UNIVERSIDADE FEDERAL DO PAMPA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

SAMARA BUENO MARQUES

EPIC: ANALISADOR DE CONFORMIDADE COM A LGPD PARA PROCESSOS E INFORMAÇÕES DE EMPRESAS

Bagé
2022

SAMARA BUENO MARQUES

EPIC: ANALISADOR DE CONFORMIDADE COM A LGPD PARA PROCESSOS E INFORMAÇÕES DE EMPRESAS

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Engenharia de Computação como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Érico Marcelo Hoff do Amaral

Bagé
2022

Ficha catalográfica elaborada automaticamente com os dados fornecidos pelo(a) autor(a) através do Módulo de Biblioteca do Sistema GURI (Gestão Unificada de Recursos Institucionais).

M357e Marques, Samara Bueno

EPIC: Analisador de Conformidade com a LGPD para Processos e Informações de Empresas / Samara Bueno Marques.

- 2022.

97 f.: il.

Orientador: Érico Marcelo Hoff do Amaral

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Pampa, Campus Bagé, Bacharelado em Engenharia de Computação, 2022.

1. Lei Geral de Proteção de Dados. 2. LGPD. 3. Privacidade de dados. 4. Segurança da informação. 5. Dados pessoais. I. Érico Marcelo Hoff do Amaral. II. Título.

SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

Universidade Federal do Pampa

SAMARA BUENO MARQUES

EPIC: ANALISADOR DE CONFORMIDADE COM A LGPD PARA PROCESSOS E INFORMAÇÕES DE EMPRESAS

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Engenharia de Computação da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Computação.

Trabalho de Conclusão de Curso defendido e aprovado em: 13 de Agosto de 2022.

Banca examinadora:

_____

Prof. Dr. Érico Marcelo Hoff do Amaral
Orientador – UNIPAMPA

_____

Prof. Dr. Leonardo Bidese de Pinho
UNIPAMPA

_____

Prof. Dr. Julio Saraçol Domingues Júnior
UNIPAMPA

Assinado eletronicamente por **JULIO SARACOL DOMINGUES JUNIOR**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 19/08/2022, às 18:07, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **LEONARDO BIDESE DE PINHO**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 19/08/2022, às 19:48, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **ERICO MARCELO HOFF DO AMARAL**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 20/08/2022, às 01:39, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0903651** e o código CRC **3C84B8FE**.

Referência: Processo nº 23100.017424/2022-02 SEI nº 0903651

AGRADECIMENTO

A minha família, especialmente minha mãe, por todo apoio, amor, dedicação e força em todos momentos difíceis que passei ao longo da graduação, sempre dando o melhor para que eu seguisse em frente.

Ao meu parceiro de vida Tiago, por todo apoio, dedicação e força. Obrigada pelos ensinamentos, por não ter deixado eu desistir.

Ao Prof. Dr. Érico Marcelo Hoff do Amaral, pela orientação, apoio e por sempre incentivar a pesquisa e extensão durante a minha trajetória acadêmica.

Ao Prof. Dr. Leonardo Bidese de Pinho, por todas as dicas e orientações durante a ministração da disciplina de Trabalho de Conclusão de Curso I (TCC I) e, também, como membro da banca do TCC I.

Ao Prof. Dr. Carlos Michel Betemps pelas orientações feitas como membro da banca de TCC I, as quais foram muito importantes para a construção do TCC II. E também por ter sido um ótimo orientador de estágio obrigatório, fase fundamental da minha formação.

Ao Leandro Bolzan Béria pelo auxílio fundamental na disponibilização da ferramenta para o público.

A todos os professores que, de alguma forma, contribuíram para que eu chegasse até aqui. Obrigada a todos que acreditaram em mim.

“Toute réussite déguise une abdication.”

— Simone de Beauvoir

RESUMO

Em um cenário onde os dados pessoais possuem grande importância para o desenvolvimento econômico surge uma preocupação quanto ao tratamento das informações e proteção da privacidade. No Brasil a Lei Geral de Proteção de Dados (LGPD), está em vigor desde agosto de 2020. Muitas empresas, principalmente do seguimento *Small and Medium Business* (SBM), ainda estão em adaptação com à lei, tornando-se necessários meios para disseminação do seu conhecimento e sua aplicabilidade. Além disso, as consequências da não conformidade com a LGPD variam de multas até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Esta pesquisa teve como objetivo a implementação de uma solução de *software*, alinhada à LGPD, que auxilia as empresas a mapear seus processos a fim de ampliar o nível de segurança desses dados, alertando sobre seus níveis de criticidade. A metodologia de desenvolvimento deste trabalho baseou-se no método dedutivo, sendo quantitativa em relação à abordagem do problema, descritiva e explicativa quanto à base nos objetivos e bibliográfica e de levantamento quanto aos procedimentos técnicos. A partir do referencial teórico estudado e da Revisão Sistemática da Literatura (RSL), foi proposta uma solução de *software* para análise de segurança de dados, com o intuito de auxiliar as empresas SMB a estarem em conformidade com a LGPD. Para isso, realizou-se a modelagem, desenvolvimento, testes e, por fim, a validação da ferramenta com empresas. Após, foi aplicado um questionário com o objetivo de obter o *feedback* e perfil dos usuários. Os resultados dos índices de segurança da informação obtidos, mostram que, de forma geral, as empresas ainda precisam adotar medidas de seguranças básicas. Já os índices de não conformidade apontam que a maioria, mesmo as empresas da área de TI, ainda precisam adequar grande parte de seus processos à LGPD. Em relação a usabilidade do EPIC a maioria dos resultados obtiveram os graus máximos de satisfação de acordo com os aspectos questionados. Sabendo-se que a maioria dos usuários afirmaram que a análise fornecida pelo EPIC corresponde totalmente à realidade da empresa, pressupõe-se que a ferramenta desenvolvida apresenta resultados condizentes com o que foi proposto. Por último, a maioria das empresas responderam que indicariam, com certeza, o EPIC para outras empresas, o que corrobora com a proposta da ferramenta.

Palavras-chave: Lei Geral de Proteção de Dados; LGPD; Privacidade de dados; Segurança da informação; Dados pessoais.

ABSTRACT

In a scenario where personal data is of great importance for economic development, a concern about the processing of these data and privacy protection arises in a way that does not interfere with freedom of information. In Brazil, the General Data Protection Law has been in force since August 2020. Many companies, especially the Small and Medium Business (SMB) ones, are still adapting, becoming useful means for the dissemination of knowledge of the law and its applicability. The objective of this research was to develop a software solution, in compliance with the General Data Protection Law (LGPD), that helps companies to map their processes and information in order to increase the security level of these data and alerting about the critical levels of these information. The development methodology of this paper was based on the deductive method, being quantitative in relation to the approach of the problem, descriptive and explanatory as to the basis of the objectives, and related to the technical procedures is bibliographical and survey. From the theoretical references studied and from Systematic Literature Review (SLR), was proposed a software solution through an mapping process to analysis data security approach, intending to help the SMB companies to be compliant to LGPD. For this, the tool was modeled, developed, tested and, finally, validated with real SMB companies. Afterwards, a questionnaire was applied in order to obtain the users feedback and profile. The results of the information security indexes obtained show that companies in the Information Technology (IT) sector are those with moderate and high levels and that, in general, the companies still need to adopt basic security measures. The non-compliance rates obtained by the companies show that most, even IT companies, still need to adapt a large part of their processes to the LGPD. Regarding the usability of the EPIC, most of the results obtained the maximum degrees of satisfaction according to the aspects questioned. Knowing that most users stated that the analysis provided by EPIC fully corresponds to the company's reality, it is assumed that the developed tool presents results consistent with what was proposed. Finally, most companies responded that they would indicate, certainly, EPIC for other companies, which corroborates the proposal of the tool.

Keywords: General Data Protection Law; LGPD; Data Privacy; Information Security; Personal Data.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
BC	Base de Conhecimento
BD	Banco de Dados
BPMN	*Business Process Modeling Notation*
DPO	*Data Protection Officer*
GDPR	*General Data Protection Regulation*
IoT	*Internet of Things*
LGPD	Lei Geral de Proteção de Dados
RSL	Revisão Sistemática da Literatura
SI	Segurança da Informação
SAD	Sistemas de Apoio à Decisão
SE	Sistema Especialista
SGPI	Sistema de Gestão de Privacidade da Informação
SMB	*Small and Medium Business*
SO	Sistema Operacional
TI	Tecnologia da Informação
UML	*Unified Modeling Language*
UNIPAMPA	Universidade Federal do Pampa

SUMÁRIO

1 INTRODUÇÃO

Em um cenário onde os dados pessoais possuem grande importância para o desenvolvimento econômico surge uma preocupação quanto ao tratamento desses dados e proteção da privacidade de uma forma que não interfira na liberdade de informação. Com o domínio da *Internet of Things* (IoT), serviços em nuvem e aplicações com frágil proteção de dados, observa-se também o aumento de vazamento de dados pessoais (BISSO et al., 2020).

Hoje, mais de 126 países no mundo possuem leis para a proteção de dados pessoais visando a regulamentação do tratamento de dados das empresas, evitando-se o mau uso destes, bem como a responsabilização das empresas por isso e também por incidentes e acidentes com dados pessoais (SOARES, 2021).

No Brasil a Lei Geral de Proteção de Dados (LGPD) assinada em agosto de 2018, e em vigor desde agosto de 2020, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Por ser uma lei recente as empresas ainda estão em adaptação, tornando-se necessários meios eficazes para disseminação do conhecimento da mesma e sua aplicabilidade.

Empresas do segmento *Small and Medium Business* (SMB) possuem, normalmente, sistemas de planejamento e controles simples com regras e procedimentos informais e tendem a ter menos padronização de processos de trabalho, o que pode vir a ser um problema já que a LGPD exige um controle total de todos os processos que contêm dados pessoais (BRODIN, 2019). Desse modo, essas empresas podem vir a enfrentar um desafio iminente de saber se os mecanismos de processo de negócios atuais estão em conformidade com a lei. Além disso, as consequências da não conformidade podem ser desde multas até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Nesse contexto, ferramentas que automatizem o processo de conformidade com a lei tornam-se necessárias para essa importante adequação que impacta diretamente na imagem e modelo de negócio especialmente das empresas do segmento SMB que possuem recursos e sistemas de gestão da informação limitados.

1.1 Problema de pesquisa

É possível implementar uma solução de *software*, alinhada à LGPD, que auxilie as empresas *Small and Medium Business* (SMB) a mapear seus processos e informações, a fim de ampliar o nível de segurança desses dados, além de fornecer recursos de monitoramento e alertas sobre os níveis de criticidade e riscos da exposição dessas informações?

1.2 Objetivo Geral

Desenvolver uma solução de *software*, *open source*, baseada em *containers*, que a partir de informações fornecidas pelo usuário torne possível a coleta de dados e mapeamento de processos. Com base nisso, a solução deverá, através de um modelo específico, ser capaz de classificar as informações verificando se as mesmas estão em conformidade com a LGPD gerando ao final desse processo um relatório com os resultados.

1.3 Objetivos Específicos

- Estudar e analisar as seções da Lei Geral de Proteção de Dados (LGPD) e normas que podem auxiliar no processo de adequação;
- Realizar uma Revisão Sistemática da Literatura (RSL) a fim de ter conhecimento do estado da arte do tema em questão e analisar as possíveis contribuições para o desenvolvimento do presente trabalho;
- Identificar os requisitos necessários para a definição de criticidade dos dados;
- Com base nos estudos realizados, propor um modelo para análise de conformidade com a LGPD para os processos de empresas do segmento SMB;
- Testar e validar o modelo proposto;
- Propor projeto de *software* para automatizar o modelo criado;
- Realizar o levantamento de tecnologias e definir a plataforma a ser adotada para a construção da solução;
- Implementar a solução;

- Testar e validar a solução;
- Analisar e discutir os resultados obtidos.

1.4 Organização do trabalho

Além da introdução apresentada no capítulo 1, são apresentadas no capítulo 2 as bases teóricas e os trabalhos correlatos à essa pesquisa. O capítulo 3 apresenta a metodologia de pesquisa, onde são descritas a classificação da pesquisa e as etapas seguidas. No capítulo 4 descreve-se o modelo proposto, cálculos utilizados para as análises, a modelagem do sistema e as tecnologias usadas. O capítulo 5 aborda os detalhes da implementação e os testes da ferramenta. O capítulo 6 apresenta os resultados e discussões das etapas de verificação e experimentação da aplicação. Por fim, o capítulo 7 aborda as considerações finais da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA E REVISÃO DA LITERATURA

Neste capítulo será apresentado o embasamento teórico considerado importante para o entendimento e desenvolvimento do projeto. Inicialmente a seção 2.1 aborda os aspectos mais relevantes relacionados à Lei Geral de Proteção de Dados (LGPD). Na seção 2.2 são apresentados os conceitos de Sistemas Especialistas e Apoio à Decisão. A seção 2.3 introduz os conceitos de virtualização e *containers* e, por fim, a seção 2.4 trata sobre a Revisão Sistematica da Literatura (RSL) e os trabalhos correlatos à esse estudo.

2.1 LGPD e *Compliance*

Conforme descrito no capítulo 1, a LGPD se aplica a todas as empresas e afeta todos os cidadãos brasileiros que tratam dados pessoais. Ela foi inspirada na *General Data Protection Regulation* (GDPR)[1], que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores. As normas gerais contidas na LGPD são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. Na figura 1 é possível se observar um panorama geral da LGPD. Ela mostra de forma resumida o que a lei regula, sua origem, missão, direitos, princípios e fundamentos.

[1] https://gdpr-info.eu/

Figura 1 – Panorama LGPD.

Fonte: Autora (2022)

No artigo 3° a lei informa sobre a questão territorial, onde a aplicação independe do país de sua sede ou onde estejam localizados os dados desde que o tratamento ou coleta dos dados seja realizado no território nacional (BRASIL, 2018). No artigo 5º são definidos os conceitos fundamentais de Dado pessoal, Dado pessoal sensível e Dado anonimizado. O Dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Entende-se por dado indentificável dados que permitam mesmo que indiretamente identificar o titular, como um e-mail que estiver na forma nome.sobrenome@empresa.com ou até mesmo número de cartão de crédito, endereço de IP e *cookies* (DONDA, 2020). Dado pessoal sensível refere-se aos que revelam 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. Esses dados merecem um atenção maio por serem muito pessoais. Já o Dado anonimizado refere-se a qualquer dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, ou seja, qualquer manipulação que possa fazer com que o dado perca a possibilidade direta ou indireta de associação ao titular (BRASIL, 2018).

Ainda no artigo 5º são definidos os papéis ligados ao tratamento de dados: Titular, Agentes de tratamento e Encarregado. O termo Titular relaciona-se à pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Os Agentes de tratamento são: o Controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais e o Operador, pessoa que realiza o tratamento de dados pessoais em nome do controlador. São os Agentes de tratamento os responsáveis por indicar a pessoa para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), definido como Encarregado (BRASIL, 2018).

Tendo como base os conceitos relacionados aos dados e os papéis envolvidos é importante que se tenha conhecimento da definição de Tratamento, o qual a lei descreve como toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

No artigo 6º a lei apresenta os 10 princípios que deverão ser observados no tratamento de dados pessoais:

- Finalidade - o tratamento deve ser realizado para propósitos legítimos informados ao titular, sem possibilidade de ser tratado posteriormente de forma incompatível com a mesma.
- Adequação - os dados devem ser tratados de forma compatível com as finalidades informadas ao titular.
- Necessidade - limitar o tratamento ao mínimo necessário para a realização de suas finalidades.
- Livre acesso - garantia de consulta fácil e gratuita ao titular quanto a forma, duração e integralidade de seus dados pessoais.
- Qualidade dos dados - exatidão, clareza e relevância dos dados de acordo com a necessidade e para cumprir a finalidade.
- Transparência - garantir ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
- Segurança - utilização de medidas 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 difusão;

- Prevenção - adoção de medidas para prevenir a ocorrência de danos.
- Não discriminação - o tratamento não deve ser realizado para fins discriminatórios ilícitos ou abusivos.
- Responsabilização e prestação de contas - demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Na seção I do capítulo II da lei são discriminados os Requisitos para o Tratamento de Dados Pessoais que traz no artigo 7º as hipóteses nas quais estão permitidos o tratamento:

> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

O artigo 7º merece uma atenção especial pois o entendimento do mesmo é de grande importância no auxilio às empresas na conformidade à lei. Donda (2020) destaca as hipóteses I e IX as quais são mais voltadas ao cenário comercial. A primeira é a que permite à empresa o tratamemto dos dados mediante o consentimento do titular, e acredita que será a mais utilizada. Assim, é importante atentar-se ao artigo 5º XII que define o conceito de consentimento: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"(BRASIL, 2018). A segunda fornece a base legal quando se tratar dos interesses legítimos do controlador (empresa) e será útil para alguns cenários de negócio em que a aplicação de mecanismos para o consentimento do titular for muito complexa.

Em seu livro, Donda (2020) cita ainda o que acredita ser a melhor maneira de ficar em conformidade com a LGPD:

- criar um comitê (governança) para análise e tomadas de decisão;
- designar um *Data Protection Officer* (DPO);
- mapear e entender o ciclo de vida dos dados;
- adotar regulamentações e padrões de segurança da informação;
- auditar e monitorar o ambiente;
- criar um relatório de impacto à proteção de dados pessoais;
- criar um plano de ação para situações de emergência.

Em relação às sanções administrativas, entraram em vigor no dia 1º de Agosto de 2021 os artigos 52, 53 e 54 da LGPD, que fazem referência às mesmas. Elas variam desde uma advertência com prazo para adoção de medidas corretivas, multa simples, de até 2% (dois por cento) do faturamento da empresa até mesmo a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. É importante destacar que essas sanções podem ser aplicadas somente pela ANPD, a qual esclarece que são aplicáveis a fatos ocorridos após a data da sua entrada em vigor ou para delitos de natureza continuada iniciados antes de tal data. A ANPD esclarece ainda que as sanções serão aplicadas em situação de descumprimento às obrigações previstar na lei, não somente as relacionadas à vazamento de dados (ANPD, 2021).

2.1.1 ISO/IEC 27701 e privacidade de dados

Diante dos impactos da LGPD nas empresas, a ISO/IEC 27701 passa a ter grande importância no processo de adequação. A norma fornece uma estrutura para auxiliar organizações a estabelecer conformidade em privacidade de dados pessoais com diversas legislações (ANWAR; GILL, 2021). Lançada no Brasil em dezembro de 2019, ela tem como objetivo especificar os requisitos e fornecer as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização. É aplicável à organizações públicas e privadas e relaciona-se com outras normas técnicas que lhe dão suporte para a implementação da conformidade (ABNT, 2019).

Em suma, a norma ISO/IEC 27001 define os requisitos para um SGSI, sendo a principal norma utilizada como base para obtenção de certificação empresarial em Gestão da Segurança da Informação. Por sua vez, a ISO/IEC 27002 estabelece código de melhores práticas com um conjunto completo de controles para apoiar a implantação do SGSI nas organizações. A ISO/IEC 27701 então, atualiza e complementa requisitos da ISO/IEC 27001 assim como controles e diretrizes da ISO 27002 com o foco em dados pessoais.

De acordo com Milagre (2019), a base continua sendo as normas ISO/IEC 27001 e ISO/IEC 27002 e nenhuma diretriz da nova ISO/IEC 27701 pode invalidar os requisitos das normas anteriores. Quanto à estrutura da norma ISO/IEC 27701, destacam-se as seções 5 a 8, bem como os seus anexos.

Na seção 5 tem-se os requisitos específicos de um SGPI e requisitos de segurança da informação da ISO/IEC 27001, apropriados para empresas que atuam como controlares ou processadores. A seção 6 trata das diretrizes específicas de SGPI e o mapeamento através das seções da ISO/IEC 27002. Na seção 7 continua-se tratando de diretrizes (ISO/IEC 27002), porém foram disciplinadas diretrizes adicionais específicas para o SGPI e para controladores de dados pessoais - a partir dessa seção é possível notar uma relação maior entre itens da norma e a LGPD. Assim como na seção 7, a seção 8 também traz diretrizes adicionais à ISO/IEC 27002 dessa vez direcionadas á operadores ou subcontratados (MILAGRE, 2019)

Ao final da norma ISO/IEC 27701 tem-se os anexos, referências importantes, os quais facilitam a implementação das normas e, consequentemente, a conformidade com as leis. O anexo A relaciona-se com o item 7 da norma, trazendo controles e objetivos de controles específicos de privacidade para controladores de dados pessoais. O anexo B, por sua vez tem relação com o item 8, ou seja, destinado aos operadores de dados pessoais. O anexo C mapeia os princípios de privacidade da ISO 29100 com os controles aplicados a controladores de dados pessoais. O anexo D traz a tabela com o mapeamento entre as subseções da ISO/IEC 27701 e os artigos da *General Data Protection Regulation* (GDPR). No anexo E observa-se a relação da ISO/IEC 27701 com as ISOs 27018 *(Cloud)* e 29151 (diretrizes e controles adicionais). O anexo F trata da orientação para aplicação da ISO/IEC 27701 com as normas "base", ISO/IEC 27001 e ISO/IEC 27002.

Por fim, um anexo importante para o *compliance* com a LGPD é o anexo N/A que, assim como o D, faz um mapeamento da estrutura da ISO/IEC 27701 com os artigos da LGPD, o que torna-o um mecanismo facilitador para as empresas no processo de

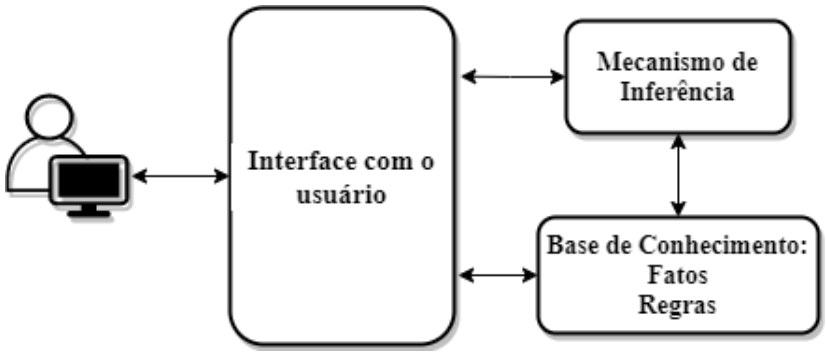
adequação à maior parte das exigências previstas na Lei.

Ainda de acordo com Milagre (2019) recomenda-se que a auditoria ou consultoria continue a análise da conformidade com base nos artigos das leis e, a partir deles, busque na norma os controles previstos para a satisfação das exigências legais.

2.2 Sistemas Especialistas e Apoio à Decisão

Os Sistemas Especialistas (SE) são sistemas computacionais que manipulam conhecimento e informações de forma inteligente. Eles são desenvolvidos para resolver problemas que requerem uma grande quantidade de conhecimento humano e de especialização. Por isso todo SE possui uma Base de Conhecimento (BC) onde é armazenado conhecimento humano sobre uma determinada área na qual o sistema será usado (COSTA; SILVA, 2005).

