Lucas Biagini Silva

Estudo e Implementação de uma Aplicação para Elaboração de Inventário de Dados Pessoais

Universidade Federal de Pernambuco

secgrad@cin.ufpe.br

portal.cin.ufpe.br/graduacao

Recife

2022

Lucas Biagini Silva

Estudo e Implementação de uma Aplicação para Elaboração de Inventário de Dados Pessoais

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

Área de Concentração: *Engenharia de Software*

Orientador: *Jéssyka Flavyanne Ferreira Vilela*

Recife

2022

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

Silva, Lucas Biagini.
Estudo e Implementação de uma Aplicação para Elaboração de Inventário de Dados Pessoais / Lucas Biagini Silva. - Recife, 2022.
87 : il.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Ciências da Computação - Bacharelado, 2022.

1. Lei Geral de Proteção de Dados Pessoais (LGPD). 2. Inventário de Dados Pessoais (IDP). 3. Processos de Negócios. I. Vilela, Jéssyka Flavyanne Ferreira. (Orientação). II. Título.

000 CDD (22.ed.)

Eu dedico este trabalho à minha mãe Liane e ao meu pai Vandilson.

AGRADECIMENTOS

Gostaria de agradecer à Prof.ª Jéssyka e à Carla Ribeiro pela oportunidade, sugestão do tema e orientação no desenvolvimento deste trabalho, principalmente por toda ajuda e compreensão durante o semestre.

Agradeço aos meus pais por todo o suporte que me deram durante os anos de faculdade, estando sempre presentes nos momentos mais difíceis.

Aos meus amigos e familiares, que também acompanharam de perto a minha saga na graduação.

Aos meus professores que colaboraram com a minha formação profissional. Especialmente a Prof.ª Renata, que me acompanhou durante toda minha formação acadêmica.

Agradeço a todos que, de forma direta ou indireta, participaram dessa fase da minha vida.

"¿Me perdonarás lo que me he perdi'o'? Son dos años ya, tú ya tienes diez"

–Rosalia (G3 N15)

RESUMO

As leis de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e General Data Protection Regulation (GDPR), foram criadas com o intuito de regulamentar o uso de dados pessoais. Uma parte importante para atingir a conformidade com essas leis é a proposição de medidas, salvaguardas e mecanismos de mitigação dos riscos associados ao tratamento de dados pessoais em processos de negócio ou serviços das organizações públicas ou privadas. A Autoridade Nacional de Proteção de Dados (ANPD), regularizada pela LGPD, pode, a qualquer momento, solicitar das organizações um documento chamado Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Para a elaboração desse documento, a LGPD sugere que para cada processo de negócio que realize tratamento de dados seja elaborado um Inventário de Dados Pessoais (IDP). Atualmente, a realização de um IDP é um procedimento manual realizado por meio de planilha de dados, o que dificulta a manutenção e aumenta a chance de erros. Este trabalho propõe a realização de uma revisão bibliográfica sobre os temas Privacidade, Lei Geral de Proteção de Dados Pessoais e Processos de Negócio. Compreender esses assuntos irá servir de base para implementação de uma aplicação *web* que substitua o IDP, a fim de auxiliar na documentação do tratamento de dados na gestão de processos de negócios. O desenvolvimento da aplicação, nomeada de Sistema de Mapeamento de Dados (SMD), foi realizado utilizando as linguagens *PHP* com *Laravel*, *Javascript* com *VueJS* e *MySQL*, seguindo sempre os princípios SOLID presentes em metodologias ágeis de desenvolvimento de *software*. Por fim, observa-se que a utilização de um sistema de mapeamento de dados como o SMD pode contribuir para a sociedade como alternativa substituta à ferramenta de IDP proposta pela Secretaria de Governo Digital (SGD).

Palavras-chave: Lei Geral de Proteção de Dados Pessoais (LGPD). Inventário de Dados Pessoais (IDP). Processos de Negócios.

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ANPD	Autoridade Nacional de Proteção de Dados
BPD	*Business Process Diagram*
BPDM	*Business Process Definition Metamodel*
BPM	*Business Project Management*
BPMI	*The Business Process Management Initiative*
BPMN	*Business Process Modeling Notation*
CAC	Centro de Artes e Comunicação
CF	Constituição Federal
CFCH	Centro de Filosofia e Ciências Humanas
CIn	Centro de Informática
CTG	Centro de Tecnologia e Geociências
DUDH	Declaração Universal dos Direitos Humanos
EPC	*Event Driven Process Chain*
GDPR	General Data Protection Regulation
IDEF3	*Integrated DEFinition Method 3*
IDP	Inventário de Dados Pessoais
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
LGPD	Lei Geral de Proteção de Dados Pessoais
MVP	Produto Mínimo Viável
ONU	Organização das Nações Unidas
Progepe	Pró-Reitoria de Gestão de Pessoas e Qualidade de Vida
Progest	Pró-Reitoria de Gestão Administrativa
Prograd	Pró-Reitoria para Graduação
Propg	Pró-Reitoria de Pós-Graduação
RAD	*Role Activity Diagram*
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
SGD	Secretaria de Governo Digital
SMD	Sistema de Mapeamento de Dados

UE	União Europeia
UFPE	Universidade Federal de Pernambuco
UML	*Unified Modeling Language*

SUMÁRIO

1

INTRODUÇÃO

1.1 CONTEXTO

As novas formas de produção, de armazenamento e de fluxo de dados apresentam desafios à privacidade e à segurança da informação [22]. Particularmente, no que diz respeito à atuação dos próprios detentores dos dados, desenvolvedores, empresas, instituições públicas e das pessoas políticas, estados e países. Tal cenário pode ser observado, especialmente, nas infraestruturas da economia digital contemporânea, nos constantes desenvolvimentos tecnológicos e na globalização [22].

A crescente importância da segurança dos dados no meio digital são previstas em razão das garantias e princípios presentes em dispositivos jurídicos. Neste sentido, observa-se a Declaração Universal dos Direitos Humanos (DUDH), que foi proclamada pela Organização das Nações Unidas (ONU) em 10 de dezembro de 1948 [22]. Este documento internacional elenca o direito à privacidade como uma garantia fundamental a ser assegurada a todos, sem qualquer forma de discriminação.

No ano de 2016, a temática de proteção de dados ganhou ainda mais relevância na União Europeia (UE), tendo em vista a promulgação do Regulamento Geral de Proteção de Dados n° 679/2016 General Data Protection Regulation (GDPR). Este foi um esforço do partido *The Greens*, com o intuito de melhorar o tratamento de dados pessoais de pessoas físicas [22]. Além disso, o regulamento europeu adotou a exigência de que as empresas e países que mantenham relações comerciais com seus membros devem adequar as suas leis para que se equiparem ao nível da legislação europeia [22].

Goddard [12], ao analisar a GDPR e seus impactos globais, definiu **dado pessoal** como

uma informação capaz de reconhecer um indivíduo, direta ou indiretamente, incluindo-se informações que transitam pelo meio virtual e especificamente trazem consigo identificadores digitais. Tais identificadores podem ser os endereços de protocolo de internet (IP), cookies, localizações, dentre outras informações. De acordo com a autora, o conceito de dado pessoal é muito mais vasto e abrangente do que aquele fornecido na legislação que trata de privacidade em vigor nos Estados Unidos.

Para Goddard [12], a conceituação de dado pessoal abrangido pela lei europeia traz significante impacto global e impulso para abordagens cada vez mais éticas no tocante à coleta de dados —- aumentando, assim, a confiabilidade da sociedade no ambiente de dados analíticos. Ao escrever seu texto, menos de um ano após a promulgação da lei, a autora obtém êxito ao prever o impacto que a legislação traria, não apenas para o território da União Europeia, mas impactos significativos para países como o Brasil.

Ainda de acordo com a autora, a GDPR possui seus princípios gerais de proteção de dados, quais sejam: legalidade e justiça, limitação de finalidade, minimização de dados, precisão, limitação de armazenamento e integridade e confidencialidade. Sendo os princípios autoexplicativos e de fácil compreensão, é possível constatar que todos eles giram em torno de uma única proteção que se traduz na proteção de dados produzidos em uma sociedade. A pesquisadora afirma que a operacionalização destes princípios requer um *design* proativo por parte de todos. E, quaisquer exercícios de coleta de dados, bem como mudanças fundamentais no equilíbrio de poder entre organizações e indivíduos, possibilita a expansão dos direitos destes últimos quando o assunto diz respeito aos seus próprios dados pessoais.

Dessa forma, com a promulgação da GDPR, em 2016, pode-se afirmar que houve uma tendência de diversos países em movimentar-se para produzir suas próprias legislações visando a proteção de dados pessoais —- como é o caso do Brasil com a Lei Geral de Proteção de Dados Pessoais (LGPD), que tem grande similaridade com a GDPR [9]. De forma geral, essas regulamentações têm como objetivo principal definir regras para o tratamento de dados pessoais [5] e garantir a proteção e privacidade dos dados de seus próprios cidadãos [9].

Passando à análise em âmbito nacional, em 2018, houve um importante passo para a regulamentação da proteção de dados na legislação brasileira. Naquele ano, foi promulgada a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais, contando com 65 artigos divididos entre dez capítulos e tendo como referência europeia a GDPR [22]. Ao comparar as duas leis, Pinheiro [22] afirma que a norma brasileira, além de mais enxuta, conta com conceitos

menos definidos e interpretações mais amplas, abrindo espaço para dubiedade e subjetividade. A autora cita como exemplo a determinação de prazos, que não é precisa na lei brasileira, que se utiliza de definições abertas como **prazo razoável**, quando comparada com a sua paralela europeia **prazo de 48 horas**.

1.2 MOTIVAÇÃO E JUSTIFICATIVA

A LGPD passou a vigorar no Brasil em 2021, momento a partir do qual empresas e entidades governamentais brasileiras deveriam obrigatoriamente se conformar às normas definidas por aquela legislação, atualizando seus processos de negócios e as formas com que tratam seus dados [6]. Dentre as suas inovações, a LGPD introduziu a necessidade de registrar as operações de tratamento de dados pessoais realizadas pela instituição [6], que podem ser documentadas por meio de um Inventário de Dados Pessoais (IDP) [18], ou também conhecido como *Data Mapping* [8].

Com atualização da LGPD, dada por meio da Medida Provisória nº. 869/2018, transformada na Lei nº. 13.853/2019, foi criada a Autoridade Nacional de Proteção de Dados Autoridade Nacional de Proteção de Dados (ANPD) com o intuito de fiscalizar e garantir que as normas elencadas pela LGPD, semelhante aos mecanismos de fiscalização existentes na União Europeia [22]. Em assim sendo, o Brasil passou a contar com uma estrutura de proteção de dados mais robusta, adequando-se cada vez mais às exigências europeias.

Um recurso importante para fiscalização do cumprimento da lei pela ANPD ocorre através da elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documento fundamental que demonstra que a entidade avaliou os riscos das operações de tratamento de dados em seus processos e serviços e que também registra as medidas adotadas para mitigar os riscos envolvidos [4]. A LGPD elenca os casos em que o RIPD deverá ou poderá ser solicitado: (1) quando o tratamento de dados pessoais realizado pela instituição ocorre para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, com exceções previstas pelo inciso III do art. 4º; (2) quando houver infrações da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos; (3) por fim, a LGPD determina que o RIPD poderá também ser solicitado a qualquer momento pela ANPD, e que o documento deverá conter, no mínimo, a descrição dos tipos dos dados coletados, as metodologias utilizadas para coleta, a garantia da segurança das informações, bem como uma

análise das medidas, salvaguardas e mecanismos que mitigam os riscos [4].

De acordo com o Guia de Boas Práticas da LGPD [4], a elaboração de um RIPD único para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema ou serviço fica à critério da instituição, que pode optar por um RIPD único caso realize o tratamento de uma quantidade reduzida de dados pessoais. De forma geral é recomendado que a criação ou atualização do RIPD seja feita sempre que houver possibilidade de ocorrer impacto na privacidade dos dados pessoais. Para contribuir no desenvolvimento do RIPD, a Secretaria de Governo Digital (SGD) propôs um guia para realização de um IDP, que serve primordialmente para documentar o tratamento de dados pessoais realizados pela instituição, além de ajudar no preparo do RIPD [18]. O IDP tem o objetivo de identificar quais dados são tratados, onde estão e que operações são realizadas com eles [18].

Para auxiliar na realização do mapeamento de dados, existe, segundo o relatório anual de produtos de *software* da área de privacidade da empresa *iapp*, algumas soluções no mercado, como, *2B Advice*, *1touch.io*, *ActiveNav*, *Alation*, *Aparavi*, entre outras [14]. Já a SGD disponibiliza um *template* em formato de planilha de dados para a execução do IDP. Contudo, a utilização de uma planilha para esta tarefa necessita de uma operação manual constante, o que pode dificultar a sua manutenção e aumentar as chances de erros [29]. Diante do exposto questiona-se **qual ferramenta alternativa permite a substituição do template do Inventário de Dados Pessoais fornecido pela Secretaria de Governo Digital?** Portanto, é com o intuito de contribuir na produção e manutenção de um IDP que este projeto propõe o desenvolvimento de uma aplicação web que implementa o *template* fornecido pela SGD.

1.3 OBJETIVOS

A presente pesquisa possui como objetivo geral prover uma ferramenta alternativa que permita a substituição do template de Inventário de Dados Pessoais fornecido pela SGD. Para a concretização deste objetivo geral, propõem-se os seguintes objetivos específicos:

1. Compreender os principais aspectos dos temas Privacidade, Lei Geral de Proteção de Dados Pessoais e Processos de Negócio que sirvam de base para o desenvolvimento de uma ferramenta web que implementa o Inventário de Dados Pessoais;

2. Desenvolver uma aplicação *web* que sirva como uma ferramenta alternativa para substituir o template do Inventário de Dados Pessoais.

1.4 METODOLOGIA

A metodologia a ser aplicada a presente pesquisa foi divida em cinco fases distintas. Inicialmente, foi realizada uma revisão bibliográfica sobre os temas Privacidade, LGPD e Processos de Negócio. Em seguida, iniciaram-se os preparativos para desenvolvimento do *software*, que incluíram definir as *features* que foram trabalhadas, bem como realizar a modelagem do banco de dados e preparar o ambiente de desenvolvimento. Em posse de todos os requisitos necessários, foi realizado o desenvolvimento e teste da aplicação.

1.5 ORGANIZAÇÃO DOS CAPÍTULOS

O presente trabalho está divido entre 5 capítulos: Introdução, Revisão Bibliográfica, Metodologia, Resultados e Conclusão. No próximo capítulo, serão discutidos os temas centrais necessários para o entendimento deste trabalho, bem como apresentação de alguns conceitos técnicos, por meio de revisão bibliográfica.

Embora já tenha sido apresentada neste capítulo de Introdução, a Metodologia será discutida com mais detalhes no capítulo 3. No capítulo 4, sobre o Resultado, será apresentada a aplicação desenvolvida. Por fim, um capítulo de Conclusão, em que será tratado sobre os benefícios da solução, bem como uma discussão sobre trabalhos futuros.

2

REVISÃO BIBLIOGRÁFICA

2.1 PRIVACIDADE

Ferraz Júnior [11], Vieira [28] e Brito [7] trazem como principal definição de privacidade o direito de toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira residente no país de obstaculizar a intromissão de terceiros aos conhecimentos que sejam pertinentes à sua vida privada, bem como o direito de controlar suas informações pessoais a fim de evitar o acesso e divulgação não autorizados. Como vida privada, entende-se *"a vida pessoal e familiar do indivíduo, que pode ser de conhecimento daqueles que desfrutam de sua convivência"* [28].

No caso do acesso não autorizado, a violação da privacidade ocorre uma vez que a aquisição dos dados é ilegítima, e no caso de divulgação não autorizada, a aquisição pode até ser legítima, mas não sua divulgação posterior [28]. A aquisição lícita de dados é prevista no inciso XII Art. 5º da Constituição Federal (CF) [28], que admite a violação do sigilo da correspondência, comunicações telegráficas, comunicações telefônicas e dos dados em caso de ordem judicial para salvaguardar interesses públicos. Ferraz Júnior [11] explicita ainda que é atribuída ao titular dos dados a *"faculdade de resistir à violação do que lhe é próprio"*, que no caso se trata da integridade moral do sujeito. Ainda segundo o autor, ninguém pode ser coagido a revelar informações pessoais e, portanto, a opção por manter sigilo ou a liberdade de negar informação é objeto do direito subjetivo fundamental à privacidade.

Em se tratando de dados pessoais, a privacidade é um aspecto imprescindível para proteção e manutenção dos interesses individuais do sujeito, para que que suas informações sejam tratadas, processadas e exploradas, por quaisquer que sejam as entidades públicas ou privadas, de forma que não resultem em atos discriminatórios. Essas entidades, que por ventura

trabalham com dados pessoais, os utilizam para obter ganho de informação, que por sua vez pode ser utilizada para auxiliar na tomada de decisão. Nesses casos, os dados são considerados como moeda de troca, pois resultam em ganhos estratégicos, comerciais e políticos [7].

Para exemplificar, uma farmácia que pede o número de CPF dos seus clientes ao vender seus produtos, pode conseguir associar, à cada indivíduo, problemas de saúde ou tratamentos que estão sendo realizados apenas baseado no seu padrão de compra. Para uma empresa de plano de saúde, uma base de dados que contém informações sobre possíveis doenças e tratamentos dos indivíduos é de grande valor comercial, pois é de seu interesse econômico cobrar um valor mais caro ou até mesmo negar seus serviços para um indivíduo que vá trazer *"prejuízos"* para a empresa. Já para o indivíduo, a comercialização e utilização dos seus dados pessoais de hábitos de consumo, de maneira discriminatória, apenas traz prejuízos.

Brito [7] aponta que é importante se atentar à falta de segurança e risco de vazamento de informações, que pode levar à uma violação da privacidade uma vez que é possível identificar indivíduos através de informações sensíveis, como, costumes sociais, doenças, preferências religiosas, sexuais, entre outras. O autor ainda deixa claro que os conceitos de segurança e privacidade são de fato temas que se relacionam, porém, podem possuir sentidos opostos: para ter segurança, um indivíduo pode ter que abrir mão da sua privacidade, como, por exemplo, disponibilizar e-mails, históricos de telefonemas e de atividades na web para que autoridades sejam capazes de prover maior segurança em casos de atentados terroristas. Todavia, em se tratando de dados, enquanto a segurança regula o acesso durante o ciclo de vida do dado, a privacidade define como será realizado o acesso. Nesse caso, a privacidade atua como controle de acesso como forma de fornecer segurança. Ademais, a falta de segurança é prejudicial às organizações, pois, em episódios de vazamentos de dados, elas podem sofrer processos legais, prejuízos financeiros, bem como perda de imagem e de clientes [7].

A privacidade é, portanto, uma forma de proteger os interesses do titular dos dados. Na busca de garanti-la como um direito para o cidadão, e controlar o acesso às informações que as organizações detêm o controle [7] em um mundo cada vez mais globalizado e conectado, governos de diversos países vêm criando leis que determinam como realizar e implementar essas garantias. No Brasil, a LGPD entrou em vigor em 2018, com o intuito de garantir e proteger os direitos à liberdade e privacidade de dados, dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado.

Segundo Magacho & Trento [19], a inclusão de um capítulo exclusivo dedicado ao setor

público na LGPD é considerado um momento importante para a história da Administração Pública no Brasil, pois passa a ser regulamentada por regras mais rigorosas a fim de evitar o uso indevido de dados coletados. Uma vez que o setor público detém um grande volume de dados pessoais, supõe-se que os seus sistemas estejam repletos de informações desnecessárias e desatualizadas, tornando as atividades de adequação à lei bastante intensas [19]. A falta de atenção no tratamento de dados pessoais é demonstrada por Queiroz & Motta [23] ao analisar a anonimização de dados aplicada ao Censo da Educação Superior brasileira de 2013 realizado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP). Em seus resultados, os autores verificaram que a anonimização da base de dados é frágil, correndo risco de re-identificação de indivíduos.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

De forma geral, a LGPD [6] traz uma série de determinações quanto à coleta e tratamento de dados, e, naturalmente, punições para o descumprimento da lei, além de indicar a ANPD como órgão responsável pela fiscalização do cumprimento da lei. Ela define o tratamento de dados como qualquer operação sobre dados pessoais, quais sejam de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração [6].

A LGPD [6] define os profissionais responsáveis pelo tratamento de dados os “Agentes de Tratamento”. São eles: o Controlador, pessoa física ou jurídica a quem compete recepcionar os dados e tomar decisões sobre como se dará o tratamento de dados e qual a finalidade; e os Operadores, pessoas física ou jurídica que de fato irão tratar os dados. Além do controlador e dos operadores, existe ainda a figura do Encarregado, que é uma pessoa física ou jurídica, indicada pelo controlador ou operadores para servir de canal de comunicação entre o controlador, os titulares dos dados e a ANPD. A LGPD define também as hipóteses de tratamento de dados, que são os casos em que a lei se aplica, e estabelece requisitos para o tratamento de dados, chamados de bases legais [22].

Quanto ao termo “titular”, entende-se a pessoa cujas informações são objetos de algum tratamento; “tratamento de dados” se refere a toda e qualquer operação e manuseio de dados pessoas, seja ela coleta, produção, recepção, classificação, utilização, acesso, armazenamento,

distribuição, eliminação, dentre outros; os “dados pessoais” são todas as informações que possibilite a identificação de uma pessoa, desde nome e sobrenome a IP, histórico e perfil de compra, dentre outros; “dados pessoais sensíveis” são informações acerca das características da personalidade do indivíduo, a exemplo de opiniões políticas, etnia, religião, sexualidade, dentre outros; “dados anonimizados” se referem aos dados cujo titular não pode ser identificado; “anonimização” é o método utilizado para a retirada de qualquer informação que identifique direta ou indiretamente o titular de um dado; “consentimento” é a manifestação livre, informada e inequívoca por parte de um titular que permite o tratamento de seus dados pessoas para alguma finalidade determinada; por fim, a “transferência internacional de dados” diz respeito à remessa de informação para país ou entidade estrangeira [22].

Como visto previamente, a LGPD possui inspiração na GDPR, na medida em que implementa muitos dos conceitos, estruturas e mecanismos de execução da lei similares à solução Europeia, enquanto tece suas próprias modificações [9]. Ambas enumeram bases legais para o processamento de dados pessoais. Para a GDPR tem-se: (1) consentimento, (2) execução contratual, (3) obrigação legal, (4) proteção da vida, (5) interesse público e (6) interesse legítimo. Enquanto que para a LGPD tem-se: (1) consentimento, (2) obrigação legal, (3) implementação de políticas públicas pela Administração Pública, (4) projetos de pesquisa, (5) execução contratual, (6) exercício de direitos em procedimentos judiciais, (7) proteção da vida, (8) proteção da saúde, (9) interesse legítimo, (10) proteção do crédito e finalmente (11) prevenção à fraude [4, 9].

