



Universidade Federal de Pernambuco
Centro de Informática

Graduação em Ciência da Computação

**Um sistema web para auxiliar soluções na
conformidade com a LGPD**

Matheus Frej Lemos Cavalcanti

Trabalho de Graduação

Recife
7 de junho de 2024

Universidade Federal de Pernambuco
Centro de Informática

Matheus Frej Lemos Cavalcanti

**Um sistema web para auxiliar soluções na conformidade com
a LGPD**

Trabalho apresentado ao Programa de Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: *Sérgio Castelo Branco Soares*
Co-orientador: *Ivonildo Pereira Gomes Neto*

Recife
7 de junho de 2024

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Cavalcanti, Matheus Frej Lemos.

Um sistema web para auxiliar soluções na conformidade com a LGPD /
Matheus Frej Lemos Cavalcanti. - Recife, 2024.
38 p. : il.

Orientador(a): Sérgio Castelo Branco Soares

Cooorientador(a): Ivonildo Pereira Gomes Neto

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de
Pernambuco, Centro de Informática, Ciências da Computação - Bacharelado,
2024.

Inclui referências.

1. LGPD. 2. Conformidade. 3. Ferramenta web. 4. Proteção de dados. I.
Soares, Sérgio Castelo Branco. (Orientação). II. Gomes Neto, Ivonildo Pereira.
(Coorientação). IV. Título.

000 CDD (22.ed.)

Matheus Frej Lemos Cavalcanti

Um sistema web para auxiliar soluções na conformidade com a LGPD

Monografia apresentada ao curso de Ciência da Computação, como requisito parcial para a obtenção do Título de Bacharel em Ciência da Computação, Universidade Federal de Pernambuco.

Aprovado em: 7 de Junho de 2024.

BANCA EXAMINADORA

Prof. Sergio Soares
Universidade Federal de Pernambuco

Prof. Ricardo Massa
Universidade Federal de Pernambuco

Prof. Juliano Iyoda
Universidade Federal de Pernambuco

Em memória do meu cachorro, Tambi.

Agradecimentos

Quero agradecer à minha mãe, Adriana, por ter sido essencial na minha educação, criação e desenvolvimento pessoal, não chegaria aonde estou se não fosse por ela. Agradeço ao meu pai, Luciano, pelo carinho e apoio incondicional durante essa jornada. Também quero agradecer à minha avó, Nena, por todos os ensinamentos, apoio e presença em toda minha vida. Meu obrigado à minha família que sempre me apoiou a seguir meus objetivos e são parte muito valiosa da minha vida.

Gostaria também de agradecer à minha namorada, Bruna, por todo suporte, carinho e por me dar forças em tudo que faço. Eu agradeço à todos os meus amigos por serem tão importantes para mim, especialmente os que conheci na faculdade, viver esse caos com vocês tornou tudo menos pesado e, com certeza, firmou ainda mais nossos laços.

Por fim, agradeço à Universidade Federal de Pernambuco, ao Centro de Informática e à todos os professores e monitores que se mostraram presentes nessa jornada, foi definitivamente a melhor experiência de educação que eu poderia ter e me ensinou muito sobre a vida acadêmica, profissional e pessoal.

Resumo

A conformidade com a Lei Geral de Proteção de Dados (LGPD) é de grande importância para as empresas brasileiras, visando garantir a proteção dos dados pessoais. Este trabalho propõe a melhoria de um checklist de conformidade com a LGPD, transformando-o em uma ferramenta web para facilitar a avaliação e a implementação das exigências legais. A construção da ferramenta incluiu análise do feedback de especialistas, com destaque para o especialista que avaliou o checklist inspirador. Além disso, o processo envolveu levantamento de requisitos, definição de critérios de melhoria, desenvolvimento e testes. A avaliação da ferramenta foi conduzida em projetos reais de empresas ligadas à inovação tecnológica. Os resultados da avaliação revelaram uma eficiência significativa na identificação e correção de lacunas de conformidade, destacando o potencial da ferramenta para melhorar a conformidade com a LGPD.

Palavras-chave: LGPD, Conformidade, Ferramenta web, Proteção de dados

Abstract

Compliance with the General Data Protection Law (LGPD) is essential for Brazilian companies in protecting personal data. This study proposes the enhancement of an LGPD compliance checklist by transforming it into a web tool to facilitate the evaluation and implementation of legal requirements. The development of the tool included analyzing feedback from experts, notably the expert who assessed the inspirational checklist. The process also involved gathering requirements, defining improvement criteria, developing, and testing. The tool's evaluation was conducted on real projects by companies involved in technological innovation. The evaluation results revealed significant efficiency in identifying and addressing compliance gaps, highlighting the tool's potential to improve LGPD compliance.

Keywords: LGPD, Compliance, Web tool, Data protection

Sumário

1	Introdução	1
2	Fundamentação Teórica	3
2.1	Surgimento da LGPD	3
2.2	Segurança em sistemas de informação e conformidade com a LGPD nas empresas	3
3	Trabalhos Relacionados	5
4	Metodologia	7
4.1	Visão preliminar do Checklist Inicial de Conformidade com a LGPD	7
4.2	Desenvolvimento da solução	8
4.2.1	Protótipo	9
4.2.2	Ideia inicial de desenvolvimento	9
4.2.3	Construção das telas	10
4.2.4	Evolução da ferramenta	12
4.3	Avaliação do sistema	14
5	Resultados	15
5.1	Resultado da Solução	15
5.2	Resultado da Avaliação	15
6	Conclusão	17

Lista de Figuras

4.1	Recorte da checklist original, incluindo gráficos e primeiro item da checklist	8
4.2	Abas da planilha do checklist.	9
4.3	Página de instruções no sistema.	10
4.4	Seleção de famílias de checklists para inspeção.	11
4.5	Exemplo do gráfico.	12
4.6	Modelo relacional da ferramenta.	13

CAPÍTULO 1

Introdução

Com o avanço acelerado da tecnologia nos últimos anos, a coleta e o processamento de dados pessoais na internet tornaram-se atividades fáceis, comuns e essenciais para empresas e instituições [12]. Esses dados, que fornecem informações valiosas para a tomada de decisões estratégicas e a evolução dos sistemas, também trazem à tona questões críticas de privacidade e segurança. A manipulação inadequada ou a exposição indevida de dados pessoais e sensíveis pode resultar em graves violações da privacidade, afetando tanto indivíduos quanto organizações [1]. Tendo em vista esse problema, foi promulgada na Europa a General Data Protection Regulation (GDPR) em 2016 [16], sendo uma lei pioneira na regulamentação do tratamento de dados pessoais e servindo como base para a lei brasileira de mesmo tema, a Lei Geral de Proteção de Dados (LGPD) [6]. Além dessas duas leis relevantes, atualmente mais de 120 países já possuem leis regulatórias nesse âmbito [40].