Figura 2 – Estrutura básica de um Sistema Especialista.



Fonte: Adaptado de Costa e Silva (2021)

A figura 2 mostra a estrutura básica de um SE. A Interface é o meio de interação e comunicação entre os usuários e o SE. O Mecanismo de Inferência é um módulo que faz parte do núcleo do SE, onde são processadas as informações obtidas na coleta de dados para se obter respostas aos usuários. Por sua vez, a Base de Conhecimento é o local onde está armazenado o conhecimento sobre o domínio de atuação do SE, o qual pode ser representado em várias linguagens de representação como: fatos ou regras (COSTA; SILVA, 2005).

De acordo com (ZUCHI et al., 2000), os SE são frutos de mais de vinte anos de pesquisa, e seu uso tem se difundido por vários países, contemplado diversas áreas entre as quais podemos citar interpretação de dados, simulação, diagnóstico,

projeto, planejamento, monitoramento, reparo, instrução e controle. Cada área apresenta particularidades que determinam o grau de dificuldade para construir sistemas aplicáveis a cada uma delas. A característica mais vantajosa de um SE é o alto nível de experiência utilizado na solução de problemas. Para representar o desempenho de especialistas humanos, o SE deve possuir não somente um conjunto de informações mas, também, a habilidade de utilizá-las na resolução de problemas de forma criativa e eficiente. Os autores afirmam ainda que, "em IA e SE, um fato é sempre referenciado como uma proposição, que é uma sentença que assume o valor de verdadeira ou falsa. Um fato muitas vezes pode ser usado como uma propriedade particular a um objeto".

O formalismo de Regras é muito conhecido, sendo um dos mais utilizados em SEs. Em geral, as regras descrevem como se resolvem os problemas. A estrutura lógica conecta um ou mais antecedentes (também chamados premissas) contendo a parte SE (*if*) para uma ou mais consequências (ou conclusões) contendo a parte Então (*then*) (ZUCHI et al., 2000).

Py (2009) define o tema SE como uma subárea da Inteligência Artificial. Desenvolvido a partir da necessidade de se processar informações não numéricas, é capaz de apresentar conclusões sobre um determinado tema desde que devidamente orientado e "alimentado".

O apoio à decisão pode ser visto como a atividade que suporta a obtenção de elementos que tornam as decisões mais claras com o propósito de propiciar aos atores do processo decisório as condições mais favoráveis possíveis para o aumento da coerência entre a evolução do processo e o atendimento dos objetivos de acordo com os valores dos atores (ROY, 1994).

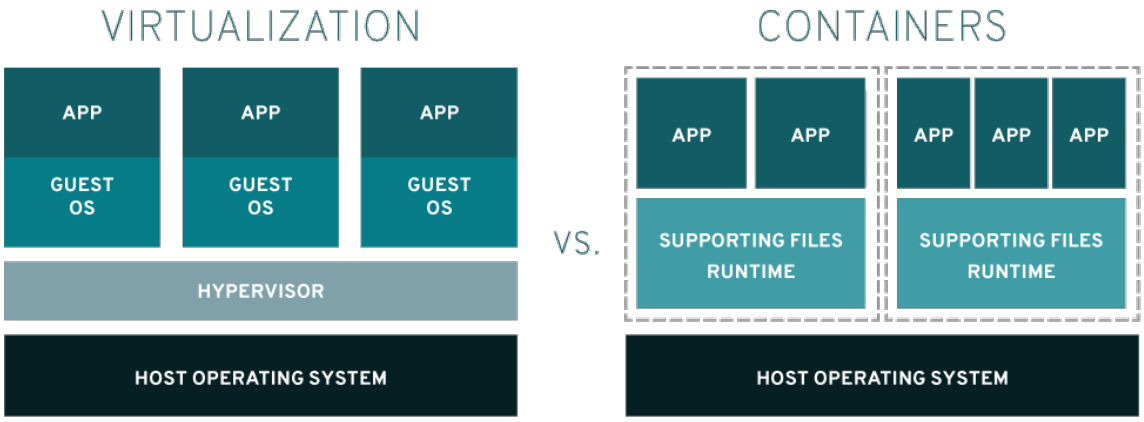
Segundo O'Brien (2001), Sitemas de Apoio a Decisão (SAD) são sistemas de informação que fornecem apoio interativo de informações durante o processo de tomada de decisão. Portanto, são capazes de apoiar diretamente os tipos específicos de decisões e os estilos e necessidades pessoais de tomada de decisão. O uso de um SAD envolve um processo interativo de modelagem analítica.

Sistemas de Apoio à Decisão possuem foco no suporte às decisões através de simulações com a utilização de modelos construídos para dar suporte às decisões gerenciais semi-estruturadas ou não-estruturadas, sobre assuntos dinâmicos, que sofrem constantes mudanças de cenário ou que não podem ser facilmente especificados (BARBOSA; ALMEIDA, 2002)

2.3 Da Virtualização aos *Containers*

Com a evolução da virtualização, onde os sistemas operacionais e suas aplicações compartilham os recursos de *hardware* de um servidor *host*, e levando em consideração o aumento do uso de *webservices* nas últimas décadas, o *container* surge como uma maneira inovadora de abstrair um ou mais processos do restante do sistema, simplificando o processo de desenvolvimento, proporcionando uma produção melhor, mais rápida e mais econômica. A figura 3 ilustra a diferença do funcionamento entre a virtualização e os *containers*.

Figura 3 – Diferença entre a virtualização e os *containers*.



Fonte: Red Hat (2021).

A virtualização é um processo pelo qual o *software* é usado para criar uma camada de abstração acima do *hardware* do computador permitindo que os elementos de *hardware* de um único computador sejam divididos em vários computadores virtuais. Essa pequena camada de software, chamada *hypervisor*, possibilita que vários Sistemas Operacionais (SO) executem compartilhando os mesmos recursos computacionais. O *hypervisor* permite que o computador físico separe seu sistema operacional e aplicações de seu hardware. Assim, ele pode dividir-se em várias "máquinas virtuais" independentes (IBM Cloud, 2021). Carissimi (2008) apresenta duas desvantagens do uso da técnica de implementação de máquina virtual de processo: desempenho e desperdício de capacidades do hardware físico. O desempenho é sacrificado já que há uma tradução de um sistema a outro, além de executarem em modo de usuário. O desperdício de capacidades físicas do hardware vem do fato que as máquinas virtuais de processo oferecem dispositivos de E/S genéricos e simples.

Por outro lado, em vez de rodar em uma máquina virtual inteira, a "conteinerização"empacota tudo o que é necessário para executar uma unica aplicação ou microsserviço. O *container* inclui todo o código, suas dependências e até o próprio sistema operacional. Isso permite que as aplicações sejam executadas em praticamente qualquer lugar - um computador desktop, uma infraestrutura de TI tradicional ou a nuvem (IBM Cloud, 2021).

Os *containers* deixam a carga "mais leve", possibilitando o trabalho em pequenos subconjuntos de código sem impactar o ambiente de execução geral. Eles também fornecem uma forma padrão de empacotar e isolar dependências, configurações e código da aplicação em um objeto (REDHAT, 2020). Em resumo, *containers* são menores, rápidos e portáteis pois, ao contrário de uma máquina virtual, não precisam incluir um SO hospedado em todas as instâncias e podem, em vez disso, simplesmente aproveitar as funcionalidades e recursos do SO hospedeiro. Uma imagem de *container* Docker é um pacote de *software* leve, autônomo e executável que inclui tudo o que é necessário para executar um aplicativo: código, tempo de execução, ferramentas do sistema, bibliotecas do sistema e configurações. As imagens de *container* se tornam *containers* em tempo de execução e, no caso de *containers* Docker, as imagens se tornam *containers* quando são executadas no Docker Engine. Disponível para aplicativos baseados em Linux e Windows, o software em *containers* sempre rodará da mesma forma, independentemente da infraestrutura (DOCKER, 2021).

Com base nesses estudos levantados, o referencial se justifica pelo interesse em se adotar a "conteinerização"com tecnologia Docker já que é uma tendência importante no desenvolvimento de software, principalmente devido à sua portabilidade.

2.4 Revisão Sistemática da Literatura e Trabalhos Correlatos

Esta seção tem como objetivo apresentar a Revisão Sistemática da Literatura (RSL) realizada para busca e seleção dos trabalhos correlatos à esta pesquisa e em seguida serão apresentados os principais aspectos e contribuições de cada trabalho bem como uma comparação em relação à presente proposta.

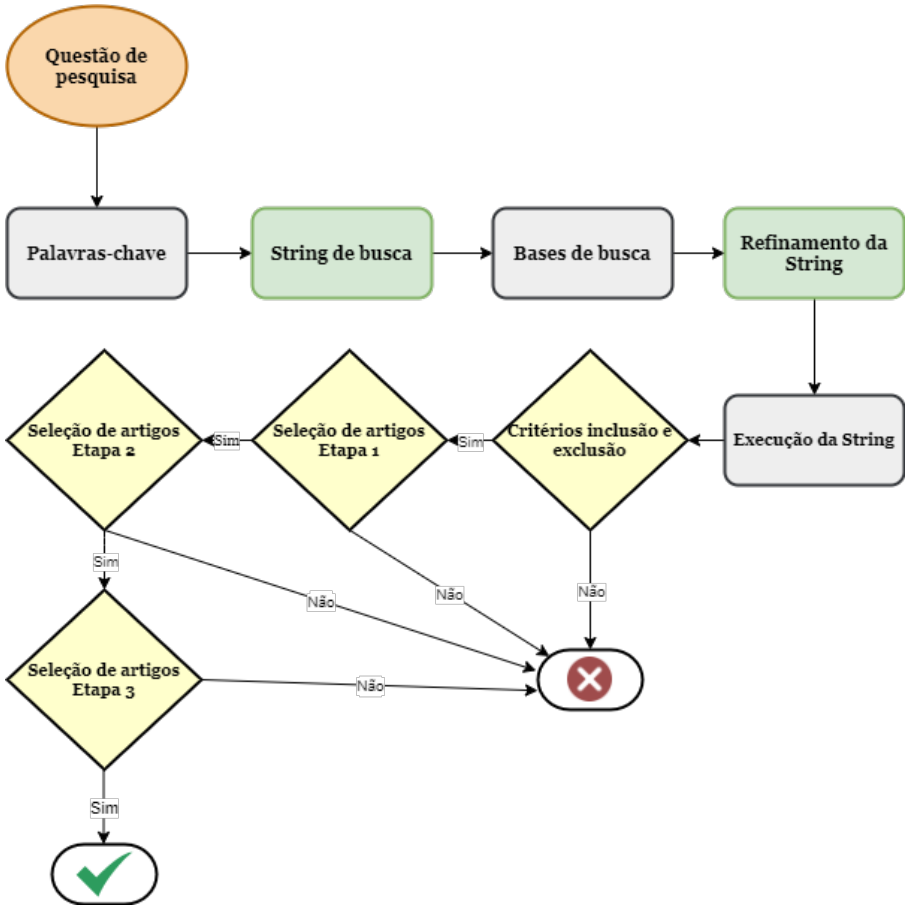
2.4.1 Revisão Sistema da Literatura (RSL)

Segundo Dermeval, Coelho e Bittencourt (2019), o levantamento do estado da arte é atividade obrigatória na realização de qualquer pesquisa científica de qualidade, e explica que, no entanto, até pouco tempo atrás, o levantamento da literatura na pesquisa em computação era realizado de maneira aleatória e não sistemática.

Uma Revisão Sistemática da Literatura (RSL) é um meio de identificar, avaliar e interpretar todas as pesquisas disponíveis relevantes para uma determinada questão de pesquisa, área de tópico, ou fenômeno de interesse. A identificação das pesquisas segue um determinado protocolo, geralmente considerando critérios de inclusão e exclusão. O método pode ser realizado com o intuito de: resumir as evidências existentes sobre um tratamento ou tecnologia; identificar quaisquer lacunas na pesquisa atual, a fim de sugerir áreas para novas investigações; prover um *framework* de maneira a posicionar apropriadamente novas atividades de pesquisa (KEELE et al., 2007).

Na realização das etapas da revisão, foi utilizado como base o guia prático proposto por Neiva e Silva (2016) para auxiliar os alunos dos cursos de Ciência da Computação e áreas afins na condução de uma RSL. O fluxo das etapas seguidas na RSL é apresentado na figura 4.

Figura 4 – Etapas RSL.



Fonte: Autora (2022)

Inicialmente define-se a questão de pesquisa, que delineará o que se espera descobrir com a pesquisa. Desse modo, a pergunta inicial definida foi: "Qual técnica está sendo usada para realização de análise de conformidade com a LGPD nas empresas?". Em seguida são definidas as palavras-chave, as quais primeiramente foram extraídas da questão de pesquisa, e novas palavras foram retiradas de artigos da área de interesse, bem como os sinônimos das que já foram encontradas.

Na etapa de criação da *string* basicamente conecta-se as palavras através do conector OR com seus devidos sinônimos e então finaliza-se a *string* conectando com AND esses grupos de palavras formados anteriormente. A escolha das bases de busca considerou as principais bases eletrônicas na área da computação, assim, foram definidas: IEEE Xplore, ScienceDirect, Springer e ACM Digital Library. Também utilizou-se o mecanismo de pesquisa Google Scholar para identificação de pesquisas focadas em repositórios nacionais. Após a definição da primeira *string* de busca, foram necessários alguns ajustes de modo que se adequasse a algumas bases e também para fim de resultados

mais relevantes. Depois de algumas calibrações, a *string* que mais fez sentido ficou na forma: *(solution OR method OR model OR tool OR framework application OR software) AND (evaluation OR analysis OR mapping OR management OR privacy OR protection OR security) AND (data OR information OR risk) AND (compliance) AND (LGPD OR GDPR OR (General Data Protection Law) OR (General Data Protection))*. Além disso, foi preciso diminuir o tamanho da mesma para a busca na base Science Direct devido à uma restrição de busca desse repositório, nesse caso, a *string* readequada foi: *(model OR framework) AND (mapping OR analysis) AND (data OR information) AND (compliance) AND (LGPD OR GDPR)*. Para a busca no Google Scholar ajustou-se a *string* para: (modelo OR framework) AND (mapeamento OR análise) AND (dados OR informações) AND (compliance OR conformidade) AND (LGPD OR GDPR), com o intuito de se identificar pesquisas em português. Critérios de busca também podem ser refinados de acordo com cada base. Posterior à execução da *string* nas devidas bases de busca, os resultados foram exportados em formato .bib, exceto aqueles que já pelo título percebia-se ser imcompatível com o que se esperava. No primeiro momento foi retornado um total de 1752 resultados nas bases internacionais e 1280 no Google Scholar.

Logo após, além do primeiro critério já mencionado, definiu-se outros critérios de inclusão e exclusão para a próxima etapa de revisão, os quais foram definidos principalmente a partir da questão de pesquisa, bem como restrições de idioma (somente inglês e português), de data - somente após a primeira publicação da GDPR (2016) - exclusão de artigos resumidos e livros. Por fim, foi feita a seleção dos artigos, que se deu em três etapas: primeiro fez-se uma análise por título e *abstract*, na segunda etapa analisou-se a introdução e conclusão dos artigos e a terceira etapa foi de uma análise mais completa dos trabalhos restantes. Foram então selecionados 24 trabalhos para a última etapa e, por fim, dentre esses 10 foram escolhidos como correlatos para o presente trabalho.

A maioria dos artigos encontrados nas bases de busca internacionais são relacionados à GDPR, lei europeia na qual a lei brasileira foi inspirada. Além disso, vale mencionar que a primeira está em vigor há mais tempo. De qualquer forma, os resultados foram importantes já que as duas leis são muito similares, porém, para etapa final de seleção, como critério de inclusão, a preferência foi por artigos relacionados à lei brasileira, sendo um total de seis artigos referentes à LGPD e quatro relacionados à GDPR. A seção 2.4.2 mostra os trabalhos selecionados e suas abordagens.

2.4.2 Trabalhos Correlatos

No trabalho de Matulevičius et al. (2020), é apresentado um modelo de GDPR e seu método de apoio para gerenciar a conformidade com o regulamento em processos de negócios. Os autores ilustram como o método é aplicado para extrair um modelo de conformidade *as-is* que descreve os problemas de não conformidade e oferece soluções para atingir a conformidade do processo. Dessa forma, considerando um cenário base, inicialmente é extraído um modelo AS-IS de conformidade que tem como entrada o modelo de negócio, o qual será avaliado de acordo com o modelo GDPR, em seguida, os dois modelos são comparados para a definição dos problemas de conformidade que servirão para um nova modelagem do processo de negócio.

Celidonio, Neves e Doná (2020) apresentam uma proposta de mapeamento dos requisitos listados na LGPD em uma instituição financeira, a partir de metodologia própria que recomenda as ações necessárias para a adequação dessa empresa à lei. A proposta tem como base a estrutura da ISO/IEC 27701 e para o mapeamento dos requisitos utiliza 325 controles que são classificados entre mandatórios, os quais se referem à privacidade de dados e altamente recomendáveis, que tratam sobre a segurança da informação baseados nas normas ISO/IEC 27001 e ISO/IEC 27702. Para isso, foi utilizado o método de pesquisa-ação e estudo de caso.

A pesquisa de Brodin (2019) usa o *design science* para desenvolver um *framework* para empresas SMB se adaptarem à GDPR. O *framework* foi avaliado empiricamente em três diferentes tipos de organizações, resultando na conformidade com o GDPR de acordo com seus *Data Protection Officers* (DPO). Também foi avaliado de forma teórica com a literatura científica incluindo as implicações identificadas da GDPR. O *framework* desenvolvido é composto pelas fases de análise, que determina inicialmente o estado atual da organização em relação à controle e segurança da informação; *design*, a qual foca na criação e atualização de rotinas, políticas e *templates*; e implementação por toda organização, focando em treinamento, comunicação e ajuste.

O trabalho de Júnior (2020) propõe uma solução para obter a conformidade dos processos de negócios em relação a LGPD com o método LGPD *for Business Process* (LGPD4BP) composto por um questionário de avaliação e um método de modelagem com um catálogo de padrões de modelagem. O método proposto orienta os analistas a avaliar a conformidade dos processos de negócio com a LGPD e guia –os a modelarem processos de acordo com a LGPD. O questionário foi elaborado a partir da análise da

LGPD e possui correspondência direta entre as perguntas e artigos da lei. Por fim, o autor ainda realiza um estudo avaliativo com o intuito de receber um *feedback* sobre a utilidade e facilidade de aplicação do método.

Na pesquisa de Agostinelli et al. (2019) é fornecida uma análise das principais restrições de privacidade na GDPR e proposto um conjunto de padrões de projeto para capturar e integrar tais restrições em modelos de processo de negócio. Utilizando o *Business Process Modeling Notation* (BPMN) como notação de modelagem, o artigo foca nas obrigações do Controlador de dados.

Como a LGPD aplica-se também ao setor público, o trabalho de Rojas (2020) busca efetuar uma avaliação da adoção da lei por parte do Instituto Federal de Santa Catarina (IFSC) para identificar seu estado atual de adequação, e por consequência, identificar pontos que necessitam ser adequados, em especial para o tratamento de dados de alunos nos sistemas do Instituto. O levantamento de dados se deu por meio de entrevista guiada por questionário elaborado por uma empresa de consultoria em gestão de riscos. O processo de avaliação adotou três critérios de avaliação: nível Básico, Intermediário e Pleno, além do nível Não Atendido.

O artigo de Chatzipoulidis, Tsiakis e Kargidis (2019) descreve uma ferramenta de avaliação de preparação para empresas, especialmente SMB, que buscam se tornar compatíveis e certificadas com o GDPR. Resume-se os pontos principais que podem ajudar na conformidade com o GDPR e, ao mesmo tempo, aumentar o desempenho geral dos negócios. Para a avaliação usa-se uma escala de pontos relacionadas ao nível de conformidade com a GDPR.

Menegazzi (2021) propõe um guia definido com foco nas obrigações estabelecidas no artigo 6º da LGPD, que prevê 10 princípios fundamentais. Ele afirma que sem saber o conceito dos princípios, é muito difícil colocar em prática as demais medidas da LGPD. O guia contém etapas que auxiliam os profissionais de TIC no alcance da conformidade com a LGPD, por meio de requisitos de negócio e de solução. Por fim, o autor realiza uma avaliação do guia proposto por meio de questionário, que, em geral, foi considerada satifastória, segundo ele.

Através de um questionário elaborado com base nos artigos da LGPD, e disponibilizado para centenas de fábricas do setor químico brasileiro, Silva et al. (2021) identificaram o grau de maturidade das empresas no que se refere à LGPD e à segurança da informação. A partir das informações obtidas no resultado do questionário, juntamente com a análise bibliográfica, foi desenvolvido e validado um *framework* composto por cinco fases para auxiliar as empresas a identificar o nível de conformidade.

Por último, Ferrão et al. (2021) fazem um diagnóstico das organizações brasileiras em relação à sua adequação para LGPD, com base na percepção de profissionais de Tecnologia da Informação (TI) que trabalham nessas organizações. Para isso, foi feita uma pesquisa com 41 perguntas a fim de diagnosticar diferentes organizações brasileiras, públicas e privadas. Segundo o autor, o resultado do diagnóstico permite que organizações e usuários de dados tenham uma visão geral de como o tratamento de dados pessoais de seus clientes estão sendo tratados e quais pontos de atenção estão em relação ao princípios da LGPD.

Tabela 1 – Trabalhos correlatos - GDPR

Critérios	**Coleta/Mapeamento de Dados**	**Avaliação de Diagnóstico de Conformidade**
Matulevičius et al. (2020)	BPMN/Modelo AS-IS de conformidade	Comparação entre o modelo AS-IS e modelo GDPR
Brodin (2019)	Entrevistas e Workshops	Design Science
Agostinelli et al. (2019)	Não se aplica	BPMN
Chatzipoulidis, Tsiakis e Kargidis (2019)	Não se aplica	Ferramenta de avaliação de preparação

Fonte: Autora (2022)

A tabela 1 apresenta os trabalhos relacionados à GDPR em comparação com o trabalho proposto, enquanto a tabela 2 refere-se aos trabalhos relacionados à LGPD. Conforme é possível observar, no trabalho de Matulevičius et al. (2020) e Agostinelli et al. (2019) usa-se a modelagem BPMN como forma de análise, onde demanda-se que o processo de negócio seja mapeado para esse modelo, o que exige uma avaliação mais complexa e detalhada. Nas pesquisas de Brodin (2019), Celidonio, Neves e Doná (2020) e Menegazzi (2021) também é necessário um contato direto e personalizado com as empresas a fim de se avaliar o estado atual das mesmas em relação a conformidade.