Outra similaridade entre as duas leis é quanto à definição de dado pessoal: enquanto a GDPR o define de forma bastante ampla *”qualquer dado sobre um indivíduo é considerado um dado pessoal”*, a LGPD o faz de maneira mais concisa, definindo-o como *“qualquer informação acerca de uma pessoa natural identificada ou identificável”* [9]. Por fim, ambas as leis possuem um escopo extraterritorial: no caso da LGPD, por exemplo, a lei aplica-se para qualquer entidade no Brasil ou que atua no Brasil e que realiza coleta de dados pessoais de indivíduos no país [9].

Ambas as leis possuem também pontos em que se divergem e nota-se a forma mais branda com que a LGPD trata sobre vazamento de dados, regula a ANPD e aplica multas em casos de descumprimento. Enquanto a GDPR determina que um vazamento de dados deve ser notificado em até 72 horas, a LGPD indica que um incidente de segurança que possa ocasionar em risco deve ser avisado em um período de tempo razoável. Uma outra característica da LGPD é a agência reguladora ANPD estar sob ordem do Poder Executivo, o que compromete a parcialidade da aplicação da lei. Por isso, Erickson [9] sugere uma transferência do órgão

regulador para o Poder Judiciário, agregando, assim, maior confiabilidade. Por fim, enquanto as multas da GDPR podem ser de 20 milhões de euros ou 4% do faturamento anual global da empresa (o que for maior), a LGPD possui valor aplicável de multa de até 2% sob faturamento anual no Brasil, não excedendo 50 milhões de reais [9, 22].

Diferenças à parte, constata-se a influência global que a GDPR ocasionou, pois passa a exigir um nível de legislação do mesmo nível que o seu de países e empresas que desejam manter relações comerciais com a UE. Muito embora o Brasil já tivesse legislações que tratassem sobre privacidade e tratamento de dados, como o Marco Civil da Internet [3] e a Lei de Cadastro Positivo [2], a LGPD inova na medida que padroniza de forma objetiva e concisa os critérios que determinam *"se houve ou não guarda, manuseio e descarte [de dados] dentro dos padrões mínimos de segurança condizentes"* [22].

As **bases legais** para o tratamento de dados pessoais são hipóteses elencadas pela LGPD que autorizam o tratamento de dados pelo agente, e que antes de inicia-lo deve se certificar que a **finalidade da operação** esteja apresentada de forma clara e seus propósitos especificados e esclarecidos para o titular dos dados [4]. De acordo com o Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD) [4] da SGD, no caso da Administração Pública, o tratamento de dados é feito principalmente com a finalidade relacionada à execução de políticas públicas, cumprimento de obrigação legal ou regulatória pelo controlador. E, nesses casos, dispensa consentimento do titular dos dados. Ainda sobre a dispensa do consentimento, o órgão público que coleta os dados deve informar claramente quais dados, com quem os está compartilhando. E mais, o órgão que solicita acesso aos dados deve justificar esse acesso, descrevendo o motivo e explicar o uso que será feito com esses dados. Ainda sobre a hipótese do tratamento mediante consentimento do titular, uma vez que esse consentimento não seja dispensado, "o titular tem a chance real de escolha sobre o tratamento de seus dados" [4]. Para ser considerado válido, o consentimento deve ser dado de forma clara, explícita e inequívoca e qualquer autorização genérica será considerada nula.

Definidas as hipóteses de tratamento de dados, o passo seguinte é a operação de **coleta**, que deve ser realizada somente mediante o atendimento das hipóteses e representa a etapa inicial do ciclo de vida do tratamento. Em seguida, devem ser aplicadas aos dados coletados, técnicas de **anonimização e pseudoanonimização**, para que não haja possibilidade de associação direta ou indireta a um indivíduo.

Por fim, para verificar se o tratamento de dados realizado pela entidade está em con-

formidade com a LGPD, a qualquer momento, a ANPD pode exigir o RIPD. Para produzir o relatório, é necessário fazer um mapeamento dos dados nos processos de negócios ou serviços da organização que trata os dados. A SGD propõe um artefato chamado IDP para que seja possível mapear, para cada processo de negócio, os dados pessoais tratados e verificar se está em conformidade com a LGPD [22]. A utilização desse artefato, contudo, não é obrigatória e serve apenas como subsídio para produzir o RIPD [18].

2.3 PROCESSOS DE NEGÓCIOS

Na área da administração, existem várias definições para processos de negócios e, de maneira geral, pode ser definido de forma ampla como uma sequência de atividades administrativas que possuem entrada e saída e que agregam valor para um grupo específico de pessoas [1, 25, 26]. Tais atividades podem compreender *"entrar em contato com fornecedores, processar diversos tipos de dados ou até mesmo realizar a entrega de produtos na residência de um cliente"* [1] e para este trabalho, interessa os processos que possuam como parte de suas tarefas o tratamento de dados pessoais.

Além de tarefas, essas atividades que compõem um processo de negócio podem envolver os recursos, os indivíduos, bem como outros elementos, como, *softwares* [25]. Segundo Squizani & Sarturi Prass [25], um processo tem como objetivo agregar valor e o pode fazer através de um produto ou serviço, bem como auxiliar no gerenciamento de outros processos. Com isso, uma organização que utiliza esse tipo de abordagem consegue reduzir seus custos, administrar melhor seu tempo e incrementar a qualidade, gerando maior flexibilidade e permitindo uma maior habilidade para as mudanças [26]. Tessari [26] ressalta que, para os consumidores, não importa como se dá o gerenciamento de uma organização e estes estão apenas preocupados com o valor que será gerado. Porém, dentro de muitas organizações não existe um cargo específico preocupado em gerar valor e é nesse sentido que se tem a importância da utilização de processos — há um olhar geral para o processo por completo, ou seja, os envolvidos no processo têm uma visão geral do mesmo [25]. Foi para melhor gerenciar os processos de negócios dentro de uma organização, seja ela do setor público ou privado, que surgiu a teoria do *Business Project Management* (BPM), que abrange desde a descoberta até a criação do projeto e a entrega dos processos de negócios [26].

A modelagem de processos é uma etapa importante do BPM, que consiste em representar

o processo de forma estruturada, podendo ser através de diagramas de fluxo de dados, especificações em português estruturado, entre outros, e tais técnicas seguiram avançando durante os anos, tornando-se cada vez mais consistentes [26]. Segundo Tessari [26], modelos de processos descrevem o funcionamento de uma organização e como se dá a execução de várias tarefas por atores como, pessoas, organizações e sistemas. Ainda na etapa da modelagem deve ser possível representar as subtarefas realizadas pelos atores, considerando que elas podem ocorrer de forma paralela ou sequencialmente, incluindo-se também repetição de tarefas.

Considera-se, portanto, que uma boa técnica de modelagem deve ser apta a representar as diversas situações de um processo [26]. Além disso, um modelo pode revelar anomalias, inconsistências, ineficiências e oportunidades de melhorias, compartilhando conhecimento através da empresa. Todavia, há também razões pelas quais certas organizações decidem não aderir à modelagem de processos: demanda tempo; custo financeiro; falta sincronia com a área de TI; certos negócios mudam rápido de mais [26].

Algumas técnicas e notações de modelagem de processos mais notórias são: *Unified Modeling Language* (UML), *Business Process Definition Metamodel* (BPDM), *Business Process Modeling Notation* (BPMN), *Event Driven Process Chain* (EPC), *Integrated DEFinition Method 3* (IDEF3), *Petri Net* e *Role Activity Diagram* (RAD) [26]. Dentre essas metodologias de modelagem de processo, destaca-se o BPMN, desenvolvida pelo *The Business Process Management Initiative* (BPMI), cuja principal preocupação é ser de fácil utilização e entendimento por todos os usuários de negócios, bem como ser capaz de modelar processos complexos [26]. O BPMN trata-se de uma notação gráfica capaz de gerar um diagrama de processos conhecido como *Business Process Diagram* (BPD), que consiste em um conjunto de elementos gráficos capazes de compor diagramas.

2.4 INVENTÁRIO DE DADOS PESSOAIS

De forma geral, o IDP registra as operações de tratamento de dados pessoais realizadas pela instituição e envolve descrever informações como (1) identificação do serviço/processo; (2) identificação dos agentes de tratamento e encarregado; (3) atuação do operador no clico de vida do dado pessoal; (4) fluxo de tratamento dos dados pessoais; (5) escopo e natureza dos dados pessoais; (6) finalidade do tratamento dos dados pessoais; (7) categorias de dados pessoais; (8) categorias de dados pessoais sensíveis; (9) frequência e totalização das categorias

de dados pessoais tratados; (10) categorias de titulares de dados pessoais; (11) compartilhamento de dados pessoais; (12) medidas de segurança/privacidade; (13) transferência internacional de dados pessoais; (14) contratos (Figura 1) [18]. Além disso, atualização do IDP é recomendada que seja feita no mínimo anualmente ou quando houver atualização no processo, para que o inventário esteja sempre em conformidade com a realidade do tratamento de dados realizado nos processos da instituição [18].

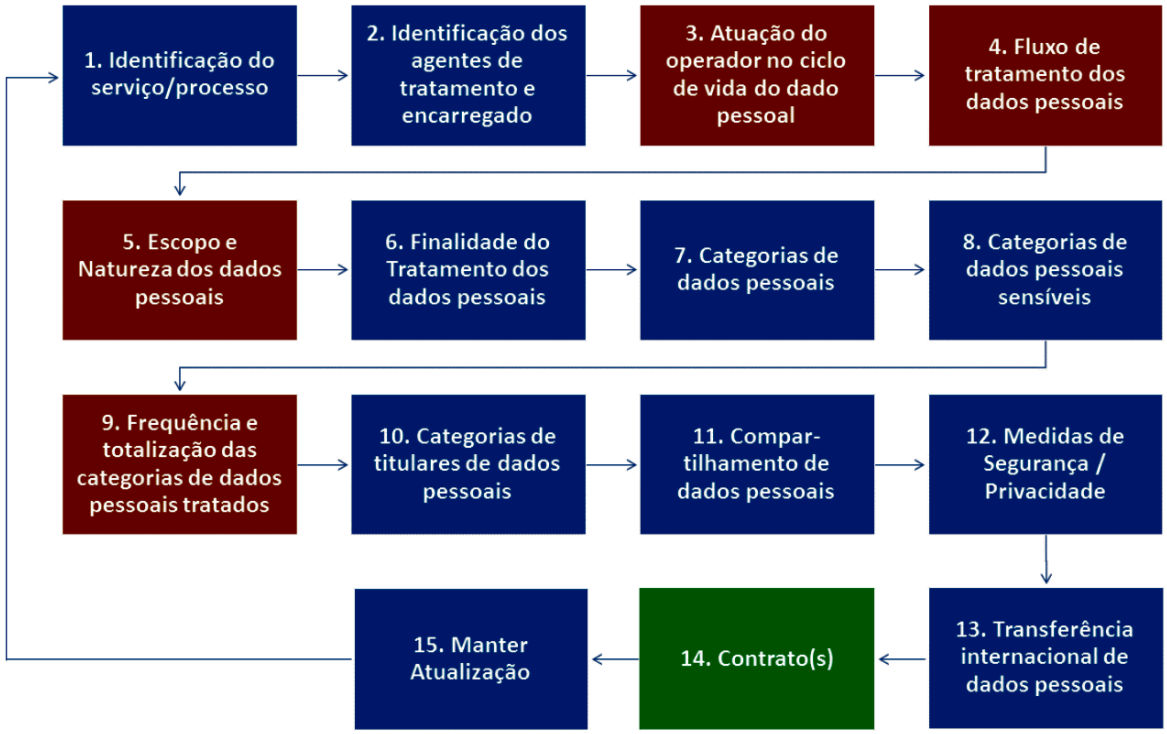

Figura 1: Fases de elaboração do Inventário de Dados Pessoais. Fonte: [18, p. 8]

O ciclo de vida do tratamento de dado pessoal inclui as fases coleta, retenção, processamento, compartilhamento e eliminação [18]. É necessário, então, identificar em quais fases do ciclo de vida os operadores atuam (Figura 2).

Figura 2: Ciclo de vida do tratamento dos dados pessoais. Fonte: [4, p. 45]

Na fase de coleta, tem-se as operações de coleta, produção ou recepção de dados pessoais, podendo ser provenientes de documento em papel, documento eletrônico, sistema de informação, etc. [4]. A fase de **retenção** configura o arquivamento ou armazenamento de dados. A fase de

processamento engloba operações como classificação, utilização, reprodução, processamento, avaliação e modificação. As operações de transmissão, distribuição, comunicação, transferência e difusão estão presentes na fase de **compartilhamento**, e, por fim, chega-se na fase de **eliminação** dos dados pessoais.

3

METODOLOGIA

3.1 REVISÃO BIBLIOGRÁFICA

Inicialmente, foi feita uma revisão bibliográfica dos temas: Privacidade, Processos de Negócios, LGPD e Inventário de Dados Pessoais. O entendimento destes assuntos específicos permitiu o conhecimento de uma série de conceitos que embasaram e favoreceram o desenvolvimento de uma aplicação web em substituição ao template do IDP.

3.2 TECNOLOGIAS UTILIZADAS

Para desenvolver a aplicação web proposta foram utilizadas como principais linguagens de programação: *PHP*, *Javascript* e *MySQL*. Para o desenvolvimento do *backend* foi escolhida a linguagem de *PHP* através do framework *Laravel* e, para o *frontend*, a linguagem de *Javascript* através do framework *VueJS*, com o código escrito em *Typescript*.

Foram usadas também bibliotecas de terceiros como *Spatie*, biblioteca para *Laravel* que implementa *features* de permissões e perfis; *DomPDF*, biblioteca para *PHP* que implementa funcionalidades relacionadas à geração de arquivo *PDF*; *Vue-Bootstrap*, um *wrapper* que integra a biblioteca de *Bootstrap* com *Vue*; *Vue-multiselect*, biblioteca para *vue* que implementa um *select* capaz de buscar as opções através de uma chamada *AJAX*; *Vue-Sweetalert2*, biblioteca também para *vue* que implementa notificações e alertas para o usuário.

3.2.1 PHP

PHP (Hypertext Preprocessor) é uma linguagem de *script* utilizada, principalmente, no desenvolvimento web [27] de múltiplos paradigmas: imperativo; funcional; orientado a objetos; procedural; e, refletivo [20].

Atualmente, embora ainda muito requisitada para manutenção de sistemas *Legacy*, *PHP*, os desenvolvedores preferem fazer uso das tecnologias e linguagens mais recentes e que se mostram como tendências do que manter sistemas mais antigos [16]. Contudo, *PHP* possui ainda uma das maiores comunidades de desenvolvedores ativos e passa por constantes modernizações e manutenções. Prova disso é o *PHP-FIG*, um grupo de representantes dos frameworks de *PHP* mais importantes que define recomendações e padrões a serem seguidos no desenvolvimento desses frameworks [21].

3.2.2 Laravel

Laravel é, atualmente, o framework mais utilizado de *PHP* e, também, a que possui a maior comunidade online. É utilizada por empresas como *Disney*, *Warner Bros* e *The New York Times* [17]. Um framework web nada mais é que um conjunto de bibliotecas escritas naquela linguagem que proporcionam, por sua vez, ferramentas para o desenvolvimento de uma aplicação web [13]

A praticidade de se trabalhar com um framework está no fato de que, com as bibliotecas disponíveis e junto à comunidade que a utiliza, é possível fazer o reuso de código para funcionalidades padrão. Tal situação tem a finalidade de acelerar de acelerar o desenvolvimento da aplicação, cortando caminho ao não necessitar trabalhar em *features* como autenticação, gerenciamento de sessão, de rotas, de requisições, etc [13]. Ou seja, muitas das *features* presentes em todos os projetos já estão prontas esperando apenas para serem configuradas, sem haver necessidade de perder tempo desenvolvendo-as. É possível, então, focar em trabalhar apenas as *features* da lógica de negócios da aplicação.

3.2.3 PHPStorm

O *PhpStorm*, da empresa *JetBrains*, foi a IDE utilizada para escrever todo o código produzido neste trabalho. Uma IDE, em português, Ambiente de Desenvolvimento Integrado,

é um software que possui funcionalidades que auxiliam no desenvolvimento. Funcionalidades estas que incluem editar o código fonte, gerar código, compilar, depurar, testaar e refatorar [15].

3.2.4 VueJS

VueJS é um framework de javascript que auxilia no desenvolvimento do *frontend*, ou seja, da interface da aplicação. É um framework moderno, cuja característica principal é a capacidade de separar partes da interface em componentes reativos. Estes útimos são capazes de serem replicados e modularizados a fim de facilitar o desenvolvimento e a manutenção do código [10].

3.3 REQUISITOS E ABORDAGEM SOLID

Antecedendo o início do desenvolvimento, foram definidos todos os requisitos desejáveis da aplicação e uma seleção daqueles que entrariam no escopo do MVP. Foi determinado também que, ao longo do desenvolvimento, seria seguido os princípios SOLID, acrônimo de cinco princípios para desenvolvimento de softwares orientados à objeto e presente em metodologias ágeis [24]: (1) *Single-responsibility principle*, em que uma classe deve ter uma única responsabilidade; (2) *Open-closed principle*, que diz que uma entidade deve estar aberta para extensão e fechada para modificação, ou seja, deve-se poder mudar o comportamento de um módulo sem que se altere o código-fonte; (3) *Liskov-substitution principle*, em que um método, que utiliza um ponteiro ou referência à uma classe base, deve poder utilizar objetos de classes que derivam da classe base sem que seja modificado; (4) *Interface segregation principle*, evitar que objetos dependam de classes cuja interface possui métodos que não são utilizados; e, por fim, (5) *dependency inversion principle*, em que classes de alto e baixo nível devem depender sempre de abstrações, tornando o código menos acoplado e facilitando sua manutenção no futuro.

4

RESULTADO

Foi desenvolvido uma aplicação web, nomeada de Sistema de Mapeamento de Dados (SMD), o qual implementa o Inventário de Dados Pessoais (IDP) sugerido pela Secretaria de Governo Digital (SGD). Desta forma, serão apresentados os requisitos propostos para o desenvolvimento da aplicação, assim como aqueles que foram selecionados para compor o escopo do Produto Mínimo Viável (MVP) da aplicação. Em seguida, há uma apresentação das arquiteturas e, também, de algumas regras de negócio.

4.1 PROPÓSITO

A aplicação possui como propósito principal servir de alternativa para o IDP da SGD. Para isso, a aplicação desenvolvida deve, para cada processo de negócio em que há tratamento de dados pessoais, ser capaz de: (1) cadastrar o processo; (2) preencher as informações sobre o tratamento de dados do processo; (3) homologar o processo ou arquivá-lo. Com essas três funcionalidades, é possível manter um registro de todos os processos da organização.

Observa-se que uma organização, seja ela pública ou privada, está internamente dividida em diversos setores. Na Universidade Federal de Pernambuco (UFPE), por exemplo, existem (1) as pró-reitorias, como, Pró-Reitoria para Graduação (Prograd), Pró-Reitoria de Pós-Graduação (Propg), Pró-Reitoria de Gestão Administrativa (Progest), Pró-Reitoria de Gestão de Pessoas e Qualidade de Vida (Progepe), etc.; (2) os centros acadêmicos, como, Centro de Artes e Comunicação (CAC), Centro de Filosofia e Ciências Humanas (CFCH), Centro de Informática (CIn), Centro de Tecnologia e Geociências (CTG), etc.; e (3) órgãos suplementares, como, Biblioteca Central, Editora da UFPE, Hospital das Clínicas e o Núcleo de Saúde Pública. Por

usa vez, cada um dessas pró-reitorias, centros acadêmicos e órgãos suplementares possuem seus próprios setores e outras subdivisões que atendem as suas particularidades. Além disso, dentro dos setores, os servidores podem exercer diferentes atividades a depender de seus cargos. Isso inclui também o cenário de que alguns deles podem ter acessos restringidos a dados ou, até mesmo, acesso total, como pode ser o caso de um cargo de chefia, por exemplo.

Visando este exemplo de uma organização com diferentes setores, a aplicação desenvolvida deve ser capaz de (1) criar, editar, ativar e desativar *Setores*; (2) criar, editar, ativar e desativar *Perfis* de *Usuários*; (3) vincular *Permissões* a um *Perfil*; e, por fim, (4) atribuir um *Perfil* em um *Setor* a um *Usuário*.

Os requisitos da aplicação foram divididos em duas partes: requisitos gerais e requisitos de IDP. Os requisitos gerais englobam as funcionalidades não-relacionadas ao cadastro de dados do IDP, como, acesso à aplicação e gerenciamento (listagem, cadastro, visualização e edição) de 4 entidades básicas: Usuário, Perfil, Permissão, Setor e Processo. Além das funcionalidades, espera-se que com a aplicação seja possível gerenciar *Processos*, *Usuários*, *Perfis* e *Setores* de uma instituição.

4.2 CICLO DE VIDA DO PROCESSO

Os requisitos do IDP envolvem todo o cadastro dos dados do processo presente o template do IDP fornecido pela SGD. Envolve também o fluxo do status processo: pendente, em análise, homologado e arquivado. Um processo, ao ser criado, inicia com status “pendente”, em que é possível editar cada uma das seções do IDP. O operador, ao finalizar o preenchimento do IDP, deve solicitar a análise do IDP e, nesse momento, o processo passa para o status “Em Análise”.

No processo de análise, os formulários nas seções do IDP ficam desabilitados e só é possível “Aprovar” ou “Rejeitar” a seção. Caso seja rejeitada, é necessário escrever uma justificativa para que, quem for revisar a seção rejeitada, entenda como proceder na correção. Ainda no caso de ter uma seção rejeitada, o processo deve ser “Rejeitado” e, quando o analista o rejeitar, o status do processo volta para pendente.

Novamente, o operador pode entrar no processo e editar apenas as seções que foram rejeitadas, para, então, solicitar novamente a análise. Em nova análise, o analista pode rejeitar quaisquer seções ou aprovar aquelas que foram corrigidas. Em caso de todas as seções estarem aprovadas, o analista pode “Homologar” o processo, e, em o fazendo, o processo muda de status

para “Homologado”.

Uma vez que o processo estiver com status de “Homologado”, é possível solicitar nova análise e o processo muda para status “Pendente”. A qualquer momento, é possível arquivar um processo ou desarquivar um processo arquivado. Na imagem abaixo pode-se visualizar o ciclo de vida de um processo (Figura 3).