Diante desse cenário regulatório complexo, os desenvolvedores de software enfrentam um desafio significativo para garantir que suas soluções estejam em conformidade com a legislação vigente. Muitos não sabem precisamente quais atributos são necessários no software para que ele esteja em conformidade com a lei [27]. Para abordar essa dificuldade, Mendes [27] propôs uma ferramenta de avaliação que consiste em uma checklist destinada à inspeção de sistemas computacionais, em formato de planilha Excel. O objetivo dessa checklist é verificar se os sistemas estão em conformidade com a LGPD e se seguem práticas recomendadas de tratamento de dados.

Após isso, Pereira *et al.* [31] expandiram a aplicabilidade da checklist para avaliar o tratamento e segurança de dados em dispositivos IoT (Internet das Coisas). Embora as questões relacionadas a esses dispositivos sejam opcionais na checklist, sua inclusão é crucial para garantir a segurança dos dados em ambientes de IoT. Tanto Mendes [27] quanto Pereira *et al.* [31] sugerem melhorias futuras para a checklist, como automatizá-la para validação de campos, expandir sua aplicabilidade para outras áreas além de IoT e atualizá-la conforme novas leis são criadas. Pereira *et al.* [31] também mencionam o desenvolvimento de uma ferramenta web para facilitar o acesso e utilização da checklist pelos inspetores de sistemas.

Considerando as demandas identificadas por Mendes [27] e Pereira *et al.* [31], surge a oportunidade de desenvolver um sistema web que integre a checklist LGPD estendida com IoT, oferecendo funcionalidades complementares. O foco desse sistema será na facilidade de uso, na intuitividade para o usuário inspetor de sistema e na abordagem de lacunas que a planilha Excel, devido às suas limitações inerentes, não consegue solucionar.

Fundamentação Teórica

Este capítulo resume a LGPD e a segurança em sistemas de informação empresariais, abordando a literatura relevante e destacando aspectos essenciais para o entendimento do conteúdo deste artigo.

2.1 Surgimento da LGPD

A proliferação do modelo de negócios digital, a partir da década de 90, foi o principal impulsionador para o surgimento de regulamentações de proteção de dados. O aumento da coleta e processamento de informações pessoais levantou preocupações sobre privacidade, levando governos a criarem legislações como a GDPR na União Europeia e a LGPD no Brasil [33]. Quando se fala de leis regulatórias de dados, a mais relevante que vem à tona é a GDPR. Ela começou a ser discutida em 2012, foi promulgada em 2016 e começou a ser aplicada no dia 25 de maio de 2018 [16]. Ela foi um marco muito importante para a Europa, até mesmo economicamente, pois a União Europeia passou a exigir que países que fossem se relacionar com ela também deveriam ter regulamentações parecidas em relação a dados [36]. Esse foi mais um fator que impulsionou o Brasil a criar a sua própria lei de regulamentação de tratamento de dados. A lei brasileira foi aprovada em agosto de 2018, mas só começou a ser aplicada dois anos depois, em agosto de 2020. Esse intervalo de tempo se deve ao fato de que as empresas precisaram entender a lei e preparar os seus sistemas para estarem conformes com a LGPD. A lei abrange qualquer um que possa tratar dados pessoais ou sensíveis, seja pessoa física, pessoa jurídica, empresa privada e empresa pública [30].

2.2 Segurança em sistemas de informação e conformidade com a LGPD nas empresas

De acordo com Batista [3], um sistema de informação é um conjunto de componentes interligados que coletam, processam, armazenam e distribuem informações para apoiar a tomada de decisões, coordenação e controle em uma organização. Esses sistemas podem conter informações sobre pessoas, locais e itens importantes e podem ser tanto computadorizados quanto físicos e manuais.

A segurança em sistemas de informação pode ser vista de vários ângulos. Um exemplo de problema é a infecção por software malicioso. Apesar dos esforços contínuos dos profissionais de segurança cibernética, os invasores sempre procuram novas vulnerabilidades [23].

Incidentes de segurança afetam diversas empresas e instituições. Em 2019, dados de mais de 60 instituições de ensino foram comprometidos por vulnerabilidades em um único sistema [25].

Diante do risco de vazamento de dados pessoais, as empresas estão intensificando seus esforços para garantir a conformidade com leis de proteção de dados [13]. Obter essa conformidade apresenta muitos desafios. Um dos principais deles é traduzir os aspectos legais em medidas técnicas viáveis para implementação [41, 37, 15, 24].

Para enfrentar esses desafios, as empresas precisam adotar uma abordagem abrangente de segurança da informação, que inclua prevenção, detecção e recuperação. Prevenção envolve proteger hardware, arquivos, dados e o perímetro da rede com ferramentas como firewalls. A detecção requer sistemas de alerta que notificam sobre invasões. A recuperação foca em criar cópias de segurança dos dados e ter hardwares de reserva [32]. Além disso, as empresas devem implementar medidas eficazes para proteger os dados pessoais, garantindo conformidade legal e evitando penalidades.

Trabalhos Relacionados

O estudo de Mendes [27] criou uma checklist para avaliar a conformidade de softwares com a LGPD, preenchendo uma lacuna na pesquisa que correlaciona sistemas com a legislação. Inspirado pela GDPR, ele desenvolveu essa ferramenta pioneira, demonstrando sua eficácia ao aplicá-la em um sistema universitário. Pereira *et al.* [31] expandiram essa checklist para incluir sistemas IoT, com resultados positivos em testes industriais. Este trabalho busca integrar essas iniciativas em uma única ferramenta, ampliando o suporte para a conformidade de diversos sistemas com a LGPD.