Tabela 2 – Trabalhos correlatos - LGPD

Critérios	**Coleta/Mapeamento de Dados**	**Avaliação de Diagnóstico de Conformidade**
Celidonio, Neves e Doná (2020)	Pesquisa-ação	Mapeamento de requisitos através dos controles das normas 27001, 27002 e 27701
Júnior (2020)	Questionário com questões objetivas	Resultado do questionário, elaborado a partir de referências à LGPD
Rojas (2021)	Questionário com questões abertas	Entrevista/Estudo de Caso
Menegazzi (2021)	Entrevista	Questionário de Análise de Lacunas/ Requisito de negócios
Silva et al. (2021)	Questionário com questões objetivas	Análise bibliográfica e resultado dos questionários
Ferrão et al. (2021)	Questionário com questões objetivas	Análise dos questionários, elaborados a partir das dimensões da LGPD
Trabalho Proposto	Questionário com questões objetivas	Análise quantitativa automatizada

Fonte: Autora (2022)

Agostinelli et al. (2019) e Chatzipoulidis, Tsiakis e Kargidis (2019) não realizam em seus estudos nenhum tipo de estudo de caso com fase inicial de diagnóstico de conformidade, em vez disso, criam um framework com base em modelagem e levantamentos bibliográficos com o intuito de auxiliar empresas à estarem em conformidade.

Nos demais trabalhos que também utilizam questionários como forma de mapeamento de dados e processos, são feitas análises mais generalizadas baseadas somente nas respostas dos questionários, na maioria das vezes mapeando questões ligadas somente aos artigos da lei. No caso de Rojas (2020), o autor avalia de forma qualitativa questões respondidas de forma aberta, atribuindo níveis de conformidade. Ferrão et al. (2021) cita, inclusive, como limitação de seu trabalho o longo questionário de 41 questões, o qual pode ter causado uma certa falta de interesse de alguns profissionais de TI ao respondê-lo, e afirma ainda que por abordar questões de vários segmentos da LGPD

pode ter sido prejudicado em algumas partes já que o conhecimento dos participantes geralmente não é completo, mas restrito a uma àrea específica. Também é importante destacar que apenas Brodin (2019) e Chatzipoulidis, Tsiakis e Kargidis (2019) focam suas pesquisas em empresas do *Small and Medium Business* (SMB).

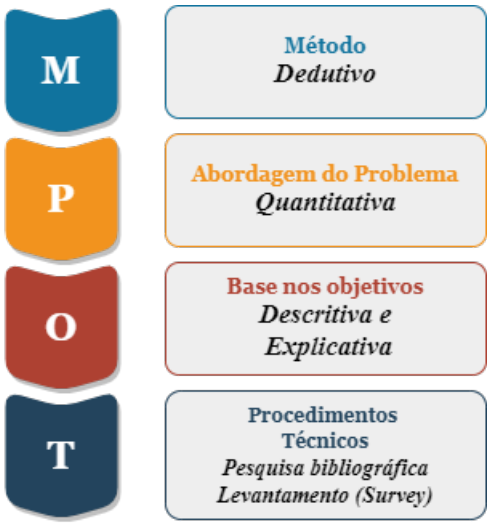
Sendo assim, o presente trabalho tem como principal contribuição uma proposta de análise de conformidade, porém utilizando os dados informados pelo usuário a respeito dos processos de negócio que estão sendo utilizados dentro de uma organização. Também pode ser observada a forma de obtenção das informações de entrada, sendo essas fornecidas por um membro da organização como forma de questionário. Por fim, a análise é feita de forma quantitativa e automatizada com intuito de facilitar o processo de diagnóstico de conformidade nas empresas, que possuem recursos limitados, o qual servirá como base para esse processo.

3 METODOLOGIA

Gil et al. (2002) definem a pesquisa como: "o procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos". Os autores destaca ainda que o desenvolvimento de uma pesquisa baseia-se na utilização cuidadosa de métodos e técnicas, envolvendo inúmeras fases desde a adequada formulação do problema até a satisfatória apresentação dos resultados.

A classificação da pesquisa é importante para que se possa mostrar o direcionamento que o estudo tomará. De acordo com Silveira (2011) há variadas formas de classificação das pesquisas. No entanto, as formas mais clássicas a determinam quanto à natureza, aos objetivos, à abordagem do problema, às fontes de informação e aos procedimentos. A figura 5 ilustra a classificação que melhor representa a presente pesquisa.

Figura 5 – Classificação da pesquisa.



Fonte: Autora (2022)

O método dedutivo “Parte de princípios reconhecidos como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente de sua lógica” (GIL, 2008). O raciocínio dedutivo tem o objetivo de explicar o conteúdo das premissas (PRODANOV, 2013). Assim, pode-se dizer que a LGPD e os dados fornecidos como entrada são as premissas do presente trabalho.

Muitas vezes os métodos qualitativos podem se transformar em quantitativos por meio do emprego de questões fechadas, por exemplo, pelo emprego da Escala Likert (PEREIRA et al., 2018). Como a pesquisa quantitativa lida com fatos, as variáveis devem

ser rigorosamente determinadas e sua mensuração já deve estar pressuposta pelo próprio método (MENEZES et al., 2019), partindo de uma análise quase sempre mediada por algum critério matemático. Portanto, quanto a sua natureza entende-se que a pesquisa pode ser classificada como quantitativa, já que através de uma coleta de dados baseada em uma escala será aplicado um modelo matemático para classificação das informações fornecidas.

Em relação aos objetivos podem-se observar características tanto descritiva quanto explicativa. Uma das características mais significativas da pesquisa descritiva está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática, o que se identifica na presente pesquisa já que será feita inicialmente uma coleta e classificação de informações dos processos da organização. Ainda afirma-se que pesquisas explicativas têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos sendo o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão das coisas, o que também se observa nesse estudo já que os resultados obtidos serão baseados na identificação dos fatores que contribuem para a análise do nível de segurança dos dados (GIL et al., 2002).

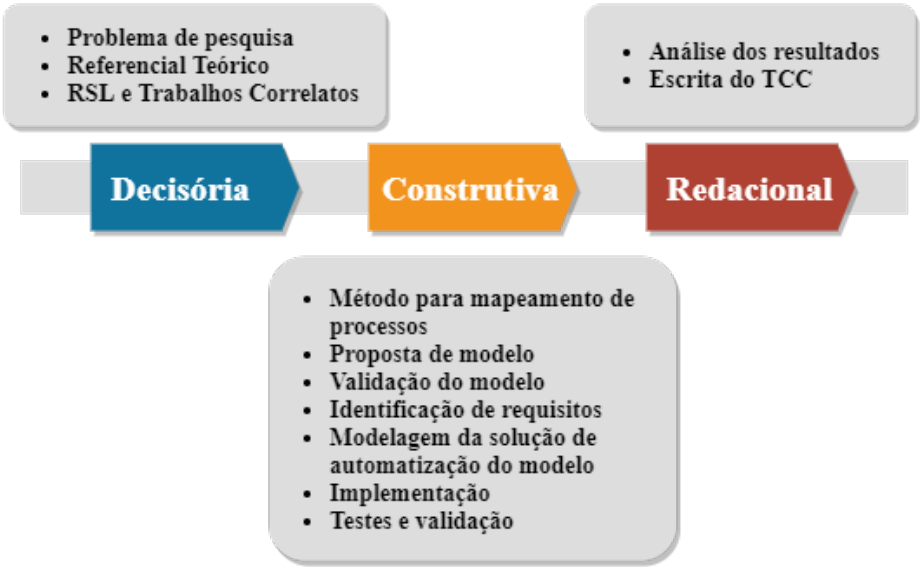
Do ponto de vista dos procedimentos técnicos a pesquisa pode ser considerada bibliográfica, pois será elaborada com base em materiais já publicados, destacando-se a LGPD. E também, como um levantamento, pois a mesma demandará a aplicação de questionários que possibilitarão acesso a dados necessários para a solução do problema de pesquisa (PRODANOV, 2013).

De acordo com Silva e Menezes (2001), o planejamento de uma pesquisa dependerá basicamente de três fases:

- Decisória - referente à escolha do tema, à definição e à delimitação do problema.
- Construtiva - refere-se à construção de um plano de pesquisa e à execução propriamente dita.
- Redacional - em relação à análise dos dados e informações obtidas na fase construtiva.

Para que os objetivos dessa pesquisa sejam alcançados, fez-se necessário a organização do trabalho em uma metodologia que siga as etapas apresentadas na figura 6.

Figura 6 – Etapas da metodologia.



Fonte: Autora (2022)

A fase decisória iniciou-se com a definição e formulação do problema de pesquisa. Nesse passo foi definido o problema que o trabalho se propôs a resolver. A decisão do problema de pesquisa se baseou na recente implantação da Lei Geral de Proteção de Dados (LGPD), visando facilitar a sua compreensão e adaptação para os processos de uma organização. A seguir foi realizado o levantamento do referencial teórico no qual se baseou o presente trabalho, através do estudo do texto da LGPD e bibliografias relacionadas ao desenvolvimento da solução proposta. Ao final dessa fase foi realizada uma Revisão Sistemática da Literatura (RSL), apresentada na Seção 2.4.1, para uma análise dos trabalhos correlatos que se mostram relevantes para a pesquisa.

No princípio da fase construtiva foi definido o método utilizado para o mapeamento de processos e informações e baseado nisso, identificou-se os requisitos que definiriam a criticidade dos dados fornecidos. Posteriormente, foi feita a modelagem e a validação do modelo proposto utilizando um caso base. Encerrando a fase construtiva tem-se a automatização da solução, onde foi desenvolvida a ferramenta de software, seguido pelos testes e validação da mesma.

Na fase final do trabalho, denominada redacional, foi feita a análise dos resultados obtidos nos passos anteriores e a escrita do trabalho de conclusão de curso.

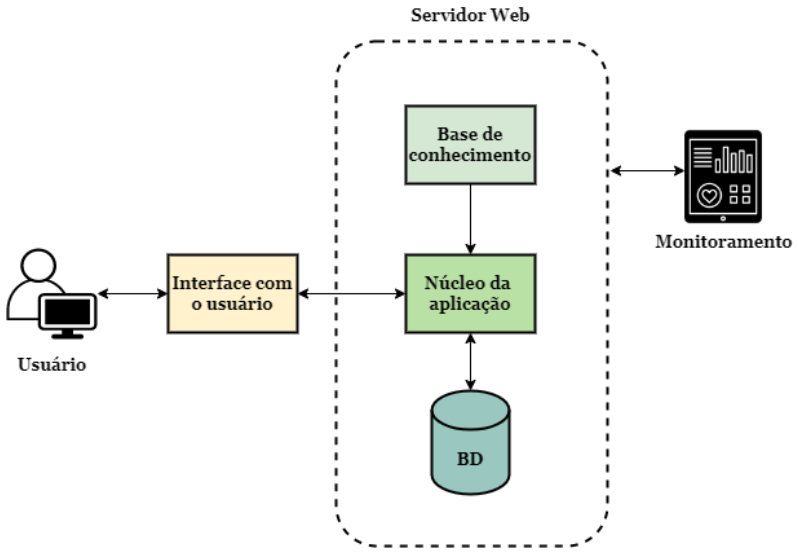
4 PROPOSTA DO MODELO EPIC

Este capítulo tem como objetivo apresentar a solução proposta para o problema de pesquisa. Inicialmente, a seção 4.1 apresenta a proposta do modelo EPIC e sua arquitetura. A seção 4.2 descreve as etapas da elaboração do questionário usado como instrumento de coleta de dados. Na seção 4.3 são explicados os cálculos propostos para a Análise de Conformidade. A seção 4.4 apresenta a modelagem do sistema a ser implementado e, por fim, a seção 4.5 mostra a infraestrutura de desenvolvimento utilizada.

4.1 Visão geral da proposta

Após os estudos e análises das pesquisas já realizadas na área, entendeu-se existir a falta de um método de análise de conformidade com a lei, de forma prática, simples e automatizada, de modo que facilitasse, principalmente, o processo inicial de conformidade nas pequenas e médias empresas, considerando as boas práticas de segurança da informação. Nesse sentido, foi proposta uma solução para auxiliar as empresas a estarem em conformidade com a Lei Geral de Proteção de Dados (LGPD), através de uma abordagem de mapeamento de processos e informações para análise e monitorimento de segurança de dados. Assim, partiu-se para a construção da arquitetura do modelo.

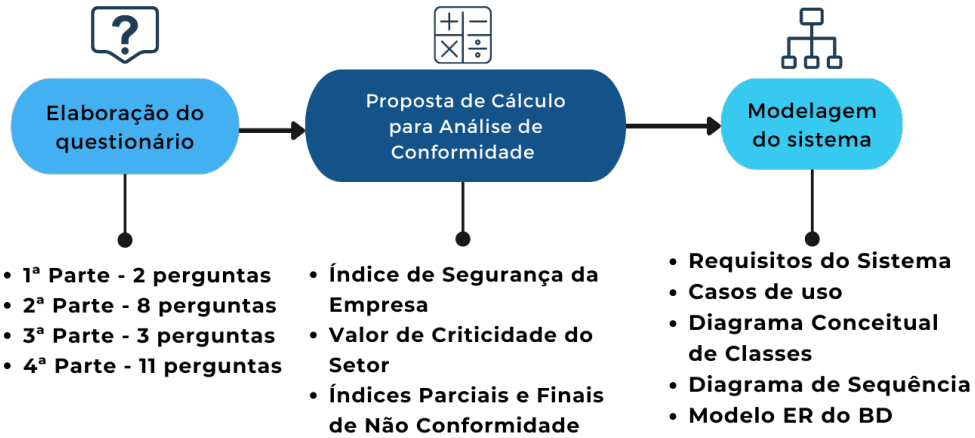
Figura 7 – Arquitetura do modelo.



Fonte: Autora (2022)

Conforme ilustrado na figura 7, a solução proposta é baseada em uma aplicação *web* composta das seguintes partes: interface com o usuário (*frontend*), núcleo da aplicação (*backend*), Banco de Dados (BD) e Base de Conhecimento (BC). A solução foi hospedada em um servidor do Grupo de Segurança da Informação (GSI) da UNIPAMPA, e "containerizada"com tecnologia Docker, sendo configurado um sistema de monitoramento de uso e desempenho da aplicação. A interface com o usuário é responsável pela apresentação das telas com as informações a serem exibidas, pelos métodos de entrada de dados para o usuário e pela comunicação com o *backend*. O núcleo da aplicação recebe os dados do *frontend*, e realiza a comunicação com o BD e o acesso à BC, realizando o processamento das informações recebidas. O Banco de Dados (BD) é utilizado para armazenamento persistente dos dados necessários para execução. Já a Base de Conhecimento (BD) é utilizada pelo núcleo da aplicação para definir a saída do sistema em conjunto com os dados fornecidos pelo usuário. Com base nessa arquitetura partiu-se então para a construção da proposta do modelo. A figura 8 apresenta as etapas desse processo, que são detalhadas nas seções posteriores.

Figura 8 – Etapas da proposta.

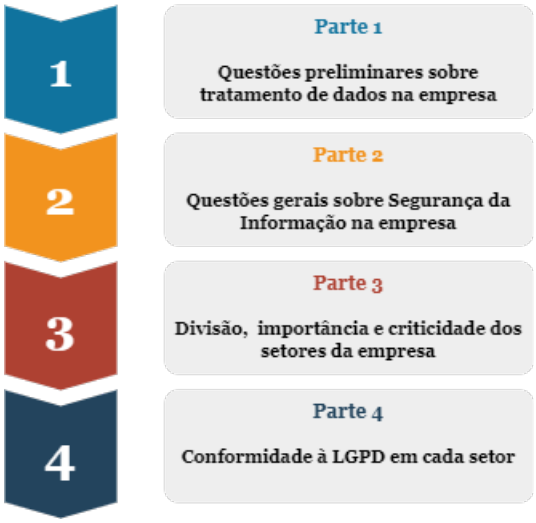


Fonte: Autora (2022)

4.2 Elaboração do Questionário

Como instrumento de coleta de dados para a entrada da solução, elaborou-se um questionário a partir da análise dos principais pontos da LGPD e também do auxílio do anexo N/A da ISO/IEC 27701, que fornece um indicativo de como a aplicação dos controles da norma podem ser relevantes para atender as obrigações da LGPD. O questionário foi dividido em 4 partes e suas questões estão dispostas no Apêndice A deste documento. A Figura 9 mostra a estrutura do questionário elaborado.

Figura 9 – Estrutura do questionário.



Fonte: Autora (2022)

A primeira parte do questionário trata sobre as questões preliminares com o objetivo de compreender a atividade fim da empresa avaliada e a natureza dos dados envolvidos ao longo do desenvolvimento de suas atividades. Nessa etapa são realizadas duas perguntas objetivas ao usuário, visando compreender se a LGPD é aplicável à empresa e seus processos. Essas perguntas foram elaboradas de acordo com o artigo 4º da lei que trata dos fins em que ela não se aplica ao tratamento de dados pessoais.

Para a construção das perguntas da segunda parte foi considerada a importância de requisitos mínimos de segurança da informação, ainda que esteja em conformidade com a lei. Para isso, foram analisados trabalhos já publicados e validados, que elencassem esses pontos. A pesquisa de Silva et al. (2021) foi a que melhor se adequou a esse objetivo, da qual foram retiradas as perguntas utilizadas nessa etapa do presente questionário. Dessa forma são realizadas oito perguntas objetivas para identificar de modo geral o cenário de segurança da informação da empresa e se a mesma possui uma estrutura que forneça meios para prover a segurança dos dados que são utilizados por ela.

Já na terceira parte do questionário é solicitado ao usuário listar os setores da empresa e atribuir graus de importância em relação aos aspectos de negócio e de criticidade da informação. O objetivo dessa etapa é compreender a estrutura organizacional da empresa.

Finalmente, para a quarta etapa foram analisados os principais pontos da LGPD, além da análise de questionários disponíveis na literatura, como o trabalho de Júnior (2020) que propõe um questionário para avaliar aspectos da LGPD nos processos de negócio de uma organização, e a pesquisa de Silva et al. (2021) que visa identificar o nível de maturidade em relação à LGPD em empresas brasileiras do setor químico. Para essa etapa foram feitas comparações entre os questionários em questão, que passaram por adequações, refinamentos, exclusões e acréscimos de acordo com o estudo feito da LGPD. A partir disso, foram elaboradas onze questões sobre as etapas de tratamento de dados nos setores, com questionamentos chave em relação ao que a empresa deve seguir de acordo com as obrigações da lei.

4.3 Proposta de Cálculo para Análise de Conformidade

As métricas apresentadas a seguir são propostas do presente trabalho e os dados são obtidos através da aplicação dos questionários apresentados ao usuário. O respondente deve ser alguém que entenda sobre a estrutura dos setores e a importância dos mesmos, bem como o fluxo de dados da empresa, ou o mesmo pode promover a distribuição da responsabilidade de preenchimento das questões para quem tenha esse conhecimento.

Após a obtenção dos dados das respostas são aplicados os passos de cálculo dos valores de importância dos setores, cálculo dos índices e classificação qualitativa. Ao final é realizada a geração de um relatório.

- Cálculo do Índice de Segurança da Empresa (ISE):
  Após respondidas as questões da etapa inicial do questionário, o próximo passo é a aplicação das questões referentes à Segurança da Informação (SI) da empresa. A partir disso, verifica-se o Número de Respostas Afirmativas (NRA) obtidas dentre o Número Total de Perguntas sobre Segurança (NPS).

O cálculo do Indíce de Segurança da Empresa (ISE) é realizado conforme a equação 1:

$$ISE = \frac{NRA}{NPS} \tag{1}$$

- Cálculo do Valor de Criticidade do Setor (VCS):

  Na terceira etapa do questionário, onde o usuário informa a lista de setores que compõem a empresa, o Grau de Importância para o Negócio (GIN) e o Grau de Criticidade para Informação (GCI) de cada setor (tabelas 3 e 4), são obtidos os dados necessários para o cálculo do Valor de Criticidade do Setor (VCS).

Tabela 3 – Graus de importância dos setores para o negócio.

Grau	**Descrição do grau**
1	Pouco importante para o negócio
2	Importante para o negócio
3	Muito importante para o negócio

Fonte: Autora (2022)

Tabela 4 – Graus de criticidade da informação dos setores.

Grau	**Descrição do grau**
1	Informações de pouca criticidade
2	Informações de criticidade média
3	Informações de muita criticidade

Fonte: Autora (2022)

Dessa forma, foi proposta a equação 2 para o cálculo do VCS.

$$VCS = \frac{GIN}{3} \times \frac{GCI}{3} \tag{2}$$

Os valores GIN e GCI são manipulados dessa maneira com o intuito de se obter um valor normalizado. Os setores mais críticos terão um valor próximo de 1, sendo esse o valor máximo para o VCS. Enquanto os setores menos críticos terão um valor próximo de 0,111..., sendo esse o valor mínimo para o VCS.

- Cálculo dos Índices Parciais de Não Conformidade (IPNC):
  Após a aplicação da quarta etapa do questionário, que contém as questões para cada um dos setores listados na etapa anterior, a equação 3 é proposta a fim de se obter o Índice Parcial de Não Conformidade por setor. O cálculo é feito a partir do Número de Respostas Negativas (NRN) e o Número de Perguntas que se Aplicam ao Setor (NPA). O NPA pode ser definido como o número de perguntas no qual as respostas foram "sim"ou "não".

$$IPNC = \frac{NRN}{NPA} \tag{3}$$

- Cálculo dos Índices Finais de Não Conformidade (IFNC):
  Os Índices Finais de Não Conformidade de cada setor são obtidos aplicando-se os Valores de Criticidade dos Setores (VCS) aos Índices Parciais de Não Conformidade (IPNC) dos setores por meio da equação 4.

$$IFNC = IPNC \times VCS \tag{4}$$

Após a execução dos cálculos apresentados tem-se como resultado um Índice de Segurança da estrutura da Empresa (ISE) e um Índice Final de Não Conformidade (IFNC) para cada um dos setores listados. Ambos são classificados de acordo com a tabela 5 onde, através da escala adotada, o resultado é apresentado ao usuário tanto de forma quantitativa quanto de forma qualitativa no relatório final gerado.

Tabela 5 – Classificação do Índice de Segurança e de Não Conformidade.

Classificação Qualitativa	**Classificação Quantitativa**
Muito Baixo	De 0 até 0,2
Baixo	Acima de 0,2 até 0,4
Moderado	Acima de 0,4 até 0,6
Alto	Acima de 0,6 até 0,8
Muito Alto	Acima de 0,8

Fonte: Autora (2022)

O valor do ISE é diretamente proporcional ao grau de segurança implementado, isto é, quanto mais segurança a empresa implementa maior esse índice.

Os Índices de Não Conformidade dos setores indicam o quanto um setor está em não conformidade com a Lei Geral de Proteção de Dados (LGPD). O valor do IFNC é diretamente proporcional ao grau de não conformidade do setor em relação à legislação, ou seja, um valor mais próximo de 0 significa que o setor não se encontra numa situação muito preocupante ao passo que um valor mais próximo de 1 indica uma situação crítica em relação à conformidade.

As classificações e os níveis quantitativos foram obtidos através de uma análise matemática, levando em consideração os valores máximos e mínimos que cada um dos indicadores pode assumir. Foram realizados testes com um conjunto de dados fictícios fornecidos como entrada para uma implementação de um protótipo do modelo e o mesmo se mostrou capaz de retornar os resultados dentro do esperado.