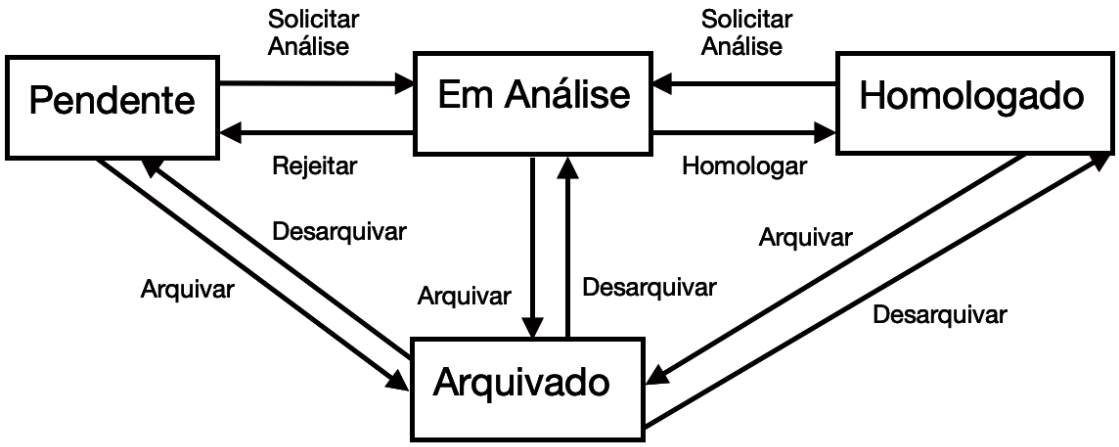

Figura 3: Ciclo de vida do status de um processo

4.3 PERFIS E PERMISSÕES

Na aplicação, é possível gerenciar Perfis e Permissões. As Permissões são as ações que podem ser feitas dentro do *software*, como, gerenciar usuários, gerenciar perfis, gerenciar setores, gerenciar processos, etc. Ao gerenciar um Perfil, há a opção de criar, editar, ativar ou desativar e atribuir as permissões desejadas ao Perfil. Existem dois perfis na aplicação que são essenciais para a manutenção do sistema: **admin** e **Administrador**.

O perfil de **admin** é atribuído ao usuário de email *admin@ufpe.br* e não pode ser atribuído a nenhum outro usuário através da plataforma, apenas manualmente e diretamente no banco de dados. O perfil de **admin** tem poder total na aplicação: acesso a todos os processos, acesso a todos os setores e possui todas as permissões.

Já o perfil de **Administrador** possui, por predefinição, todas as permissões atribuídas a si, porém, diferente do **admin**, é um perfil que pode ser atribuído a um usuário através da aplicação normalmente como qualquer outro perfil. Contudo, o perfil de **Administrador** não

aparece na listagem de perfis, pois não é possível editar suas informações nem as permissões atribuídas a ele.

De forma geral, os perfis foram pensados para refletir os cargos dos funcionários em cada setor de uma organização. A priori, para tornar um perfil o equivalente a um **Operador** definido pela Lei Geral de Proteção de Dados Pessoais (LGPD), deve ser necessário atribuir ao perfil as permissões de gerenciamento de processos. As permissões de gerenciamento de Perfis, Setores e Usuários não caberia ao Operador, por exemplo, pois ficariam a cargo de um perfil que refletisse o gestor do setor.

4.4 REQUISITOS

Para apresentar os requisitos desejados para aplicação, foi utilizada a técnica de descrição através de *User Stories*, muito utilizada em metodologias ágeis de desenvolvimento *software*. Assim, os *user stories* foram divididos em *Epics*: (1) Acesso ao Sistema, (2) Gerenciar Setores, (3) Gerenciar *Perfis*, (4) Gerenciar Permissões, (5) Gerenciar *Usuários*, (6) Gerenciar Processos, (7) Gerenciar Dados do Processo e (8) Gerenciar Ciclo de Vida do Processo.

1. Acesso ao Sistema
    - Primeiro Acesso
        - Como um usuário do sistema sem acesso, eu gostaria de me cadastrar para começar a usar o sistema.
    - Login
        - Como um usuário do sistema, eu gostaria de fazer login para poder ter acesso ao sistema.
    - Recuperar Senha
        - Como usuário do sistema, eu gostaria de recuperar a senha para poder re-obter acesso ao sistema.
    - Logout
        - Como usuário do sistema, eu gostaria de realizar logout na aplicação para que a minha sessão seja excluída do servidor.
    - Logout por Inatividade

        - Como um usuário do sistema, eu gostaria de ter minha sessão excluída automaticamente após um determinado tempo de inatividade para que o acesso ao sistema seja interrompido de forma automática.
    - Preencher *Perfil*
        - Como um usuário, eu gostaria de preencher informações do meu perfil para facilitar a aprovação do meu perfil pelo gestor responsável.

2. Gerenciar Setores
    - Listar Setores
        - Como um usuário, eu gostaria de listar os setores cadastrados para que seja possível ativar, inativar ou visualizar um setor.
    - Cadastrar Setor
        - Como um usuário, eu gostaria de cadastrar um setor para que seja possível associar usuários a um setor, bem como cadastrar processos em um setor.
    - Visualizar Setor
        - Como um usuário, eu gostaria de visualizar um setor para que seja possível editar suas informações.
    - Editar Setor
        - Como um usuário, eu gostaria de editar as informações de um setor para que o mesmo tenha informações corretas e atualizadas.
    - Ativar/Desativar Setor
        - Como um usuário, eu gostaria de ativar ou desativar um setor para que usuários de um determinado setor possam facilmente ser também ativados ou desativados de maneira *global*.

3. Gerenciar *Perfis*
    - Listar *Perfil*

        - Como um usuário, eu gostaria de listar os perfis cadastrados para que seja possível visualizar, editar, ativar e desativar um perfil.
    - Cadastrar *Perfil*
        - Como um usuário, eu gostaria de cadastrar um perfil para que ele seja atribuído a um usuário.
    - Editar *Perfil*
        - Como um usuário, eu gostaria de editar um perfil para poder atualizar suas informações.
    - Ativar/Desativar *Perfil*
        - Como um usuário, eu gostaria de ativar ou desativar um perfil para que usuários com um determinado perfil possam facilmente ser também ativados ou desativados de maneira *global*.

4. Gerenciar Permissões
    - Listar Permissões
        - Como um usuário, eu gostaria de listar as permissões para poder atribuí-las a um determinado perfil.

5. Gerenciar *Usuários*
    - Visualizar *Usuário*
        - Como um usuário, eu gostaria de visualizar um usuário para poder acessar as informações do mesmo.
    - Editar *Usuário*
        - Como um usuário, eu gostaria de editar as informações de um usuário para poder mudar o perfil, setor, nome ou mesmo ativá-lo ou desativá-lo caso necessário.
    - Listar *Usuários*
        - Como um usuário, eu gostaria de listar os usuários cadastrados para que seja possível inativar, reativar ou atribuir perfil e setor a um usuário.

- Desativar *Usuário*
    - Como um usuário, eu gostaria de desativar um usuário para que o mesmo perca acesso à aplicação.
- Ativar *Usuário*
    - Como um usuário, eu gostaria de ativar um usuário para que o mesmo ganhe acesso à aplicação.
- Atribuir *Perfil* e Setor a um *Usuário*
    - Como um usuário, eu gostaria de atribuir um perfil em determinado setor a um usuário para que o mesmo tenha, para o setor escolhido, permissões definidas de acordo com o novo perfil atribuído.

6. Gerenciar Processos

- Listar Processos
    - Como um usuário, eu gostaria de listar os processos cadastrados no sistema para que eu possa gerenciar os dados do processo, bem como visualizar, arquivar ou desarquivar um processo.
- Cadastrar Processo
    - Como um usuário, eu gostaria de cadastrar um processo para que eu possa realizar o mapeamento de dados do mesmo.
- Visualizar Processo
    - Como um usuário, eu gostaria de visualizar um processo para que eu possa verificar com rapidez os principais dados de um processo.
- Editar Processo
    - Como um usuário, eu gostaria de editar um processo para que as informações, como, nome e arquivo de imagem do processo, estejam sempre atualizados.
- Filtrar lista de Processos por Status

        - Como um usuário, eu gostaria de filtrar a lista de processos por status para encontrar mais facilmente um processo a partir do seu status.

7. Gerenciar Dados do Processo

    - Cadastrar Agentes de Tratamento e Encarregado

        - Como um usuário, eu gostaria de cadastrar as informações do Controlador para que fique registrado quem é o Controlador no processo especificado.
        - Como um usuário, eu gostaria de cadastrar as informações do Encarregado para que fique registrado quem é o Encarregado no processo especificado.
        - Como um usuário, eu gostaria de cadastrar as informações de um ou mais Operadores para que fique registrado quem são os Operadores no processo especificado.

    - Cadastrar Fases do Clico de Vida do Operador

        - Como um usuário, eu gostaria de cadastrar informações sobre as fases do ciclo de vida do Operador para indicar em quais fases do ciclo de vida do tratamento do dado cada Operador atua.

    - Cadastrar Fluxo de Tratamento dos Dados

        - Como um usuário, eu gostaria de cadastrar informações sobre o fluxo de tratamento dos dados para especificar uma descrição e carregar arquivos necessários para o entendimento do fluxo de dados.

    - Cadastrar Escopo e Natureza dos Dados Pessoais

        - Como um usuário, eu gostaria de cadastrar informações sobre o escopo e natureza dos dados pessoais para que seja possível descrever a (1) abrangência da área geográfica e a (2) fonte de dados utilizada para a obtenção de dados pessoais.

    - Cadastrar Finalidade do Tratamento de Dados Pessoais

        - Como um usuário, eu gostaria de cadastrar informações sobre a finalidade do tratamento de dados pessoais para que seja possível descrever (1) as hipóteses de tratamento, (2) a finalidade, (3) a previsão legal, (3) os resultados pretendidos para o titular de dados e (4) os benefícios esperados para o órgão entidade ou para a sociedade como um todo.

- Cadastrar Categoria de Dados Pessoais
    - Como um usuário, eu gostaria de cadastrar informações sobre a categoria de dados pessoais (incluindo dados pessoais sensíveis) para que seja possível (1) fornecer uma breve descrição sobre o dado sendo tratado, (2) o tempo de retenção dos dados, (3) a fonte de retenção e (4) o nome da base de dados se a principal fonte de retenção dos dados for uma base de dados.
- Cadastrar Frequência e Totalização das Categorias de Dados Pessoais Tratados
    - Como um usuário, eu gostaria de cadastrar informações sobre a frequência e totalização das categorias de dados pessoais tratados para que seja possível descrever (1) a frequência de tratamento dos dados pessoais e (2) a quantidade de dados pessoais e dados pessoais sensíveis tratados.
- Cadastrar Categorias dos Titulares de Dados Pessoais
    - Como um usuário, eu gostaria de cadastrar as categorias dos titulares de dados pessoais para que seja possível descrever a qual categoria o titular dos dados pertence, como, pessoa com deficiência ou pessoa de baixa renda. Deve ser possível também informar se o processo trata dados de crianças, adolescentes ou outros grupos vulneráveis.
- Cadastrar Compartilhamento de Dados Pessoais
    - Como um usuário, eu gostaria de cadastrar informações sobre o compartilhamento de dados pessoais para que seja possível descrever (1) com quais instituições os dados são compartilhados,

(2) quais dados são compartilhados e (3) qual a finalidade do compartilhamento.

- Cadastrar Medidas de Segurança e Privacidade
  - Como um usuário, eu gostaria de cadastrar as medidas de segurança e privacidade para que seja possível descrever quais os tipos e medidas de segurança e privacidade adotados no tratamento de dados do processo de negócio.
- Cadastrar Transferência Internacional de Dados pessoais
  - Como um usuário, eu gostaria de cadastrar informações sobre transferência internacional de dados pessoais para que seja possível informar (1) para quais organizações internacionais há transferência de dados, (2) o país da organização, (3) quais dados pessoais são transferidos e (4) o tipo de garantia para transferência.
- Cadastrar Contratos de Serviços e/ou Soluções de TI
  - Como um usuário, eu gostaria de cadastrar informações sobre contratos de serviços e/ou soluções de TI adotadas em um processo para que seja possível informar (1) o número do processo que referencia a documentação da contratação e (2) o objeto do contrato.

8. Inventário de Dados Pessoais

- Solicitar Análise do IDP
  - Como um usuário, eu gostaria de solicitar análise do IDP para que seja possível que um usuário com permissão de análise possa avaliar cada sessão do IDP.
- Homologar Seção do IDP
  - Como um usuário, eu gostaria de homologar uma seção do IDP para indicar que aquela seção está em correta.
- Rejeitar Seção do IDP

        - Como um usuário, eu gostaria de rejeitar uma seção do IDP para indicar que aquela seção contém erros.
        - Como um usuário, ao rejeitar uma seção eu gostaria de registrar uma mensagem destinada ao usuário que fará a correção para que seja possível indicar exatamente o que precisa ser corrigido.
    - Homologar IDP
        - Como um usuário, eu gostaria de homologar um IDP para que o processo mude de status de **Em Análise** para **Homologado**.
    - Rejeitar IDP
        - Como um usuário, eu gostaria de rejeitar um IDP para que o processo mude de status de **Em Análise** para **Pendente**.
    - Arquivar IDP
        - Como um usuário, eu gostaria de arquivar um processo para que o mesmo fique com status de **Arquivado** e desapareça da listagem não-filtrada de processos.
    - Desarquivar IDP
        - Como um usuário, eu gostaria de desarquivar um processo para que o mesmo fique com o status que possuía antes do arquivamento e apareça na listagem não-filtrada de processos.
    - Gerar PDF
        - Como um usuário, eu gostaria de gerar um arquivo em PDF do IDP para que seja possível guardar uma cópia digital das informações de tratamento de dados do Processo.

4.5 BANCO DE DADOS

A entidade *Usuário* guarda as informações pessoais e credenciais de acesso do *Usuário* (nome, e-mail e senha), a entidade *Permissão* guarda informações sobre permissões. Significa que cada objeto *Permissão* está atrelado à uma funcionalidade única da aplicação, a entidade

Perfil serve para atrelar diversas *Permissões* e a entidade *Processo* guarda informações sobre o processo a ser mapeado. Tem-se, então, as seguintes relações entre as entidades (Figura 4):

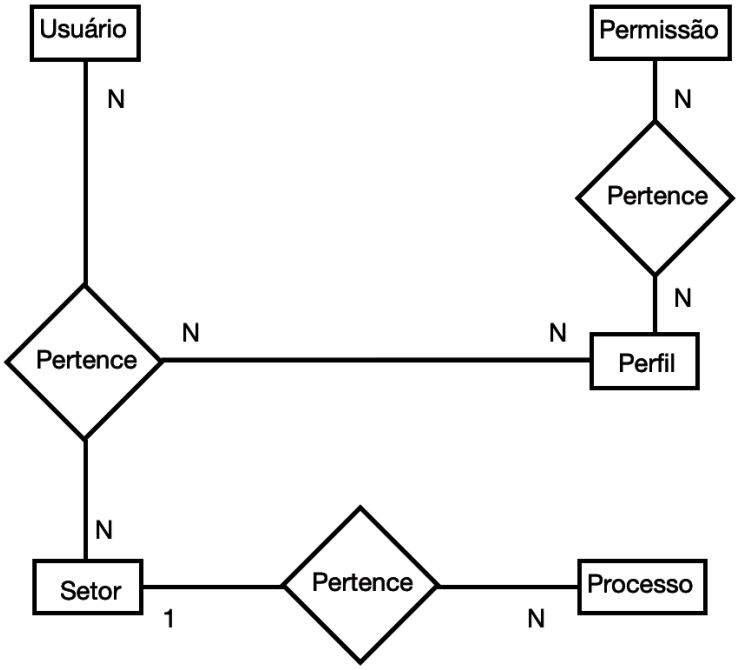

Figura 4: Esquema relacional do banco de dados

- Um *Usuário*, associado a um *Setor*, possui um determinado *Perfil*; um *Usuário* pode estar associado a mais de um *Setor*; e, cada relação *Usuário-Setor* pode estar associada a mais de um *Perfil*.
- Um *Perfil* possui muitas *Permissões* e uma *Permissão* pertence a muitos *Perfis*.
- Um *Setor* possui muitos *Processos* e um *Processo* pertence à um único *Setor*.

O esquema relacional se dá da seguinte forma:

Usuário (id, nome, email, email_verified_at, password, remember_token, status)

Setor (id, nome, descrição)

SetorUser (id, setor_id, user_id)

setor_id referencia id em *Setor*

user_id referencia id em *Usuário*

Perfil (id, nome, status)

ModelHasRole (role_id, model_type, model_id)

role_id referencia id em *Perfil*

*OBS: aqui, uma particularidade do framework Laravel, model_id é uma referencia ao id da classe indicada em model_type, que pode ser *Usuário* ou *SetorUser*.

Permissão (id, nome, descrição, grupo)

RoleHasPermission (role_id, permission_id)

role_id referencia id em *Perfil*

permission_id referencia id em *Permisssão*

Processo (id, setor_id, nome, ref, descrição, imagem)

setor_id referencia id em *Setor*

Os requisitos gerais foram divididos em 7 categorias: (1) Acesso à Aplicação, (2) Gerenciar Setores, (3) Gerenciar *Perfis*, (4) Gerenciar Permissões, (6) Gerenciar *Usuários* e (7) Gerenciar Processos.

4.6 REQUISITOS GERAIS

4.6.1 Acesso à Aplicação

1. Login

   - A tela de login apresenta um formulário para inserção dos campos E-mail e Senha, bem como links para as telas de Recuperar Senha e Primeiro Acesso, através do link “Criar conta” (Figura 5).

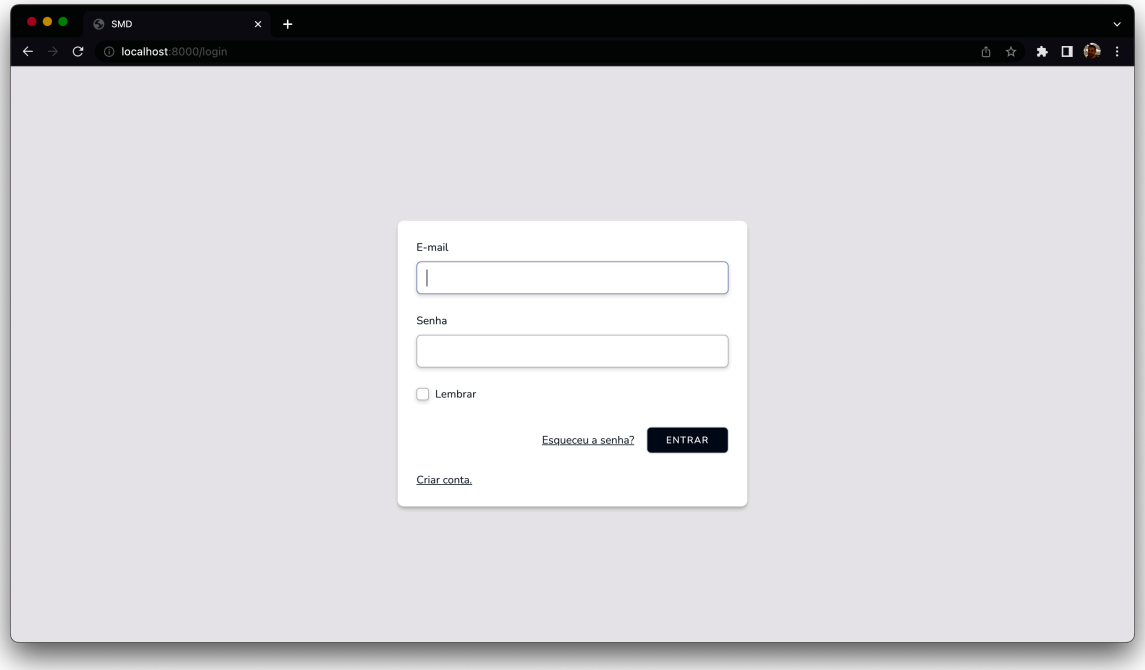

Figura 5: Tela de login

2. Primeiro Acesso

   - O primeiro acesso ocorre pelo cadastro do usuário, preenchendo os campos Nome, E-mail, Senha e Confirmação de senha (Figura 6)

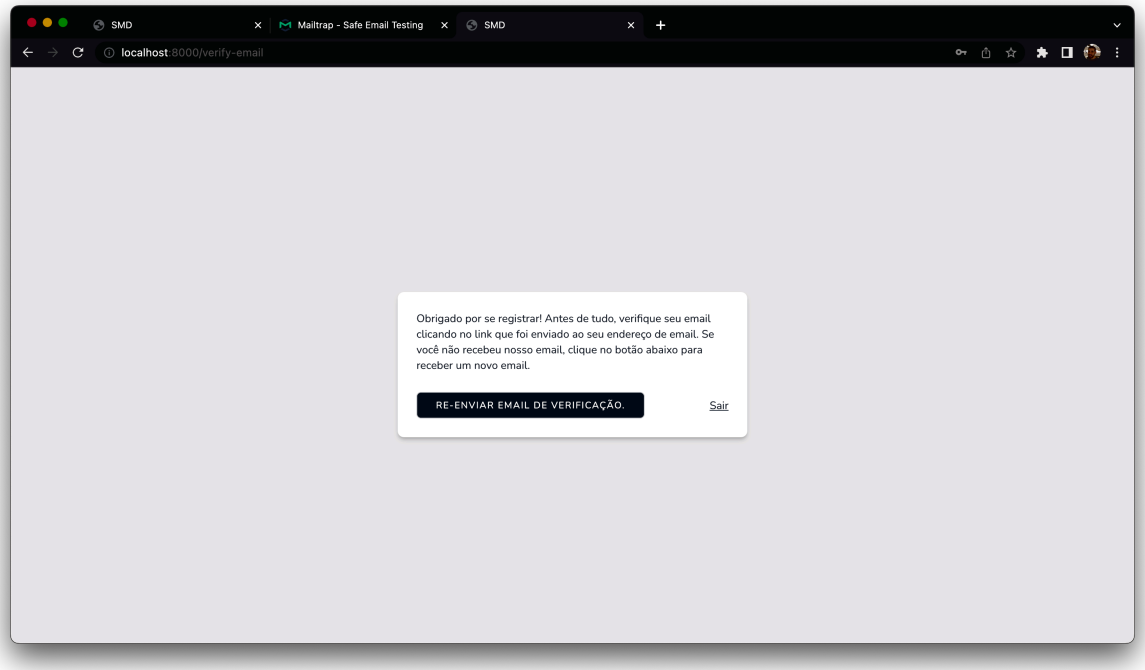

Figura 6: Tela após o cadastro

- O *Usuário* recém criado é inserido no banco de dados com status de inativo e espera por uma confirmação do e-mail. Para isso, um e-mail de confirmação é enviado para o endereço usado pelo usuário (Figura 7).

