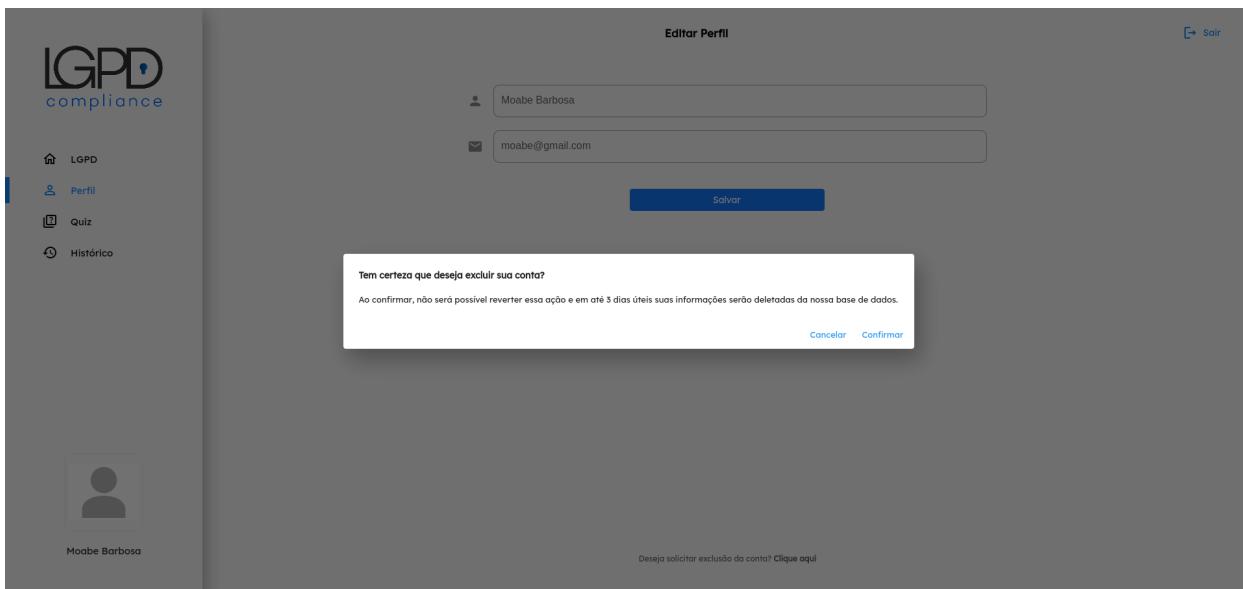


Figura 5.9: *Pop-up para confirma solicitação de exclusão do usuário.*

Ao clicar na aba do "*Quiz*", o usuário será redirecionado para a tela da Figura 5.10 onde ele transitará entre 3 etapas. A primeira etapa contém apenas informações referentes ao *quiz* e um botão para iniciar-lo.

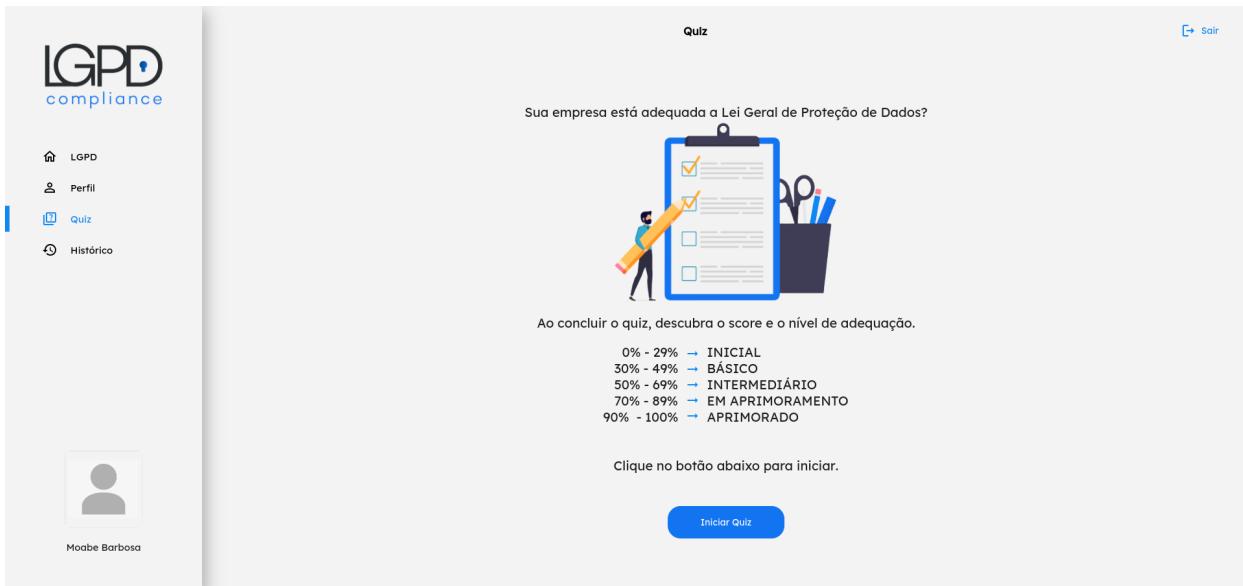


Figura 5.10: Aba da Etapa 1 do Quiz.

Após o usuário clicar no botão de iniciar o *quiz*, será redirecionado para segunda etapa (Figura 5.11) onde serão exibidas várias perguntas objetivas referentes a LGPD separada entre as seções de governança, conformidade legal e respeito aos princípios e transparência e direitos do titular. É importante mencionar que todas as questões deverão ser respondidas com o objetivo de descobrir se a empresa ou projeto do usuário está em conformidade com a LGPD.

Figura 5.11: Aba da Etapa 2 do Quiz.

Em seguida, após a conclusão do *quiz* e clicar no botão de finalizar, será exibido a tela da terceira etapa (Figura 5.12) que exibe um pequeno relatório referente a resposta do usuário. Inicialmente, é exibido o score em forma de gráfico com um pequeno texto abaixo informando o nível de adequação a LGPD. Em seguida, é apresentado um conjuntos de *feedbacks* separados contendo indicações de "ações necessárias" para melhorar a adequabilidade do sistema frente a LGPD.