Ainda no campo de checklists de inspeção, Cerqueira, Mello e Travassos [9] desenvolveram a técnica LGPDCheck. Esta ferramenta foi criada por meio de várias etapas, incluindo entrevistas com especialistas, revisão bibliográfica, análise da LGPD, construção dos artefatos e sua avaliação. O checklist foi projetado para três níveis de inspeção: requisitos do sistema (verificação de documentos de requisitos), sistemas em execução (verificação durante a execução dos sistemas) e práticas organizacionais (investigação das práticas relacionadas à segurança e responsabilidade). Os resultados mostraram que o checklist foi eficaz na identificação de defeitos relacionados aos princípios da LGPD em artefatos de software. A avaliação experimental com três equipes de desenvolvimento em um sistema IoT real demonstrou a viabilidade e utilidade da LGPDCheck. Diferente da ferramenta utilizada neste trabalho, que se concentra em facilitar o uso do checklist através de uma plataforma web, a LGPDCheck é voltada para verificar a conformidade com a LGPD por meio de uma abordagem estruturada em três níveis de inspeção.

Por fim, Cejas *et al.* [8] apresentam uma abordagem inovadora que automatiza a verificação de conformidade de Acordos de Processamento de Dados (DPAs) em relação à GDPR. DPAs são contratos estabelecidos entre controladores e operadores de dados que ditam os termos e condições para o processamento de dados pessoais. Embora o trabalho se concentre na GDPR, o objetivo é relevante e se encaixa no escopo desta seção. Na pesquisa, foram empregadas técnicas de Processamento de Linguagem Natural (NLP) para identificar a conformidade dos DPAs com a lei europeia. A ferramenta desenvolvida alcançou uma acurácia média de 84%. Em comparação com outras pesquisas existentes que utilizam ferramentas NLP prontas para uso, a abordagem proposta obteve um ganho de 20% de acurácia, demonstrando uma melhoria considerável. A ferramenta se distingue da ferramenta web, pois a deste trabalho promove uma inspeção manual e minuciosa para garantir a total adequação do sistema. Em contraste, a ferramenta de NLP realiza uma inspeção automática dos textos dos DPAs.

CAPÍTULO 4

Metodologia

A metodologia desse trabalho é dividida em três etapas e é representada por seções. Na seção 4.1, é feita uma análise da checklist existente, em que se caracterizam pontos a melhorar e partes essenciais da planilha. Depois, a seção 4.2 fala sobre todo o processo do desenvolvimento, debatendo as tomadas de decisão e as dificuldades encontradas no caminho. Por fim, a seção 4.3 aborda como será feita a avaliação do sistema desenvolvido.

4.1 Visão preliminar do Checklist Inicial de Conformidade com a LGPD

Mendes, Viana e Rivero [26] criaram um checklist inicial para avaliar a conformidade de sistemas com a LGPD, usando uma Revisão Sistemática da Literatura (RSL) e análises comparativas entre a LGPD e a GDPR. A versão inicial em PDF continha 52 itens distribuídos em quatro colunas, com identificadores, descrições e fontes dos itens.

Posteriormente, o checklist foi aprimorado, resultando em uma planilha com 47 itens obrigatórios da LGPD e 9 itens recomendados, além de 27 itens adicionais para soluções de IoT. Esta versão inclui grau de severidade (leve, grave ou catastrófico) e recomendações para resolver inconformidades [31].

Foi conduzida uma análise minuciosa da checklist existente, examinando seu funcionamento geral, suas funcionalidades essenciais e identificando elementos que poderiam ser reaproveitados, aprimorados ou incrementados. A Figura 4.1 oferece uma visualização da checklist original.



Figura 4.1 Recorte da checklist original, incluindo gráficos e primeiro item da checklist

Após essa análise, tornou-se evidente que a checklist atual não atende completamente às necessidades, e que um sistema web seria mais adequado por várias razões:

- A personalização do preenchimento, validação e geração de gráficos é mais viável em um sistema web.
- Um sistema web é significativamente mais acessível do que uma planilha, pois pode ser acessado de qualquer navegador.
- O controle de versão não pode ser efetivamente implementado em uma planilha.
- A manutenção e escalabilidade de um sistema web oferecem vantagens significativas em comparação com uma planilha.

No estudo conduzido por Pereira *et al.* [31], os participantes identificaram uma área principal de aprimoramento: a necessidade de tornar obrigatórios os comentários sempre que um avaliador considerar um item não conforme com o sistema. Esta medida visa garantir que os motivos por trás de uma marcação sejam claramente comunicados, evitando ambiguidades decorrentes da falta de explicações no checklist anterior. Com base nesse apontamento, torna-se evidente a necessidade de desenvolver um sistema que mantenha os conteúdos e funcionalidades essenciais da planilha, ao mesmo tempo em que incorpora as melhorias sugeridas. Além disso, serão consideradas as sugestões de trabalhos futuros de Mendes [27] e Pereira *et al.* [31].

Ademais, foram conduzidas reuniões com os desenvolvedores do checklist da primeira versão, a fim de compreender integralmente sua operacionalização, identificar suas funcionalidades fundamentais e explorar oportunidades de reutilização, aprimoramento e expansão.

4.2 Desenvolvimento da solução

Esta seção detalha o desenvolvimento da solução, incluindo a criação do protótipo, a implementação inicial do *frontend* com React e TypeScript, a construção das telas de interface, e a

evolução do sistema com a adição de um *backend* usando Express e Prisma para maior funcionalidade e segurança.

4.2.1 Protótipo

A prototipagem é um processo no desenvolvimento de sistemas que envolve criar um modelo preliminar, permitindo ajustes antes da implementação. Este método gera ideias sobre o design da interface e avalia a qualidade da solução em um estágio inicial [4].