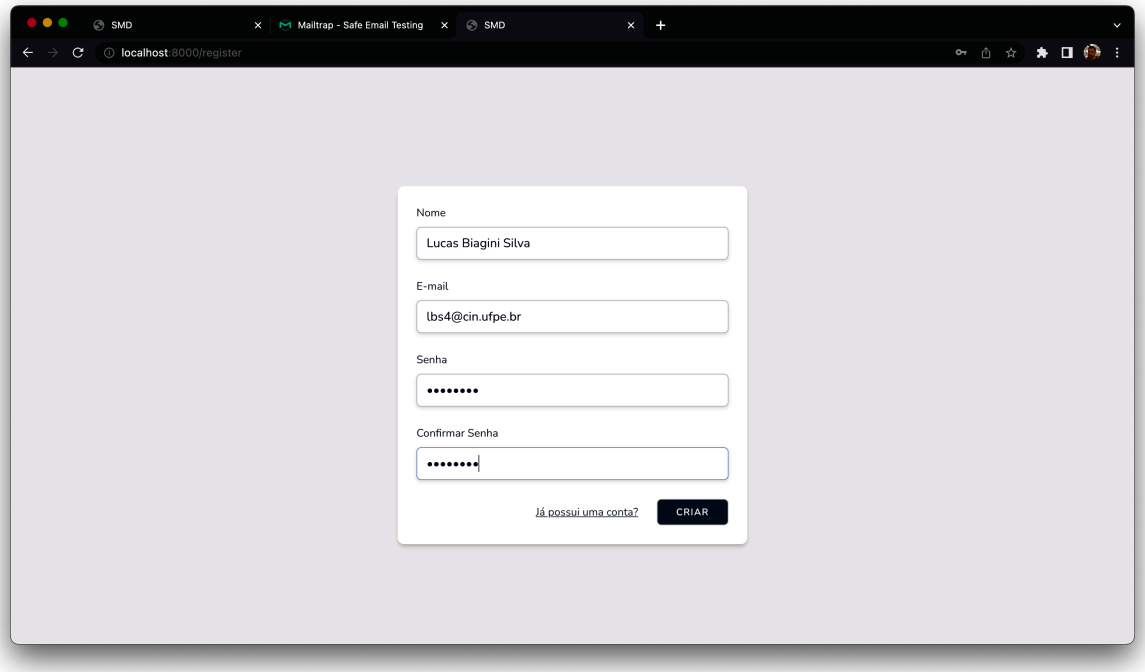

Figura 7: Tela de cadastro

- Abaixo, e-mail de confirmação (Figura 8).

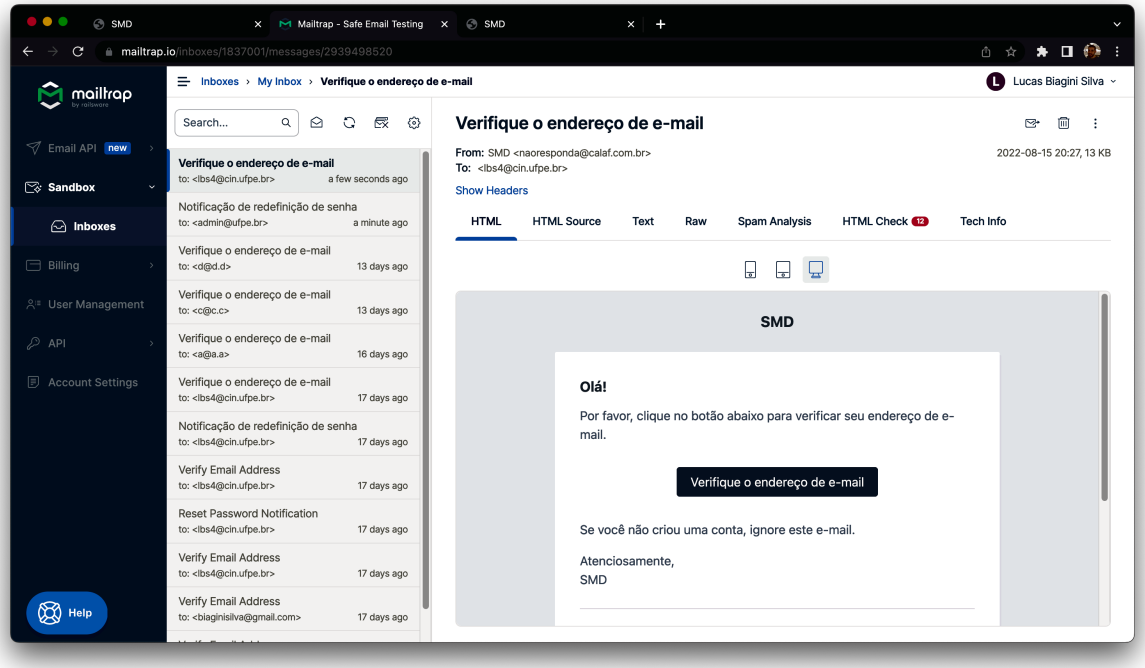

Figura 8: Visualização do e-mal de confirmação

- Ao clicar no link de verificação, o usuário realiza o login automaticamente e, caso ainda esteja com status inativo, a seguinte tela aparecerá (Figura 9).

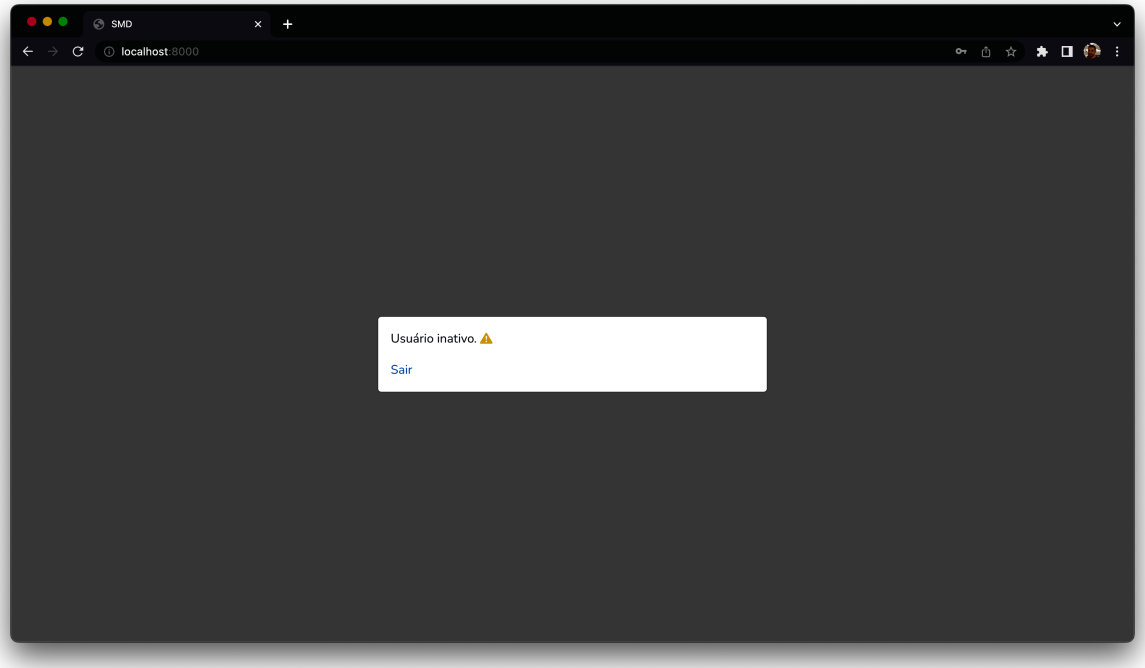

Figura 9: Tela de usuário inativo

- Caso o usuário esteja com o status ativo, porém não possua nenhum setor

e perfil associado, aparecerá a seguinte tela (Figura 10):

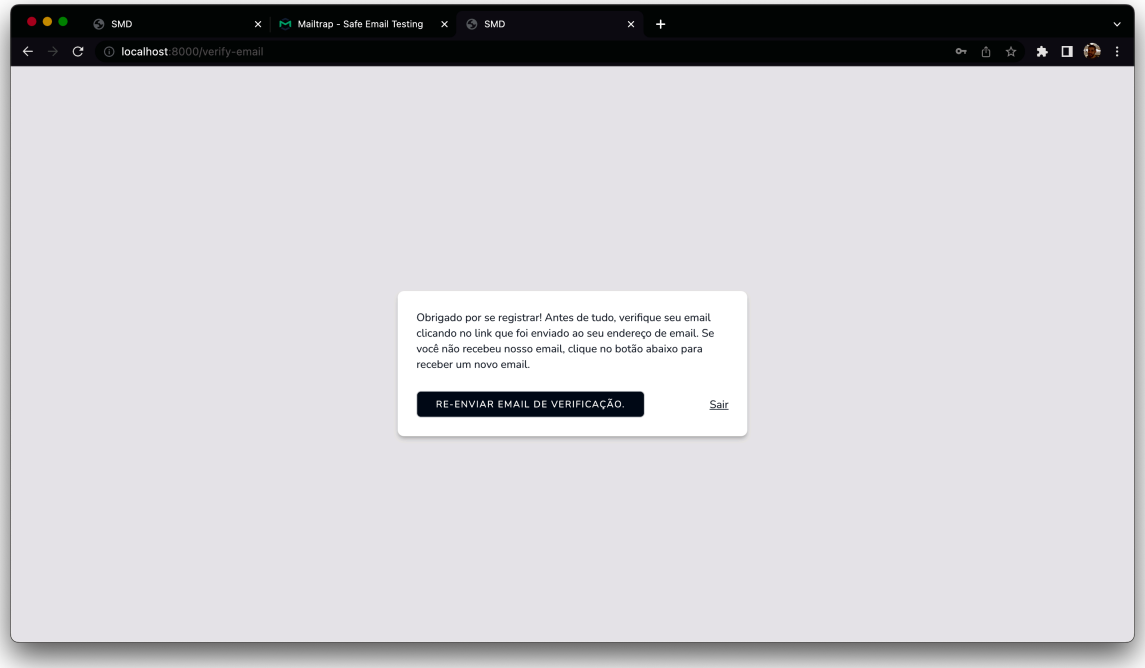

Figura 10: Tela de usuário sem perfil associado

- Caso o usuário esteja ativo e com um setor e perfil associado, uma tela para selecionar o setor desejado irá aparecer (Figura 11):

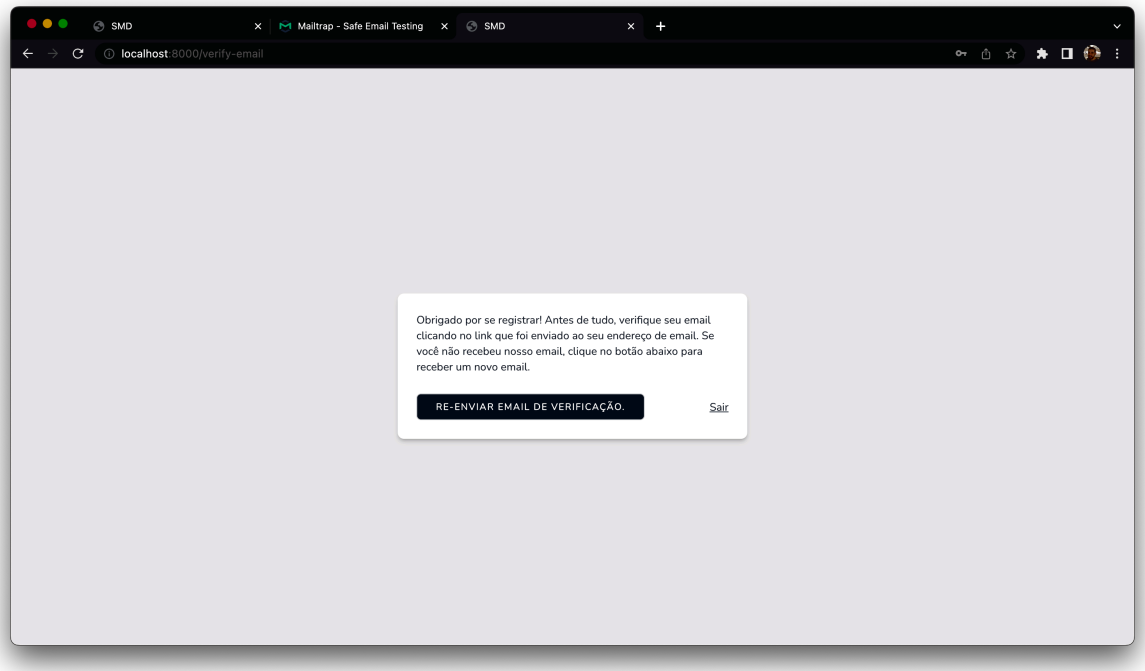

Figura 11: Tela de selecionar setor

3. Recuperar Senha

   - Para recuperar a senha, é necessário preencher o e-mail e verificar a caixa de entrada do e-mail para clicar no link de redefinir senha (Figura 12):

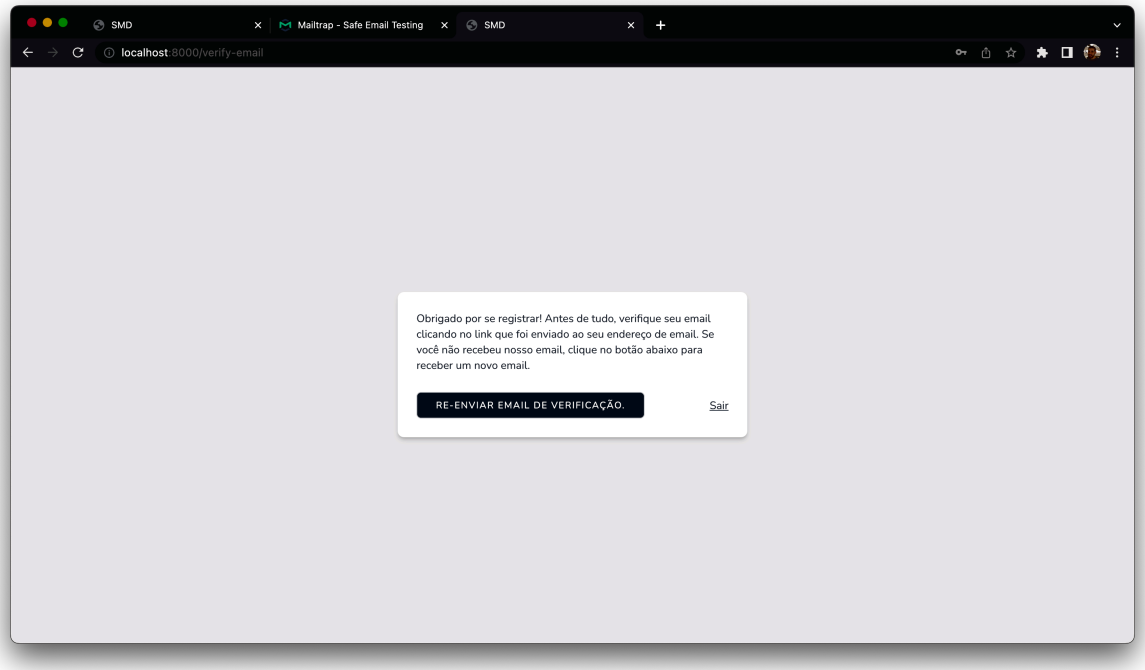

Figura 12: Tela de recuperação de senha

   - Abaixo, o e-mail de redefinição de senha (Figura 13):

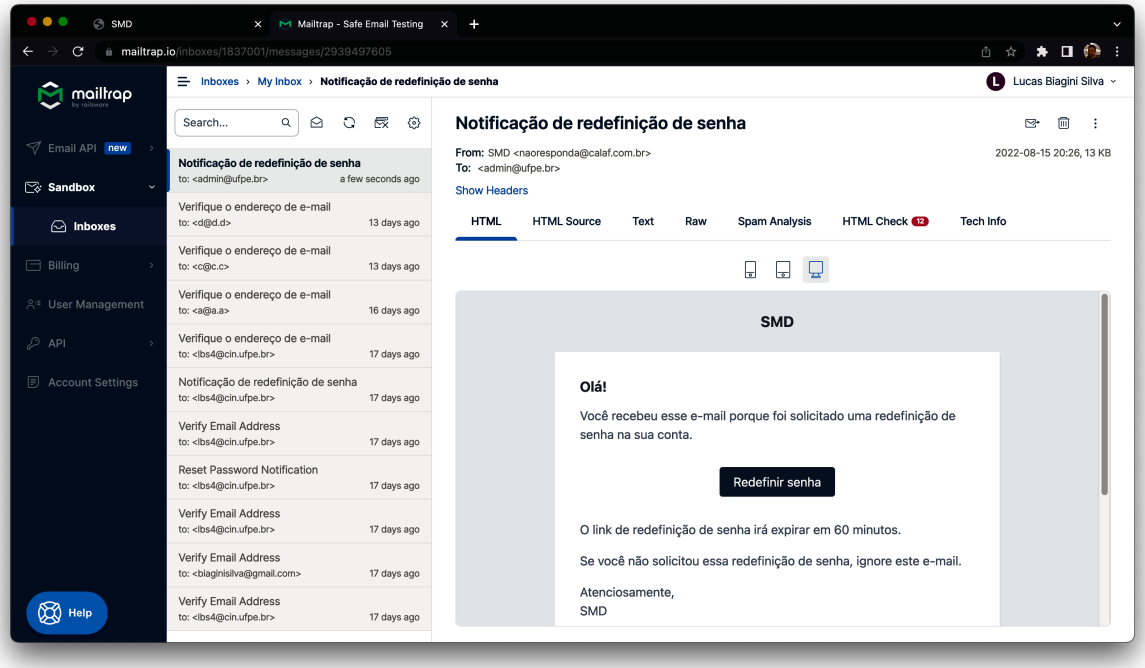

Figura 13: E-mail de recuperação de senha

- Para redefinir a senha, é necessário confirmar o e-mail, digitar a senha e confirmar a senha (Figura 14):

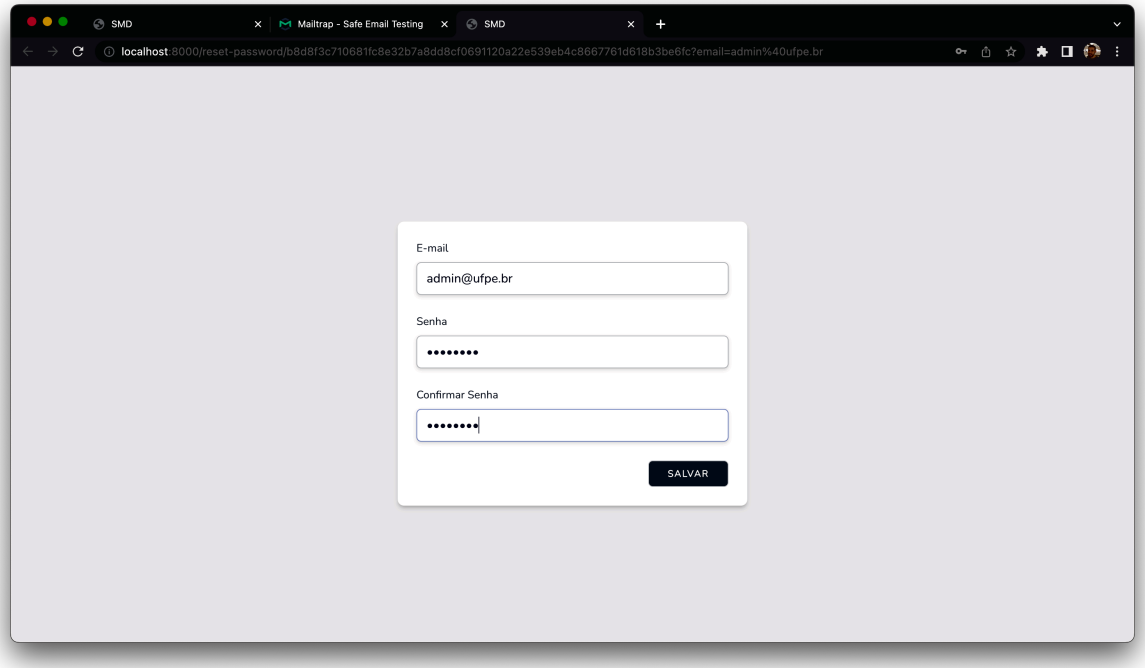

Figura 14: Tela de recuperação de senha

4. Logout

- As funcionalidades de Logout e Logout por inatividade, em que a sessão do usuário possui uma validade de 2 horas, redirecionam o usuário para a tela de login.

4.6.2 Gerenciar Setores

1. Listar Setores

   - A tela listagem de setores apresenta nome, descrição e status do setor, botão de editar setor e de cadastrar setor (Figura 15).