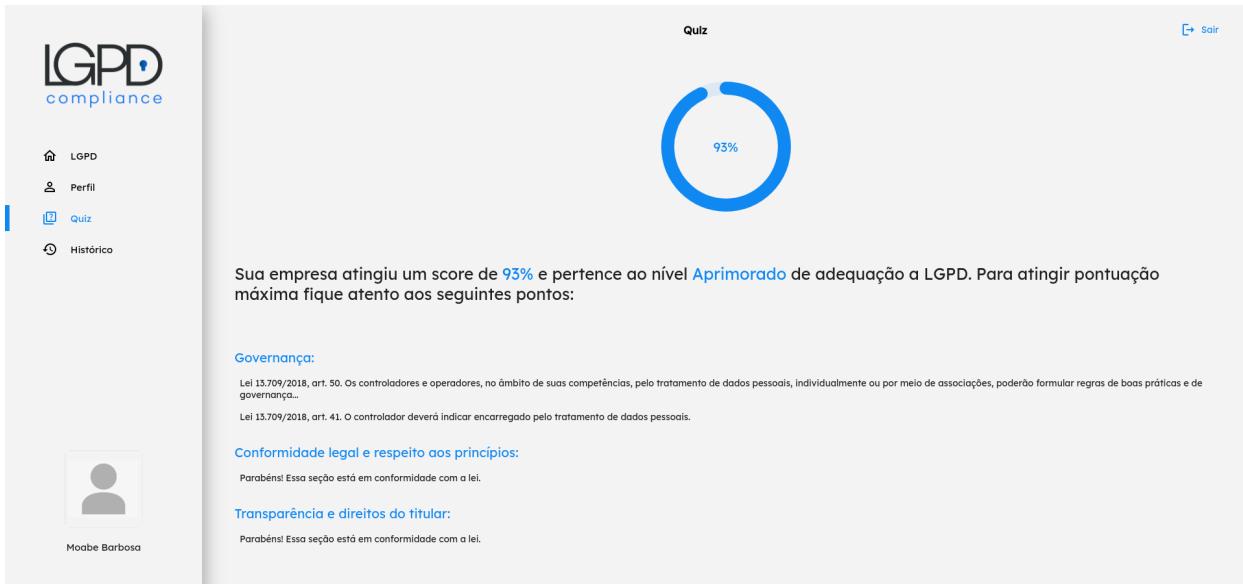


Figura 5.12: Aba da Etapa 3 do Quiz.

Por fim, na aba de "Histórico", é exibido uma lista de todos os *quiz* no qual o usuário respondeu (Figura 5.13) contendo a data, score e um botão de ver detalhes. Além disso, é possível selecionar um filtro de exibição por score e data crescente ou decrescente.

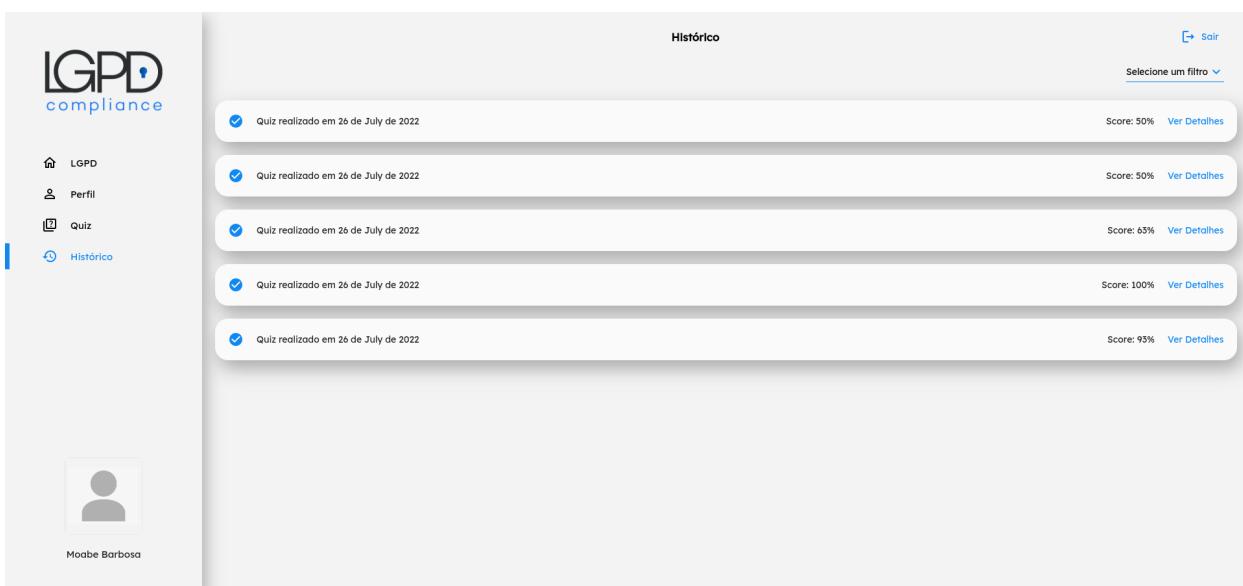


Figura 5.13: Aba de Histórico

Ao clicar no botão de "ver detalhes", o usuário é redirecionado para a página contendo o *quiz* e as alternativas que foram marcadas pelo usuário durante sua realização (Figura 5.14). Caso a resposta de uma determinada pergunta esteja em conformidade com a lei, será apresentada o *check* da cor verde e caso contrário, da cor vermelha, sendo exibido conjuntamente um *feedback* que ajude na adequação da LGPD.

The screenshot shows the 'Histórico' (History) section of the LGPD Compliance platform. On the left, there's a sidebar with icons for 'LGPD', 'Perfil' (Profile), 'Quiz', and 'Histórico'. The main area displays three completed quizzes:

- 9. Foram definidos indicadores que serão utilizados para medir os resultados do Programa Institucional de Privacidade de Dados?**
 - Adota parcialmente
 - Não adota
 - Iniciou plano para adotar
 - Adota integralmente
- Feedback:** Lei 13.709/2018, art. 50. 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...
- 10. A(s) área(s) envolvidas com tratamento de dados participou(aram) de algum treinamento relacionado com o tema de proteção de dados pessoais?**
 - Iniciou plano para adotar
 - Adota integralmente
 - Adota parcialmente
 - Não adota
- 11. O órgão já realizou a indicação de um encarregado com conhecimento e experiência suficientes e autonomia para implementar a LGPD?**
 - Não adota

On the right side of the interface, there are 'Sair' (Logout) and 'Histórico' (History) buttons.