Em sistemas web, a prototipagem desempenha um papel fundamental. Além de facilitar a elicitación de requisitos, ela define a aparência visual da interface do usuário, fornecendo uma base essencial para o desenvolvimento [18]. Neste trabalho, a checklist original atua como protótipo, pois contém todos os elementos necessários para a construção do sistema web. Conforme ilustrado na Figura 4.2, a planilha possui abas, cada uma representando uma etapa distinta, o que permitiu o mapeamento dessas abas para páginas do sistema.

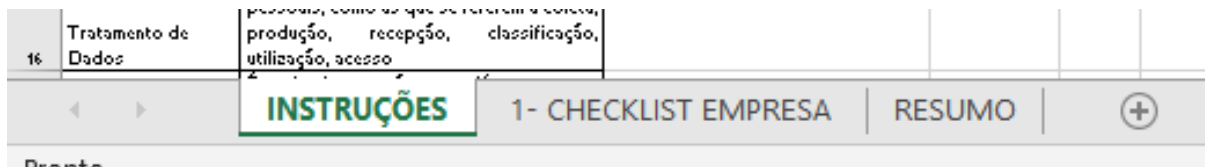


Figura 4.2 Abas da planilha do checklist.

4.2.2 Ideia inicial de desenvolvimento

Na análise inicial deste estudo de desenvolvimento, foi determinado que não seria necessário implementar persistência de dados do usuário. A checklist opera eficientemente em um formato de planilha, dispensando a necessidade de armazenamento centralizado dos dados.

Considerando esses aspectos, iniciou-se o desenvolvimento do *frontend* do sistema web. *Frontend* é encarregado de apresentar a interface ao usuário e possibilitar sua interação com o sistema [17]. Nesta parte, optou-se pelo framework React¹ como principal recurso de desenvolvimento, dado seu amplo uso e reconhecimento na comunidade de desenvolvimento *frontend*, como observado em estudos anteriores [43, 22, 29]. Sua popularidade se reflete em uma comunidade ativa e vasto conteúdo online para suporte. O React, fundamentado na modularização e reutilização de código por meio de componentes, prioriza a eficiência e manutenibilidade do código [5]. Além disso, assim como outros frameworks de ponta no mercado, destaca-se pela reatividade, possibilitando a atualização automática da interface conforme as variáveis reativas são modificadas, resultando em uma experiência do usuário fluida e dinâmica.

O React, concebido para interoperar com JavaScript, também se integra notavelmente com TypeScript. Optamos por TypeScript devido à sua forte tipagem, que aumenta a segurança para os desenvolvedores e para o código. Além disso, o sistema foi projetado para ser responsivo, adaptando-se a diferentes tamanhos de tela. A tipagem estática do TypeScript ajuda a detec-

¹<https://react.dev/>

tar inconsistências durante o desenvolvimento, facilitando a manutenção e escalabilidade do projeto

4.2.3 Construção das telas

Ao abrir o sistema web, o usuário é direcionado inicialmente à página de instruções, conforme ilustrado na Figura 4.3. Esta página foi especificamente adaptada para o sistema, oferecendo orientações claras para o usuário. Na mesma figura, observa-se a presença de um cabeçalho, um componente comum em sistemas web, que contém o nome do sistema e um botão para alternar instantaneamente entre os temas claro e escuro.



Figura 4.3 Página de instruções no sistema.

Na sequência do fluxo do usuário, a próxima tela permite escolher quais famílias de checklists serão avaliadas na inspeção do sistema atual. Esta funcionalidade atende a uma das sugestões para trabalhos futuros propostas por Pereira *et al.* [31]. Dessa forma, a checklist adapta-se às necessidades específicas do sistema avaliado, filtrando os itens com base na escolha do usuário. O resultado da implementação desta tela pode ser observado na Figura 4.4.

ist LGPD



Selecione abaixo quais famílias de checklists você quer incluir nessa avaliação, além da checklist geral:

☐ Checklist IoT

Ao voltar, você não perde o seu progresso

[Voltar](#) [Continuar](#)

Figura 4.4 Seleção de famílias de checklists para inspeção.

Após esta etapa, o usuário da ferramenta encontrará a primeira tela de itens a serem respondidos. Na checklist original, tanto os itens obrigatórios quanto os não obrigatórios estão na mesma aba. No entanto, constatou-se que separá-los em duas páginas distintas no sistema web é mais eficiente, pois divide melhor as etapas e reduz o cansaço do inspetor.

Na checklist original, o usuário responde aos itens marcando "Sim", "Não" ou "Não se aplica". Durante os testes realizados por Pereira *et al.* [31], concluiu-se que seria benéfico obrigar o inspetor a preencher os campos "Grau de Severidade" e "Comentário do Avaliador" caso a resposta seja "Não". Essa regra foi implementada no desenvolvimento do sistema, e o usuário só pode avançar se cumprir essa exigência.

Além disso, Mendes [27] sugere, como trabalho futuro, a possibilidade de filtrar a visualização da checklist por tipo de resposta, como mostrar apenas os itens respondidos com "Não". Esta funcionalidade foi incorporada como um requisito do sistema.

A próxima tela no fluxo do usuário trata dos itens não obrigatórios. Um destaque desta tela é a inclusão de itens relacionados à IoT [31], caso o inspetor tenha selecionado essa opção. Após essa parte, chega-se à etapa final do processo de inspeção do sistema, a tela de "Relatório". Nessa tela, o usuário pode visualizar gráficos que mostram as estatísticas de preenchimento dos itens obrigatórios e não obrigatórios de maneira centralizada. A Figura 4.5 apresenta um exemplo dos gráficos. Abaixo deles, todos os itens da checklist são exibidos. Uma nova funcionalidade desta etapa, em relação à planilha, é a geração de relatórios em PDF.