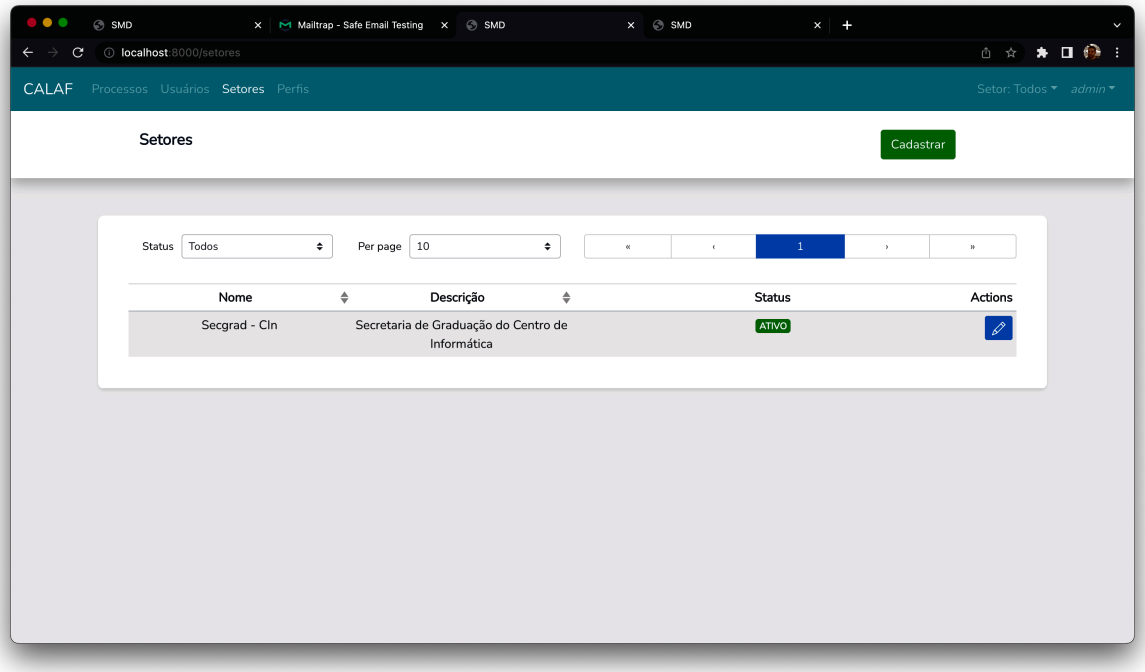

Figura 15: Tela de listagem de setores

2. Cadastrar Setor (Figura 16).

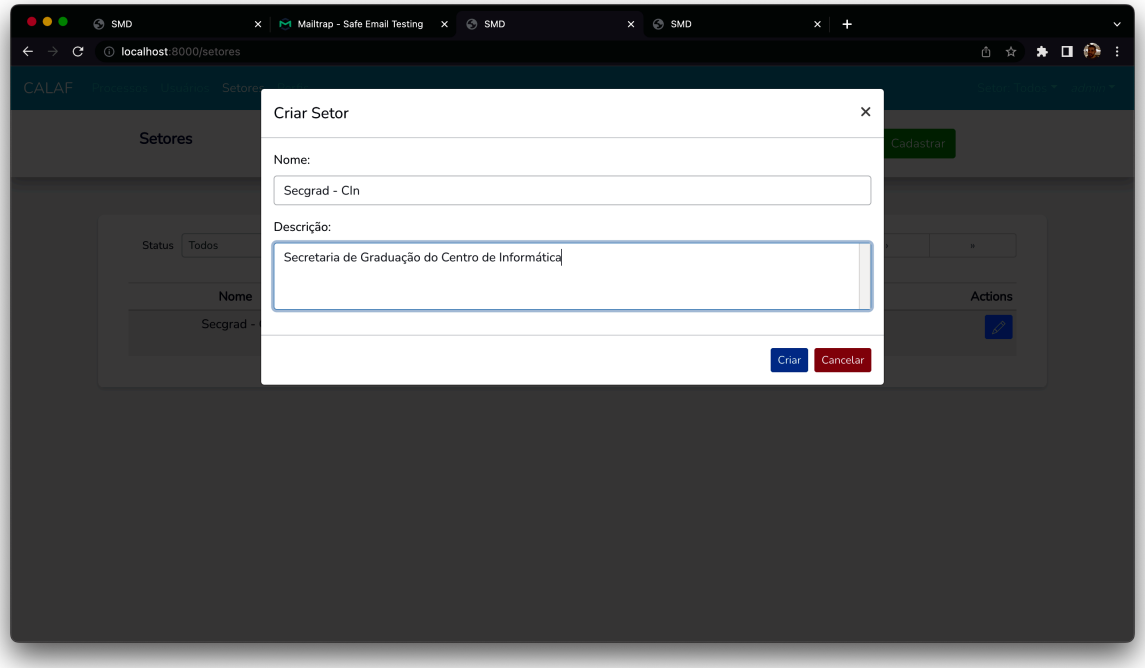

Figura 16: Tela de cadastro de setor

3. Editar Setor (Figura 17).

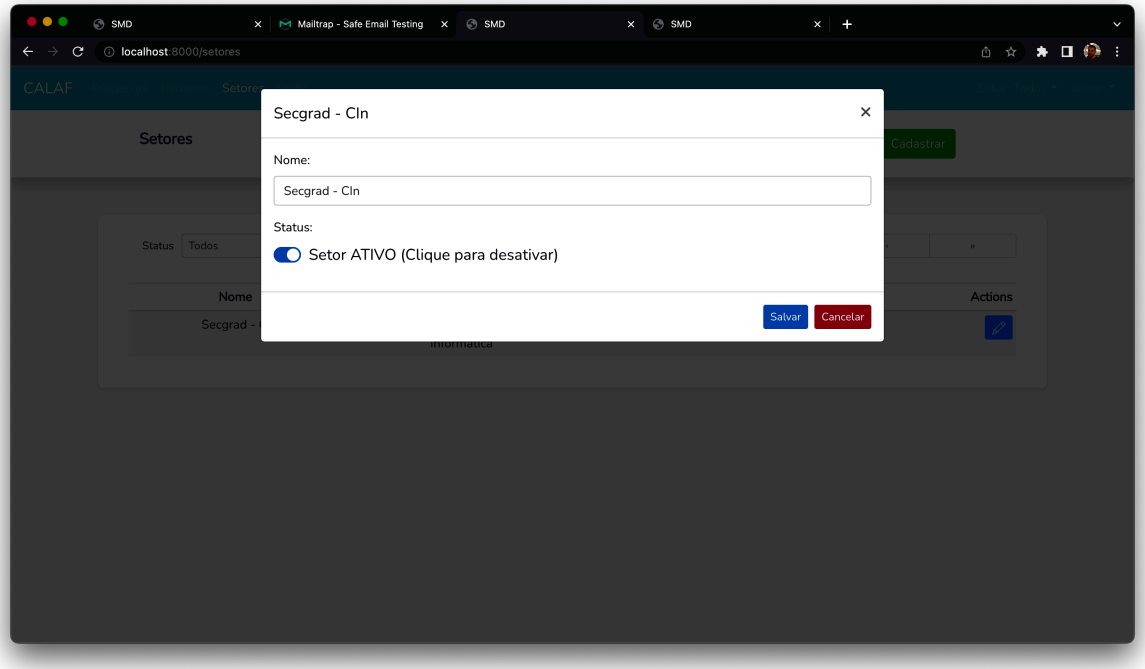

Figura 17: Tela de edição de setor

4.6.3 Gerenciar *Perfis*

1. Listar *Perfis* (Figura 18).

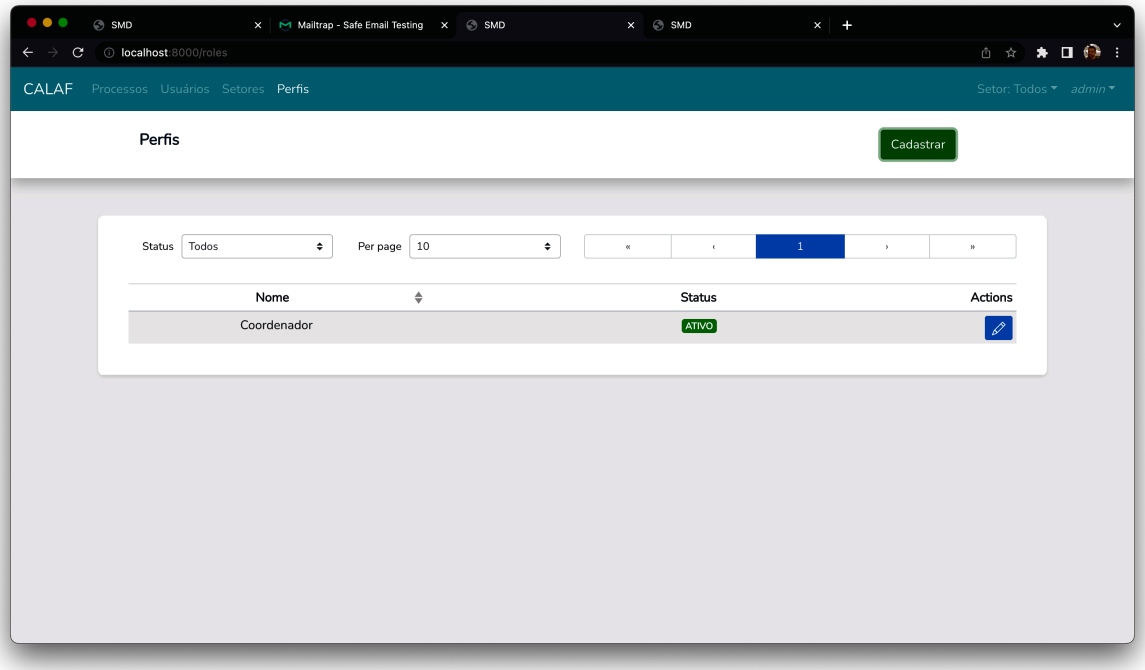

Figura 18: Tela de listagem de perfis

2. Cadastro de *Perfil* (Figura 19).

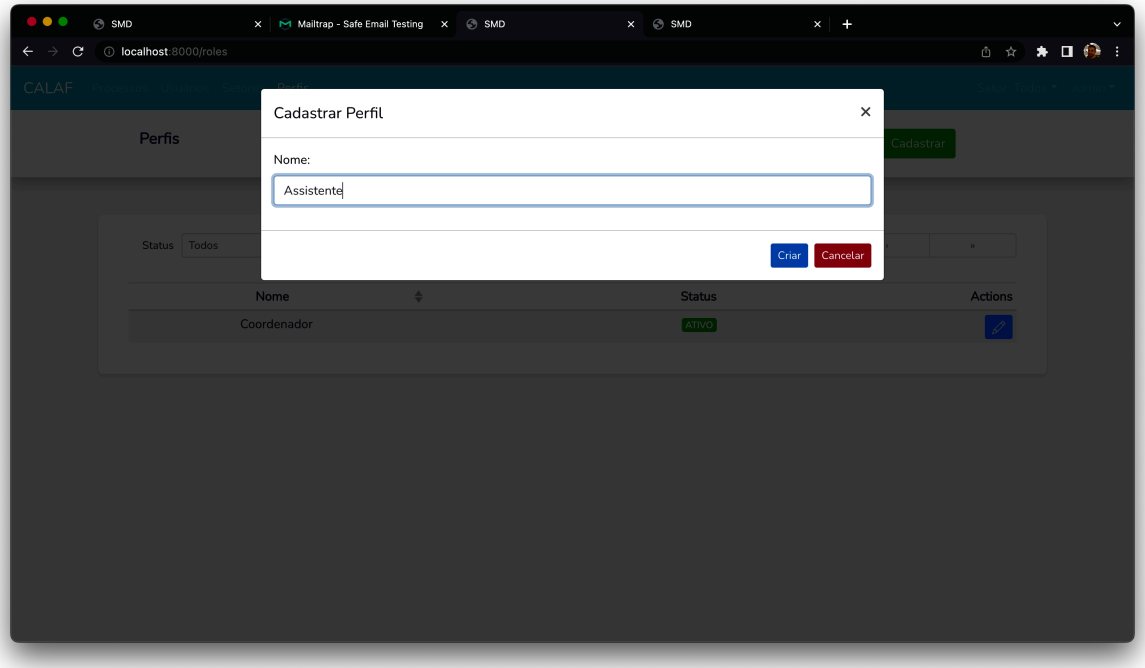

Figura 19: Tela de cadastro de perfil

3. Editar *Perfil* (Figura 20).

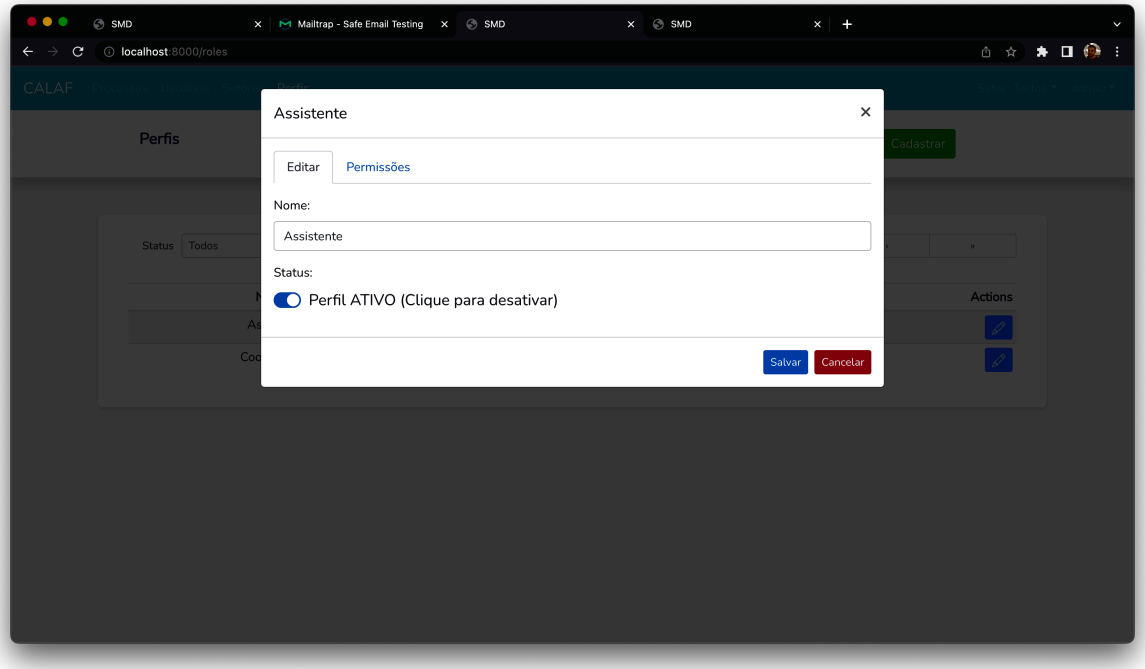

Figura 20: Tela de edição de perfil

4. Editar Permissões de um *Perfil*

- Na tela de editar permissões de um perfil, é possível escolher individualmente quais permissões o perfil terá acesso (Figura 21).

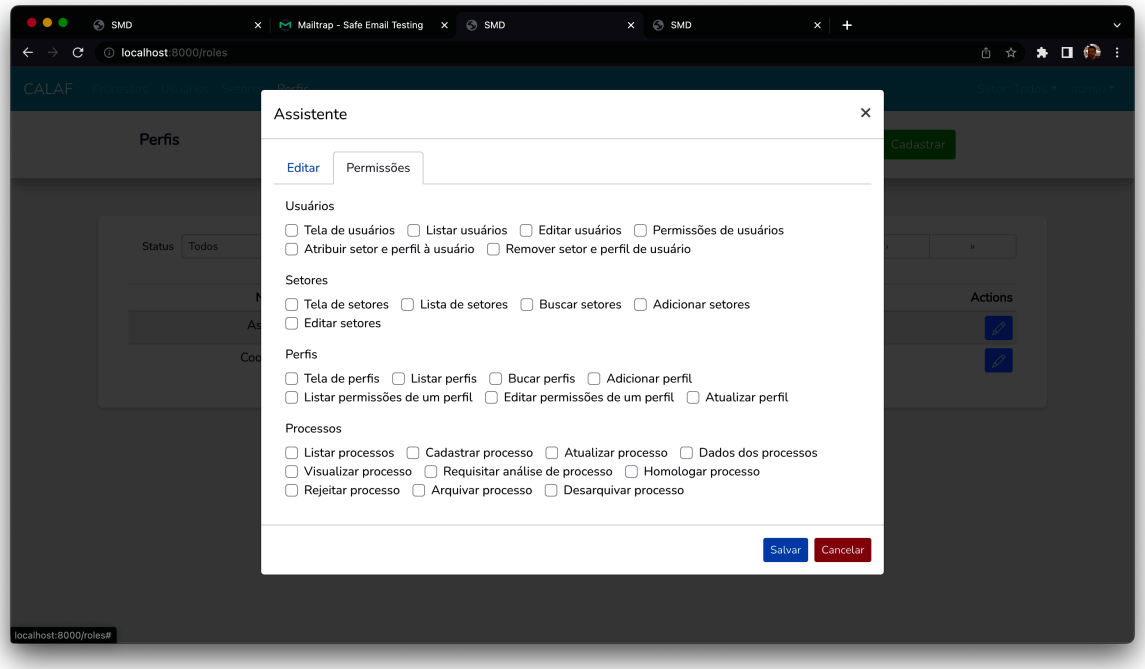

Figura 21: Tela de edição de permissões

4.6.4 Gerenciar *Usuários*

1. Listar *Usuários* (Figura 22).

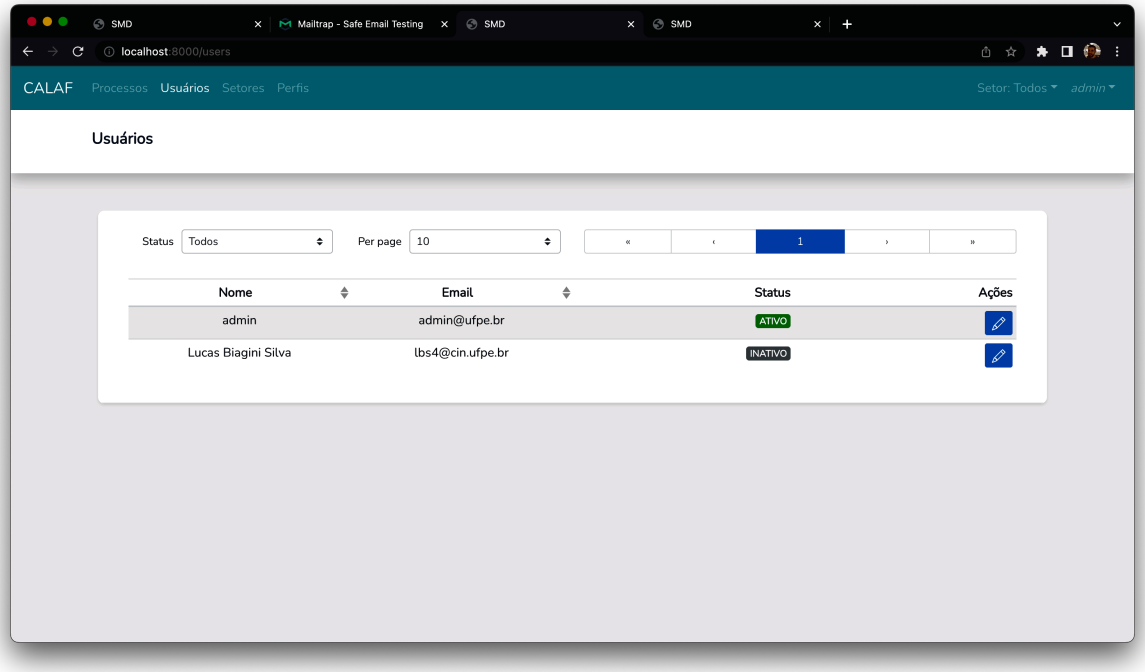

Figura 22: Tela de listagem de usuários

2. Editar *Usuário* (Figura 23).

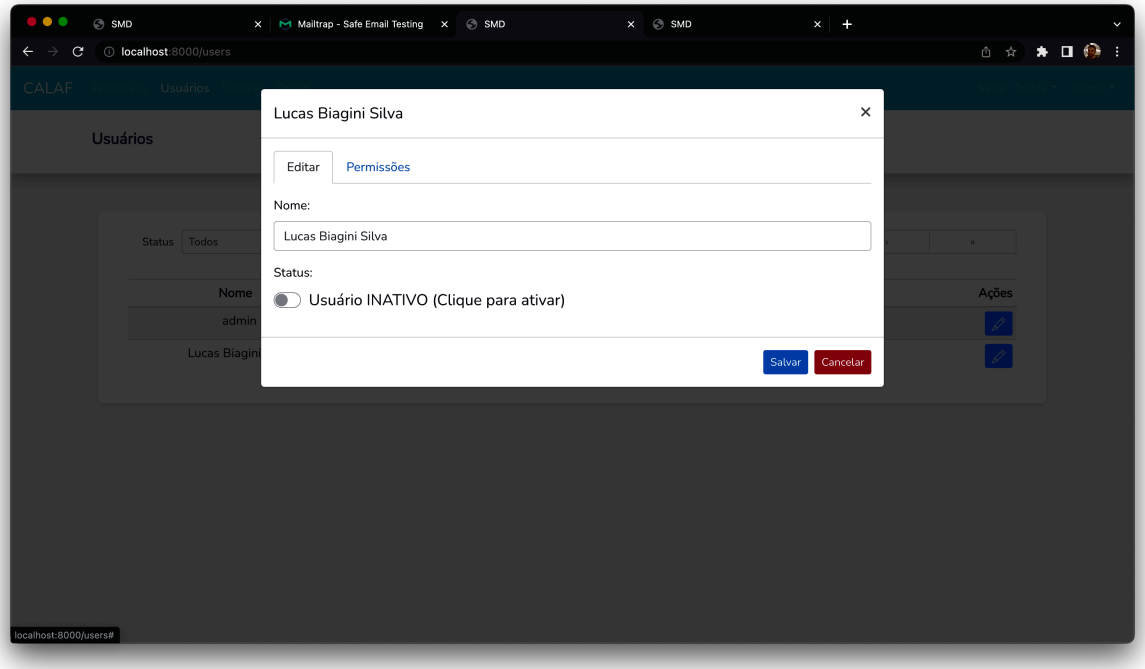

Figura 23: Tela de edição de usuários

3. Associar *Perfil*

- Na tela de associar setor e perfil ao usuário, é necessário escolher um setor e um perfil e, então, clicar no botão incluir. Para excluir uma associação, deve-se apertar no botão com o ícone da lixeira (Figura 24).