Figura 5.14: Aba de Histórico: ver detalhes

5.1.4 Funcionalidades do Usuário administrador

Para usuários com permissões de administrador, ao realizar o login, é mostrado a tela da Figura 5.15 onde é exibido um primeiro gráfico representando a quantidade de *quizzes* respondidos pelos usuários cadastrados na plataforma. No segundo, é exibido um gráfico de barras verticais mostrando a quantidade de *quizzes* respondidos em cada intervalo.



Figura 5.15: Aba LGPD do administrador

Na aba de "Usuários" mostrado na Figura 5.16, o administrador é capaz de visualizar todos os usuários cadastrados na plataforma. Além disso, pode-se filtrar um usuário específico inserindo seu nome no campo de busca.

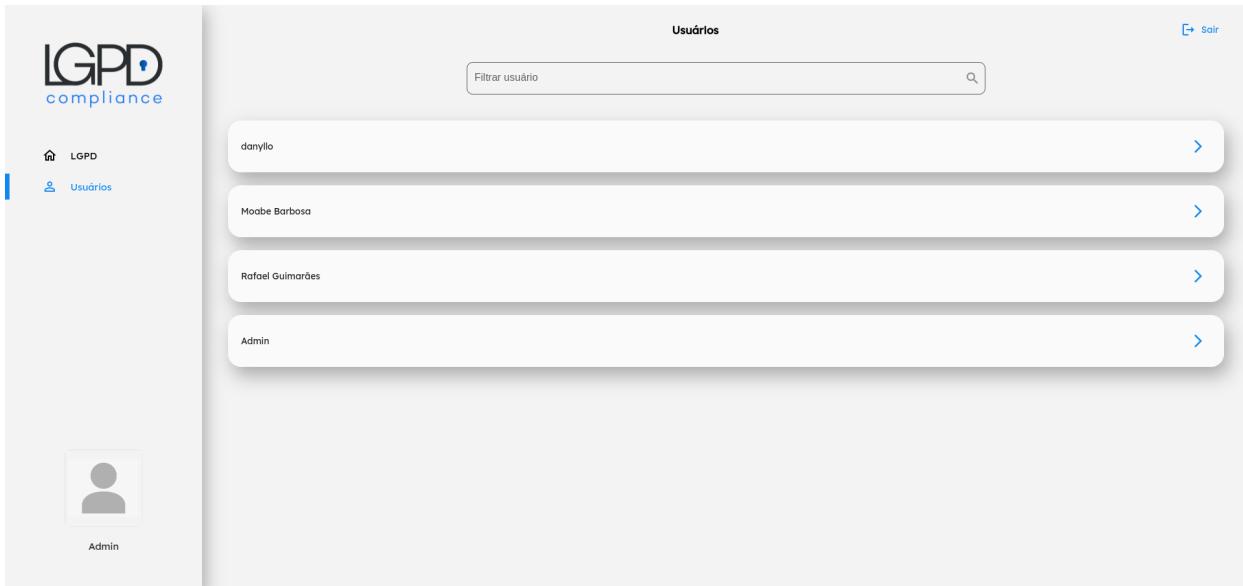


Figura 5.16: Aba de lista de usuários

Após clicar em algum usuário específico, o usuário administrador é redirecionado para a tela da Figura 5.17 similar a tela descrita na Figura 5.13, tendo como diferença principal a exibição do nome do usuário no topo desta tela. Apesar disso, possui as mesmas funções

e ao clicar no botão de ver detalhes é exibido a tela da Figura 5.18 similar a tela da Figura 5.14, mostrando as alternativas que o usuário marcou em um *quiz* específico.

The screenshot shows the 'Usuários' (Users) section of the LGPD Compliance platform. On the left, there's a sidebar with the 'LGPD compliance' logo, a user icon, and navigation links for 'LGPD' and 'usuários'. The main area displays a user profile for 'danyillo'. A message at the top says 'Quiz realizado em 26 de July de 2022' (Quiz taken on July 26, 2022) with a checkmark, and 'Score: 50%' with a link to 'Ver Detalhes' (View Details). There's also a 'Selecionar um filtro' (Select a filter) button and a 'Sair' (Logout) link.

Figura 5.17: Aba de lista de usuários

The screenshot shows the 'Histórico' (History) section of the LGPD Compliance platform. It displays two quiz questions. Question 1: 'O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado?' (The organization adopts systems and procedures to fulfill the right of rectification of information of the data subject?). The options are: Iniciou plano para adotar, Não adota, Adota integralmente, and Adota parcialmente. Question 2: 'O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD estão sendo respeitados durante o desenvolvimento de serviços que tratarão dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?' (The organization establishes a procedure or methodology to verify if the principles of the LGPD are being respected during the development of services that handle personal data from conception to execution (Privacy by Design)?). The options are: Não adota, Iniciou plano para adotar, Adota parcialmente, and Adota integralmente. Feedback for Question 1: 'Feedback: Lei 13.709/2018, 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: III - correção de dados incompletos, inexatos ou desatualizados'. Feedback for Question 2: 'Feedback: Lei 13.709/2018, 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.'

Figura 5.18: Aba de lista de usuários

5.1.5 Responsividade das telas

Por último, vale salientar que todas as telas até aqui apresentadas nessa sessão de resultados são todas responsivas, ou seja, de acordo com a disposição dos elementos, o conteúdo

se adaptam de acordo com o tamanho da tela do usuário. Isso significa que, independentemente do dispositivo de utilização (e.g., computadores ou dispositivos móveis), o layout será carregado sem erros, mantendo a navegação simples e intuitiva como mostrado nas figuras a seguir.

Telas das Funcionalidades Públicas. No que segue, serão exibidas as telas associadas as funcionalidades públicas. Essas telas são similares as exibidas na seção 5.1.1.