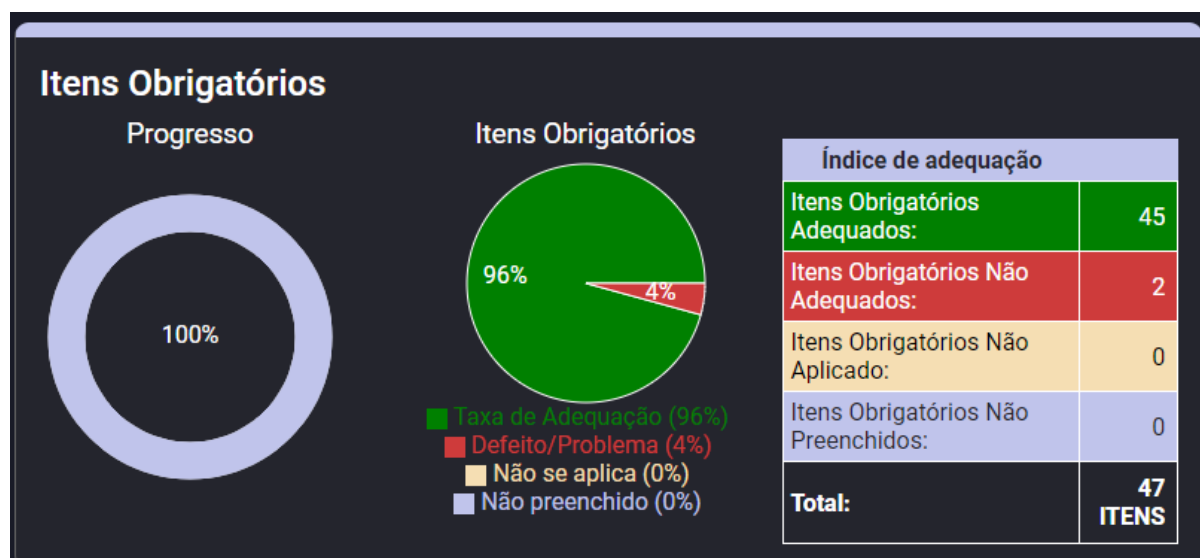


Figura 4.5 Exemplo do gráfico.

Ao concluir a primeira versão, verificou-se que a implementação do sistema web apenas com *frontend* limitava a presença de funcionalidades promissoras, que seriam diferenciais em comparação com a planilha. Considerando essa limitação, iniciou-se o desenvolvimento da segunda versão da ferramenta, agora incluindo um *backend* com banco de dados. O *backend* é o núcleo de uma aplicação, abrangendo o servidor e suas operações. Ele lida com o armazenamento, manipulação de dados e execução das lógicas de negócio, funcionando sem contato direto com os usuários [21].

4.2.4 Evolução da ferramenta

Para desenvolver o *backend*, é essencial inicialmente definir a estrutura do banco de dados, uma vez que ele determina os atributos das entidades e suas interações. A abordagem mais comum para essa estruturação é a utilização do modelo relacional [10]. A Figura 4.6 apresenta o modelo da ferramenta.

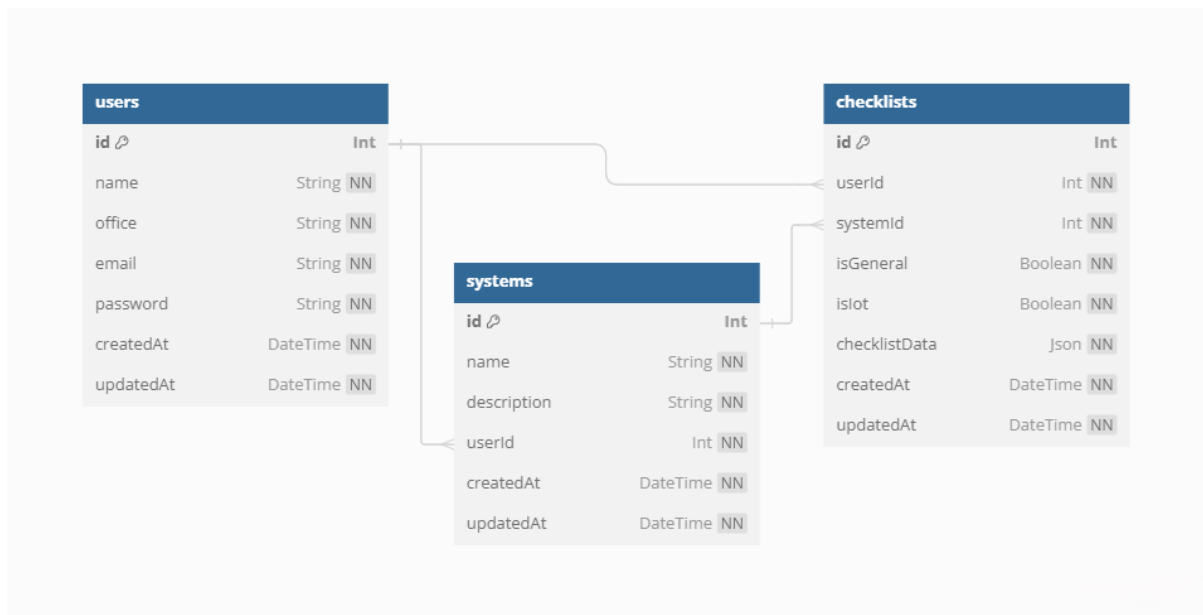


Figura 4.6 Modelo relacional da ferramenta.

O modelo apresentado inclui três tabelas principais. A tabela de usuários armazena informações sobre os usuários cadastrados na ferramenta, como nome e cargo. A tabela de sistemas contém os atributos nome e descrição do sistema, sendo que cada sistema está associado a um usuário. A tabela de checklists registra avaliações, associando cada avaliação a um usuário e a um sistema. Com a definição do banco de dados concluída, foi possível prosseguir para o desenvolvimento do *backend*.

Para o *backend*, foi utilizada a linguagem TypeScript [28]. Ela é uma linguagem em constante evolução que se baseia em JavaScript, adicionando recursos de verificação de tipo estático [38]. Por ser a mesma empregada no *frontend*, a manutenção da ferramenta é facilitada, pois um desenvolvedor precisa conhecer apenas essa linguagem para entender ambas as partes do sistema. Considerando a natureza do *backend*, a utilização de um framework que gerencie requisições é benéfica. O framework escolhido foi o Express, devido à sua simplicidade, velocidade e escalabilidade.

Além disso, para comunicar o *backend* com o banco de dados, utilizou-se uma ORM (Object Relational Mapper) [14]. A ORM escolhida foi o Prisma [34]. Ele simplifica o gerenciamento do banco de dados, lidando bem com migrações do banco e da comunicação com ele. Com o *backend* estruturado, ele começou a ser codificado.