4.4 Modelagem do Sistema

A implementação da modelagem do sistema foi feita com base na arquitetura apresentada no modelo da seção 4.1. A *Unified Modeling Language* (UML) é uma família de notações gráficas que ajuda na descrição e no projeto de sistemas de *software*. Um dos modos pelo qual se utiliza essa notação é como esboço no desenvolvimento de *software* para transmitir alguns aspectos do sistema (BOOCH, 2006). Assim, optou-se por realizar a modelagem desse sistema utilizando UML.

Inicialmente, por meio da linguagem UML, o primeiro passo realizado foi o levantamento dos requisitos do sistema, que estão apresentados de forma resumida na tabela 6, e de forma mais detalhada no Apêndice B deste documento.

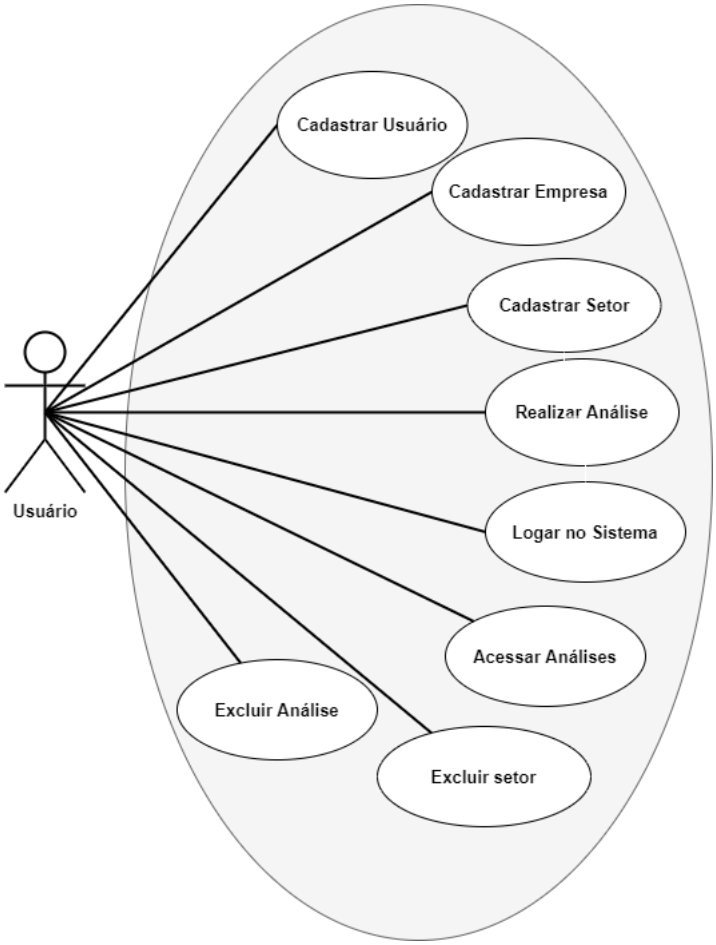
Tabela 6 – Requisitos do Sistema.

Requisitos Funcionais	**Requisitos Não Funcionais**
[RF01] Cadastro de Usuário	[RNF01] Implementação e tecnologias.
[RF02] Cadastro de Empresa	[RNF02] Usabilidade
[RF03] Cadastro de Setor	
[RF04] Análise de segurança e de não conformidade	
[RF05] Exclusão de setor	
[RF06] Exclusão de análise	

Fonte: Autora (2022)

A partir desses requisitos, foi desenvolvido o diagrama de casos de uso da perspectiva do usuário, conforme apresentado na figura 10. Um caso de uso descreve um conjunto de ações que representam a interação de itens externos ao sistema com o próprio (BOOCH, 2006).

Figura 10 – Casos de uso do usuário.



Fonte: Autora (2022)

Cenários:

Caso de Uso - Cadastrar Usuário

Objetivo: Permitir o cadastro de usuários interessados em realizar análise de conformidade.

Fluxo principal:

1. O usuário acessa a página inicial;
2. O usuário clica no botão "Registrar";
3. O usuário insere as informações necessárias;
4. O usuário clica no botão "Entrar";
5. O sistema registra o cadastro;
6. O sistema redireciona o usuário para a página de login.

Fluxo alternativo:

Se o usuário digitar um formato de e-mail inválido ou uma senha de menos de 8 digítos

for inserida, uma mensagem de erro é mostrada.

Caso de Uso - Cadastrar Empresa

Objetivo: Permitir aos usuários o cadastro da empresa.

Fluxo principal:

1. O usuário cadastrado e autenticado no sistema acessa a página de empresas;
2. O usuário clica no botão "Criar empresa";
3. O usuário insere o nome da empresa;
4. O sistema registra o cadastro;
5. O sistema lista a empresa cadastrada na página de empresas.

Fluxo alternativo:

Caso o usuário ainda não possua empresa cadastrada, o sistema exibe um aviso.

Caso de Uso - Cadastrar Setor

Objetivo: Permitir aos usuários o cadastro de setor.

Fluxo principal:

1. O usuário cadastrado e autenticado no sistema acessa a página de empresas e clica no botão "Setores";
2. O usuário clica no botão "Adicionar setor";
3. O usuário insere o nome do setor;
4. O sistema registra o cadastro;
5. O sistema lista o novo setor na página de setores.

Fluxo alternativo:

Caso o usuário ainda não possua setor cadastrado, o sistem exibe um aviso.

Caso de Uso - Realizar Análise

Objetivo: Permitir aos usuários realizarem a análise de segurança da informação de sua empresa e de não conformidade dos seus setores.

Fluxo principal:

1. O usuário cadastrado e autenticado acessa a página de setores e clica no botão "Análises";
2. O usuário clica no botão "Nova Análise";
3. O usuário responde as duas perguntas preliminares sobre tratamento de dado e clica em "Prosseguir";

4. O usuário responde as perguntas de segurança e clica em "Avançar";
5. O usuário responde as perguntas sobre cada setor e clica em "Avançar";
6. O sistema exibe o resultado da análise e registra.

Fluxo alternativo:

Caso uma das duas perguntas iniciais, sobre tratamento de dados, seja "não", o sistema exibe o aviso: "A LGPD não se aplica à empresa, portanto, caso não deseje, não há necessidade de utilização do questionário".

O usuário escolhe clicar em "voltar"ou "prosseguir".

Caso de Uso - Excluir Setor

Objetivo: Permitir aos usuários a exclusão de um ou mais setores.

Fluxo principal:

1. O usuário cadastrado e autenticado acessa a página de empresas e clica em "Setores";
2. O usuário clica no botão de exclusão do setor que deseja excluir;
3. O sistema exclui o setor e não o lista mais na página de setores.

Fluxo alternativo: Não há.

Caso de Uso - Excluir Análise

Objetivo: Permitir aos usuários excluirem uma ou mais análises.

Fluxo principal:

1. O usuário autenticado, e com ao menos uma análise realizada, acessa a página de empresas e clica em "Análises";
2. O usuário clica no botão de exclusão da análise que deseja excluir;
3. O sistema exclui a análise e não a lista mais na página de análises.

Fluxo alternativo: Não há.

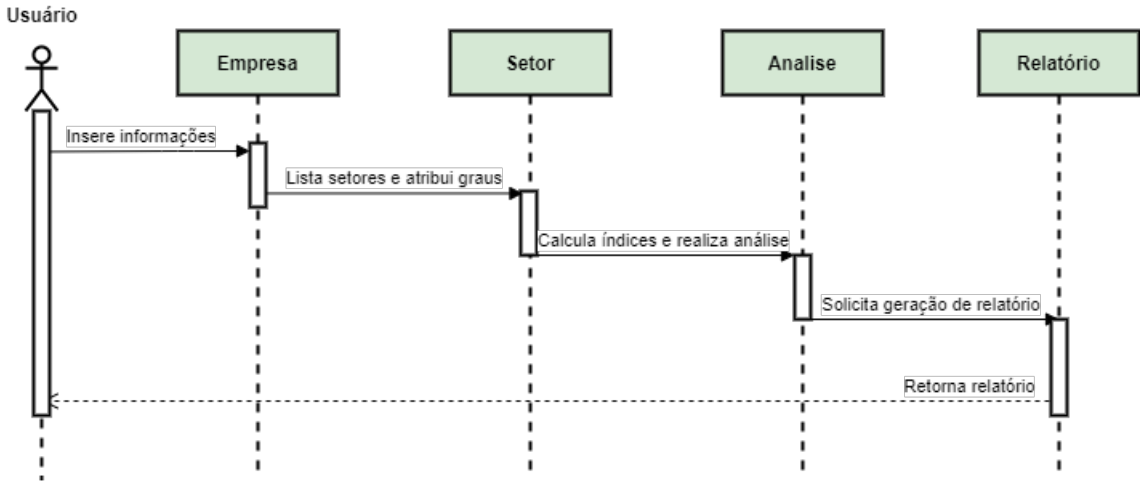
A partir do entendimento dos elementos necessários para o sistema, foi implementado, também, um Diagrama de Classes Conceitual como uma forma abstrata de se observar as classes e objetos, independente da linguagem de programação (BOOCH, 2006). Dessa forma, o diagrama (figura 11) foi desenvolvido a partir do levantamento das classes do sistema, e a inclusão das operações e outros atributos não foi considerada na totalidade.

Figura 11 – Diagrama conceitual de classes.

Fonte: Autora (2022)

Ainda de acordo com Booch (2006), um diagrama de sequência dá ênfase à ordem com que as atividades ocorrem no tempo, mostrando um conjunto de papéis e as mensagens enviadas e recebidas pelas instâncias que representam os papéis. Assim, a Figura 12 apresenta o diagrama de sequência de quando o usuário gera o relatório.

Figura 12 – Diagrama de sequência para gerar relatório.

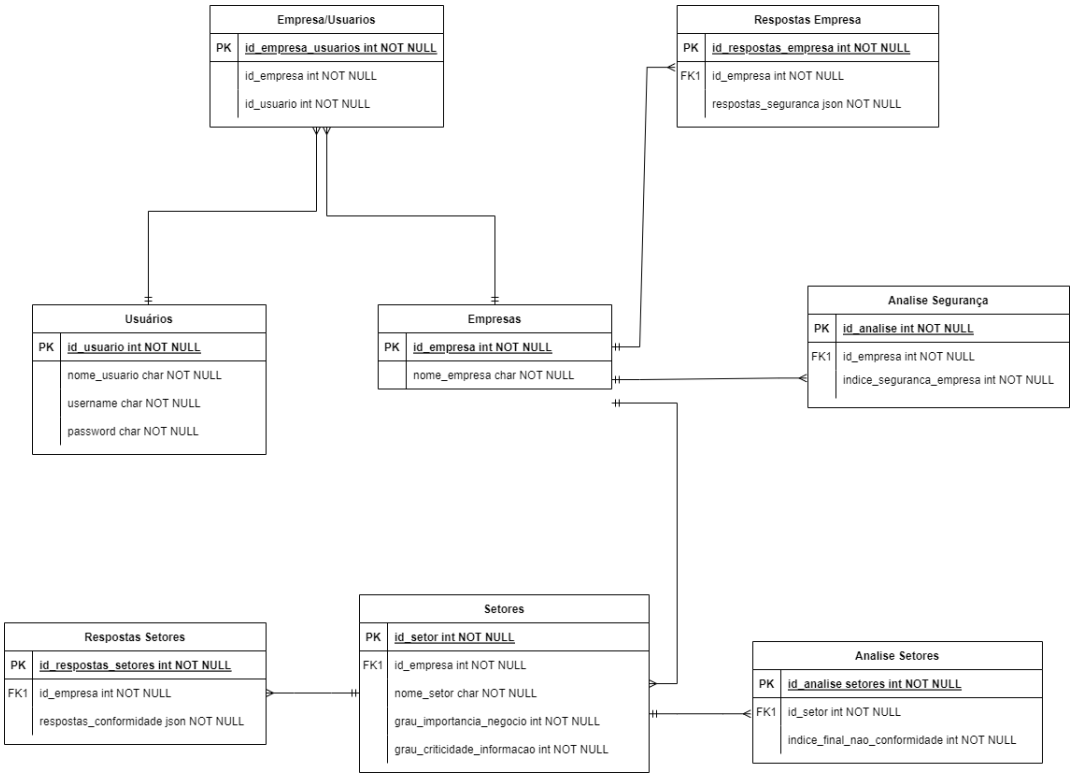


Fonte: Autora (2022)

Inicialmente o usuário deve inserir as informações da empresa e de sua estrutura de segurança, após, deve listar os setores que compõem a empresa e atribuir os graus de importância e de criticidade para cada setor. A partir desses dados informados os índices são calculados, é realizada a análise de conformidade e, por fim, gerado um relatório.

Para representar o Banco de Dados criou-se um Modelo Entidade Relacionamento (ER). O Modelo ER consiste em uma abordagem gráfica para criar a estrutura de um banco de dados. Ele é baseado em uma percepção de um mundo real que descreve os dados principalmente como entidades, relacionamentos e atributos. O objeto básico que o modelo ER representa é uma entidade, algo do mundo real, com uma existência independente. Uma entidade pode ser um objeto com uma existência física (por exemplo, os usuários representados na figura 13) ou um objeto com uma existência conceitual (as empresas, setores). Cada entidade possui atributos - propriedades particulares que a descrevem. Na figura os atributos da entidade empresas, por exemplo, são o id (número de identificação) do usuário e nome da empresa (ELMASRI et al., 2005). O relacionamento define um conjunto de associoações entre as entidades. No modelo criado as empresas podem possuir um ou mais setores.Também pode ser visto no modelo que a empresa e seus setores podem ter um ou mais conjuntos de respostas e análises de segurança.

Figura 13 – Modelo de Entidade Relacionamento.



Fonte: Autora (2022)

4.5 Tecnologias e Plataforma de Desenvolvimento

A solução implementada é um *website* sendo, portanto, uma aplicação que utiliza uma arquitetura no modelo cliente-servidor. A partir da arquitetura e da modelagem estudou-se um conjunto de ferramentas que poderiam ser utilizadas como plataforma de desenvolvimento. Para o desenvolvimento utilizou-se o editor de código fonte Visual Studio Code[1]. Para validação do modelo no Projeto Piloto, descrito na seção 5.1, foi utilizado o *software* Node.js[2] para execução de códigos Javascript. Para o *backend* optou-se pela linguagem de programação PHP, para isso foi usado o *framework* Laravel[3], por oferecer uma plataforma gratuita e segura para desenvolver aplicações *web*, além de ser amplamente utilizado e possuir uma documentação completa. O banco de dados utilizado é o MySQL. Por sua vez o *frontend* foi desenvolvido utilizando as tecnologias HTML e CSS e a linguagem de programação JavaScript com o *framework* Next.js[4].

Figura 14 – Tecnologias Utilizadas.

Fonte: Autora (2022)

A figura 14 ilustra as tecnologias escolhidas dentre as pesquisadas. A decisão

[1] https://code.visualstudio.com/
[2] https://nodejs.org/en/about/
[3] https://laravel.com/
[4] https://nextjs.org/

pela utilização das tecnologias citadas deu-se devido à ampla documentação existente na Internet e também ao extenso número de *frameworks* disponíveis. As partes da aplicação foram encapsuladas em *containers* utilizando a tecnologia Docker (DOCKER, 2021). Conforme o objetivo geral da presente pesquisa, a solução foi desenvolvida utilizando a abordagem colaborativa *open source*[5], desse modo o *software* está compartilhado em repositório de código fonte público para que outros desenvolvedores possam utilizá-lo como base, bem como propor melhorias, contribuindo assim para a evolução e qualidade do mesmo.

[5]https://opensource.org/about

5 IMPLEMENTAÇÃO DO EPIC

Este capítulo apresenta as etapas e resultados referentes ao desenvolvimento da aplicação. A seção 5.1 aborda sobre o projeto piloto da ferramenta; na seção 5.2 é mostrado o desenvolvimento da aplicação *web*; a seção 5.3 apresenta os resultados da ferramenta e, por fim, na seção 5.4 são apresentados os testes funcionais realizados.

5.1 Projeto Piloto

Com a finalidade de testar o modelo e verificar a viabilidade de implementação do mesmo foram desenvolvidos algoritmos que realizam os cálculos apresentados na seção 4.3. Nessa etapa foi utilizado o editor de código-fonte Visual Studio Code para a criação de um conjunto de métodos na linguagem JavaScript. Para a execução desses métodos utilizou-se o software Node.js pela familiaridade e facilidade de uso.

Inicialmente foram definidos conjuntos de dados fictícios estruturados, conforme pode ser observado na figura 15. Esses dados foram criados com a intenção de representar as respostas retornadas pelo usuário como produto da aplicação do questionário.

Figura 15 – Dados para validação do modelo.

input1.js

```
/**
 * 0 = não
 * 1 = sim
 * 2 = não se aplica
 */
export default {
  respostasEstruturaSeguranca: [0, 1, 1, 0, 1, 1, 1, 1],
  setores: [
    {
      nome: "administrativo",
      grauNegocio: 2,
      grauCriticidadeInfo: 2,
      respostasTratamentoDados: [0, 1, 0, 1, 2, 1, 1, 1, 1, 0, 1],
    },
    {
      nome: "financeiro",
      grauNegocio: 3,
      grauCriticidadeInfo: 3,
      respostasTratamentoDados: [0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1],
    },
    {
      nome: "tecnologia",
      grauNegocio: 2,
      grauCriticidadeInfo: 3,
      respostasTratamentoDados: [1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1],
    },
  ],
};
```

Fonte: Autora (2022)

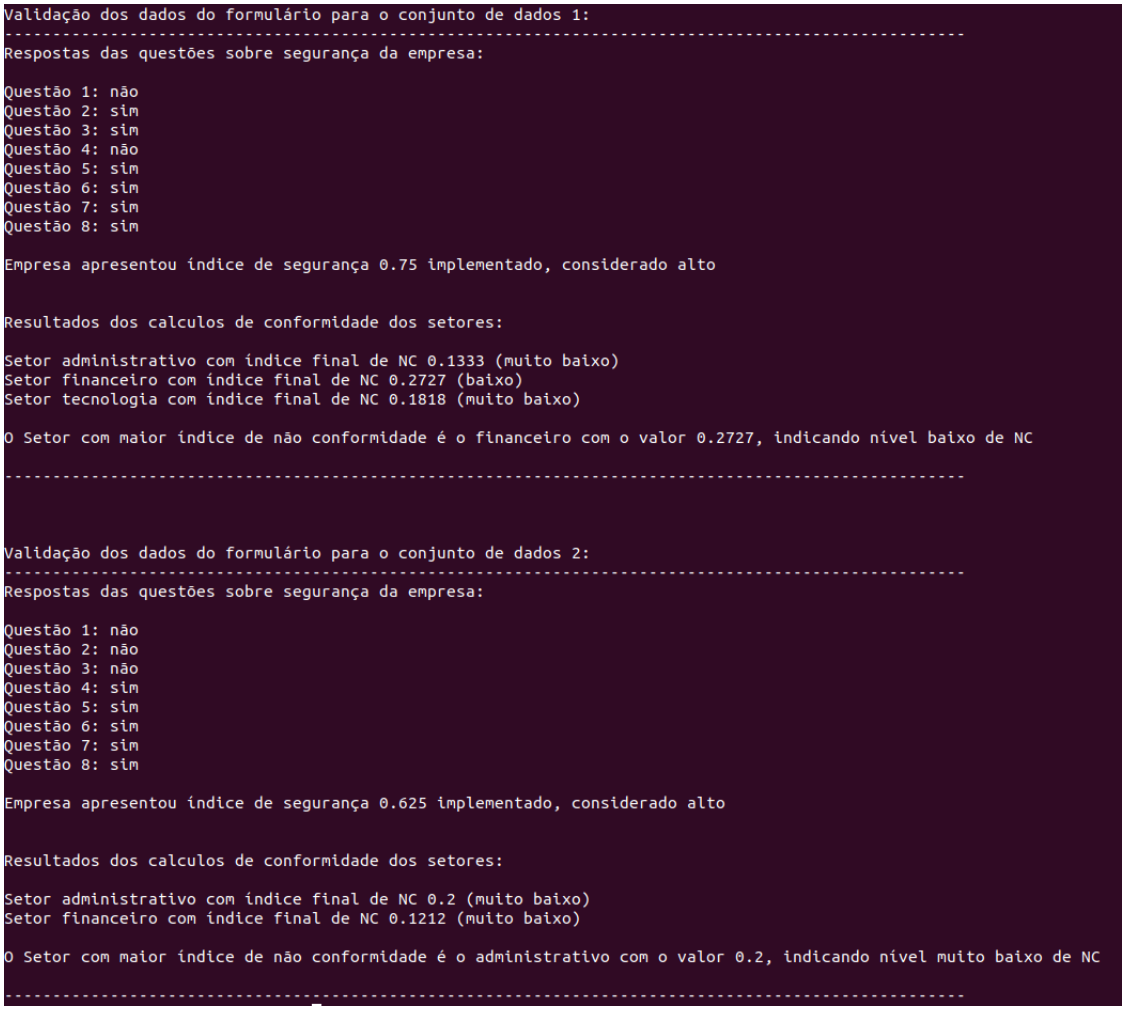
A estrutura apresentada foi importada e fornecida como entrada para o método ‘validadorModelo’. Esse método é responsável pelo desmembramento dos dados recebidos e pela invocação de outros métodos responsáveis por implementar as equações do modelo. Após o retorno dos resultados pelos métodos invocados a informação é apresentada na tela de maneira simplificada. As regras de negócio especificadas no código foram utilizadas como base para o desenvolvimento da versão inicial da solução.

5.1.1 Resultados do Projeto Piloto

A partir do Projeto Piloto executou-se um experimento com dados fictícios. Foram considerados dois conjuntos de dados fictícios e os resultados obtidos nessa etapa são conforme descrito a seguir. O primeiro caso mostra um índice de segurança de 0,75, o que segundo o modelo é considerado alto. Em relação aos resultados nos setores, foram listados os setores administrativo, financeiro e de tecnologia, sendo o maior Índice de Não Conformidade (INC) o do setor financeiro, com 0,2727, indicando nível baixo de NC. Já no segundo caso, o Índice de Segurança gerado foi de 0,625, considerado alto. Porém em relação aos setores (administrativo e financeiro), o setor administrativo resultou no maior índice de NC, 0,2, considerado muito baixo, conforme pode ser observado na figura 16.

Com o presente trabalho visava-se disponibilizar uma abordagem simples e que ao mesmo tempo não tivesse apenas perguntas gerais para a organização, considerando a sua estrutura organizacional, não servindo somente para uma pesquisa estatística, mas sim, possibilitando um diagnóstico imediato com o intuito de reduzir os esforços das empresas SMB.

Figura 16 – Resultados da execução dos testes.