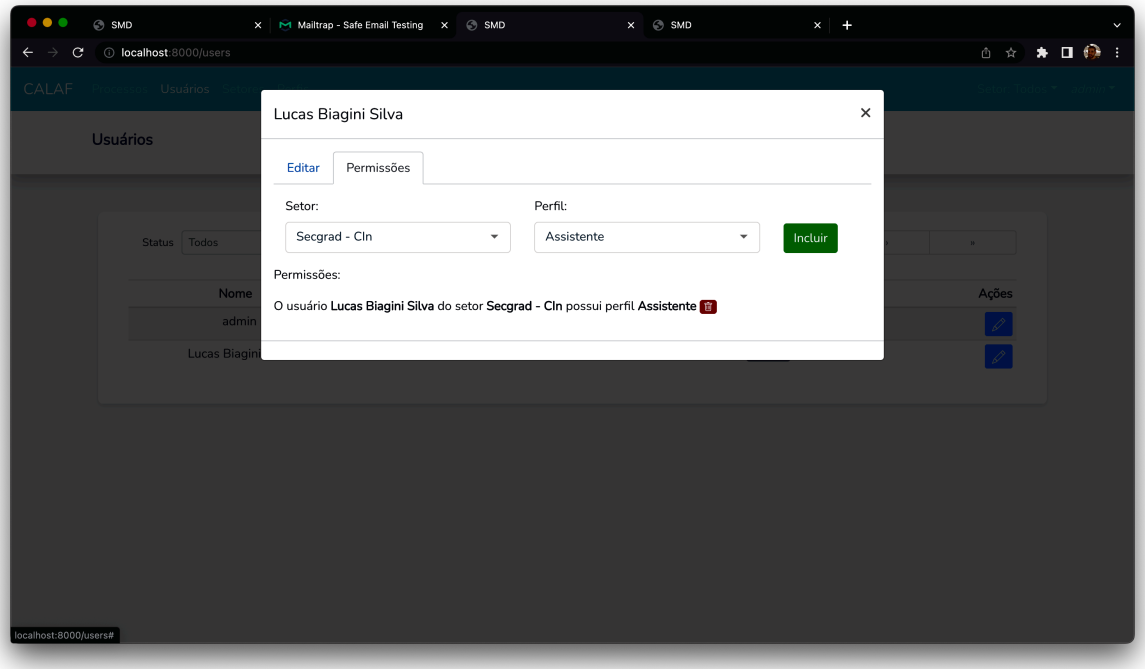

Figura 24: Tela de associação de permissões a um usuário

4.6.5 Gerenciar Processos

1. Listar Processos (Figura 25).

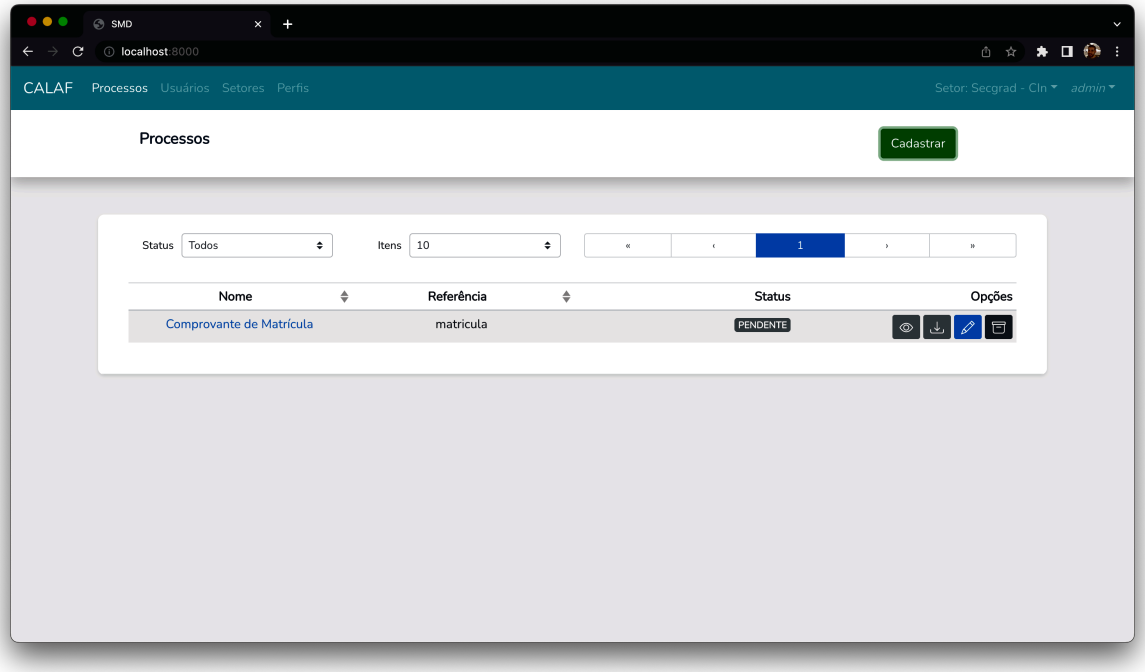

Figura 25: Tela de listagem de processos

- Para visualizar um processo dentro da listagem, é necessário clicar o botão com ícone do olho aberto e aparecerá uma área, dentro da tabela, com mais informações sobre o processo (Figura 26).

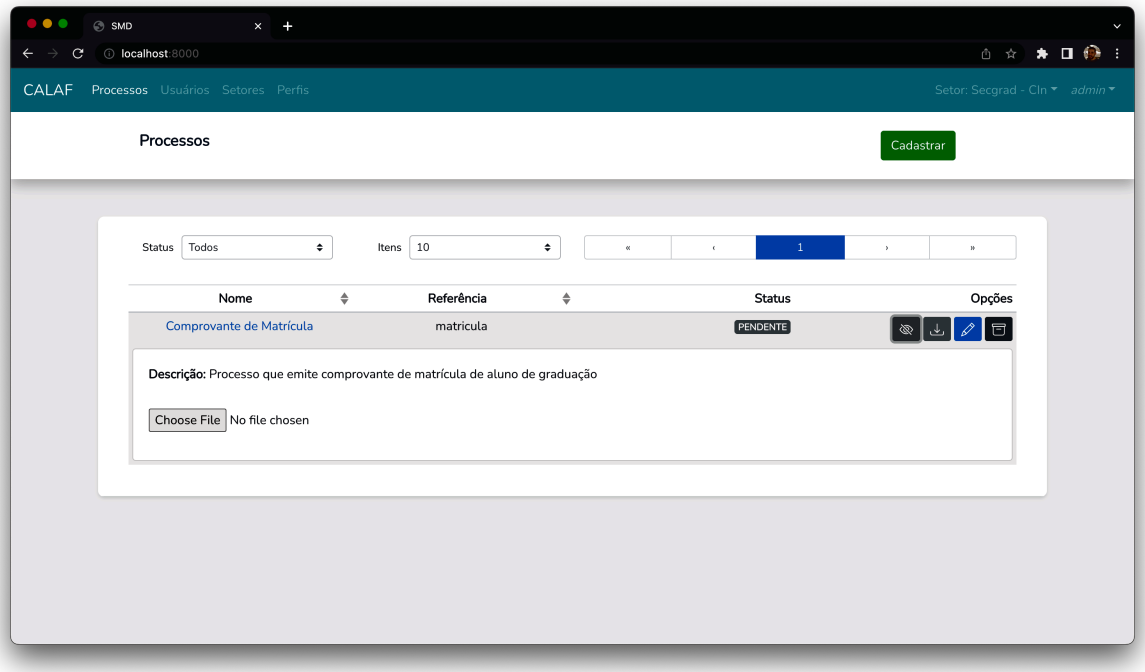

Figura 26: Tela de cadastro de processo

- É possível adicionar uma imagem para o processo, preferencialmente uma imagem de fluxo do processo. Para excluir a imagem, clicar em “excluir” (Figura 27).

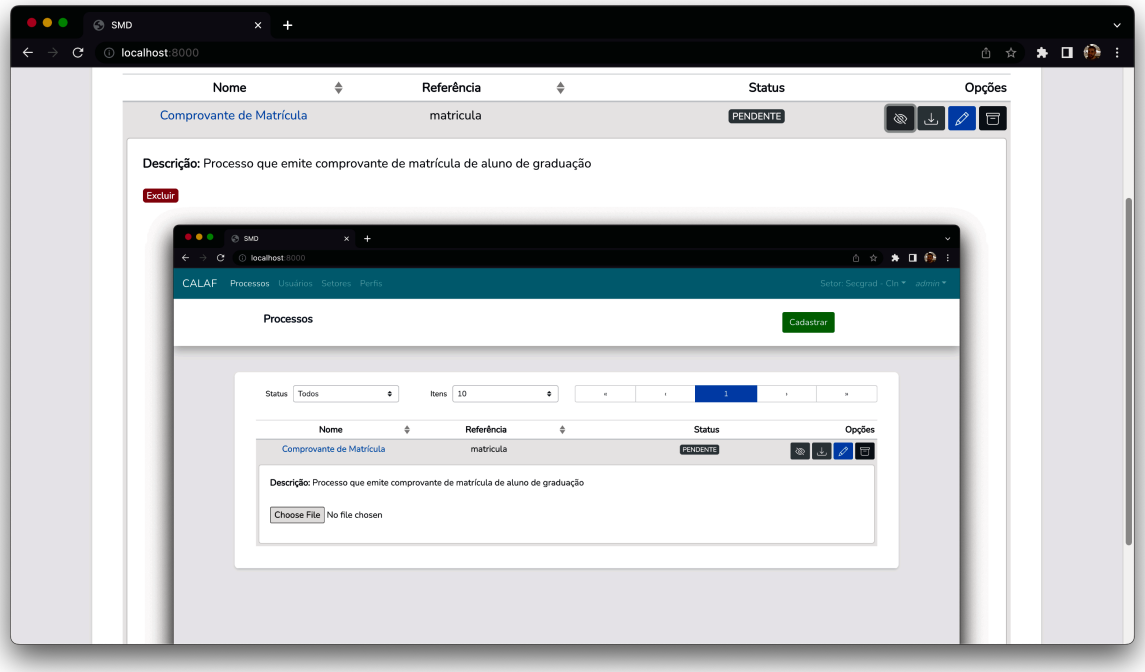

Figura 27: Tela de visualização de processo

2. Cadastro de Processo (Figura 28).

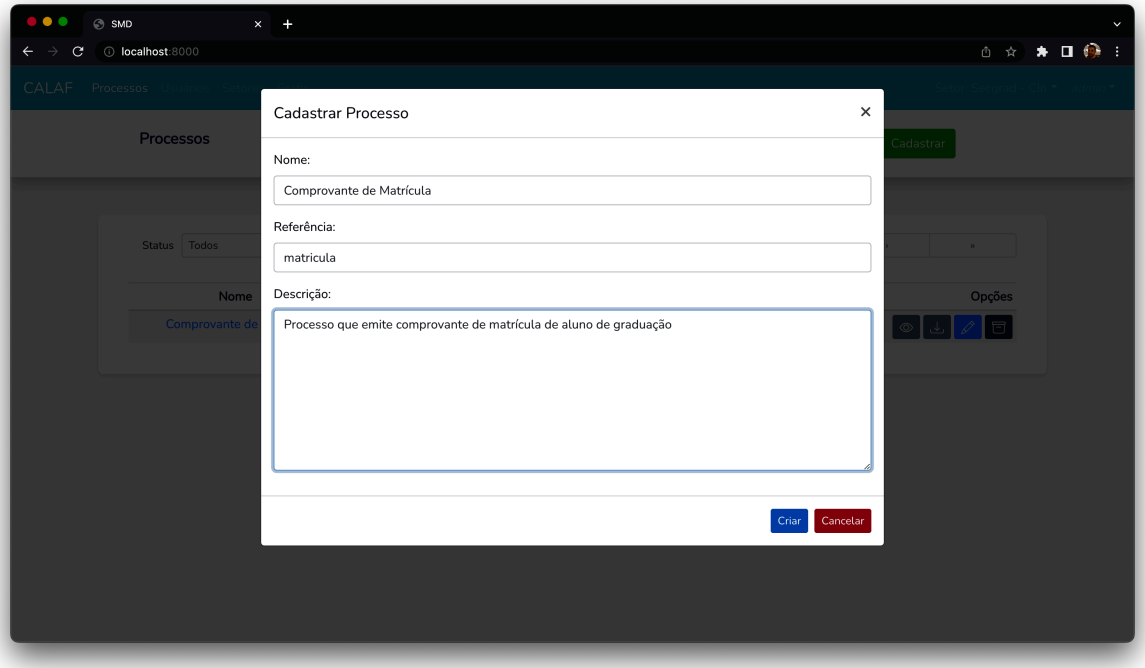

Figura 28: Exclusão da imagem de um processo

3. Editar Processo (Figura 29).

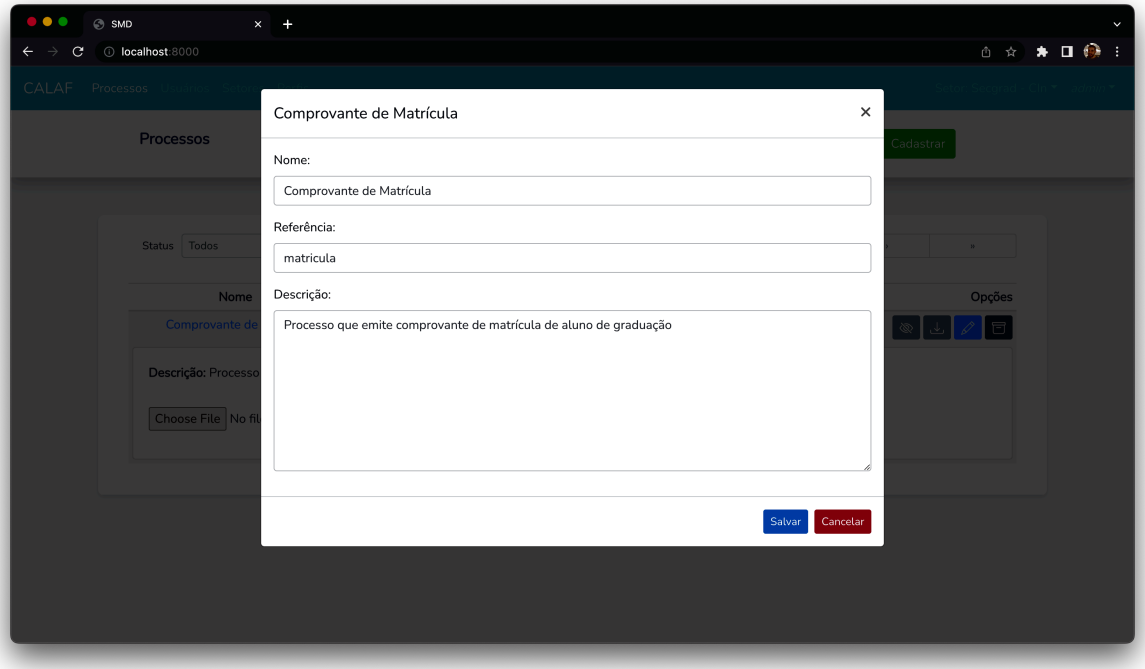

Figura 29: Tela de edição de processo

4.7 REQUISITOS DE INVENTÁRIO DE DADOS PESSOAIS

4.7.1 Cadastrar Dados do IDP

- Esta é a tela principal do IDP, nela aparece a opção de solicitar análise caso o processo esteja “pendente” ou “homologado”; opção de “homologar” ou “rejeitar” caso esteja com status “em análise” (Figura 30):

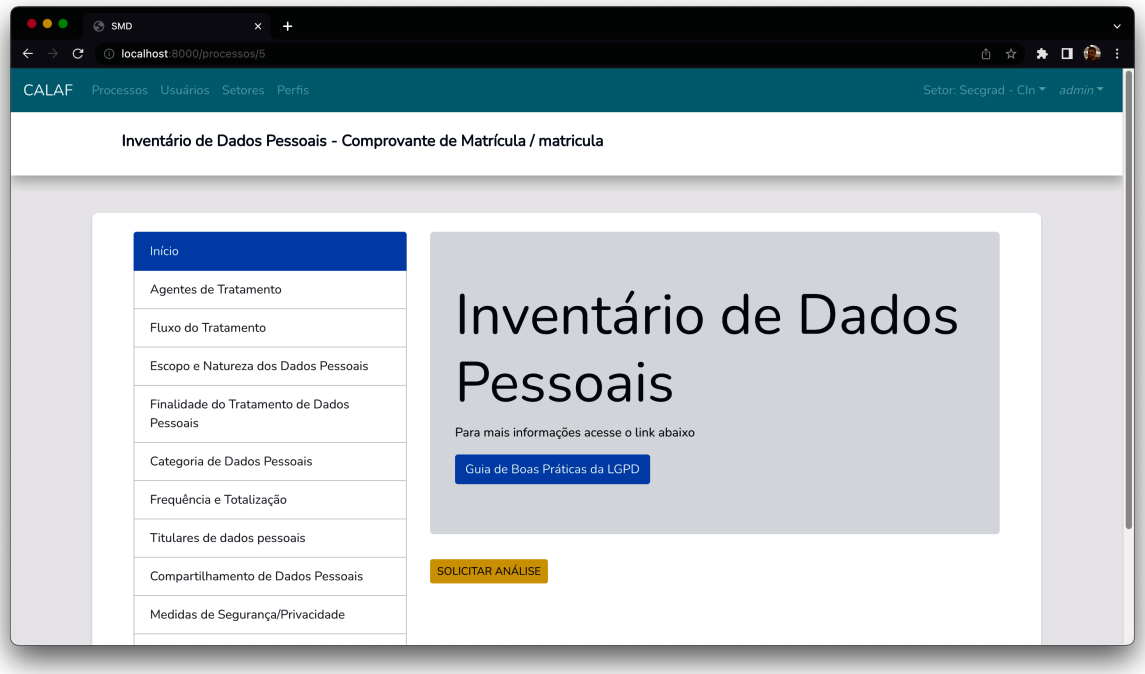

Figura 30: Tela de Inventário de Dados Pessoais de um processo

- Seção de cadastro de agentes de tratamento, é necessário cadastrar um Controlador e um Encarregado (Figura 31):

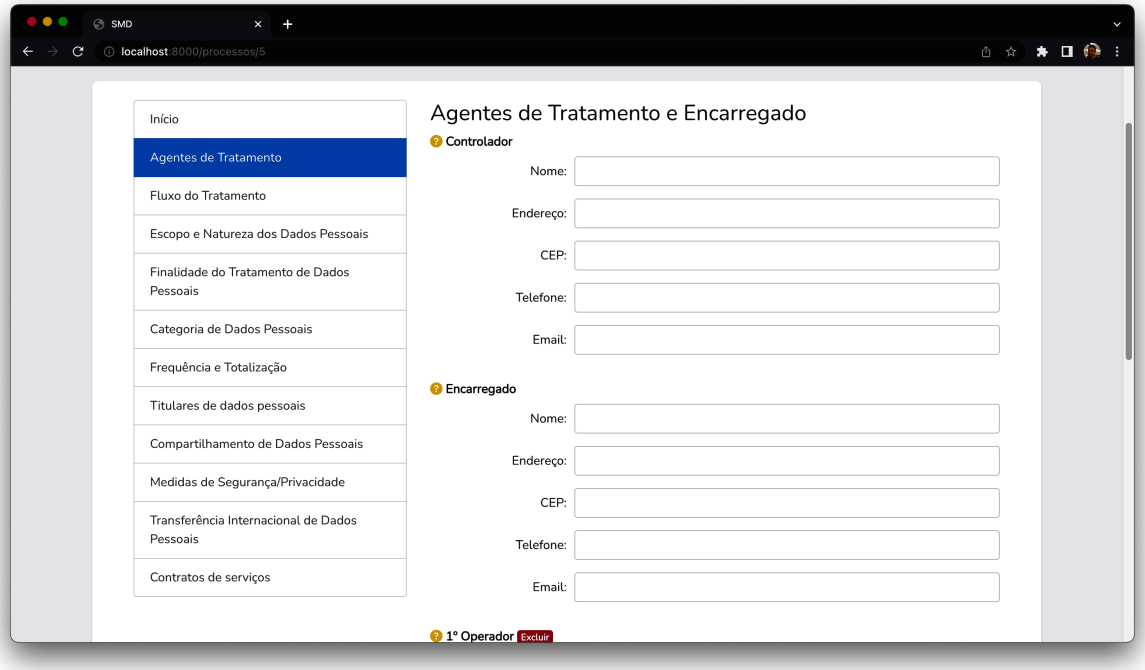

Figura 31: Tela de cadastro dos agentes de tratamento e encarregado

- Ainda na mesma tela, o usuário precisa cadastrar um ou mais Operadores. Para que apareça quantos formulários de cadastro de Operador forem necessários. Para isto basta clicar em “Adicionar Operador”. Caso queira excluir um Operador, clicar em “Excluir”. A qualquer momento do cadastro do IDP, as informações são salvas de forma automática, salvos os casos em que explicitamente aparece o botão de “Salvar” ou “Criar” (Figura 32):

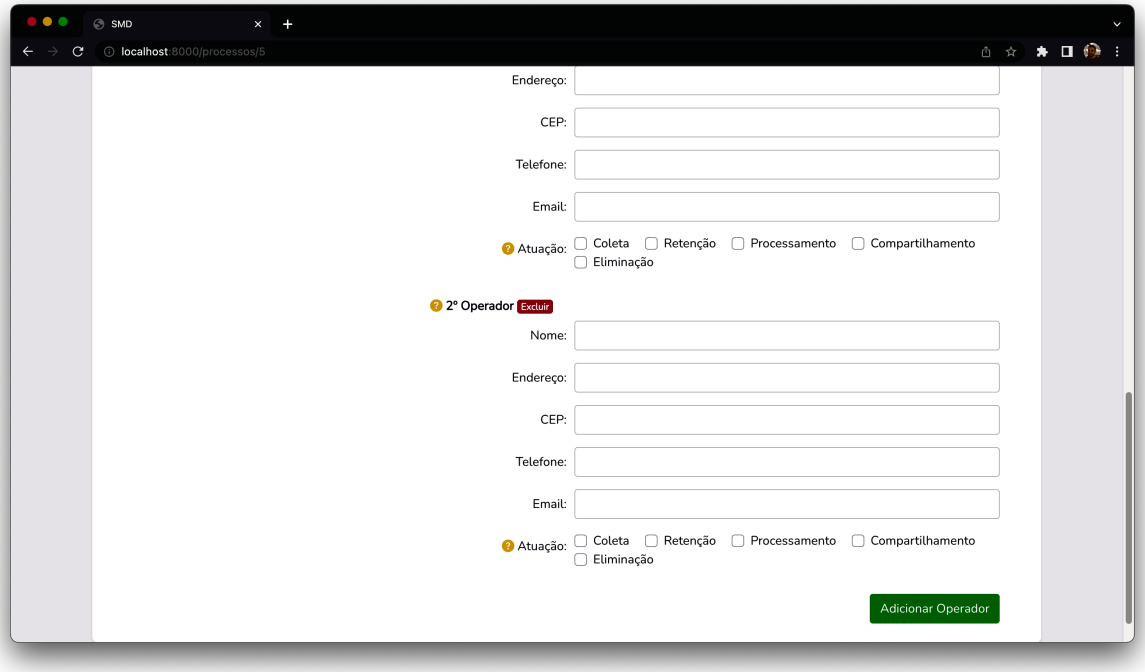

Figura 32: Cadastro do operador

- Seção para descrever fluxo do tratamento dos dados. É possível adicionar vários arquivos na lista de arquivos (Figura 33):