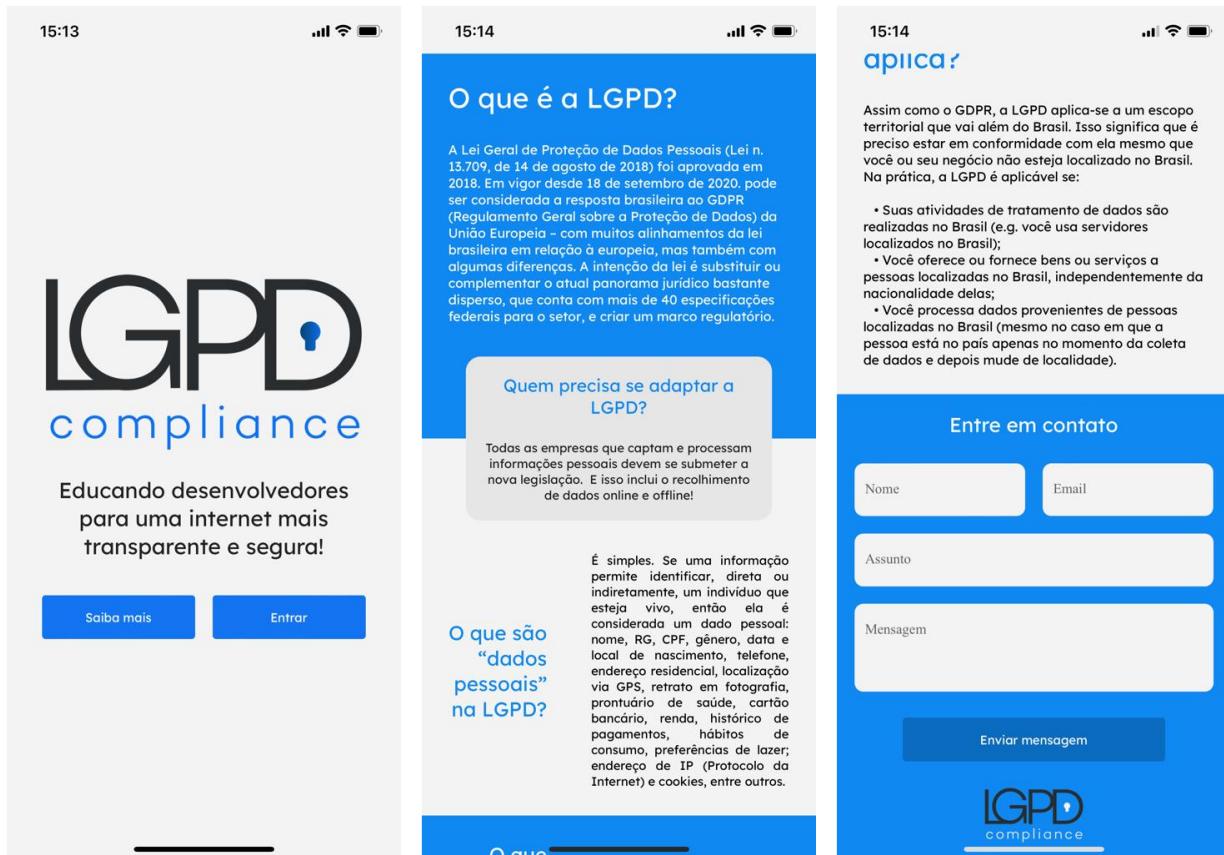


Figura 5.19: Fluxo das funcionalidades públicas

Telas do Mecanismo de Autenticação. No que segue, serão exibidas as telas associadas ao mecanismo de autenticação. Essas telas são similares as exibidas na seção 5.1.2.

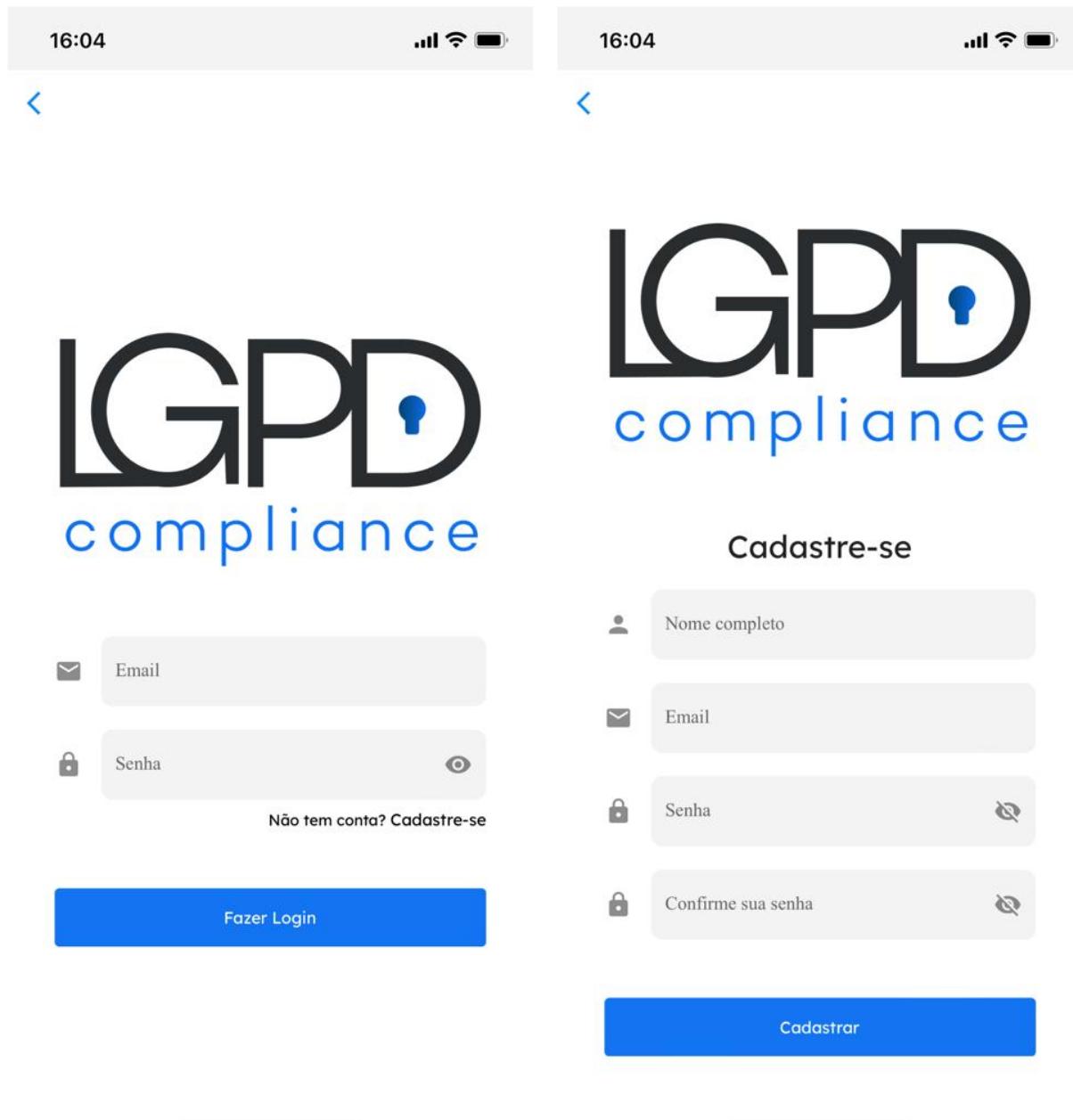


Figura 5.20: Fluxo de autenticação

Telas do Usuário Comum. No que segue, serão exibidas as telas associadas as funcionalidades de um usuário com perfil comum da plataforma LGPD *Compliance*. Essas telas são similares as exibidas na seção 5.1.3.