Fonte: Autora (2022)

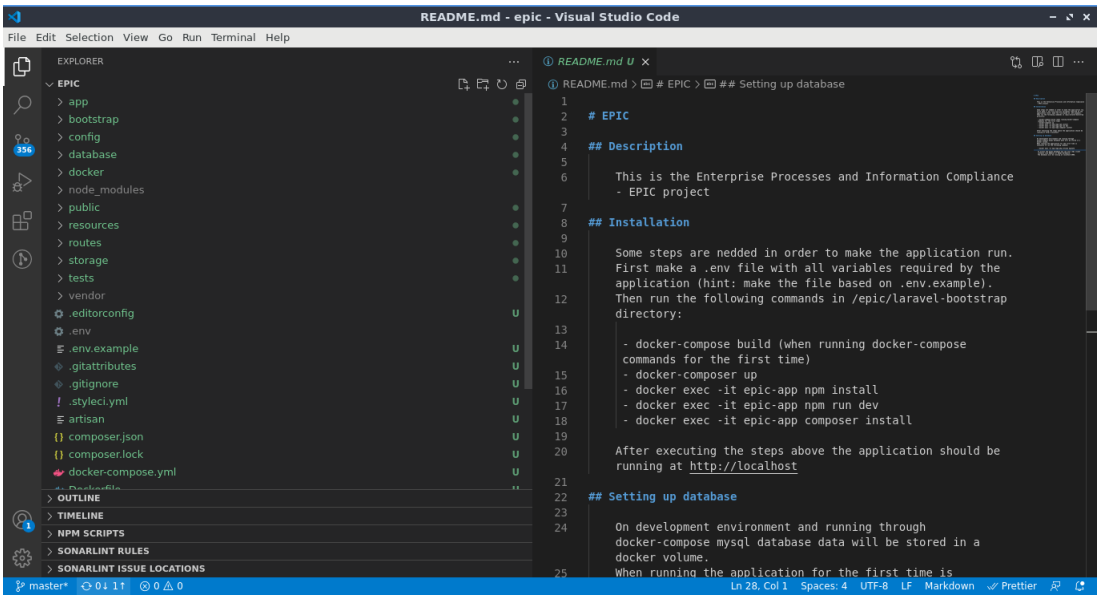
As equações do índice de segurança da empresa e do índice final de não conformidade do setor foram analisadas a fim de concluir qual faixa de valor os resultados deveriam se encontrar. Foi verificado que para o índice de segurança da estrutura da empresa os valores deveriam estar entre 0 e 1. Um ISE igual a 0 é o valor mínimo da equação desse índice, obtido quando a estrutura de segurança da empresa não implementa nenhum dos itens apresentados no questionário. Já o ISE igual a 1 é o valor máximo da equação desse índice, obtido quando todos os itens apresentados no questionário são implementados pela empresa. De maneira similar, para o índice final de não conformidade do setor os valores deveriam estar entre 0 e 1. Um IFNC com valor 0 indica que o setor realiza todas as etapas de tratamento de dados de acordo com a LGPD nos itens questionados, independente do VCS obtido a partir dos dados informados. Já um IFNC com valor 1 indica que o setor é crítico (VCS igual a 1) e que ele realiza todas as etapas de tratamento de dados questionadas em não conformidade com a LGPD.

Conforme os resultados dos métodos implementados, apresentados na seção 5.1, foi observado que os valores obtidos como saída se encontram dentro da faixa esperada e que é possível realizar com sucesso uma implementação do modelo.

5.2 Desenvolvimento do EPIC

Nas etapas iniciais de desenvolvimento foi feita a criação do projeto do Laravel para o *backend* da aplicação seguindo a documentação do *framework*. Foi criado também um *template* básico de *frontend* de maneira a facilitar o desenvolvimento conjunto das duas *stacks*. A estrutura de pastas e arquivos que compõem a aplicação podem ser observados na figura 17.

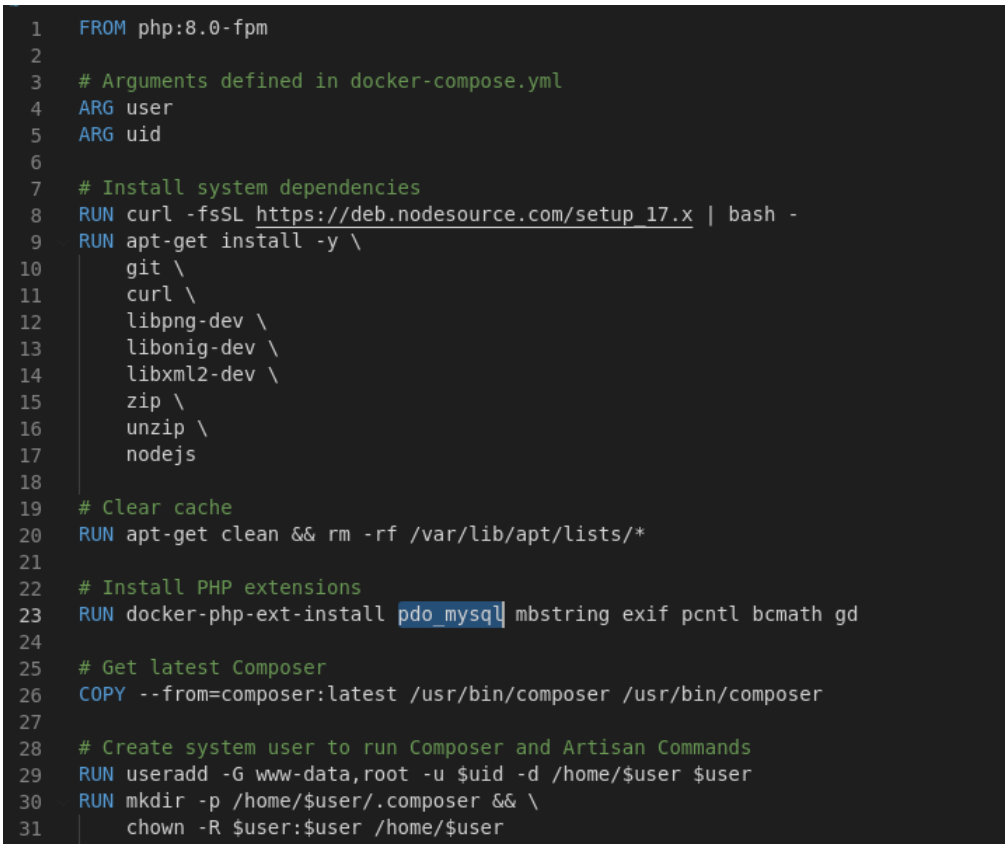
Figura 17 – Estrutura de arquivos do projeto EPIC.



Fonte: Autora (2022)

Como próximo passo de desenvolvimento decidiu-se realizar a etapa de "containerização"das aplicações. Essa etapa foi feita na sequência de forma a facilitar a execução das aplicações ao longo do desenvolvimento em conjunto com um banco de dados também "containerizado", sendo necessário apenas invocar o comando para inicialização dos *containers* no ambiente local, possibilitando a realização de testes. Para realizar a "containerização"é necessário definir alguns arquivos na raiz do projeto. Os arquivos definidos foram o dockerfile e o docker-compose.yaml, conforme recomendado na documentação do Docker.

Figura 18 – Dockerfile da aplicação EPIC.

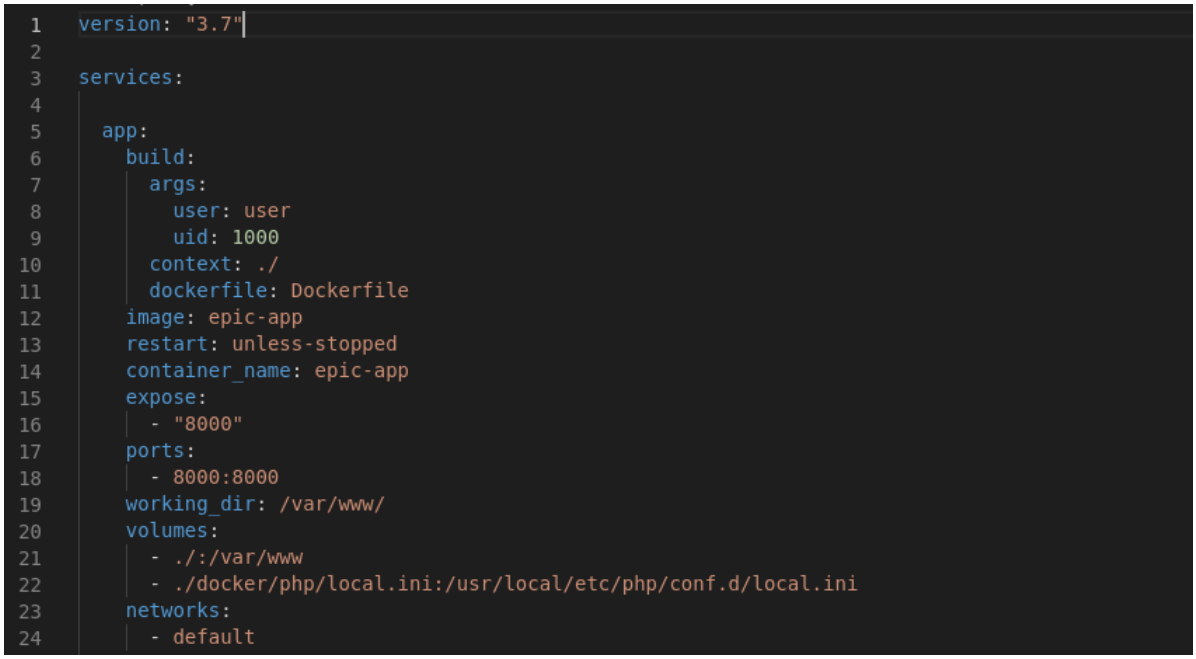


```
FROM php:8.0-fpm

# Arguments defined in docker-compose.yml
ARG user
ARG uid

# Install system dependencies
RUN curl -fsSL https://deb.nodesource.com/setup_17.x | bash -
RUN apt-get install -y \
    git \
    curl \
    libpng-dev \
    libonig-dev \
    libxml2-dev \
    zip \
    unzip \
    nodejs

# Clear cache
RUN apt-get clean && rm -rf /var/lib/apt/lists/*

# Install PHP extensions
RUN docker-php-ext-install pdo_mysql mbstring exif pcntl bcmath gd

# Get latest Composer
COPY --from=composer:latest /usr/bin/composer /usr/bin/composer

# Create system user to run Composer and Artisan Commands
RUN useradd -G www-data,root -u $uid -d /home/$user $user
RUN mkdir -p /home/$user/.composer && \
    chown -R $user:$user /home/$user
```

Fonte: Autora (2022)

O arquivo Dockerfile contém uma lista de comandos necessários para preparar a imagem de um *container* para a execução da aplicação instalando todas as dependências, conforme pode ser observado na figura 18. Já o arquivo docker-compose.yaml, apresentado na figura 19, é um arquivo que define um conjunto de serviços a serem executados em *multi-containers*, nesse caso o *backend*, o *frontend*, o banco de dados e o servidor *web*.

Figura 19 – Arquivo docker-compose.yaml.



```yaml
version: "3.7"

services:

  app:
    build:
      args:
        user: user
        uid: 1000
      context: ./
      dockerfile: Dockerfile
    image: epic-app
    restart: unless-stopped
    container_name: epic-app
    expose:
      - "8000"
    ports:
      - 8000:8000
    working_dir: /var/www/
    volumes:
      - ./:/var/www
      - ./docker/php/local.ini:/usr/local/etc/php/conf.d/local.ini
    networks:
      - default
```

Fonte: Autora (2022)

Para a definição do banco de dados primeiramente tomou-se como base o diagrama ER apresentado anteriormente. Cada entidade representada no diagrama é implementada na forma de classes denominadas *models*, seguindo o padrão do *framework* Laravel. Nessa classe são definidos os atributos que irão compor a respectiva tabela e que irão facilitar a criação, edição e acesso aos dados, e também os relacionamentos entre as tabelas, conforme pode ser visto na figura 20.

Figura 20 – Classe *model.*

```php
<?php

namespace App\Models;

use Illuminate\Database\Eloquent\Factories\HasFactory;
use Illuminate\Database\Eloquent\Model;

class EnterpriseAnswer extends Model
{
    use HasFactory;

    /**
     * The attributes that are mass assignable.
     *
     * @var string[]
     */
    protected $fillable = [
        'analysis_id',
        'enterprise_id',
        'answers',
    ];

    /**
     * The analysis that this enterprise answer belongs to
     */
    public function analysis()
    {
        return $this->belongsTo('App\Models\Analysis');
    }

    /**
     * The enterprise that this enterprise answer belongs to
     */
    public function enterprise()
    {
        return $this->belongsTo('App\Models\Enterprise');
    }
}
```

Fonte: Autora (2022)

Para a criação das tabelas em si é necessária a implementação de *migrations*. As *migrations* são classes que modificam a estrutura do banco de dados, realizando a criação de tabelas ou colunas, como pode ser observado na figura 21. Com a definição dos *models* e das *migrations* o *framework* fornece diversos métodos que facilitam o acesso aos dados e também de suas respectivas relações.

Após a etapa descrita anteriormente foram criados os métodos que realizam as operações de criação, edição e exclusão das entradas das tabelas do banco de dados. Esses métodos foram definidos em classes chamadas *controllers* e são responsáveis por receber os parâmetros informados nas requisições HTTP realizadas nas rotas citadas acima e executar toda a lógica para qual a rota foi definida.

Figura 21 – Classe *migration.*

```php
class AddColumnsToSectorsTable extends Migration
{
    /**
     * Run the migrations.
     *
     * @return void
     */
    public function up()
    {
        Schema::table('sectors', function (Blueprint $table) {
            $table->unsignedBigInteger('enterprise_id')->after('id');
            $table->foreign('enterprise_id')->references('id')->on('enterprises');
            $table->string('name')->after('enterprise_id');
        });
    }

    /**
     * Reverse the migrations.
     *
     * @return void
     */
    public function down()
    {
        Schema::table('sectors', function (Blueprint $table) {
            $table->dropForeign(['enterprise_id']);
            $table->dropColumn('enterprise_id');
            $table->dropColumn('name');
        });
    }
}

```

Fonte: Autora (2022)

Pode ser citada como exemplo a rota de criação de empresas que irá receber os parâmetros necessários e invocará o método do *controller*, efetivando a criação de uma entrada no banco de dados com os dados da empresa e a relação entre o usuário logado e esta empresa, conforme a figura 22.

Figura 22 – Classe *controller.*

```php
public function create(CreateEnterpriseRequest $request)
{
    $alreadyExists = User::find(Auth::id())->enterprises()->where('name', $request->name)->first();

    if ($alreadyExists) {
        throw new HttpException(409, 'An enterprise with this name already exists');
    }

    $enterpriseAttributes = array('name' => $request->name);
    $enterprise = Enterprise::create($enterpriseAttributes);

    $enterpriseUserAttributes = array('user_id' => Auth::id(), 'enterprise_id' => $enterprise->id);
    EnterpriseUser::create($enterpriseUserAttributes);

    return response('Enterprise created successfully', 201);
}
```

Fonte: Autora (2022)

Após as informações necessárias serem persistidas no banco de dados é feito o uso da rota que realiza os cálculos e retorna o resultado de uma análise de conformidade.

Essa rota recebe o número de identificação de uma análise e retorna uma estrutura com os dados da empresa, seus setores, as respostas e os índices relacionados à empresa e a cada um dos setores, provendo esses dados para serem exibidos no *frontend*, bem como para a geração de um relatório que pode ser exportado. O código fonte do método de cálculo de resultado pode ser observado na figura 23.

Figura 23 – Método de cálculo do resultado.

```
63      public function result(string $analysisId)
64      {
65          $analysis = Analysis::find($analysisId);
66
67          if (!$analysis) {
68              throw new HttpException(404, "Analysis not found");
69          }
70
71          $enterprise = User::find(Auth::id())->enterprises()->where('enterprise_id', $analysis->enterprise_id)->first();
72
73          if (!$enterprise) {
74              throw new HttpException(404, 'Enterprise not found');
75          }
76
77          $enterpriseAnswers = json_decode(EnterpriseAnswer::where('analysis_id', $analysisId)->first()->answers);
78
79          $enterpriseSecurityIndex = $this->calculateEnterpriseSecurity($enterpriseAnswers->answers);
80
81          $sectorAnswers = $analysis->sectorsAnswers->map(function ($sectorAnswer) {
82              $answers = json_decode($sectorAnswer->answers);
83              return ['name' => $sectorAnswer->sector->name, 'gin' => $sectorAnswer->gin, 'gci' => $sectorAnswer->gci, 'answers' => $answers->answers];
84          })->toArray();
85          $sectorsConformityIndex = $this->calculateSectorsConformity($sectorAnswers);
86
87          return response([
88              'enterprise' => ['name' => $enterprise->name, 'index' => $enterpriseSecurityIndex, 'answers' => $enterpriseAnswers->answers, 'id' => $enterprise->id],
89              'sectors' => $sectorsConformityIndex,
90              'created_at' => $analysis->created_at
91          ], 200);
92      }
93
```

Fonte: Autora (2022)

Na etapa de implementação do *backend* inicialmente foram analisadas quais rotas deveriam ser disponibilizadas para o *frontend*. Foram implementadas rotas de *login* e registro do usuário, criação e edição de empresas, criação e exclusão de setores, criação e exclusão de análises, criação de respostas de setores e de empresas e por fim a rota para obtenção do resultado de uma análise.

Em relação às funcionalidades implementadas, inicialmente tem-se a página de *login* onde o usuário deverá informar o seu usuário e senha, conforme pode ser observado na figura 26. Caso o usuário ainda não possua cadastro, ele poderá realizá-lo através da página de cadastro de usuário, como pode ser observado na figura 25. Para o cadastro de um novo usuário são solicitados o nome, e-mail e senha. Após logado o usuário será direcionado para uma página que irá listar as empresas já cadastras, e caso não haja ele deverá fazer o cadastro informando o nome da respectiva empresa e em seguida informar também os setores que fazem parte da mesma. Apartir disso o *backend* cria a análise e o usuário passará então a responder primeiramente as perguntas referentes a segurança da empresa e logo após as perguntas para cada setor.

O *frontend* foi implementado utilizando Next.js, um *framework* que fornece blocos de construção para criar aplicativos da *web*. Dessa forma, foram criadas as seguintes telas:

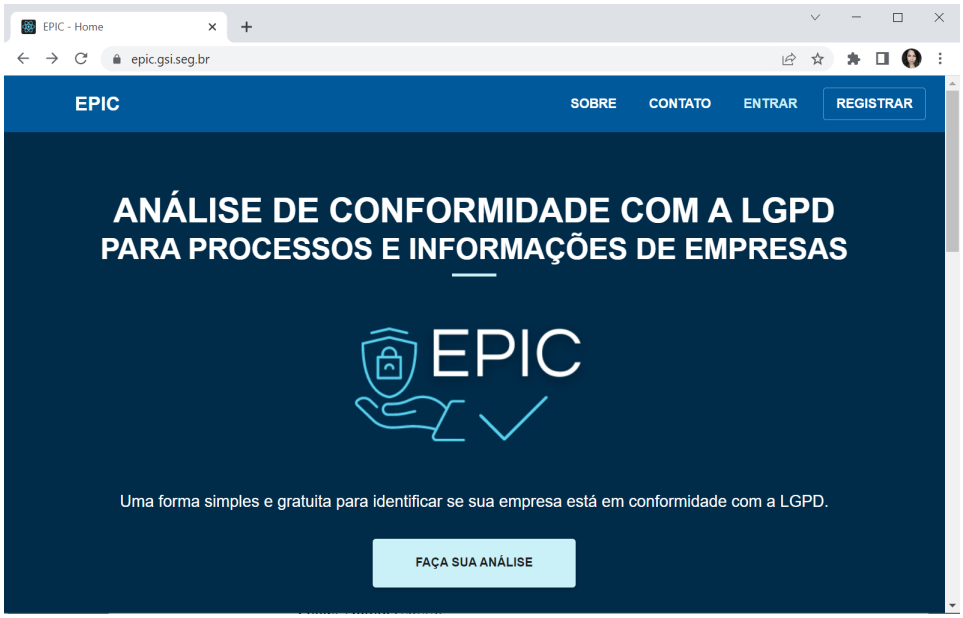
- Página inicial;
- Registro de usuário;
- Login de usuário;
- Criação e exibição de empresas;
- Criação, exibição e exclusão de setores de uma empresa;
- Questionários;
- Resultados das análises de uma empresa;
- Histórico e exclusão de análises.

Cada tela foi definida como uma função em JavaScript que é usada pelo *framework* Next.js para renderizar páginas HTML. Essas funções podem utilizar o retorno de requisições feitas no *backend* no conteúdo dessas páginas HTML.

5.3 Resultados da ferramenta

Ao acessar a página inicial do EPIC o usuário verá a tela conforme mostra a figura 24. Nela é apresentada a ferramenta com seu logotipo e algumas opções: no canto superior direito tem-se o botão “Sobre” onde o usuário terá acesso as informações sobre o projeto e objetivo da ferramenta, em “Contato” é possível acessar as informações de contato da criadora e desenvolvedora da ferramenta e nas opções “Entrar” e “Registrar” o usuário será redirecionado para as páginas de login e registro de usuário, respectivamente.

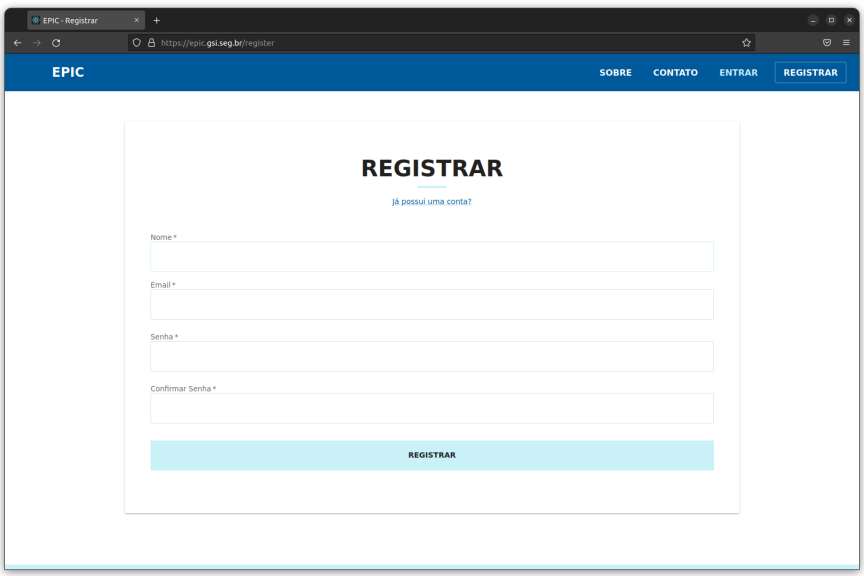
Figura 24 – Página inicial do EPIC.



Fonte: Autora (2022)

Para realizar a análise é necessário que o usuário registre-se na página de registro de usuário. Essa página possui os campos de entrada para inserção do nome, e-mail, senha, confirmação de senha e um botão pra submeter a entrada de dados, conforme pode ser observado na figura 25.