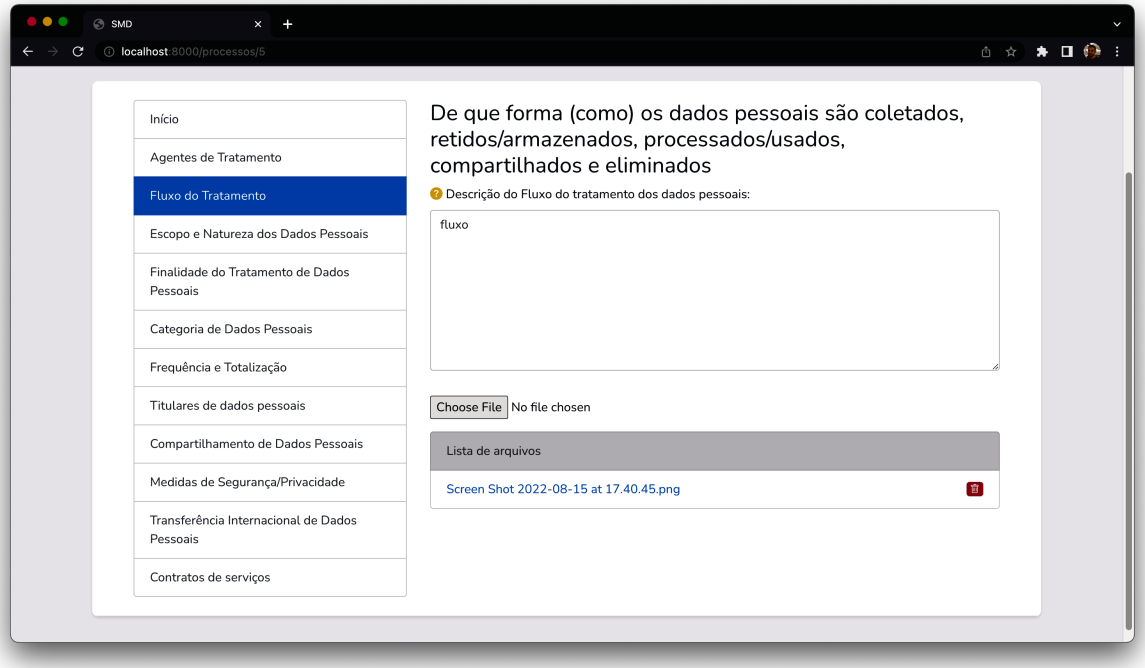

Figura 33: Tela de cadastro do fluxo de tratamento

- Seção para descrever o escopo e a natureza dos dados pessoais (Figura 34):

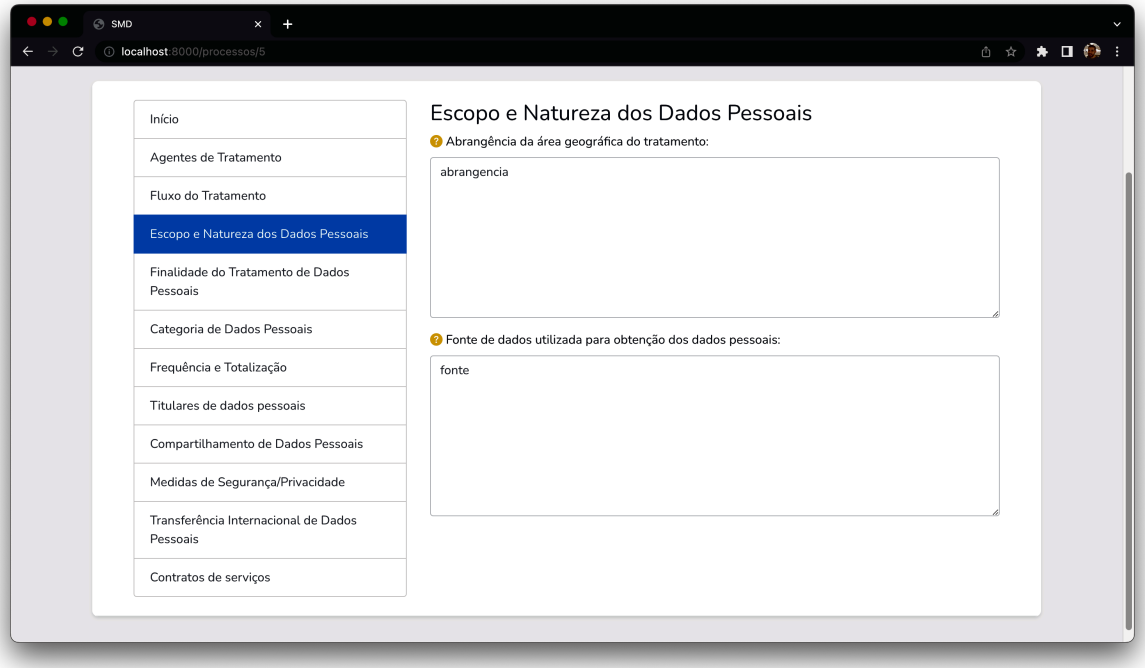

Figura 34: Tela de cadastro do escopo e natureza dos dados pessoais

- Seção para descrever a finalidade do tratamento de dados pessoais (Figura 35):

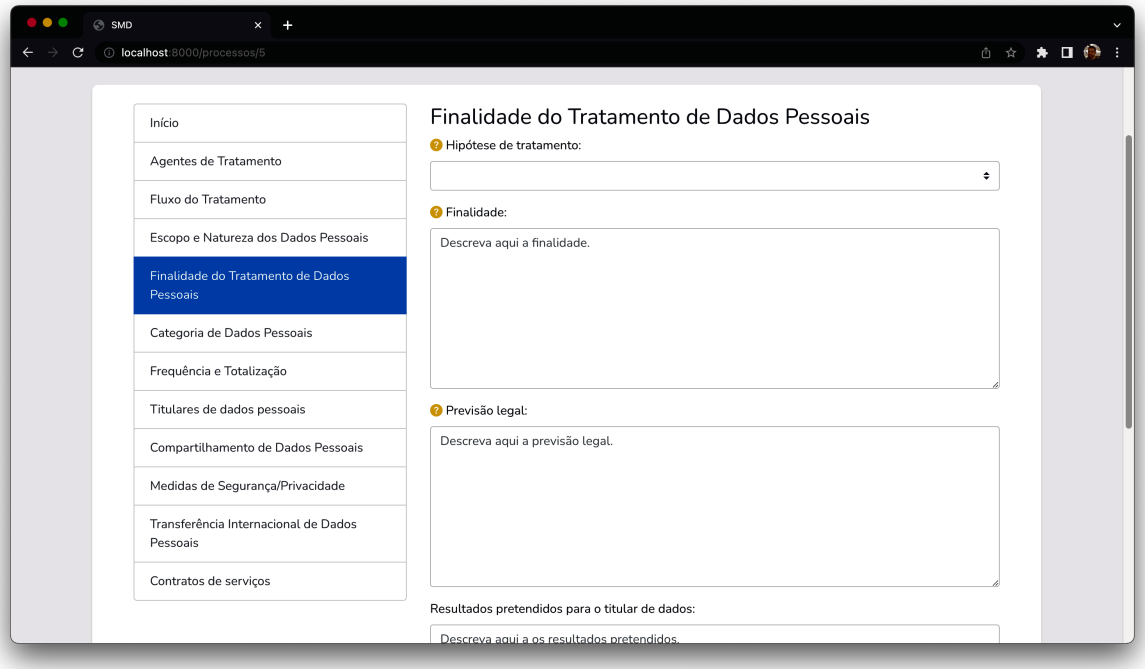

Figura 35: Tela de cadastro da finalidade do tratamento de dados pessoais

- Seção para cadastrar/listar/visualizar/excluir categoria de dados pessoais (Figura 36 e Figura 37):

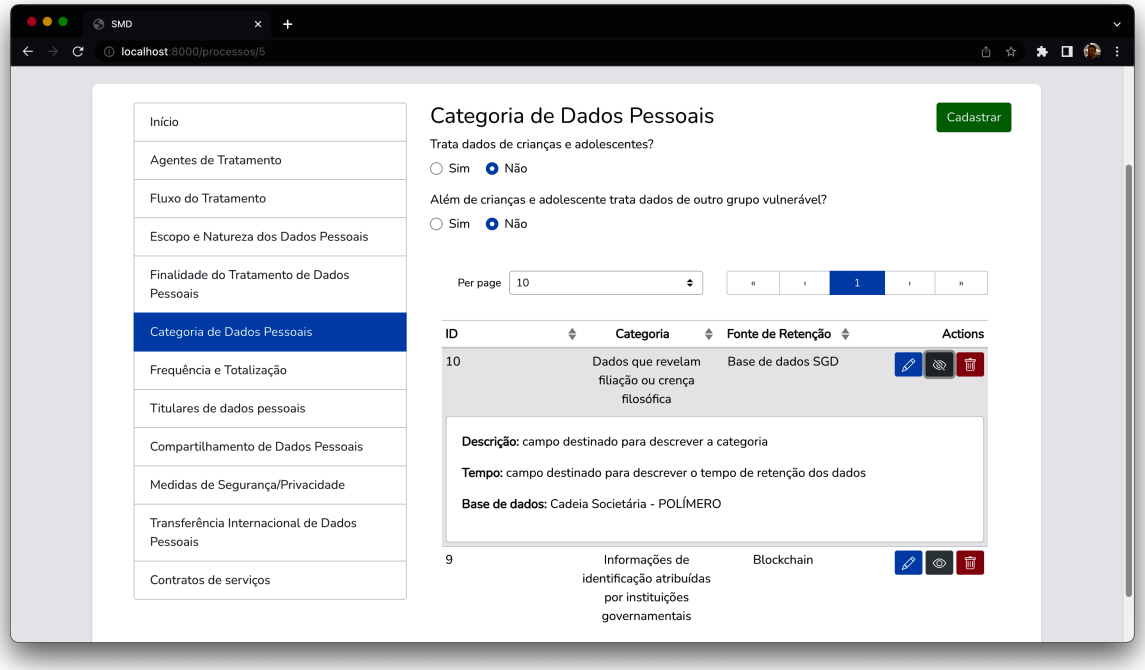

Figura 36: Tela de gerenciamento das categorias de dados pessoais

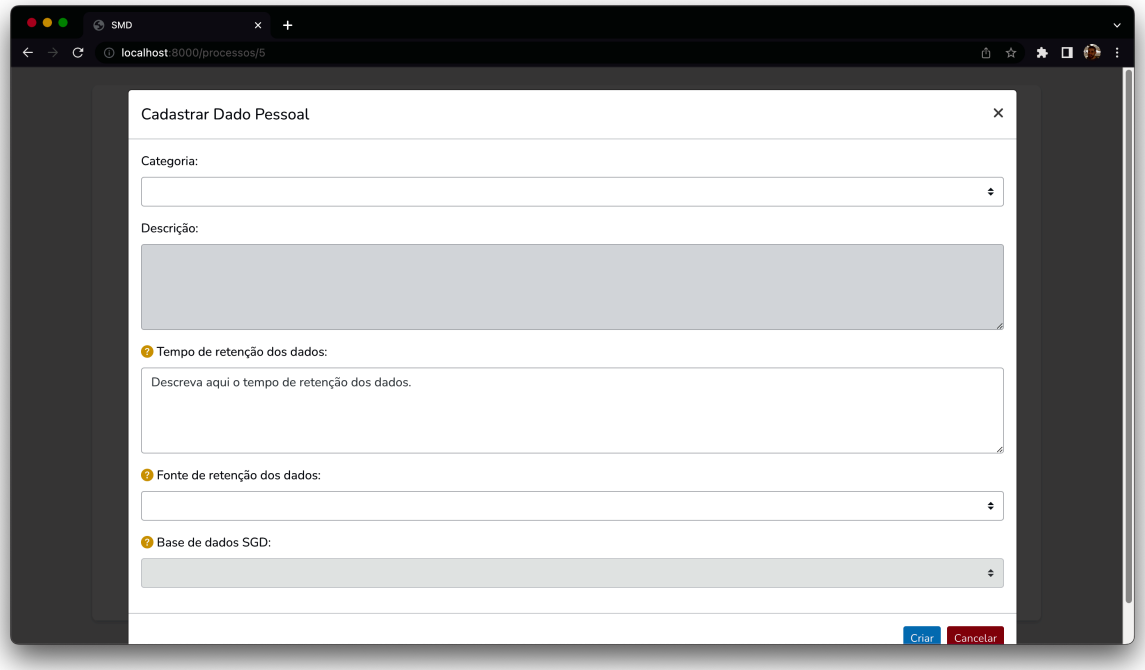

Figura 37: Tela de cadastro da categoria de dado pessoal

- Seção para descrever frequência e totalização das categorias de dados pessoais tratados (Figura 38):

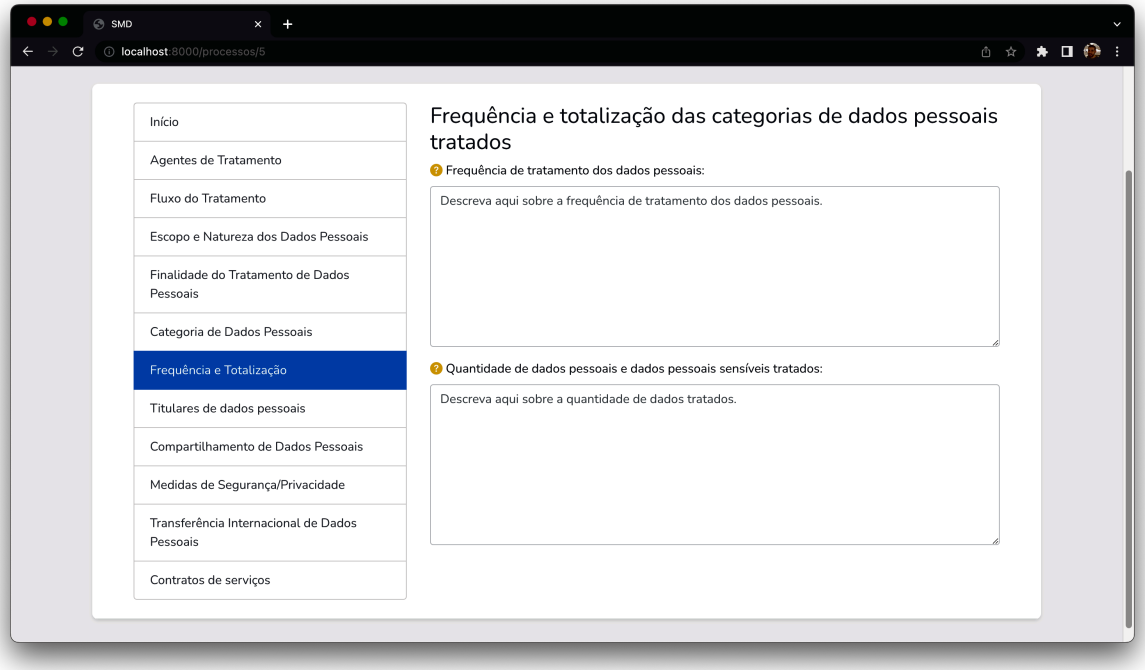

Figura 38: Tela de cadastro da frequência e totalização das categorias de dados pessoais tratados

- Seção para cadastrar/listar/visualizar/excluir categorias dos titulares de dados pessoais (Figura 39 e Figura 40):

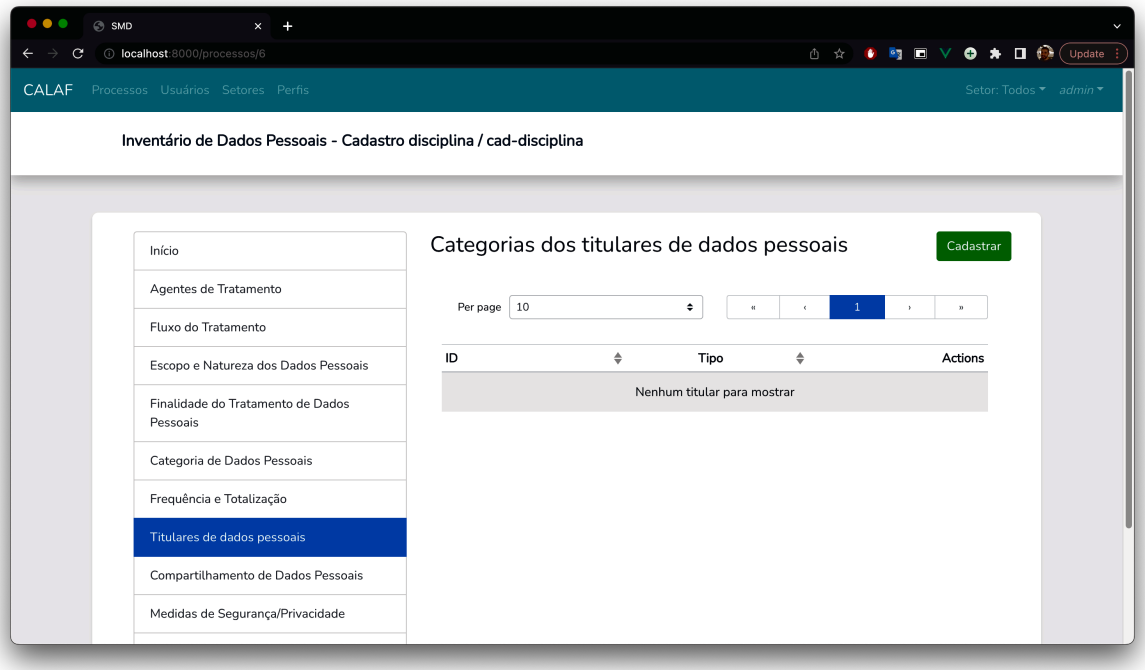

Figura 39: Tela de gerenciamento das categorias dos titulares de dados pessoais

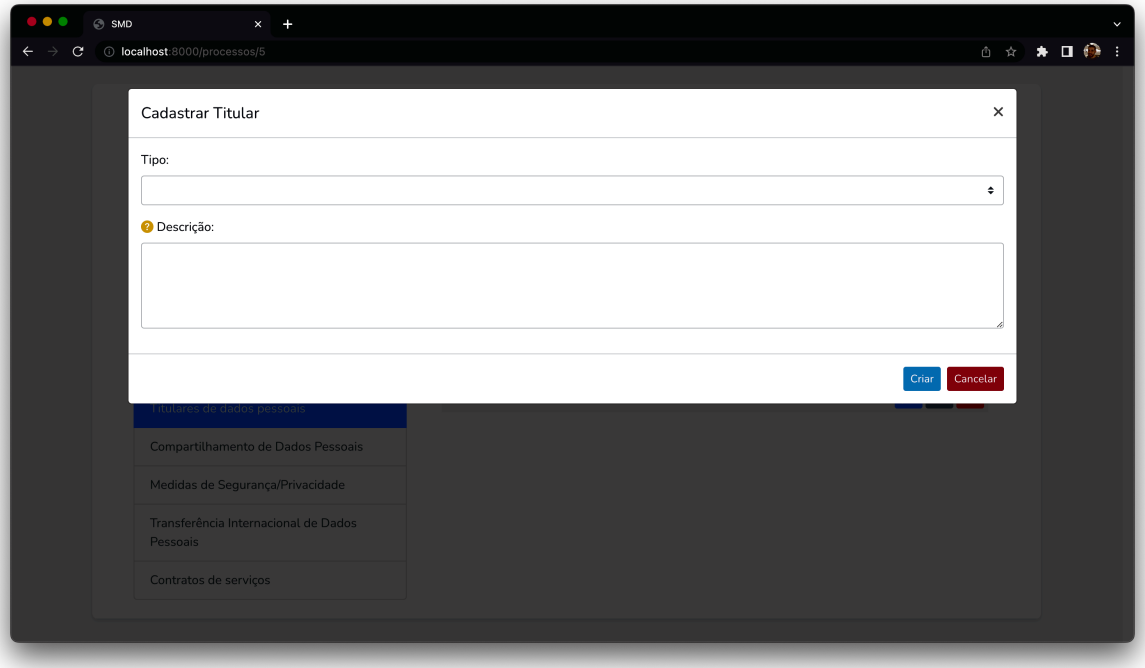

Figura 40: Tela de cadastro de categoria do titular de dados pessoais

- Seção para cadastrar/listar/visualizar/excluir compartilhamento de dados pessoais (Figura 41 e Figura 42):

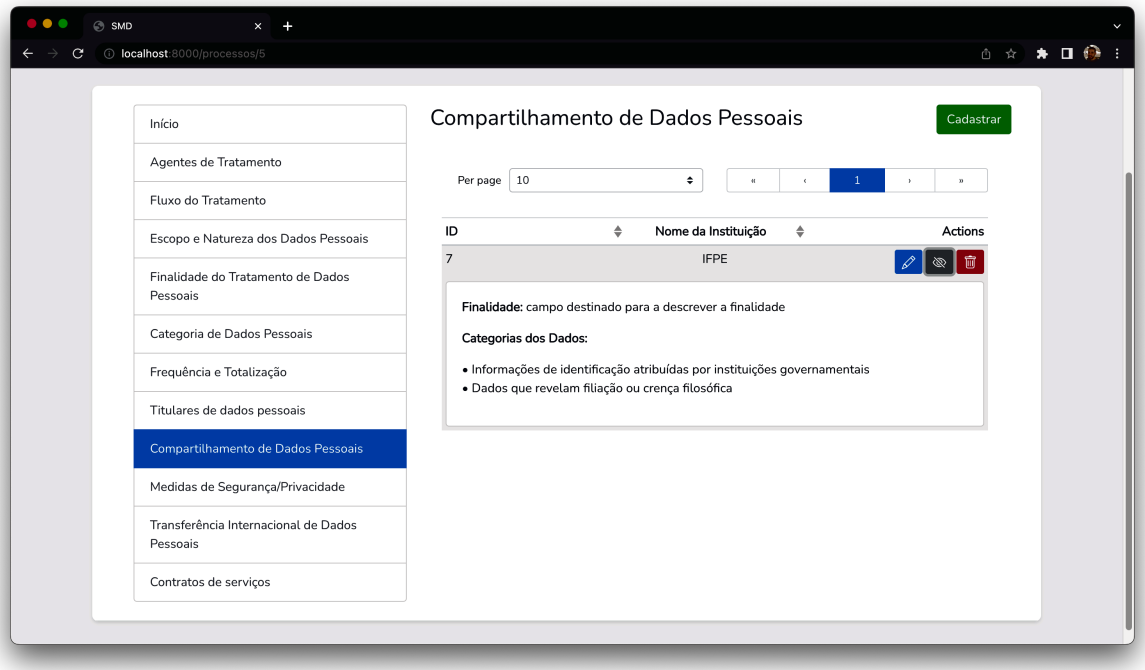

Figura 41: Tela de gerenciamento de compartilhamentos de dados pessoais

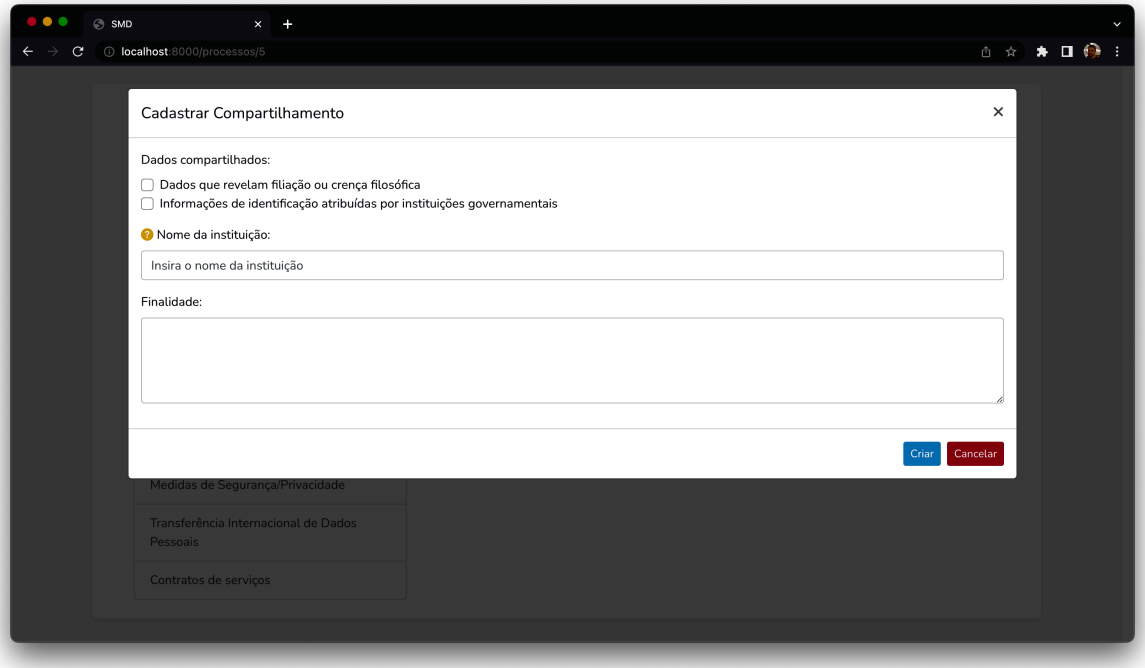

Figura 42: Tela de cadastro de compartilhamento de dados pessoais

- Seção para cadastrar/listar/visualizar/excluir medidas de segurança e privacidade (Figura 43 e Figura 44):