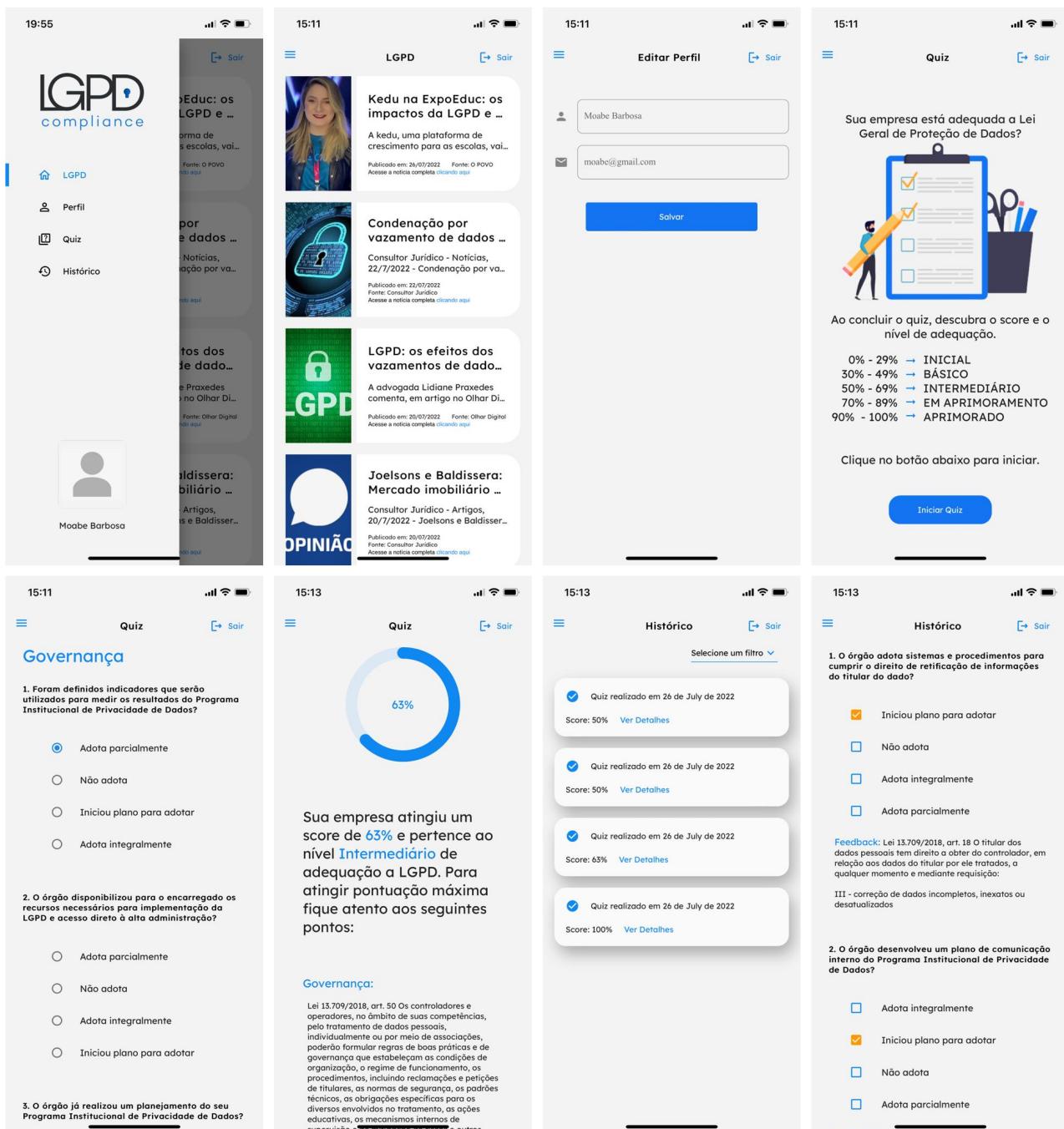


Figura 5.21: Fluxo de um usuário comum

Telas do Usuário Administrador. No que segue, serão exibidas as telas associadas as funcionalidades de um usuário com perfil administrador da plataforma LGPD *Compliance*. Essas telas são similares as exibidas na seção 5.1.4.