Figura 25 – Página de registro de usuário.

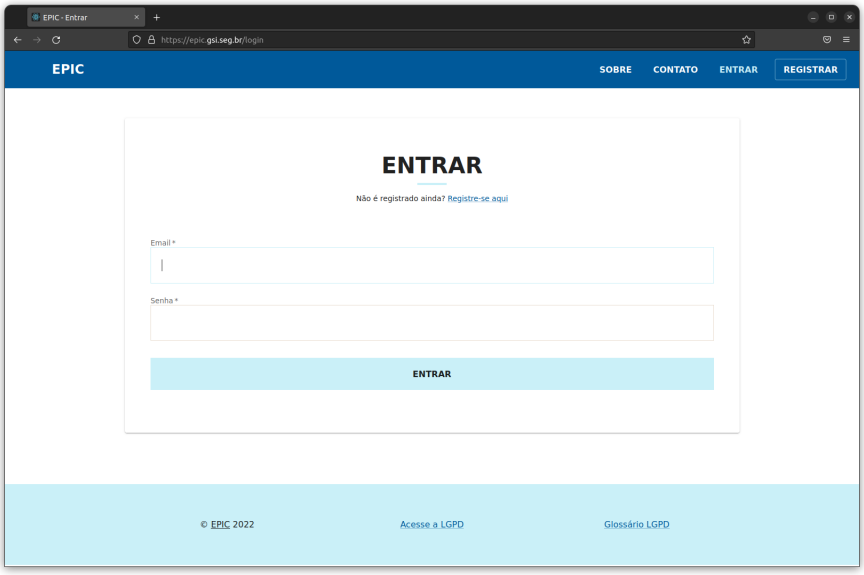


Fonte: Autora (2022)

Ao ser pressionado o botão “Registrar”, os dados são enviados para o *backend* no *endpoint* de criação de usuário e a criação do mesmo é efetuada. Se já existir um usuário

cadastrado com o email informado a página exibirá um erro com essa informação. Caso o usuário já tenha sido cadastrado anteriormente ele poderá utilizar a tela de login, exibida na figura 26.

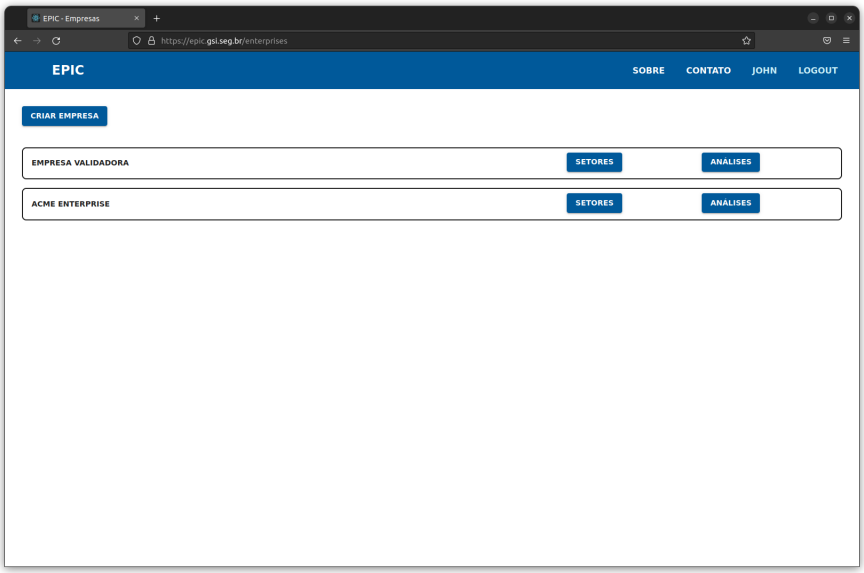
Figura 26 – Página de login de usuário.



Fonte: Autora (2022)

Na página de login o usuário poderá digitar e submeter seus dados de acesso, e caso os mesmos sejam validados pelo *backend* o navegador será redirecionado para a página onde são exibidas as empresas do usuário, conforme exemplo na figura 27.

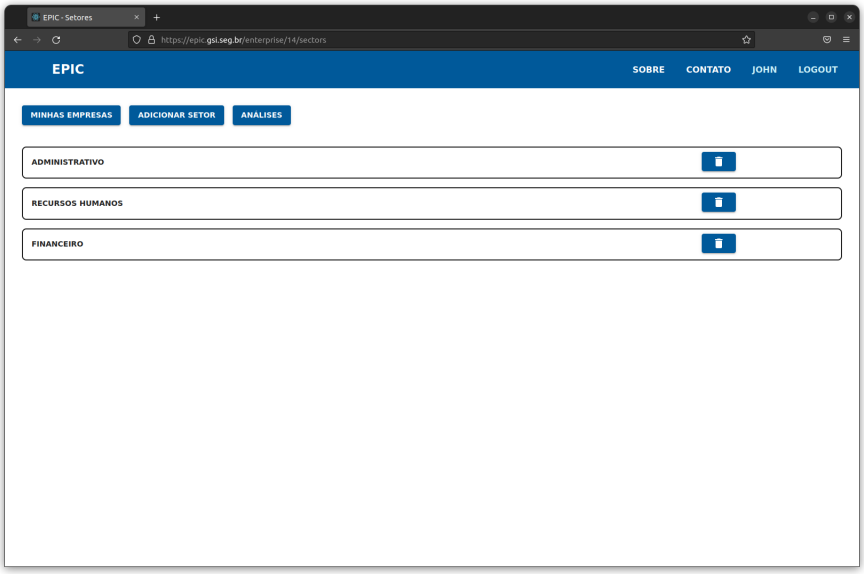
Figura 27 – Página de exibição de empresas.



Fonte: Autora (2022)

Cada empresa listada possui botões para acessar a lista de setores e menu de análises da empresa. A lista de setores da empresa exibe todos os setores cadastrados relacionados com a empresa em questão e permite ao usuário adicionar e excluir setores, conforme pode ser visto na figura 28.

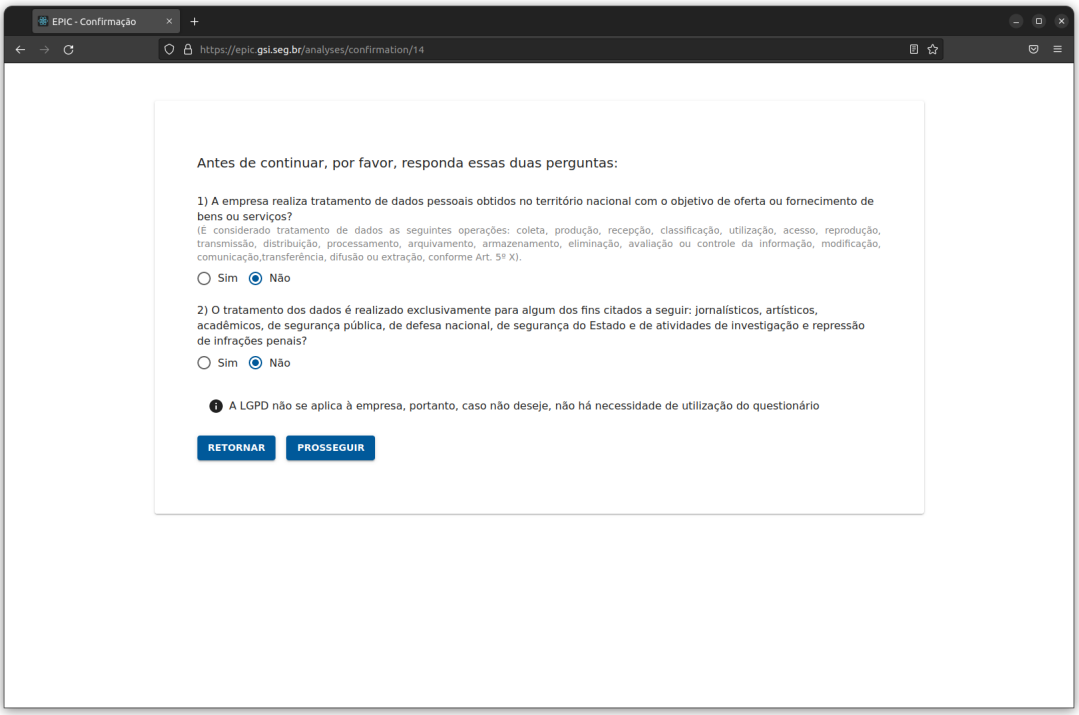
Figura 28 – Página de exibição de setores.



Fonte: Autora (2022)

Após a criação dos setores o usuário poderá acessar o menu de análises. Nesse menu se encontram listadas as análises já realizadas pelo usuário na respectiva empresa. Na parte superior da página há um botão que permite a criação de uma nova análise. Ao clicar nesse botão o usuário dá início ao processo de aplicação dos questionários com as etapas descritas anteriormente. Na primeira tela de questionário são exibidas as questões preliminares. Essa etapa visa verificar se a LGPD se aplica ao cenário da empresa e caso as respostas do usuário para as questões sejam negativas é exibido um aviso informando o usuário da não necessidade de realização do questionário, porém oferecendo a opção de prosseguir, conforme pode ser observado na figura 29.

Figura 29 – Questões preliminares.



Fonte: Autora (2022)

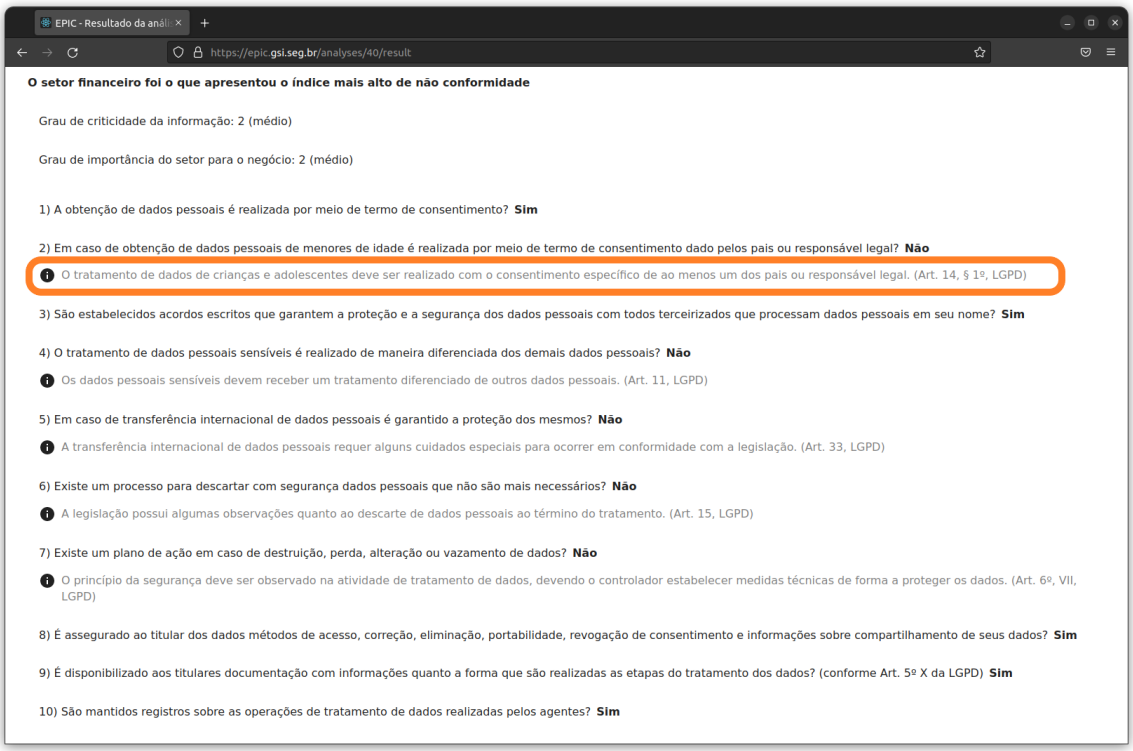
Ao prosseguir com a realização do questionário o usuário responderá as questões de segurança da empresa e também as questões de conformidade para cada setor, sendo apresentado ao final o resultado da análise em forma de relatório. No relatório estão contidas informações sobre o índice de segurança da empresa e também uma tabela com os dados das análises de conformidade de cada setor, conforme a figura 30.

Figura 30 – Resultado das análises.

Fonte: Autora (2022)

No relatório é apresentada também uma descrição da análise do setor crítico, que é aquele que apresenta o nível mais alto de não conformidade. Esta análise verifica quais respostas indicam pontos de não conformidade e apresenta o trecho da lei relacionado às respectivas questões. Um exemplo da seção da análise do setor crítico do relatório pode ser visto na figura 31.

Figura 31 – Análise do setor crítico.



Fonte: Autora (2022)

Conforme a arquitetura proposta, foi implementado o monitoramento de métricas da aplicação, com isso se tornou possível a exportação, obtenção e visualização das mesmas. A exportação é realizada diretamente pelo servidor *web* da aplicação e as métricas ficam disponíveis em um *endpoint*, podendo ser obtidas por meio de uma request HTTP. Para a obtenção das métricas de desempenho foi utilizado o Prometheus[1], um software de monitoramento de eventos e alertas. Elas são obtidas e armazenadas em um banco de dados de séries temporais e podem ser utilizadas pelo Grafana para visualização em formas de gráficos, tabelas ou ainda a geração de alertas configuráveis. Na figura 32 é possível observar a página inicial da instância do Grafana do EPIC. Assim como no *backend* e no *frontend* as ferramentas citadas acima foram hospedadas em *containers* que são executados no servidor que hospeda a aplicação.

[1] https://prometheus.io/

Figura 32 – Instância do Grafana - EPIC.

Fonte: Autora (2022)

No gráfico da imagem 32 é possível visualizar a taxa de requisições HTTP recebidas pelo servidor da aplicação em um intervalo de tempo.

5.4 Testes de Software

Conforme Sommerville (2011) testes de software podem ser usados para verificar se um software está se comportando da maneira esperada. Durante o desenvolvimento do software foram elaborados e implementados testes para garantir o funcionamento correto da aplicação.

- **Casos de Testes**

Segundo Myers (1979), o teste funcional, também conhecido como teste caixa preta, trata o software como uma caixa cujo conteúdo é desconhecido e da qual só é possível visualizar o lado externo, ou seja, os dados de entrada fornecidos e as respostas produzidas como saída. Nessa técnica são verificadas as funções do sistema sem se preocupar com os detalhes de implementação. Ela envolve dois passos principais: identificar as funções que o software deve realizar e criar Casos de Testes capazes de checar se essas funções estão sendo realizadas pelo software (PRESSMAN, 2005). Nas tabelas 7 à 14 são descritos os Casos de Testes implementados para o EPIC.

Tabela 7 – Casos de Teste - Cadastrar Usuário

Caso Nº	CT001 - Cadastrar Usuário
Objetivo do Teste	Verificar se o cadastro de usuário é efetivado.
Dados de Teste	• Nome. • Endereço de e-mail válido. • Senha de no mínimo 8 caracteres.
Passos	1. Acessar a página inicial; 2. Clicar no botão “Registrar”; 3. Inserir as informações necessárias; 4. Clicar botão “Entrar”.
Resultados Esperados	O cadastro é salvo no Banco de Dados. A página é redirecionada para a página de login. Se o usuário digitar um formato de e-mail inválido, uma mensagem de erro é mostrada. Se uma senha de menos de 8 digítos for inserida, a mensagem de erro é mostrada.

Fonte: Autora (2022)

Tabela 8 – Casos de Teste - Cadastrar Empresa

Caso Nº	CT002 - Cadastrar Empresa
Objetivo do Teste	Verificar se o cadastro de empresa é efetivado.
Dados de Teste	• Usuário cadastrado e autenticado no sistema. • Nome da empresa.
Passos	1. O usuário autenticado é redirecionado para página de empresas; 2. Clicar no botão “Criar empresa”; 3. Inserir o nome da empresa.
Resultados Esperados	Caso o usuário ainda não possua empresa cadastrada, é exibida a mensagem: “Você ainda não possui empresas cadastradas”. O cadastro é salvo no Banco de Dados. A nova empresa é listada na página.

Fonte: Autora (2022)

Tabela 9 – Casos de Teste - Cadastrar Setor

Caso Nº	CT003 - Cadastrar Setor
Objetivo do Teste	Verificar se o cadastro de setor é efetivado.
Dados de Teste	• Usuário cadastrado e autenticado no sistema. • Empresa cadastrada. • Nome do setor.
Passos	1. Na página de empresas, clicar no botão “Setores”; 2. Clicar no botão “Adicionar setor”; 3. Inserir o nome do setor.
Resultados Esperados	Caso o usuário ainda não possua setor cadastrado, é exibida a mensagem: “Você ainda não possui setores cadastrados”. O cadastro é salvo no Banco de Dados. A novo setor é listada na página.

Fonte: Autora (2022)

Tabela 10 – Casos de Teste - Realizar Análise

Caso Nº	CT004 - Realizar Análise
Objetivo do Teste	Verificar se a análise é realizada e o relatório disponibilizado ao usuário.
Dados de Teste	• Usuário cadastrado e autenticado no sistema. • Empresa cadastrada. • Pelo menos um setor cadastrado.
Passos	1. Na página de setores, clicar no botão “Análises”; 2. Clicar no botão “Nova Análise”; 3. Responder as duas perguntas preliminares sobre tratamento de dado e clicar em “Prosseguir”; 4. Responder as perguntas de segurança e clicar em “Avançar”; 5. Responder as perguntas sobre cada setor e clicar em “Avançar”.
Resultados Esperados	Caso uma das duas perguntas iniciais, sobre tratamento de dados, seja “não”, é exibida a mensagem “A LGPD não se aplica à empresa, portanto, caso não deseje, não há necessidade de utilização do questionário”. O usuário poderá escolher clicar em “voltar” ou “prosseguir”. O resultado da análise é exibido e salvo no Banco de Dados.

Fonte: Autora (2022)

Tabela 11 – Casos de Teste - Logar no Sistema

Caso Nº	CT005 - Logar no Sistema
Objetivo do Teste	Verificar se o Login do usuário cadastrado é efetivado.
Dados de Teste	• E-mail cadastrado. • Senha relacionada ao e-mail cadastrado.
Passos	1. Acessar a página inicial; 2. Clicar no botão “Entrar”; 3. Inserir o e-mail cadastrado 4. Inserir a senha corretamente.
Resultados Esperados	O usuário é redirecionado para a página de sua(s) empresas(s). Caso o e-mail e/ou senha digitadas não correspondam ao cadastro, a mensagem de erro “E-mail ou senha inválida” é exibida.

Fonte: Autora (2022)

Tabela 12 – Casos de Teste - Acessar e imprimir análise

Caso Nº	CT006 - Acessar e imprimir análise
Objetivo do Teste	Verificar se o usuário acessa e imprime corretamente a(s) análise(s) realizada(s).
Dados de Teste	• Usuário autenticado no Sistema. • Ao menos uma análise já realizada.
Passos	1. Ao acessar a página de empresas, clicar em “Análises”; 2. Clicar no botão “Entrar”; 3. Clicar no botão da Análise que deseja visualizar.
Resultados Esperados	Caso o usuário ainda não possua análise realizada, é mostrada a mensagem: “Você ainda não possui análise realizada”. As análises são listadas por data. Ao clicar na análise é mostrado o relatório com a análises de segurança da empresa e de não conformidade do(s) setor(es). Para imprimir o relatório basta clicar em “Imprimir análise”.

Fonte: Autora (2022)

Tabela 13 – Casos de Teste - Excluir setor

Caso Nº	CT007 - Excluir setor
Objetivo do Teste	Verificar se a exclusão de um setor é efetivada.
Dados de Teste	• Usuário autenticado no Sistema. • Ao menos um setor cadastrado.
Passos	1. Ao acessar a página de empresas, clicar em “Setores”; 2. Clicar no botão, com ícone de lixeira, do setor que deseja excluir.
Resultados Esperados	O setor não é mais exibido na lista e é excluído do Banco de Dados.

Fonte: Autora (2022)

Tabela 14 – Casos de Teste - Excluir análise

Caso Nº	CT007 - Excluir análise
Objetivo do Teste	Verificar se a exclusão de uma análise é efetivada.
Dados de Teste	• Usuário autenticado no Sistema. • Ao menos uma análise realizada..
Passos	1. Ao acessar a página de empresas, clicar em “Análises”; 2. Clicar no botão, com ícone de lixeira, da análise que deseja excluir.
Resultados Esperados	A análise não é mais exibida na lista e é excluída do Banco de Dados.

Fonte: Autora (2022)

Todos os passos dos Casos de Testes apresentados foram executados primeiramente em ambiente de desenvolvimento, processo pelo qual foi possível identificar *bugs* e corrigi-los e, também, implementar melhorias. Em seguida, a ferramenta foi disponibilizada em um servidor *web*, onde foi possível executar os mesmos testes em ambiente de produção. Assim, os resultados esperados representam a realidade, atingindo os objetivos de cada caso.

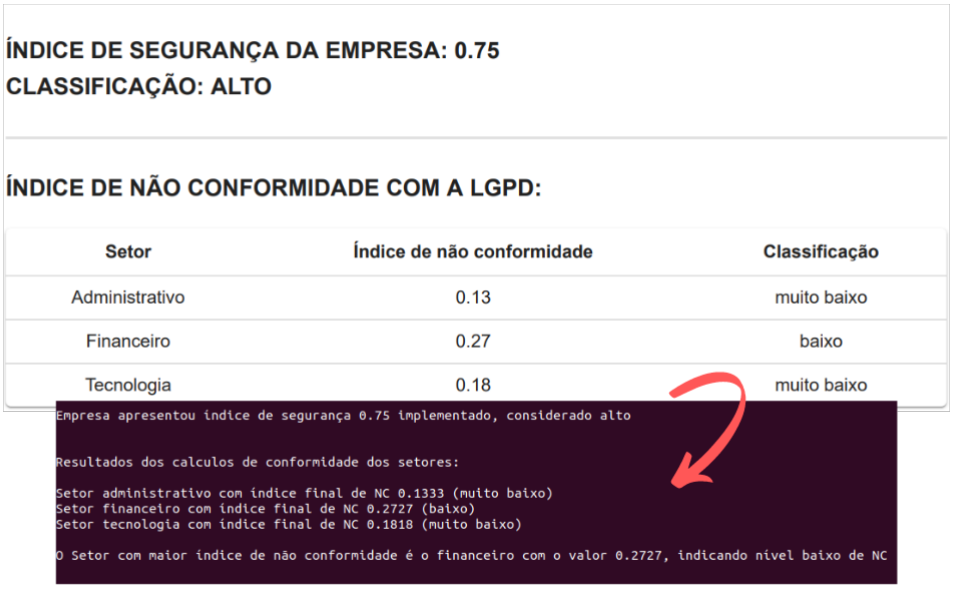
6 RESULTADOS E DISCUSSÕES

Com a ferramenta funcional, partiu-se então para as etapas de verificação e experimentação. Inicialmente foram utilizados os dados fictícios usados para os testes do protótipo. No segundo momento foi realizada a validação do *software* com o site em produção e disponível para acesso por empresas reais. A etapa de verificação é descrita na seção 6.1, a seção 6.2 apresenta a etapa de experimentação e na seção 6.3 tem-se as discussões finais diantes dos resultados obtidos.