Durante o desenvolvimento da ferramenta, o tratamento correto dos dados foi uma prioridade constante. Boas práticas foram implementadas no *backend* para garantir a segurança dos dados pessoais dos usuários. Uma dessas práticas foi a criptografia das senhas ao armazená-las no banco de dados. Além disso, utilizou-se JWT (JSON Web Token) [19] para a autenticação dos usuários. O JWT é um tipo de *token* que contém informações essenciais e é protegido por uma assinatura digital, gerada com uma chave secreta [2]. Essa chave é uma variável de ambiente que permanece exclusivamente no servidor e não é enviada para o sistema de ver-

sionamento do código, garantindo maior segurança. Após o login, o servidor envia um JWT de autenticação ao *frontend*. Esse JWT é anexado ao cabeçalho de todas as requisições HTTP feitas pelo *frontend* ao servidor. Se o JWT estiver ausente, corrompido ou inválido, as requisições que requerem autenticação não serão processadas pelo *backend*. Além disso, mesmo que um usuário mal-intencionado consiga o *token* de outra pessoa, ele será inútil após o prazo de expiração.

Com a integração do banco de dados e do *backend*, diversas funcionalidades importantes se tornam disponíveis. O usuário pode cadastrar sistemas e preencher checklists associadas a esses sistemas. Além disso, o usuário tem a capacidade de visualizar uma listagem das checklists já preenchidas, bem como editá-las e excluí-las.

Por fim, foi necessário adaptar o código do *frontend* para se conectar ao *backend* e criar novas telas. É importante mencionar que, embora o usuário possa fazer login, ele também pode realizar avaliações de sistemas sem ter uma conta. No entanto, sem autenticação, o usuário não terá o histórico salvo e não terá acesso a todas as funcionalidades disponíveis apenas para usuários autenticados.

4.3 Avaliação do sistema

O checklist de Pereira *et al.* [31] foi submetido a uma avaliação em um renomado instituto privado de inovação tecnológica. O contato foi estabelecido com o instituto para apresentar essa nova versão, obtendo a participação de um desenvolvedor e pesquisador, que também fez parte da avaliação da primeira versão do checklist. Além disso, houve a valiosa contribuição de três desenvolvedores de um núcleo de inovação em tecnologia da informação, comunicação e automação, bem como a avaliação de um desenvolvedor de uma empresa privada. Dessa forma, cinco profissionais experientes no desenvolvimento de sistemas participaram dessa avaliação.

A ferramenta foi testada e avaliada. Após um período de testes, eles responderam a um formulário. Esse formulário contém itens divididos em três categorias: facilidade de uso, utilidade do uso e intenção de uso. Em cada uma dessas categorias, existem afirmações, nas quais os entrevistados responderam seu grau de concordância, utilizando a escala Likert [20]. No final desse formulário, há campos de resposta aberta para que os entrevistados deixem comentários e sugestões adicionais sobre a ferramenta.

CAPÍTULO 5

Resultados

5.1 Resultado da Solução

Após a conclusão do desenvolvimento, a ferramenta foi disponibilizada na internet para testes de usuários em um processo conhecido como *deploy*. Considerando que o sistema web é composto por dois projetos interdependentes, o *backend* e o *frontend*, ambos necessitaram de *deploy* individual. Além disso, o banco de dados, inicialmente executado localmente, também precisou ser disponibilizado remotamente.

Para o *deploy* do *frontend*, foi utilizada a plataforma Vercel [42], um serviço de nuvem focado em *frontend*. Uma das principais vantagens do Vercel é seu sistema de entrega contínua [39], que automatiza a publicação de novas versões. Sempre que um novo *commit* é feito na *branch* principal, a plataforma executa o *pipeline* de publicação, disponibilizando a nova versão do site. O Vercel também gera um *link* único para acesso ao site.

Para o *deploy* do *backend* e do banco de dados, foi escolhida a plataforma Render [35]. Embora ofereça serviços pagos, a opção selecionada foi a gratuita, que, apesar de limitada, atende aos requisitos deste trabalho. Similar ao Vercel, o Render integra-se com o GitHub [11], permitindo a entrega contínua e publicação automática de novas versões mediante novos *commits* na *branch* principal. A ferramenta está atualmente acessível online ¹.

Os repositórios dos projetos são de código aberto, alinhados com os princípios do software livre [7]. O código-fonte do *frontend* pode ser acessado neste repositório no GitHub². Já o código-fonte do *backend* está disponível neste outro repositório no GitHub³.

A ferramenta criada neste trabalho é liberada sob a licença MIT [7]. Esta licença autoriza qualquer pessoa a usar, copiar, modificar e distribuir o software, desde que a atribuição original seja preservada. A licença MIT, conhecida por sua flexibilidade, é uma das mais populares entre as licenças de código aberto, promovendo a colaboração e o intercâmbio de melhorias entre os desenvolvedores.

5.2 Resultado da Avaliação

Com base na avaliação da ferramenta, três participantes concordaram totalmente com sua facilidade de uso, enquanto um concordou parcialmente e outro discordou parcialmente. Em relação à intuição do sistema, três participantes concordaram totalmente, um concordou parcialmente

¹<https://lgpd-checklist.vercel.app/>

²<https://github.com/Matheusfrej/LGPD-checklist-frontend>

³<https://github.com/Matheusfrej/LGPD-checklist-api>

e outro discordou parcialmente. Os participantes identificaram áreas de melhoria para tornar a ferramenta mais acessível e intuitiva, incluindo a sugestão de um participante para tornar o vocabulário da LGPD acessível durante todo o processo de preenchimento, em vez de apenas no início. Isso sugere que a dificuldade encontrada pode estar relacionada à compreensão dos termos legais, em vez da usabilidade direta do sistema.

Além disso, os desenvolvedores apontaram algumas melhorias para a ferramenta, incluindo a utilização de mais gráficos ou outros recursos visuais para tornar a apresentação mais intuitiva e informativa. Aconselharam também destacar campos importantes não preenchidos, como comentários ou seleção de severidade, para facilitar a identificação de áreas que precisam de atenção. Por fim, comentaram que o preenchimento se torna cansativo e, para mitigar essa dificuldade, sugeriram a adição de paginação dentro da checklist, a fim de evitar a necessidade de rolar a tela durante o preenchimento.