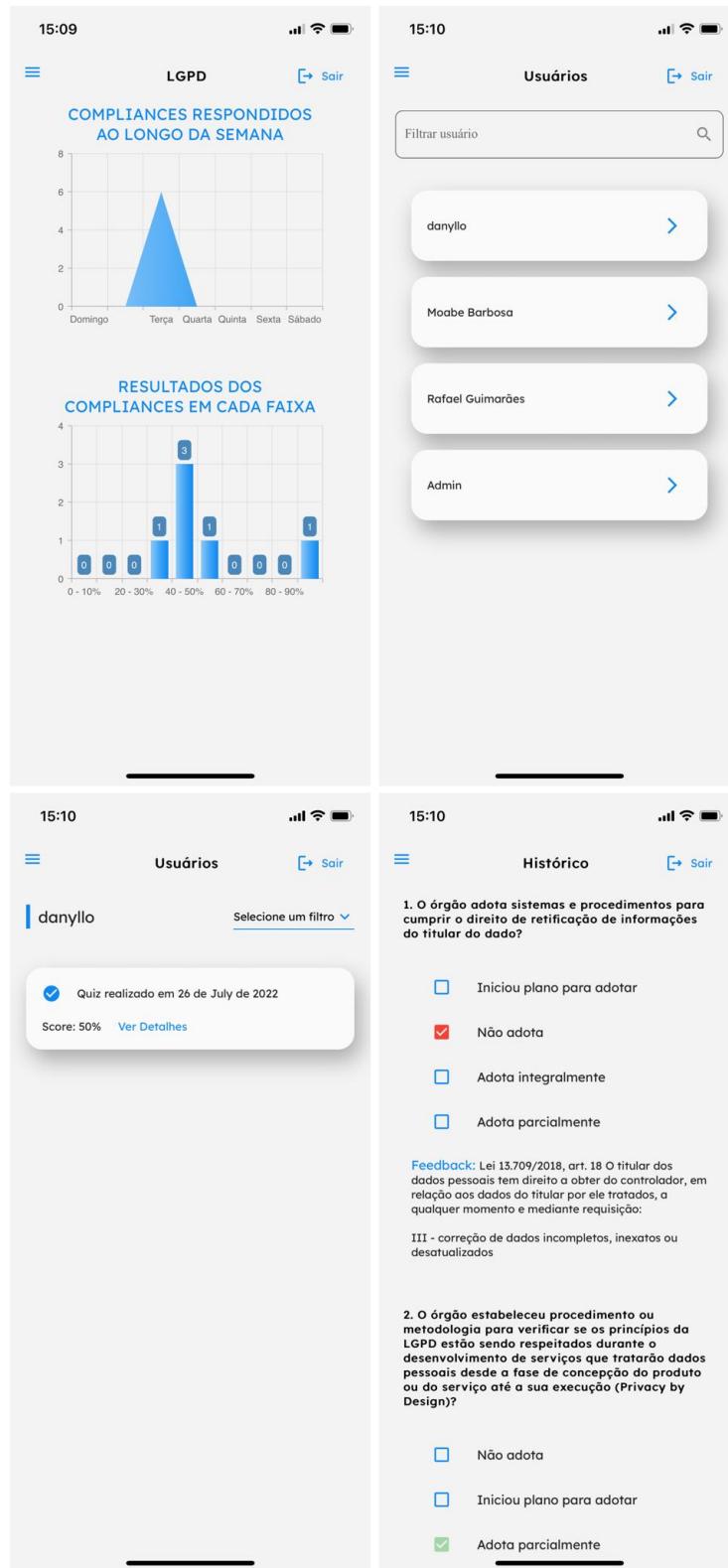


Figura 5.22: Fluxo de um usuário administrador

5.2 Validação da plataforma

Esta seção aborda as etapas realizadas visando a validação da plataforma LGPD *Compliance*. Nas subseções a seguir, descreve-se detalhes sobre o projeto do questionário (Seção 5.2.1), execução de testes-piloto (5.2.2), amostra de participantes (5.2.3) bem como os resultados obtidos a partir da aplicação do *survey* de validação (5.2.4).

5.2.1 Projeto do Questionário

Elaborou-se um questionário para coleta de dados onde um conjunto de perguntas específicas foram organizadas para prover suporte às questões de pesquisa definidas neste estudo. O questionário foi construído de acordo com as diretrizes apresentadas no trabalho de Linåker *et al.* (Linaker et al., 2015) e operacionalizado a partir da ferramenta *Google Forms*. A Tabela 5.1 descreve as seções do questionário.

Tabela 5.1: Seções do Questionário.

| Seção | Tópico | Descrição/Motivação |
|-------|-------------------------------|--|
| 1 | Consentimento de participação | Obter o consentimento explícito do respondente em relação a participação na pesquisa. |
| 2 | Perfil do participante | Obter informações pessoais tais como idade, gênero, quantidade de pessoas que residem com o mesmo, renda familiar e rede de ensino utilizada para conclusão do ensino fundamental. |
| 3 | Conhecimento e uso da LGPD | Obter um panorama do conhecimento e utilização desta normativa sob ponto de vista do respondente. |
| 4 | Utilização da Plataforma | Demonstrar alguns fluxos e funcionalidades com objetivo de guiar o respondente na utilização da plataforma. |
| 5 | Usabilidade da Plataforma | Coletar informações a respeito da experiência do respondente com a realização de algumas funcionalidades da plataforma. |
| 6 | Sugestões de Melhoria | Obter indicativos de possíveis oportunidades de melhoria da plataforma em termos de funcionalidades bem como na usabilidade desta plataforma. |
| 7 | Comentários gerais | Fornecer espaço para o respondente acrescentar outros comentários não cobertos em outras questões deste formulário. |
| 8 | Encerramento | Apresentar os agradecimento pela participação na pesquisa. |

O questionário continha questões subjetivas e objetivas com vistas a coletar dados quantitativos e qualitativos relacionados à evasão considerando diversos aspectos sob a perspectiva dos alunos. Ao final de cada seção, havia uma questão subjetiva para os respondentes discutirem algum ponto que eventualmente não foi coberto pelas perguntas ao longo da seção. Para mais detalhes sobre o projeto e construção do formulário, consulte sua versão digital disponível de forma *online*¹.

¹<https://bit.ly/3vffO7B>

5.2.2 Execução de Testes-piloto

Testes-piloto foram conduzidos usando os mesmos artefatos e procedimentos projetados para o estudo, incluindo o questionário e o método de execução, mas com um pequeno número de participantes. Quatro participantes foram convidados a responder o questionário e retornar seus comentários sobre o tempo de resposta, compreensão adequada, integridade entre outros aspectos. Todos os participantes dos testes-piloto responderam à pesquisa dentro do período de uma semana. O tempo médio de resposta foi de 12 minutos. Os comentários mais relevantes foram associados a problemas de usabilidade, clareza de perguntas e algumas sugestões de mudanças de terminologias ao longo do questionário. Tais sugestões foram posteriormente discutidas entre os autores desta pesquisa, e modificações foram aplicadas ao questionário final. No geral, não observou-se comentários negativos ou dúvidas sobre as opções de respostas ou mesmo nas descrições das perguntas. Isso sugere que o questionário tinha qualidade suficiente e os requisitos necessários para ser empregado no estudo.

5.2.3 Definição da Amostra e Coleta de Dados

Profissionais das áreas do direito e de desenvolvimento de software foram selecionados como público-alvo da validação da plataforma LGPD *Compliance*. Nossa amostra representa um universo particular desta população, sendo considerada não-probabilística e de conveniência. Como forma de recrutamento, um convite direto para responder ao questionário foi enviado através de mensagens de *e-mail* e de serviços de mensageria (i.e., *Whatsapp* e *Telegram*). É importante mencionar que os contatos dos profissionais foram obtidos a partir da rede de contatos dos autores desta pesquisa. Contamos com o apoio de outros pesquisadores e profissionais visando maximizar o número de respondentes desta pesquisa.