6.1 Verificação Inicial - Projeto Piloto

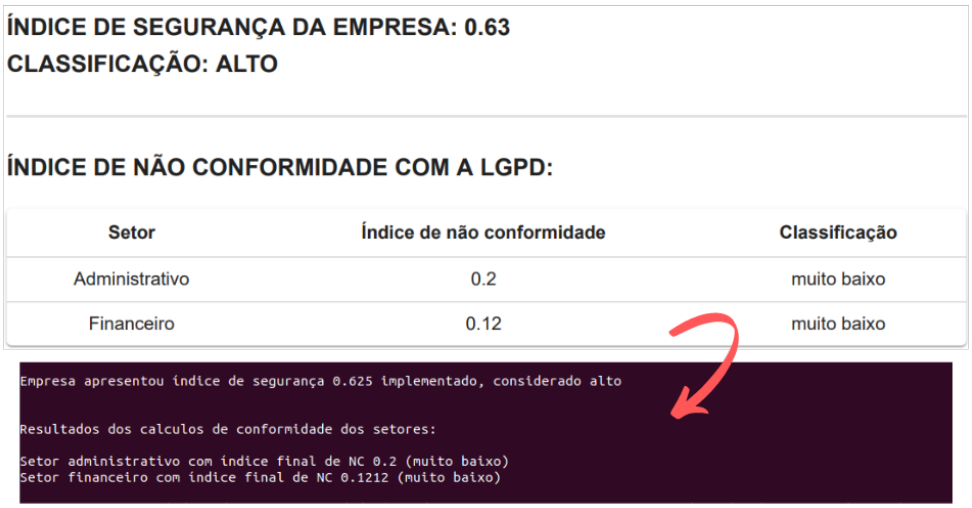
A etapa de verificação foi realizada com base nos mesmos dados do projeto piloto, apresentados na seção 5.1, com objetivo de se obter os mesmos resultados. As figuras 33 e 34 mostram que os resultados obtidos são os mesmos encontrados nos testes de protótipo apresentados na figura 16.

Figura 33 – Resultados - Empresa de Teste 1



Fonte: Autora (2022)

Figura 34 – Resultados - Empresa de Teste 2



Fonte: Autora (2022)

A partir dos resultados apresentados, é possível observar que estes condizem com o esperado, havendo, apenas, uma redução de casas decimais dos índices para uma melhor apresentação para usuário.

6.2 Experimentação

Travassos, Gurov e Amaral (2002) afirmam que a experimentação é o centro do processo científico e somente experimentos verificam as teorias. Os autores dizem ainda que novas ferramentas não deveriam ser publicadas sem experimentação e validação. O método experimental propõe e submete repetidamente o método proposto a situações para observação do comportamento com o objetivo de comprovação e aprimoramento.

Nessa etapa, dez empresas *Small and Medium Businnes* (SMB) foram contatadas e convidadas a acessar a página da ferramenta, disponível em https://epic.gsi.seg.br/. Foi solicitado, então, que elas cadastrassem suas empresas; adicionassem ao menos um setor; realizassem e imprimissem a análise de segurança e de não conformidade. Dessas empresas, oito realizaram a análise e as outras duas optaram por não prosseguir após responderem as duas perguntas preliminares ao processo de análise, as quais tratam dos casos em que a LGPD não se aplica (figura 29). Nesse caso, quando a resposta era

negativa para as duas perguntas, os usuários poderiam escolher se gostariam de prosseguir para o próximo passo. Os resultados das análises de segurança e de não conformidade podem ser visualizados nas tabelas 15 e 16.

Tabela 15 – Resultado dos Índices de Segurança das Empresas

Empresa	**Índice de Segurança**	**Classificação**
1	0.57	Moderado
2	0.25	BAIXO
3	0.43	Moderado
4	0.63	Alto
5	0.63	Alto
6	0.29	BAIXO
7	0.57	Moderado
8	0.57	Moderado

Fonte: Autora (2022)

Observando-se os índices gerados nas análise de segurança das empresas, na tabela 15, nota-se que 25% das empresas que realizaram a análise apresentam Índice de Segurança considerados como "Baixo"(entre 0.2 e 0.4), 50% como "moderado"(entre 04 a 0.6) e outros 25% correspondem classificados como "Alto"(entre 0.6 e 0.8). Observa-se também que nenhuma empresa apresentou Índice de Segurança "Muito baixo"(menor que 0.2) nem "Muito alto"(maior que 0.8).

Na segunda parte da análise as empresas responderam questões relacionadas a LGPD para cada setor cadastrado. A análise também considera os graus de importância para o negócio e de criticidade das informações atribuidos a esses setores. Na tabela 16 são listados os setores de cada empresa e seus respectivos Índices de Não Confirmidade e a classificação correspondente.

Tabela 16 – Resultado dos Índices de Não Conformidade dos setores

Empresa	Setores	Índice de Não Conformidade	Classificação
1	Administrativo	0.44	Moderado
	Financeiro	0.5	Moderado
2	Administrativo	0.67	ALTO
3	Informática	0.9	MUITO ALTO
4	Desenvolvimento de Software	0.33	Baixo
5	Tecnologia	0.56	Moderado
	Diretoria	0.44	Moderado
6	Vendas	0.9	MUITO ALTO
	Financeiro	0.7	ALTO
7	Tecnologia	0.8	ALTO
8	Desenvolvimento	0.56	Moderado

Fonte: Autora (2022)

Os nomes dos setores apresentados na tabela 16 correspondem aos que foram criados pelas empresas no momento do cadastro. A partir desses resultados, é possível observar que 50% das empresas apresentaram Índice de Não Conformidade classificado como "Alto"(entre 0.6 e 0.8) ou "Muito Alto"(acima de 0.8), 37,5% como "Moderado"(entre 0.4 e 0.6) e 12,5% - ou seja, apenas uma empresa - apresentou Índice de Não Conformidade "Baixo"(menor que 0.4).

Diante dos resultados das análises, observa-se que a maioria das empresas precisam de maior atenção para a Segurança da Informação, e principalmente, em relação a conformidade com a LGPD, já que a maioria apresenta índices preocupantes de não conformidade, tendo em vista que apenas uma empresa apresentou classificação "Baixo"pra esse índice e nenhuma apresentou classificação "Muito baixo". A empresa que apresentou Índice de Não Conformidade "Baixo"obteve esse índice para seu único setor que é de Desenvolvimento de Software o que acredita-se estar relacionado a empresas dessa área, normalmente, possuir uma maior preocupação e entendimento relacionados a proteção de dados.

Após a utilização da ferramenta e a realização das análises, as empresas foram convidadas a responder um questionário que tinha como objetivo obter um *feedback* dos usuários da ferramenta EPIC, bem como identificar o perfil dos mesmos. O questionário é composto de 8 perguntas, sendo 3 relacionadas ao perfil do usuário e 5 relacionadas a usabilidade do EPIC, o qual pode ser observado na tabela 17.

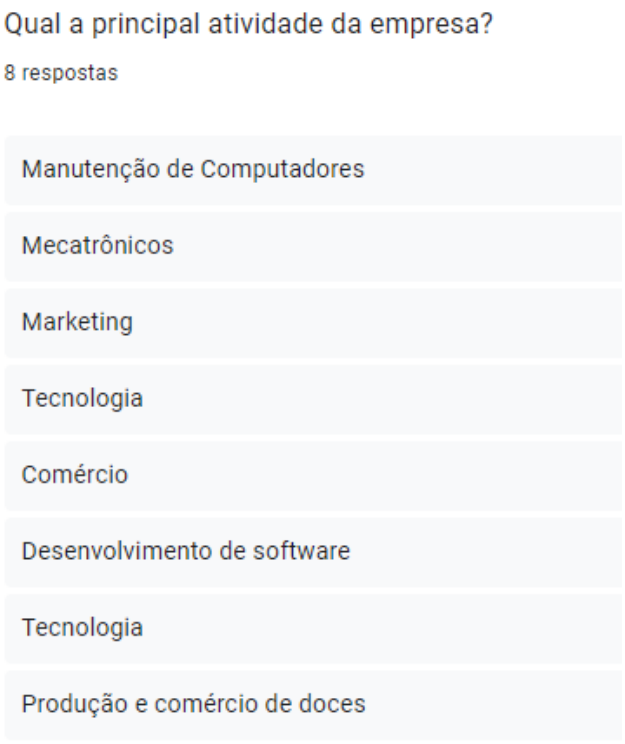
Tabela 17 – Questionário de Usabilidade do EPIC

PERFIL DO USUÁRIO
1. Qual a principal atividade da empresa?
2. Qual o porte da empresa?
3. Como você considera o seu nível de conhecimento sobre a LGPD: (1-nenhum a 5-avançado)
USABILIDADE DA FERRAMENTA
4. Facilidade de utilização do EPIC: (1-difícil a 5-fácil)
5. Organização das informações: (1-ruim a 5-boa)
6. Layout das telas: (1-confuso a 5-claro)
7. Você achou que a análise fornecida pelo EPIC corresponde a realidade da empresa? (1-muito pouco a 5-totalmente)
8. Você indicaria o EPIC para outras empresas? (1-não a 5-com certeza)

Fonte: Autora (2022)

Os testes de usabilidade são atividades de pesquisa realizadas para avaliar a usabilidade de um *design*, produto ou serviço. É um processo no qual participantes representativos avaliam o grau que um produto se encontra em relação a critérios específicos de usabilidade (por exemplo, sua facilidade de uso, eficiência, acessibilidade, satisfação de uso, entre outros aspectos) (HASS, 2019). As respostas relacionadas ao perfil do usuário são apresentadas nas figuras 35 a 37. Já as respostas referente à usabilidade do EPIC podem ser observadas nas figuras 38 a 42.

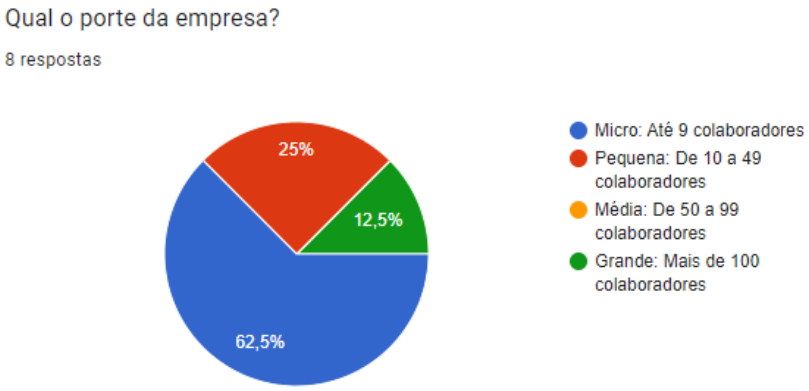
Figura 35 – Respostas - Questão 1.



Fonte: Autora (2022)

A partir das respostas apresentadas na figura 35, nota-se que a maioria das empresas analisadas são da área ou lidam com Tecnologia da Informação (TI), ou seja, até mesmo essas empresas não demonstram cuidado em estar em conformidade com a lei porém apresentam níveis "Moderados"a "Alto"em relação a Segurança da Informação, já que é possível observar, através das tabelas 15 e 16, que as empresas que mostraram níveis "Baixos"de Segurança são as mesmas que não possuem algum setor de TI.

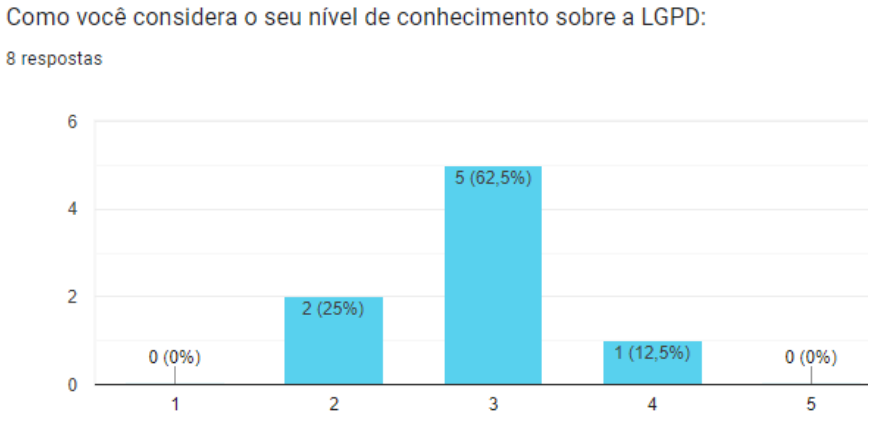
Figura 36 – Respostas - Questão 2



Fonte: Autora (2022)

A maioria das empresas são de micro ou pequeno porte, conforme pode ser observado na figura 36, o que pode estar relacionado aos níveis altos de não conformidade já que essas empresas, normalmente, possuem somente um setor que, por ser o único, torna-se o mais importante e mais crítico. Também pode-se dizer que a baixa maturidade e a falta de uma cultura de proteção de dados pessoais pelas empresas de pequeno porte, tendem a dificultar a adequação à LGPD e inviabilizar a sua existência.

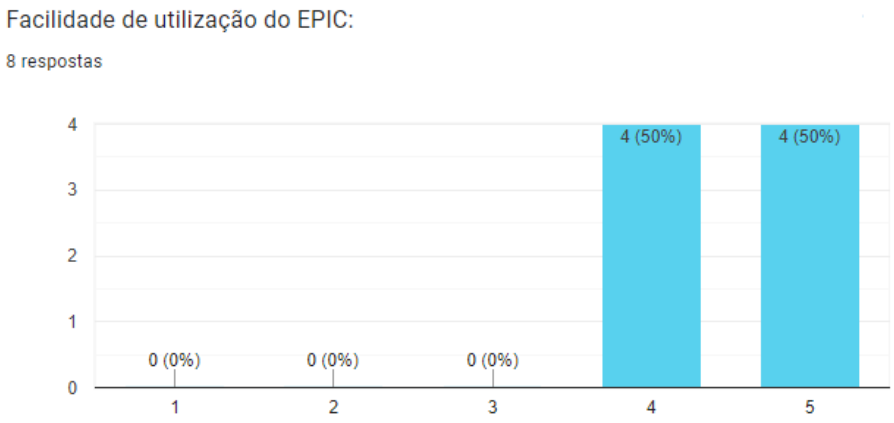
Figura 37 – Respostas - Questão 3



Fonte: Autora (2022)

Sobre o nível de conhecimento sobre a LGPD, a avaliação foi realizada em uma escala de 1 (nenhum) a 5 (avançado). A maioria das empresas afirmaram possuir conhecimento médio da lei, conforme pode ser observado na figura 37, porém isso não se reflete totalmente nas ações relacionadas a conformidade, observadas nos resultados das análises, onde a maioria apresenta níveis importantes de não conformidade.

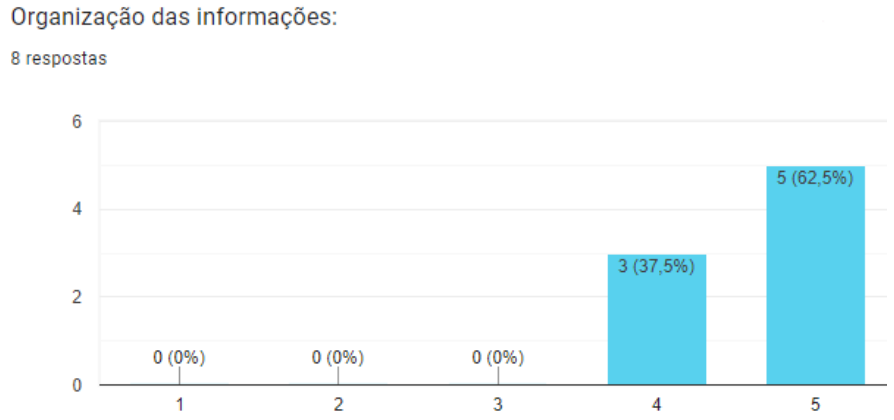
Figura 38 – Respostas - Questão 4



Fonte: Autora (2022)

A primeira questão referente a usabilidade do EPIC perguntava sobre a facilidade de utilização da ferramenta, apresentada na figura 38, onde atribuiam-se graus de 1(fácil) a 5(difícil) de acordo com a opinião do usuário. Nesse caso metade dos usuários atribuiram valor 4 e outra metade atribui valor 5. Analisando-se os perfis dessas respostas, notou-se que três dessas quatro empresas que responderam com valor 4 são da área de tecnologia, o que pode se justificar pelo fato de que, em geral, esses usuários são mais exigentes com aspectos de usabilidade de ferramentas.

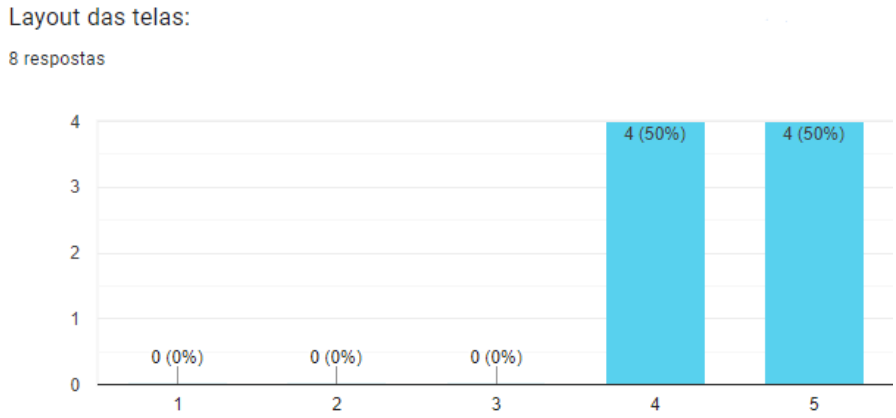
Figura 39 – Respostas - Questão 5



Fonte: Autora (2022)

Sobre a organização das informações, a maioria das empresas consideraram o grau máximo, de 1(ruim) a 5(boa), da escala em suas respostas. Porém é possível observar na figura 39 que três empresas atribuíram o nível 4 na resposta. Duas, dessas três empresas, foram as mesmas que também responderam com grau 4 para a facilidade de utilização, o que pode estar relacionado ao fato de que se as informações estão mais organizadas o uso da ferramenta também se torna mais fácil. Dessa forma, entende-se a importância de uma revisão da organização das informações do site, como clareza nos textos e hiearquia das informações, para a implementação de melhorias.

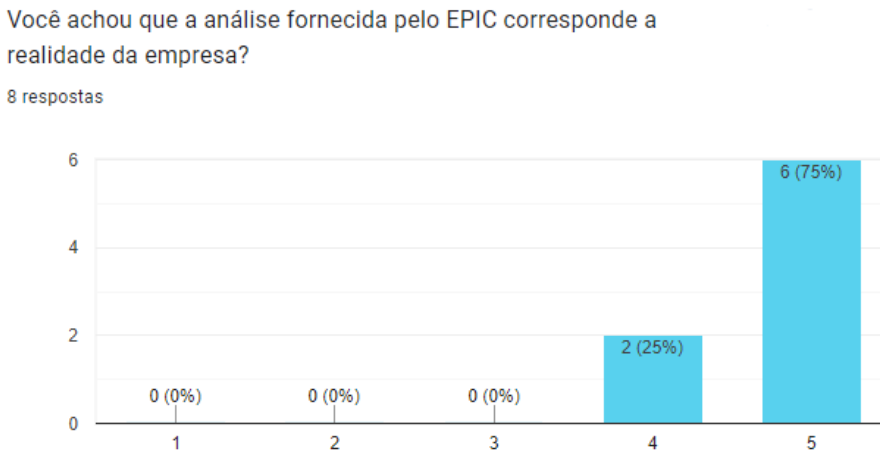
Figura 40 – Respostas - Questão 6



Fonte: Autora (2022)

Em relação ao *layout* das telas do EPIC, a escala atribuída também foi de 1 a 5, onde 1 significa "Confuso"e 5 "Claro". Nesse aspecto teve-se como resultados: metade das respostas com grau 4 e a outra metade com grau 5, assim como na questão referente a facilidade de uso da ferramenta. Verificou-se que a maioria das empresas que não atribuiram o grau máximo nesse quesito, também não o atribuiram para ao menos uma das outras questões relacionadas a interface com o usuário, o que também torna importante melhorias em padrões de *layout*, como distribuição, alinhamentos e cores de elementos, visando uma navegação mais rápida e prática do usuário.

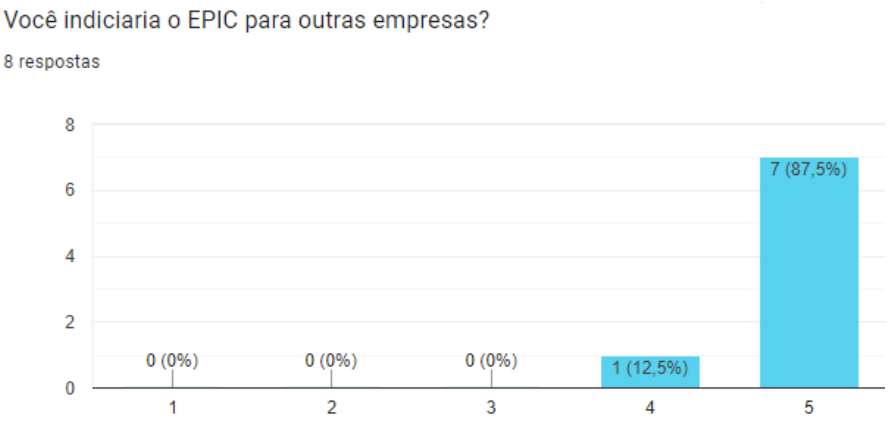
Figura 41 – Respostas - Questão 7



Fonte: Autora (2022)

Ao serem questionados se a análise fornecida pelo EPIC correspondia a realidade da empresa, em uma escala de 1(muito pouco) a 5(totalmente), a maioria dos usuários respondeu que correspondia totalmente. Conforme a figura 41, duas empresas não acharam que a análise correspondia totalmente a realidade, porém é importante salientar que as duas empresas em questão responderam com graus 2 e 3 a pergunta 3, referente ao conhecimento das empresas em relação a LGPD. Assim, pode se dizer que o fato dessas empresas terem pouco ou médio conhecimento da lei, pode leva-las a não saber opinar seguramente em relação ao resultado.

Figura 42 – Respostas - Questão 8



Fonte: Autora (2022)

Por fim, perguntou-se aos usuários se indiciariam o EPIC para outras empresas. De 1(não) a 5 (com certeza), a maioria atribuiu o grau máximo e apenas uma empresa respondeu com grau 4. Essa empresa também atribuiu grau 4 as questões referentes a

interface da ferramenta com o usuário (questões 4,5 e 6), ou seja, por não estar 100% satisfeita com a usabilidade da ferramenta, a empresa pode não estar totalmente segura de indicá-la a outras empresas.