Na avaliação da utilidade do Sistema LGPD, observou-se que todos os participantes concordaram que ele permite realizar a inspeção do sistema de forma mais rápida. Em relação à melhoria da produtividade ao identificar defeitos ou problemas no sistema, três concordaram totalmente e dois concordaram parcialmente. Quanto à percepção de utilidade para encontrar defeitos ou problemas no sistema, dois concordaram totalmente, um concordou parcialmente e um discordou parcialmente. Esses resultados indicam uma percepção geral positiva em relação à utilidade do Sistema LGPD para melhorar a inspeção e identificação de problemas no sistema, embora haja ressalvas expressas por alguns participantes.

Com base na intenção de uso do Sistema LGPD, observou-se que dois participantes concordaram totalmente e três concordaram parcialmente que pretendem utilizar a ferramenta para encontrar defeitos ou problemas em sistemas futuramente. Quanto à recomendação do Sistema LGPD para outras empresas, três participantes concordaram totalmente e dois concordaram parcialmente. Esses resultados sugerem um interesse significativo em utilizar o Sistema LGPD como uma ferramenta para inspeção e identificação de problemas em sistemas, com a maioria dos participantes manifestando intenção de uso e disposição para recomendar a ferramenta para outras empresas.

CAPÍTULO 6

Conclusão

Este trabalho apresentou o desenvolvimento de uma ferramenta para facilitar a conformidade das empresas com os requisitos da LGPD. A partir da necessidade de otimizar um checklist em Excel, buscou-se oferecer uma solução mais eficiente e acessível para lidar com os desafios regulatórios impostos pela legislação de proteção de dados.

Embora progressos significativos tenham sido feitos, reconhece-se que há áreas que podem ser melhoradas. Por exemplo, identificou-se que a interface do usuário e a linguagem legal utilizada podem ser aprimoradas para facilitar a compreensão e utilização da ferramenta pelos usuários finais. Além disso, o número limitado de avaliadores pode restringir a generalização dos resultados.

Como próximos passos, planeja-se realizar avaliações com um grupo mais amplo de avaliadores, visando obter uma perspectiva mais abrangente sobre a eficácia e usabilidade da ferramenta. Também se pretende implementar uma nova versão, levando em consideração os feedbacks dos profissionais que participaram desta avaliação. Além disso, há planos de expandir a aplicabilidade da ferramenta para diversas outras áreas de especialização em sistemas, além de IoT.

Ao final, acredita-se que esta ferramenta representa um avanço significativo na simplificação e melhoria dos processos de conformidade com a LGPD, fornecendo às empresas uma solução prática e eficaz para enfrentar os desafios regulatórios em constante evolução.

Referências Bibliográficas

- [1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.
- [2] Stenly Ibrahim Adam, Jimmy H Moedjahedy, and Jeremiah Maramis. Restful web service implementation on unklab information system using json web token (jwt). In *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, pages 1–6, Makassar, Indonesia, 2020. IEEE.
- [3] Emerson O Batista. *Sistemas de informação*. Saraiva Educação SA, Sao Paulo, Brazil, 2017.
- [4] D. Baumer, W. Bischofberger, H. Lichter, and H. Zullighoven. User interface prototyping-concepts, tools, and experience. In *Proceedings of IEEE 18th International Conference on Software Engineering*, pages 532–541, Berlin, Germany, 1996. IEEE.
- [5] Chandradeep Bhatt, Divyanshu Tiwari, Deepika Dua, Shefali Gupta, and Teekam Singh. Elevating online retail: An in-depth look at the implementation of react js in advanced e-commerce. In *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, pages 1–4, New York, NY, USA, 2024. IEEE.
- [6] Brasil. Lei geral de proteção de dados pessoais (lgpd). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm., August 2018. Acesso em: 24 de abril de 2024.
- [7] Augusto Campos. O que é software livre. Disponível em: <http://br-linux.org/linux/faq-softwarelivre>, março 2006. Acesso em: 15 de maio de 2024.
- [8] Orlando Amaral Cejas, Muhammad Ilyas Azeem, Sallam Abualhaija, and Lionel C. Briand. Nlp-based automated compliance checking of data processing agreements against gdpr. *IEEE Transactions on Software Engineering*, 49(9):4282–4303, 2023.
- [9] Diego André Cerqueira, Rafael Maiani de Mello, and Guilherme Horta Travassos. Experimental evaluation of a checklist-based inspection technique to verify the compliance of software systems with the brazilian general data protection law, 2023.
- [10] Edgar F Codd. *The relational model for database management: version 2*. Addison-Wesley Longman Publishing Co., Inc., MA, United States, 1990.