Todas as respostas foram obtidas e organizadas de forma automática em uma planilha de dados do *Google Sheets*. Esta planilha foi utilizada no contexto deste estudo como principal fonte de dados quantitativos e qualitativos. Dados pessoais (e.g., nome, telefone e *e-mail*) não foram requeridos com intuito de garantir o anonimato dos participantes deste estudo. Todos os participantes foram submetidos a um “Termo de Consentimento Livre e Esclarecido” para alinhamento das condições de participação da pesquisa. Apenas participantes que declararam concordância com este termo estariam aptos a responder o questionário.

5.2.4 Resultados da validação

Esta validação foi realizada durante o mês de julho de 2022. Mais de 60 convites de participação foram enviados e 20 participantes responderam ao questionário de modo adequado. Devido a restrições de espaço, aqui exibiremos apenas os resultados mais relevantes. Informações detalhadas podem ser consultadas no material suplementar deste estudo (<https://github.com/LGPDCompliance>).

Caracterização da amostra. As respostas da segunda seção do questionário forneceram dados para constituição do perfil dos participantes. Com relação ao gênero, 25 afirmaram ser do gênero masculino (65%) enquanto que 12 afirmaram ser do gênero feminino (35%). A maioria destes respondentes possuem renda familiar entre 1 e 2 salários mínimos (67%) e residem com no máximo 3 pessoas (53%). Relacionado a formação básica, 26 respondentes foram oriundos de escola pública (70%). Com relação ao curso, 16 deles estavam inscritos no curso técnico integrado em informática (45%), 11 no curso técnico subsequente em informática (cerca de 30%) e 10 no curso técnico subsequente em manutenção e suporte em informática (cerca de 25%). Importante mencionar que mais de 80% dos respondentes evadiram nos últimos 5 anos (i.e., entre 2017 e 2021).

Conhecimento e uso da LGPD.

Usabilidade da LGPD.

Sugestão de melhoria.

...

Capítulo 6

Ameaças a Validade

Este capítulo descreve as principais ameaças identificadas bem como algumas ações adotadas com intuito de mitigar os seus efeitos. No que segue, utilizamos o arcabouço de classificação proposto por Wohlin (Wohlin et al., 2012) para expor as ameaças associadas à validade de conclusão (Seção 6.1), validade interna (Seção 6.2), validade de construção (Seção 6.3) bem como validade externa (Seção 6.4).

6.1 Validade de conclusão

Os achados desse estudo limitaram-se à utilização de alguns segmentos da LGPD. Concluímos que o uso da técnica de *checklist* foi adequada para os segmentos da LGPD empregados no presente estudo (i.e.,). Contudo, não podemos concluir que o uso de *checklist* possa ser promissor para todos os segmentos desse ordenamento jurídico. Além disso, a técnica utilizada nesse trabalho fornece um status de adequação, que considera aspectos genéricos relativos à LGPD e portanto não substitui por completo uma consultoria especializada.

6.2 Validade interna

Existe uma relação direta entre as sugestões de melhorias disponibilizadas ao final do *quiz* e as ações realizadas pelo usuário baseadas no *feedback* recebido. Logo, se houver algum erro no *feedback* mostrado no resultado do *quiz* isso pode comprometer o resultado da adequação. Contudo, não observou-se críticas relevantes em relação às ações recomendadas pela plataforma a partir do processo de validação descrito na seção 5.2.

Outro ponto a ser observado é que o conteúdo técnico das questões e dos *feedbacks* podem comprometer o entendimento de alguns usuários não familiarizados com textos jurídicos. Buscamos mitigar os efeitos dessa ameaça a partir da indicação de notícias relevantes para que os usuários possam se familiarizar com as terminologias desta área. Adicionalmente, fruto de recomendações advindas do processo de validação, considera-se a implementação

de recursos colaborativos para que usuários possam trocar informações. Acreditamos que isso possa contribuir significativamente para compreensão dos termos e conceitos da citada legislação.

6.3 Validade de construção

Durante a construção do *checklist* foi solicitado a participação dos especialistas da área de direito para assegurar a corretude desse instrumento. Por essa razão, não podemos assegurar que houve um entendimento completo da regulamentação. Para minimizar o efeito dessa ameaça foram consultados materiais científicos para verificar a aderência do conteúdo. Adicionalmente, sempre que necessário, rodadas de discussão foram realizadas a fim de esclarecer os pontos a respeito da LGPD bem como possíveis interpretações ambíguas descritas nesta lei.

6.4 Validade externa

Buscamos ter uma amostra de conveniência para realizar uma validação mínima da ferramenta. Embora a amostra possa não ser estatisticamente significante, ela demonstrou a viabilidade de uso da técnica de *checklist* no contexto da LGPD. No entanto, a capacidade de generalização dos resultados associados a validação da ferramenta pode ter sofrido ameaça em relação a amostra utilizada nessa atividade. Procuramos minimizar essa ameaça através da escolha aleatória de participantes.

Capítulo 7

Considerações Finais

A presente pesquisa tem como foco projetar, desenvolver e implantar uma plataforma que auxilie organizações e profissionais a obter conhecimento sobre a LGPD no intuito de adequação de seus projetos de software. Para isso, através do uso da técnica de *checklist*, foi construída uma plataforma que disponibiliza um questionário para avaliação da adequabilidade de projetos de software frente supracitada lei.

Para se atingir uma compreensão do *checklist* de adequação à LGPD, definiu-se alguns objetivos específicos. Destes, o principal que podemos destacar foi o desenvolvimento de um sistema baseado na web¹ multiplataforma chamada LGPD *Compliance*. Este sistema foi projetado com auxílio de profissionais especialistas na área de direito e de engenharia de software que, através de um processo iterativo com os autores desta pesquisa, auxiliaram na realização das diversas etapas desse estudo (i.e., análise de requisitos, definição de arquitetura, desenvolvimento, validação e implantação).

Mediante utilização de um *survey*, cerca de 20 respondentes avaliaram as funcionalidades e usabilidade da plataforma. Conclui-se que a aplicação do *checklist* mostrou-se adequada ao contexto da LGPD e contribuiu para avaliação dos projetos de software à luz da legislação vigente, além de prover dicas e ações práticas visando a conformidade destes projetos. Ademais, a plataforma atendeu aos objetivos propostos, proporcionando aos seus usuários uma ferramenta de fácil uso e compressão.