6.3 Discussões Finais

Diantes dos resultados apresentados nesse capítulo, nota-se que foi possível verificar e validar a ferramenta. A verificação da aplicação com os dados do projeto piloto tornou possível que ela fosse disponibilizada para o público e, assim, validada com empresas de pequeno e medo porte, objetivo principal da pesquisa.

Os resultados dos índices de segurança obtidos, mostram que as empresas do ramo de TI sãos as que possuem os níveis moderados e altos. Nenhuma empresa atingiu o nível máximo de segurança, ou seja, de forma geral, as empresas ainda precisam adotar medidas de seguranças básicas, já que as perguntas levaram em consideração os requisitos mínimos de segurança esperados.

Os índices de não conformidade obtidos pelas empresas mostram que a maioria, mesmo as empresas da área de TI, ainda precisam adequar grande parte de seus processos á LGPD. Também observa-se que ainda que a maioria das empresas analisadas possuam nível médio e até alto de conhecimento sobre à lei, na prática isso ainda não reflete totalmente. Em sua pesquisa, com maioria das empresas também sendo da área de Tecnologia, Machado et al. (2021) afirma que, apesar de muitos participantes afirmarem conhecer a LGPD, a maioria não soube explicar em detalhes suas características e o impacto que a lei está causando em sua empresa. Assim, acredita-se que essa afirmação corrobora com os resultados da presente pesquisa.

Em relação a usabilidade do EPIC a maioria dos resultados obtiveram os graus máximos de satisfação (5) de acordo com os aspectos questionados. Sabendo-se que a maioria dos usuários afirmaram que a análise fornecida pelo EPIC corresponde totalmente à realidade da empresa, pressupõe-se que a ferramenta desenvolvida apresenta resultados condizentes com o que foi proposto. Por último, a maioria das empresas responderam que indicariam, com certeza (5), o EPIC para outras empresas, o que corrobora com a proposta da ferramenta.

7 CONSIDERAÇÕES FINAIS

Com o objetivo de oferecer uma solução de *software* para auxiliar as empresas a terem conhecimento dos seus níveis de conformidade com a Lei Geral de Proteção de Dados (LGPD), fez-se então um estudo do referencial teórico e, através de uma Revisão Sistemática da Literatura (RSL), foi possível elencar os principais trabalhos correlatos à essa pesquisa. A partir disso foi proposta a arquitetura da solução, a qual deu origem a um conjunto de equações baseadas em um instrumento de pesquisa em forma de questionário. Para a automatização do modelo proposto foi realizada a modelagem do sistema. Logo após, iniciou-se o desenvolvimento da ferramenta, a partir das tecnologias selecionadas, onde foram aplicados os casos de testes em ambiente de desenvolvimento. Por fim, após finalizada, a ferramenta foi implantada em ambiente de produção de forma automatizada através da tecnologia Docker, sendo possível acessá-la a partir da página https://epic.gsi.seg.br/.

A ferramenta foi testada e validada a partir de empresas reais que, além de utiliza-la, responderam a um questionário criado com o objetivo de obter o *feedback* da mesma e os perfis dos usuários. Os resultados mostraram que apenas metade das empresas analisadas possuem nível "Moderado"de Segurança da Informação e, apenas, 25% possuem nível "Alto". Metade das empresas também apresentaram nível "Alto"de Não Conformidade com a LGPD e apenas uma empresa apresentou nível "Baixo". Em relação a usabilidade, o EPIC demonstrou boa aceitação entre os usuários, atingindo também o objetivo principal de permitir uma análise de segurança e de não conformidade com a LPGD voltada a empresas de pequeno e médio porte, já que a maioria dos usuários afirmaram que os resultados obtidos correspondem a realidade da empresa e que indicariam a ferramenta para outras empresas.

Assim, pode-se afirmar que o EPIC é uma das possíveis soluções para o problema de pesquisa, pois foi possível implementar uma solução de *software*, alinhada à LGPD, de forma a auxiliar as empresas *Small and Medium Business* (SMB) a ampliar o nível de segurança de seus processos e informações, fornecendo um relatório com resultados quantitavos e qualitativos das análises de Segurança e de Não Conformidade e alertando em relação aos pontos de não conformidade com a lei.

Conforme o objetivo da pesquisa a ferramenta foi desenvolvida baseada em *containers* e os códigos-fonte do *frontend* e *backend* encontram-se hospedados em repositório público, podendo ser acessados através dos endereços: <https://github.com/SamaraMarques/

epic-frontend> e <https://github.com/SamaraMarques/epic-backend>.

Apesar de não existir uma definição única de conformidade com a LGPD para empresas SMB, a estrutura simples proposta no presente trabalho é capaz de auxiliar no desafio dessas empresas em interpretarem a lei para suas áreas. No entanto, salienta-se que a ferramenta não garante a conformidade com a lei, contudo, ela pode ser utilizada como base para empresas que possuem pouco conhecimento da lei, possibilitando agilidade no processo de diagnóstico. Sendo assim, acredita-se que o presente trabalho traz uma importante contribuição para a área de segurança da informação nas empresas. Através de um relatório simples e gratuito, empresas, que antes possuiam pouco ou nenhum conhecimento da LGPD, passam a ter mais interesse e uma noção da lei através dos pontos principais abordados na análise com o EPIC. Ao identificar seus níveis de não conformidade e passarem a considerar um processo de adequação a lei, essas empresas podem evitar sanções indesejadas e, principalmente, garantir o tratamento correto e, consequentemente, a segurança dos dados pessoais.

Como trabalhos futuros sugere-se melhorias na ferramenta Grafana, já integrada a aplicação, a ampliação do número de empresas em uma nova experimentação e, também, uma análise recorrente do histórico das análises das empresas, de forma que se possa verificar a evolução do processo de conformidade após a utilização do EPIC.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27701 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação.** Rio de Janeiro: ABNT, 2019.

AGOSTINELLI, S. et al. Achieving GDPR compliance of BPMN process models. In: SPRINGER. **International Conference on Advanced Information Systems Engineering**. Tartu, 2019. p. 10–22.

ANPD. **Sanções Administrativas: o que muda após 1º de agosto de 2021?** [Brasil]: Presidência da República, 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 08 Jun. 2021.

ANWAR, M. J.; GILL, A. Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. In: **Australasian Conference on Information Systems 2020**. [S.l.: s.n.], 2021. Acesso em: 09 set. 2021.

BARBOSA, G. R.; ALMEIDA, A. d. Sistemas de apoio à decisão sob o enfoque de profissionais de TI e de decisores. **Anais XXII Encontro Nacional de Engenharia de Produção 2002**, Curitiba, p. 1–8, 2002.

BISSO, R. et al. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 3, n. 1, 2020.

BOOCH, G. **UML: guia do usuário**. [S.l.]: Elsevier Brasil, 2006.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Brasília: Presidência da República, 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 set. 2021.

BRODIN, M. A framework for gdpr compliance for small-and medium-sized enterprises. **European Journal for Security Research**, Springer, v. 4, n. 2, p. 243–264, 2019.

CARISSIMI, A. Virtualização: da teoria a soluções. **Minicursos do Simpósio Brasileiro de Redes de Computadores–SBRC**, v. 2008, p. 173–207, 2008.

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso. **Brazilian Journal of Business**, BrJ, São José dos Pinhais, v. 2, n. 4, p. 3626–3648, 2020.

CHATZIPOULIDIS, A.; TSIAKIS, T.; KARGIDIS, T. A readiness assessment tool for gdpr compliance certification. **Computer Fraud & Security**, v. 2019, n. 8, p. 14–19, 2019. ISSN 1361-3723. Disponível em: https://www.sciencedirect.com/science/article/pii/S1361372319300867.

COSTA, W. S.; SILVA, S. C. M. Aquisição de conhecimento: O grande desafio na concepção de sistemas especialistas. **Holos**, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Natal, v. 2, p. 37–46, 2005.

DERMEVAL, D.; COELHO, J. A. d. M.; BITTENCOURT, I. I. **Mapeamento sistemático e revisao sistemática da literatura em informática na educaçao**. [S.l], 2019. Acesso em: 10 set. 2021. Disponível em: https://metodologia.ceie-br.org/wp-content/uploads/2019/11/livro2_cap3.pdf.

DOCKER. 2021. Acesso em: 16 ago. 2021. Disponível em: <https://www.docker.com.>

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

ELMASRI, R. et al. Sistemas de banco de dados. Pearson Addison Wesley São Paulo, 2005.

FERRÃO, S. É. R. et al. Diagnostic of Data Processing by Brazilian Organizations — A Low Compliance Issue. **Information**, Multidisciplinary Digital Publishing Institute, v. 12, n. 4, p. 168, 2021.

GIL, A. C. **Métodos e técnicas de pesquisa social. 6**. Atlas, São Paulo, v. 199, 2008.

GIL, A. C. et al. **Como elaborar projetos de pesquisa**. [São Paulo]: Atlas São Paulo, 2002. v. 4.

HASS, C. A practical guide to usability testing. In: **Consumer Informatics and Digital Health**. [S.l.]: Springer, 2019. p. 107–124.

IBM Cloud. **Containers vs. Virtual Machines (VMs): What's the Difference?** 2021. Disponível em: <https://www.ibm.com/cloud/blog/containers-vs-vm.>

JÚNIOR, E. A. da C. **Análise de conformidade de processos de negócios em relação a LGPD**. Tese (Doutorado) — UNIVERSIDADE FEDERAL DE PERNAMBUCO, 2020.

KEELE, S. et al. **Guidelines for performing systematic literature reviews in software engineering**. [S.l.], 2007.

MACHADO, J. G. C. et al. Lgpd: você está preparado? **ANAIS DA MOSTRA DE INICIAÇÃO CIENTÍFICA DO CESUCA-ISSN 2317-5915**, n. 15, 2021.

MATULEVIčIUS, R. et al. A Method for Managing GDPR Compliance in Business Processes. In: SPRINGER. [S.l.], 2020. p. 100–112. ISBN 978-3-030-58134-3.

MENEGAZZI, D. **Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução**. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2021.

MENEZES, A. et al. **Metodologia científica: teoria e aplicação na educação a distância.[e-book] Petrolina-PE**. 2019.

MILAGRE, J. A. **5 Passos para entender a ABNT NBR ISO/IEC 27701:2019**. [S.l.]: CyberExperts, 2019. v. 1.

MYERS, G. J. **IBM Systems Research Institute, Lecturer in Computer Science, Polytechnic Institute of New York, The Art of Software Testing, by John Wiley & Sons**. [S.l.]: Inc, 1979.

NEIVA, F.; SILVA, R. **Revisão Sistemática da Literatura em Ciência da Computação - Um Guia Prático**. [S.l.], 2016.

O'BRIEN, J. Sistemas de informação para apoio à decisão gerencial. In: UPF. São Paulo: Saraiva, 2001. p. 246–258.

PEREIRA, A. S. et al. **Metodologia da pesquisa científica**. UFSM, Santa Maria, 2018.

PRESSMAN, R. S. **Software engineering: a practitioner's approach**. [S.l.]: Palgrave macmillan, 2005.

PRODANOV, C. C. Freitas, ernani cesar de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**, v. 2, p. 274, 2013.

PY, M. X. **Sistemas especialistas: uma introdução**. Instituto de informática, UFRGS, Porto Alegre, 2009.

REDHAT. **Building modern apps with Linux containers**. 2020. Acesso em: 10 jun 2021. Disponível em: <https://www.redhat.com/rhdc/managed-files/RED19-0059_Intro_to_Linux_Containers_for_Developers_Ebook_D3%20%281%29.pdf.>

ROJAS, M. A. T. **Avaliação da adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais**. IFSC, [Santa Catarina], 2020.

ROY, B. On operational research and decision aid. **European Journal of Operational Research**, Citeseer, v. 73, n. 1, p. 23–26, 1994.

SILVA, E. L. d.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. rev. atual, Florianópolis, 2001.

SILVA, R. H. d. et al. **Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais**. UFSC, Araranguá, 2021.

SILVEIRA, C. R. **Metodologia da pesquisa**. [S.l.]: Florianópolis: IFSC, 2011.

SOARES, P. **GUIA LGPD: Lei Geral de Proteção de Dados Simplificada**. 2021. <https://d335luupugsy2.cloudfront.net/cms/files/92859/1565723282Guia_-_LGPD.pdf>. Acesso em: 09 jun. 2021.

SOMMERVILLE, I. Software engineering (2011). **Sl: sn ISBN**, v. 13, p. 978–0, 2011.

TRAVASSOS, G. H.; GUROV, D.; AMARAL, E. **Introdução à engenharia de software experimental**. [S.l.]: UFRJ, 2002. v. 9.

ZUCHI, I. et al. **Desenvolvimento de um Protótipo de Sistema Especialista Baseado em Técnicas de RPG para o Ensino de Matemática**. UFSC, Florianópolis, 2000.

APÊNDICE A – QUESTIONÁRIO PARA TESTES DE PROTÓTIPO

QUESTIONÁRIO PARA TESTES DE PROTÓTIPO

Parte 1 - Perguntas preliminares à aplicação do questionário:

Obs.: Se as respostas para as duas perguntas abaixo forem negativas significa que a LGPD não se aplica à empresa, portanto, caso não deseje, não há necessidade de utilização do questionário.

1. A empresa realiza tratamento de dados pessoais obtidos no território nacional com o objetivo de oferta ou fornecimento de bens ou serviços?
   (É considerado tratamento de dados as seguintes operações: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme Art. 5º X).
   ( ) Sim ( ) Não

2. O tratamento dos dados é realizado exclusivamente para algum dos fins citados a seguir: jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado e de atividades de investigação e repressão de infrações penais.
   ( ) Sim ( ) Não

Parte 2 - Segurança da Informação na empresa:

1. Sua empresa gerencia riscos de segurança da informação?
   ( ) Sim ( ) Não

2. Sua empresa possui controles de entrada para restringir o acesso às instalações a fim de impedir o acesso físico não autorizado?
   ( ) Sim ( ) Não

3. Sua empresa possui uma política de segurança da informação aprovada que suporta a segurança da informação de acordo com as necessidades do negócio?
   ( ) Sim ( ) Não

4. Sua empresa possui treinamento regular de conscientização sobre segurança da informação para todos os funcionários?
   ( ) Sim ( ) Não

5. Sua empresa faz backup rotineiramente dos dados armazenados para ajudar a restaurar as informações em caso de desastre?
   ( ) Sim ( ) Não

6. Sua empresa gerencia com segurança os colaboradores que trabalham remotamente a partir de suas casas (teletrabalho)?
   ( ) Sim ( ) Não

7. Sua empresa possui firewalls de limite para proteger os computadores contra ataques externos e ajudar a evitar violações de dados?
   ( ) Sim ( ) Não

8. Sua empresa possui defesas anti malware com gestão centralizada para proteger os computadores contra infecções por malware?
   ( ) Sim ( ) Não

Parte 3 - Questões relacionadas aos setores da empresa:

1. Informe o nome do setor da empresa: _____
2. Informe o grau de importância do setor para o negócio: _____
3. Informe o grau de criticidade do setor para informação: _____

Parte 4 - Questões relacionadas à LGPD sobre etapas de tratamento de dados por setor.

1. A obtenção de dados pessoais é realizada por meio de termo de consentimento?
   (O consentimento é definido como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada não podendo existir vícios de consentimento, conforme Art. 8º da LGPD).
   ( ) Sim ( ) Não ( ) Não se aplica

2. Em caso de obtenção de dados pessoais de menores de idade é realizada por meio de termo de consentimento dado pelos pais ou responsável legal?
   ( ) Sim ( ) Não ( ) Não se aplica

3. São estabelecidos acordos escritos que garantem a proteção e a segurança dos dados pessoais com todos terceirizados que processam dados pessoais em seu nome?
   ( ) Sim ( ) Não ( ) Não se aplica

4. O tratamento de dados pessoais sensíveis é realizado de maneira diferenciada dos demais dados pessoais?
   ( ) Sim ( ) Não ( ) Não se aplica

5. Em caso de transferência internacional de dados pessoais é garantido a proteção dos mesmos?
   ( ) Sim ( ) Não ( ) Não se aplica

6. Existe um processo para descartar com segurança dados pessoais que não são mais necessários?
   ( ) Sim ( ) Não

7. Existe um plano de ação em caso de destruição, perda, alteração ou vazamento de dados?
   ( ) Sim ( ) Não

8. É assegurado ao titular dos dados métodos de acesso, correção, eliminação, portabilidade, revogação de consentimento e informações sobre compartilhamento de seus dados?
( ) Sim ( ) Não

9. É disponibilizado aos titulares documentação com informações quanto a forma que são realizadas as etapas do tratamento dos dados? (conforme Art. 5º X)
( ) Sim ( ) Não

10. São mantidos registros sobre as operações de tratamento de dados realizadas pelos agentes?
( ) Sim ( ) Não

11. São adotadas medidas de segurança de modo a proteger os dados pessoais de acessos não autorizados ou de qualquer forma de tratamento ilícito?
( ) Sim ( ) Não

APÊNDICE B – DOCUMENTO DE REQUISITOS

[Adaptado de Sommerville (2007) e Pressman e Maxim (2016)]

1. Introdução

Este documento especifica os requisitos do sistema e fornece as informações necessárias para o desenvolvimento do projeto, testes e homologação.

O documento de requisitos está organizado com as seguintes seções descritas abaixo, além da seção introdutória.

Seção 2 – Descrição do sistema: Apresenta uma visão do sistema, seu escopo e seus usuários.

Seção 3 – Requisitos funcionais: Enumera os requisitos funcionais, especificando o modo de operação, suas entradas e saídas.

Seção 4 – Requisitos não funcionais: Enumera os requisitos não funcionais e os classifica segundo os critérios de usabilidade, confiabilidade, desempenho, segurança, distribuição, adequação a padrões e requisitos de software e hardware.

Identificação dos requisitos: A referência dos requisitos será feita utilizando-se das siglas RF para requisitos funcionais e RNF para requisitos não funcionais, seguidos de um número a ser atribuído de maneira crescente para cada um dos requisitos apresentados.

Prioridades dos requisitos: Os requisitos são divididos em 3 prioridades, denominadas "essencial", "importante" e "desejável". Requisito essencial é aquele que é de suma importância para o funcionamento do sistema, impossibilitando o funcionamento do mesmo em caso de não implementação. Requisito importante é aquele que caso não seja implementado o sistema será capaz de entrar em funcionamento, mesmo que de forma não satisfatória. Requisito desejável é aquele que não compromete o funcionamento básico do sistema e permite a utilização de forma satisfatória caso não seja implementado.

2. Descrição geral do sistema

O sistema é um modelo automatizado para análise de conformidade com a Lei Geral de Proteção de Dados (LGPD), visando auxiliar empresas de pequeno e médio porte a verificar se seus fluxos de tratamento de dados estão em conformidade com a lei, bem como identificar seus níveis de segurança da informação.

3. Requisitos Funcionais

Requisito Nº: [RF01] Cadastro de Usuário

Descrição: Permitir o cadastro de usuários interessados em realizar análise de conformidade.

Entradas: Nome, endereço de e-mail e senha.

Processo:

1. O usuário acessa a página inicial;
2. O usuário clica no botão "Registrar";
3. O usuário insere as informações necessárias;
4. O usuário clica no botão "Entrar".

Saída: O sistema registra o cadastro. A página é redirecionada para a página de login. Se o usuário digitar um formato de e-mail inválido, uma mensagem de erro é mostrada. Se uma senha de menos de 8 digítos for inserida, a mensagem de erro é mostrada.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RF02] Cadastro de Empresa

Descrição: Permitir aos usuários o cadastro da empresa.

Entradas: Usuário cadastrado e autenticado no sistema, endereço de e-mail e nome da empresa.

Processo:

1. O usuário acessa a página de empresas;
2. O usuário clica no botão "Criar empresa";
3. O usuário insere o nome da empresa.

Saída: Caso o usuário ainda não possua empresa cadastrada, o sistema exibe um aviso.
O sistema registra o cadastro.
O sistem lista a empresa cadastrada na página de empresas.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RF03] Cadastro de Setor

Descrição: Permitir aos usuários o cadastro de setor.

Entradas: Usuário cadastrado e autenticado no sistema, empresa cadastrada e nome do setor.

Processo:

1. O usuário acessa a página de empresas e clica no botão "Setores";
2. O usuário clica no botão "Adicionar setor";
3. O usuário insere o nome do setor.

Saída: Caso o usuário ainda não possua setor cadastrado, o sistem exibe um aviso.

O sistema registra o cadastro.

O sistema lista o novo setor na página de setores.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RF04] Análise de segurança e de não conformidade

Descrição: Permitir aos usuários a identificação do nível de segurança da informação de sua empresa e do nível de não conformidade dos seus setores.

Entradas: Usuário cadastrado e autenticado no sistema, empresa cadastrada e ao menos um setor cadastrado.

Processo:

1. O usuário acessa a página de setores e clica no botão "Análises";
2. O usuário clica no botão "Nova Análise";
3. O usuário responde as duas perguntas preliminares sobre tratamento de dado e clica em "Prosseguir";
4. O usuário responde as perguntas de segurança e clica em "Avançar";
5. O usuário responde as perguntas sobre cada setor e clica em "Avançar".

Saída: Caso uma das duas perguntas iniciais, sobre tratamento de dados, seja "não", o sistem exibe o aviso: "A LGPD não se aplica à empresa, portanto, caso não deseje, não há necessidade de utilização do questionário".

O usuário escolhe clicar em "voltar"ou "prosseguir".

O sistema exibe o resultado da análise e registra.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RF05] Exclusão de setor

Descrição: Permitir aos usuários a exclusão de um ou mais setores.

Entradas: Usuário autenticado no Sistema e ao menos um setor cadastrado.

Processo:

1. O usuário acessa a página de empresas e clica em "Setores";

2. O usuário clica no botão de exclusão do setor que deseja excluir.

Saída: O sistema exclui o setor e não o lista mais na página de setores.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RF06] Exclusão de análise

Descrição: Permitir aos usuários a exclusão de uma ou mais análises.

Entradas: Usuário autenticado no Sistema e ao menos uma análise realizada.

Processo:

1. O usuário acessa a página de empresas e clica em "Análises";

2. O usuário clica no botão de exclusão da análise que deseja excluir.

Saída: O sistema exclui a análise e não a lista mais na página de análises.

Prioridade:

	Essencial	**X**	Importante		Desejável

---

4. Requisitos Não Funcionais

Requisito Nº: [RFN01] Implementação e tecnologias

Descrição: O sistema deve ser desenvolvido em linguagem de programação PHP juntamente com o framework Laravel, para o *backend*. Para o *frontend* deve ser utilizada a linguagem de programação JavaScript com a estrutura web Next.js. O banco de dados deve ser o MySQL. O desenvolvimento deve ser realizado no editor de código-fonte Visual Studio Code.

Prioridade:

X	Essencial		Importante		Desejável

Requisito Nº: [RFN02] Usabilidade

Descrição: O sistema deverá apresentar informações claras e possuir uma interface que facilite o seu uso.

Prioridade:

X	Essencial		Importante		Desejável