- [11] Valerio Cosentino, Javier L Cánovas Izquierdo, and Jordi Cabot. A systematic mapping study of software development with github. *Ieee access*, 5:7173–7192, 2017.
- [12] Lorrie Faith Cranor. Internet privacy. *Commun. ACM*, 42(2):28–38, feb 1999.
- [13] Evandro Thalles Vale de Castro, Geovana RS Silva, and Edna Dias Canedo. Ensuring privacy in the application of the brazilian general data protection law (lgpd). In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, pages 1228–1235, Salamanca, Spain, 2022. ACM.
- [14] DevMedia. Orm (object-relational mapper). Disponível em: <https://www.devmedia.com.br/orm-object-relational-mapper/19056>, 2024. Acesso em: 10 de maio de 2024.
- [15] Anirudh Ekambaranathan, Jun Zhao, and George Chalhoub. Navigating the data avalanche: Towards supporting developers in developing privacy-friendly children’s apps. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(2):1–24, 2023.
- [16] European Parliament and Council of the European Union. Regulation (eu) 2016/679 of the european parliament and the council (general data protection regulation). Disponível em: <https://gdpr-info.eu/>, 2016. Acesso em: 24 de abril de 2024.
- [17] Fang He. Implementation of secure login and access methods for web frontend. In *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*, pages 1–5, New York, NY, USA, 2023. IEEE, IEEE.
- [18] Martti Jeenicke, Wolf-Gideon Bleek, and Ralf Klischewski. Revealing web user requirements through e-prototyping. In *SEKE*, pages 9–16, San Francisco, USA, 2003. Citeseer, Citeseer.
- [19] Michael Jones, John Bradley, and Nat Sakimura. Json web token (jwt). Technical report, Internet Engineering Task Force (IETF), 2015.
- [20] A. Joshi, S. Kale, S. Chandel, and D. K. Pal. Likert scale: Explored and explained. *Current Journal of Applied Science and Technology*, 7(4):396–403, 2015. Acesso em: 26 de abril de 2024.
- [21] Altino Alves Júnior, Letícia de Souza Meireles, Lucas Alves Rossi Figueira, Vítor Marcondes Moraes Carmo, Humberto T Marques-Neto, and Laerte Xavier. Entendendo o engajamento das comunidades front-end e back-end nos repositórios do github. In *Anais do X Workshop de Visualização, Evolução e Manutenção de Software*, pages 26–30, Virtual Event, 2022. SBC, SBC.
- [22] Gursheen Kaur and Raj Gaurang Tiwari. Comparison and analysis of popular frontend frameworks and libraries: An evaluation of parameters for frontend web development. In *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pages 1067–1073, New York, NY, USA, 2023. IEEE, IEEE.

- [23] R.A. Kemmerer. Cybersecurity. In *25th International Conference on Software Engineering, 2003. Proceedings.*, pages 705–715, Portland, OR, USA, 2003. IEEE Computer Society.
- [24] Pedro Machado, Jéssyka Vilela, Mariana Peixoto, and Carla Silva. A systematic study on the impact of gdpr compliance on organizations. In *Proceedings of the XIX Brazilian Symposium on Information Systems*, pages 435–442, Maceió, Brazil, 2023. SBC.
- [25] Rodrigo Machado, Diego Kreutz, Giulliano Paz, and Gustavo Rodrigues. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. In *Anais da XVII Escola Regional de Redes de Computadores*, pages 154–159, Porto Alegre, RS, Brasil, 2019. SBC.
- [26] João Mendes, Davi Viana, and Luis Rivero. Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In *Proceedings of the XXXV Brazilian Symposium on Software Engineering*, pages 263–268, Porto Alegre, RS, Brasil, 2021. ACM.
- [27] João Pedro Marques Mendes. LGPD-CHECK: Um checklist para avaliação da aderência de sistemas computacionais à lei geral de proteção de dados brasileira. Master’s thesis, Universidade Federal do Maranhão, 2022.
- [28] Microsoft. TypeScript. Disponível em: <https://www.typescriptlang.org/>, 2012. Acesso em: 09 de maio de 2024.
- [29] Cornelia Mihaela Novac, Ovidiu Constantin Novac, Raluca Marina Sferle, Mircea Ioan Gordan, Gyöngyi Bujdosó, and Camelia Maria Dindelegan. Comparative study of some applications made in the vue.js and react.js frameworks. In *2021 16th International Conference on Engineering of Modern Electric Systems (EMES)*, pages 1–4, Oradea, Romania, 2021. IEEE.
- [30] Fabrício Peloso Piurcosky, Marcelo Aparecido Costa, Rodrigo Franklin Frogeri, and Cristina Lelis Leal Calegario. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de negocios*, 10(23):89–99, 2019.
- [31] Ivonildo Pereira, João Mendes, Davi Viana, Luis Rivero, Waldemar Ferreira, and Sergio Soares. Extending an LGPD compliance inspection checklist to assess IoT solutions: An initial proposal. In *Trilha da Indústria - Congresso Brasileiro de Software: Teoria e Prática (CBSOFT), 13.*, pages 28–31, Uberlândia, Brazil, 2022. SBC.
- [32] José Maurício dos Santos Pinheiro. Ameaças e ataques aos sistemas de informação: Prevenir e antecipar. *Cadernos UniFOA*, 3(5):11–21, mar. 2017.
- [33] Patricia Peck Pinheiro. *Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd*. Saraiva Educação SA, Brasil, 2020.
- [34] Prisma Labs, Inc. Prisma. Disponível em: <https://www.prisma.io/>, 2024. Acesso em: 10 de maio de 2024.

- [35] Render, Inc. Render - The Easiest Cloud For All Your Apps And Websites. Disponível em: <https://render.com/>, Accessed 2024. Acesso em: 15 de maio de 2024.
- [36] Cedric Ryngaert and Mistale Taylor. The gdpr as global data protection regulation? *AJIL Unbound*, 114:5–9, 2020.
- [37] Pattaraporn Sangaroonsilp, Hoa Khanh Dam, Morakot Choetkiertikul, Chaiyong Ragkhitwetsagul, and Aditya Ghose. A taxonomy for mining and classifying privacy requirements in issue reports. *Information and Software Technology*, 157:107162, 2023.
- [38] Joshua D Scarsbrook, Mark Utting, and Ryan KL Ko. Typescript’s evolution: An analysis of feature adoption over time. In *2023 IEEE/ACM 20th International Conference on Mining Software Repositories (MSR)*, pages 109–114, Melbourne, Australia, 2023. IEEE, IEEE.
- [39] Mojtaba Shahin, Muhammad Ali Babar, and Liming Zhu. Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. *IEEE access*, 5:3909–3943, 2017.
- [40] Jefferson Silva, Newton Calegari, and Eduardo Gomes. After brazil’s general data protection law: Authorization in decentralized web applications. In *Companion Proceedings of the 2019 World Wide Web Conference*, pages 819–822, New York, NY, USA, 2019. ACM.
- [41] Sean Sirur, Jason RC Nurse, and Helena Webb. Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pages 88–95, Toronto, Canada, 2018. ACM.
- [42] Vercel, Inc. Vercel - Develop. Preview. Ship. Disponível em: <https://vercel.com/>, Accessed 2024. Acesso em: 15 de maio de 2024.
- [43] Rishi Vyas. Comparative analysis on front-end frameworks for web applications. *International Journal for Research in Applied Science and Engineering Technology*, 10(7):298–307, 2022.