Em relação a atividades futuras, este trabalho fornece algumas opções no que diz respeito a continuidade do desenvolvimento do LGPD *Compliance*: (i) Criação de mais seções do *checklist* abordando outros segmentos elencados na LGPD; (ii) Criação da aba "LGPD Comentada", semelhante a um fórum, com tópicos definidos para cada artigo da lei, onde as pessoas possam comentar; (iii) Criação de uma seção de "Perguntas Frequentes" para o autoatendimento de possíveis dúvidas dos usuários da plataforma; (iv) Utilização de uma amostra maior de respondentes visando retificar ou ratificar os resultados obtidos na validação da plataforma; (v) Geração de um documento de resultados em formato de PDF que o usuário consiga exportar.

¹Plataforma LGPD *Compliance* disponível em: <https://lgpdcompliance.com/>

Referências Bibliográficas

Awad, M. A. A comparison between agile and traditional software development methodologies , this report is submitted as partial fulfillment of the requirements for the honours. In: *The University of Western Australia*. 2005. 3

B, L.; Wiegers, K.; Ebert, C. The top risk of requirements engineering. *IEEE Software*, v. 18, n. 6, p. 62–63, 2001. 20

Bhavsar, K.; Shah, V.; Gopalan, S. Scrum: An agile process reengineering in software engineering. *International Journal of Innovative Technology and Exploring Engineering*, v. 9, n. 3, p. 840–848, 2020. 15

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF, 2018. Available on: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. 5

Bui, T. Sanalysis of docker security. *Aalto University School of Science*, p. 7, 2014. 11

Camoglu, K.; Kandemir, R. A survey of software requirements engineering practices in turkey. *International Journal of Science and Research (IJSR)*, v. 8, p. 256 – 262, 07 2019. 20

CANTELON MARC HARTER, T. H. N. R. M. *Node.js in Action*. : Editora Manning, 2014. ISBN 9781617290572. 11

Carvalho, H. E. R. D.; Freitag, A. E. B. Adequação das organizações à lgpd: Aspectos a serem considerados para evitar a vulnerabilidade humana na exposição indevida de dados pessoais. 18

Conexorama. *Validação de Softwares, o guia definitivo – Parte I: como começar um processo de validação*. 2018. Disponível em: <https://vistosistemas.com.br/validacao-de-softwares/> Acessado em: 23/03/2022. 4

Enterprise, J. *HTML, PHP, dan MySQL untuk Pemula*. : Elex Media Komputindo, 2018. 14

Fernandes, M. Catalog of security requirements aligned with the general data protection regulation (gdpr) (eu) 2016 / 679. In: . 2018. 19

FOKUS Mercury Computer Systems, R. C. F. Specification for deployment and configuration of component-based distributed applications. *Proposal to the OMG MARS RFP: Deployment and Configuration of Component-based Distributed Applications Joint Revised Submission*, p. 160, 2003. 4

Garcia, L.; Aguilera-Fernandes, E.; Gonçalves, R.; Pereira-Barretto, M. *Lei Geral de Proteção de Dados (LGPD): Guia de implantação*. Editora Blucher, 2020. ISBN 9786555060164. Available on: <<https://books.google.com.br/books?id=ls3sDwAAQBAJ>>. 6, 18

Lima, C. J. M. d. et al. Desenvolvimento e validação de um aplicativo móvel para o ensino de eletrocardiograma. *Revista brasileira de educação médica*, SciELO Brasil, v. 43, p. 157–165, 2020. 32

Linaker, J.; Sulaman, S. M.; Höst, M.; Mello, R. M. de. Guidelines for conducting surveys in software engineering v. 1.1. *Lund University*, 2015. 49

Mardan, A. Putting frontend and backend together. In: *Full Stack JavaScript*. : Springer, 2018. p. 257–287. 11, 12

Neto, N. N.; Madnick, S.; Paula, A. M. G. D.; Borges, N. M. Developing a global data breach database and the challenges encountered. *J. Data and Information Quality*, Association for Computing Machinery, New York, NY, USA, v. 13, n. 1, jan 2021. ISSN 1936-1955. Available on: <<https://doi.org/10.1145/3439873>>. 5

Oliveira, N. de; Gomes, M.; Lopes, R.; Nobre, J. Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019. 19

Pinheiro, P. P. *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD*. : Saraiva Educação S.A., 2020. 4

Pinheiro, P. P. Nova lei brasileira de proteção de dados pessoais (lgpd) e o impacto nas instituições públicas e privadas. *Nova Lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas*, 2021. 6

Ponemom. Cálculo e gerenciamento dos riscos cibernéticos para as operações comerciais. 2018. 5

Pressman, R. *Engenharia de software*. McGraw-Hill, 2006. ISBN 9788586804571. Available on: <<https://books.google.com.br/books?id=MNM6AgAACAAJ>>. 15

Prisma, D. *What is Prisma?* 2022. Disponível em:
<https://www.prisma.io/docs/concepts/overview/what-is-prisma> Acessado em: 06/07/2022. 12

Rapôso, C. F. L.; Lima, H. M. de; Junior, W. F. de O.; Silva, P. A. F.; Barros, E. E. de S. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. *RACE-Revista de Administração do Cesmac*, v. 4, p. 58–67, 2019. 18

RDStation. *Empresas e LGPD: Cenários, desafios e caminhos*. 2021.
<Https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F2%2F1628275980relatorio-adequacao-lgpd-rd-manar.pdf>. Accessed: 2022-02-23. 4

Roque, A. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (lgpd). *Revista Eletrônica de Direito Processual*, v. 20, n. 2, 2019. 18

Schwaber, K.; Sutherland, J. The scrum guide. *Scrum Alliance*, v. 21, n. 19, p. 1, 2011. 15, 16

Silva, M. S. *Criando sites com HTML: sites de alta qualidade com HTML e CSS.* : Novatec Editora, 2008. 14

Silva, M. S. *JavaScript-Guia do Programador: Guia completo das funcionalidades de linguagem JavaScript.* : Novatec Editora, 2010. 14

Sutherland, J. *SCRUM: A arte de fazer o dobro de trabalho na metade do tempo.* : Leya, 2014. 15

Sánchez, D.; Viejo, A.; Batet, M. Automatic assessment of privacy policies under the gdpr. *Applied Sciences*, v. 11, n. 4, 2021. ISSN 2076-3417. Available on: <<https://www.mdpi.com/2076-3417/11/4/1762>>. 19

Teffé, C. S. de; Viola, M. Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. *Civilistica. com*, v. 9, n. 1, p. 1–38, 2020. 18

Wohlin, C. et al. *Experimentation in software engineering.* : Springer Science & Business Media, 2012. 52

Zat, D. A validação de requisitos com foco na melhoria em projetos de software. Universidade do Vale do Rio dos Sinos, 2016. 10