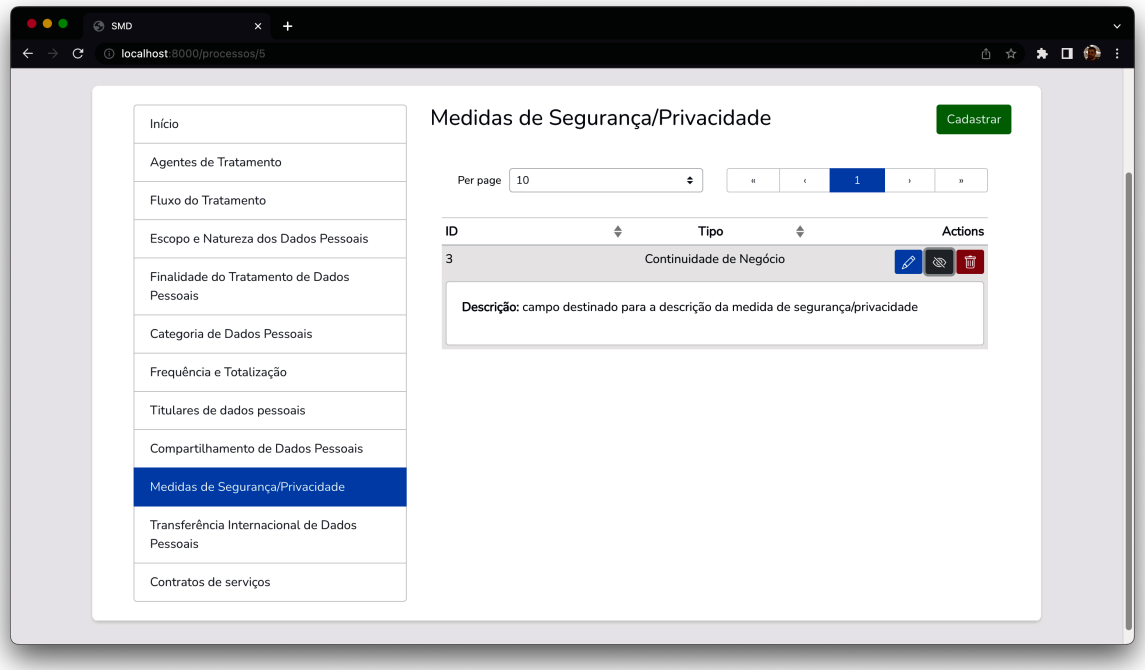

Figura 43: Tela de gerenciamento de medidas de segurança e privacidade

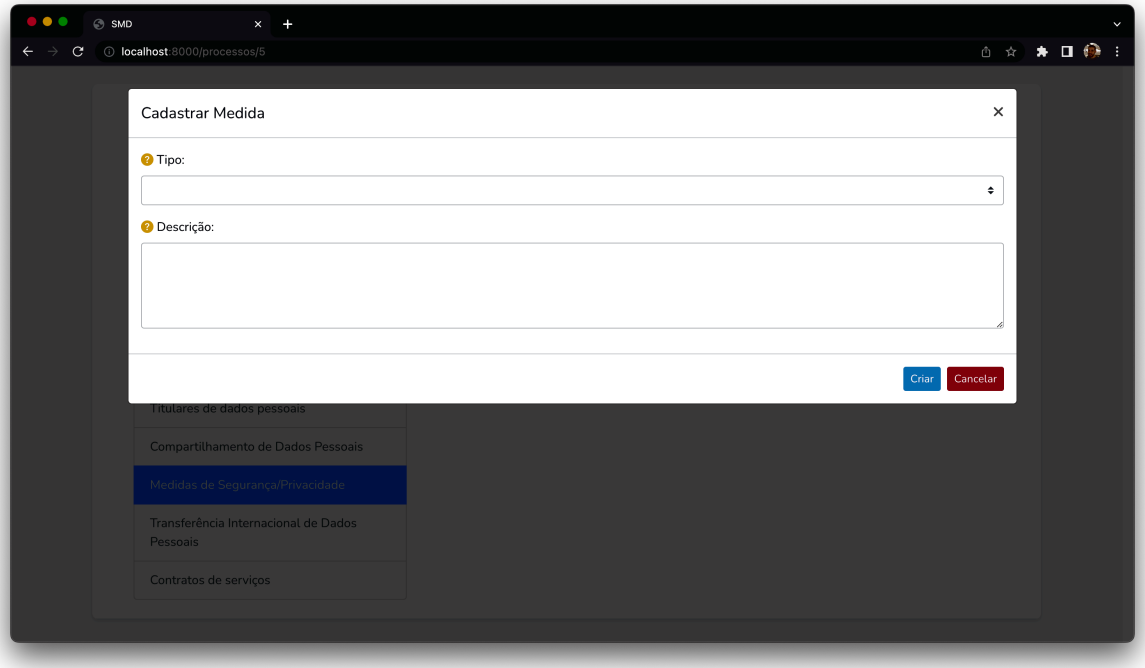

Figura 44: Tela de cadastro de medida de segurança e privacidade

- Seção para cadastrar/listar/visualizar/excluir transferência internacional de dados pessoais (Figura 45 e Figura 46):

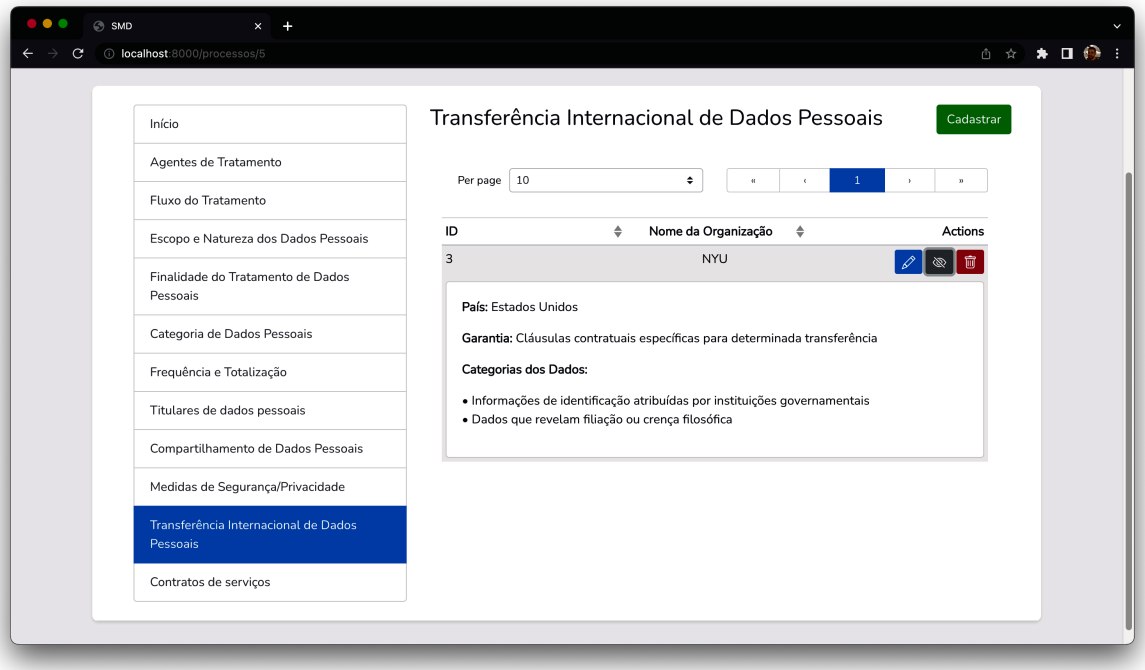

Figura 45: Tela de gerenciamento de transferências internacional de dados pessoais

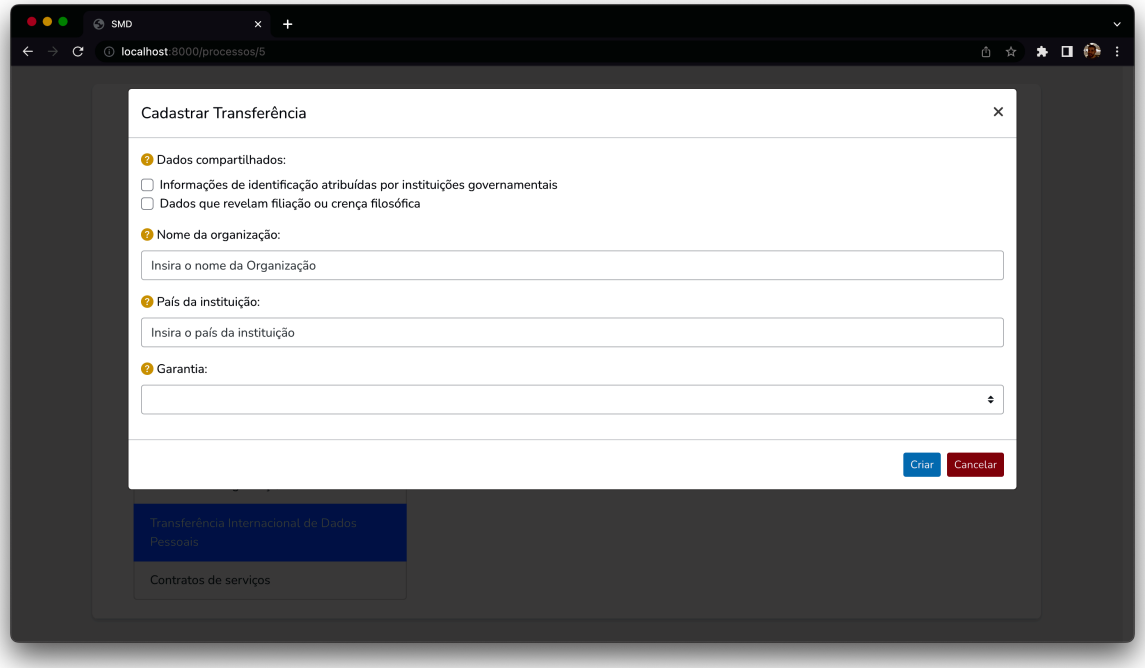

Figura 46: Tela de cadastro de transferência de dados pessoais

- Seção para cadastrar/listar/visualizar/excluir contratos de serviços e/ou soluções de TI (Figura 47 e Figura 48):

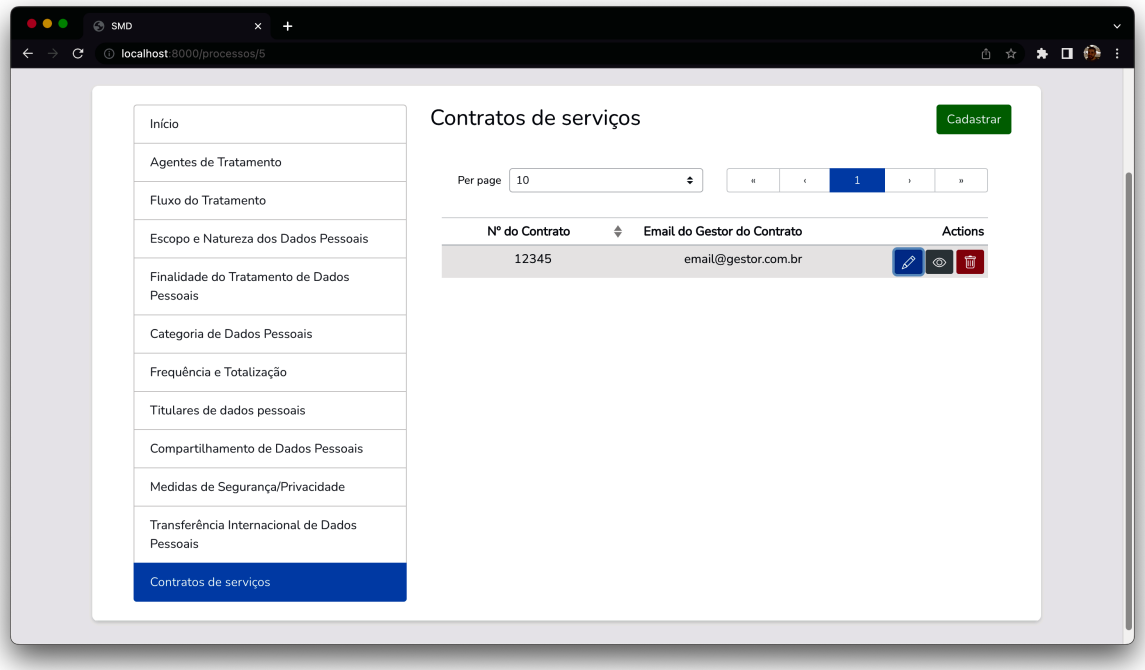

Figura 47: Tela de gerenciamento de contratos de serviços

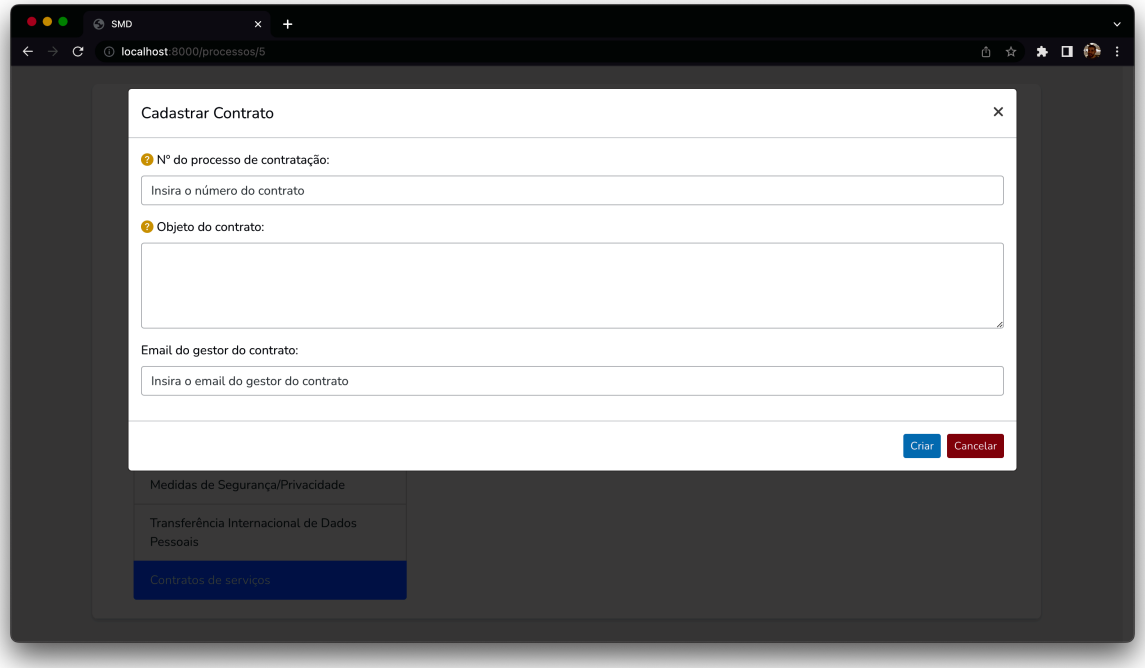

Figura 48: Tela de cadastro de contrato de serviço

4.7.2 IDP em Análise

- Quando o processo se encontra em análise, o status aparece da seguinte forma (Figura 49):

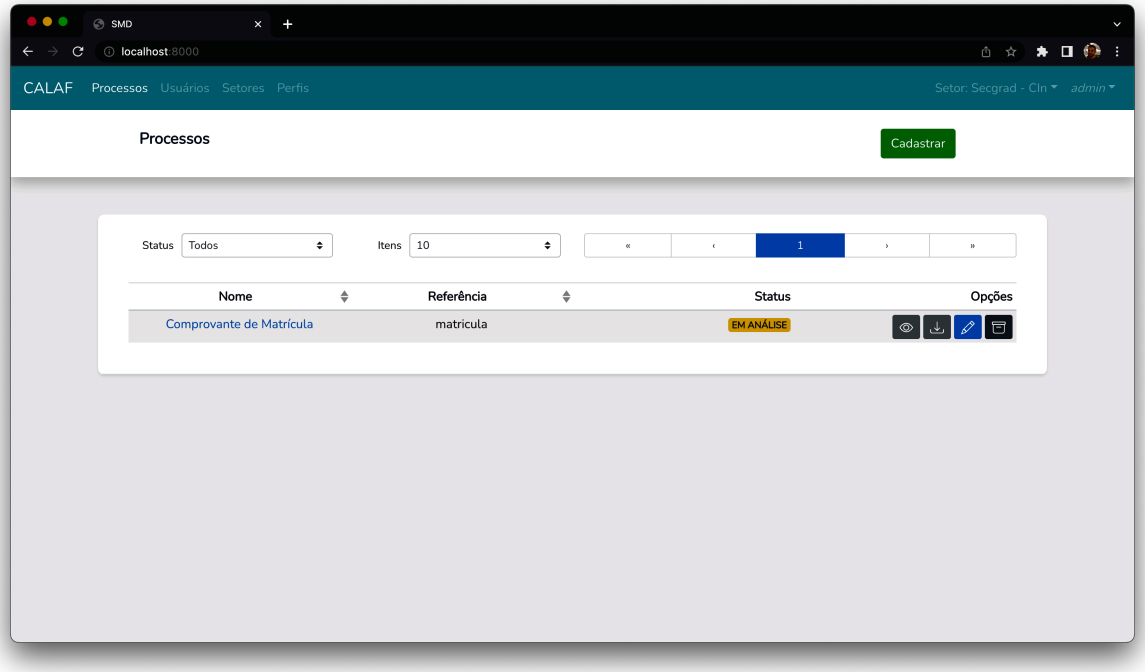

Figura 49: Processo em análise

- Na tela de IDP, as seções aparecem como “pendente” de análise (Figura 50):

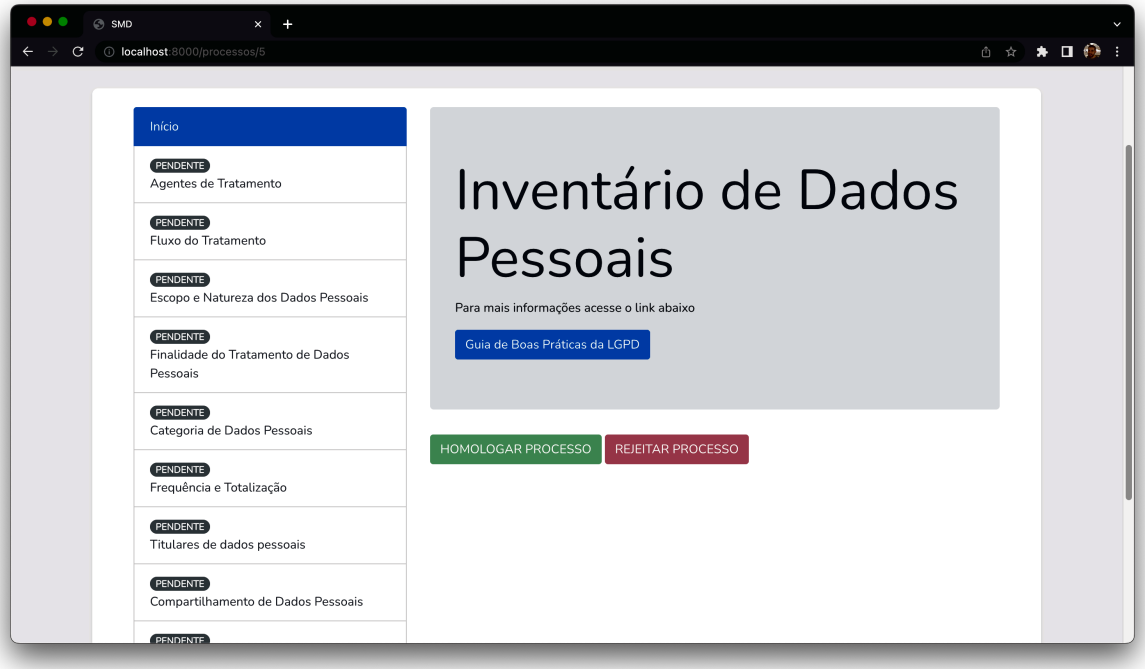

Figura 50: Tela de IDP quando o processo está em análise

- É necessário Aprovar ou Rejeitar cada uma das seções individualmente (Figura 51):

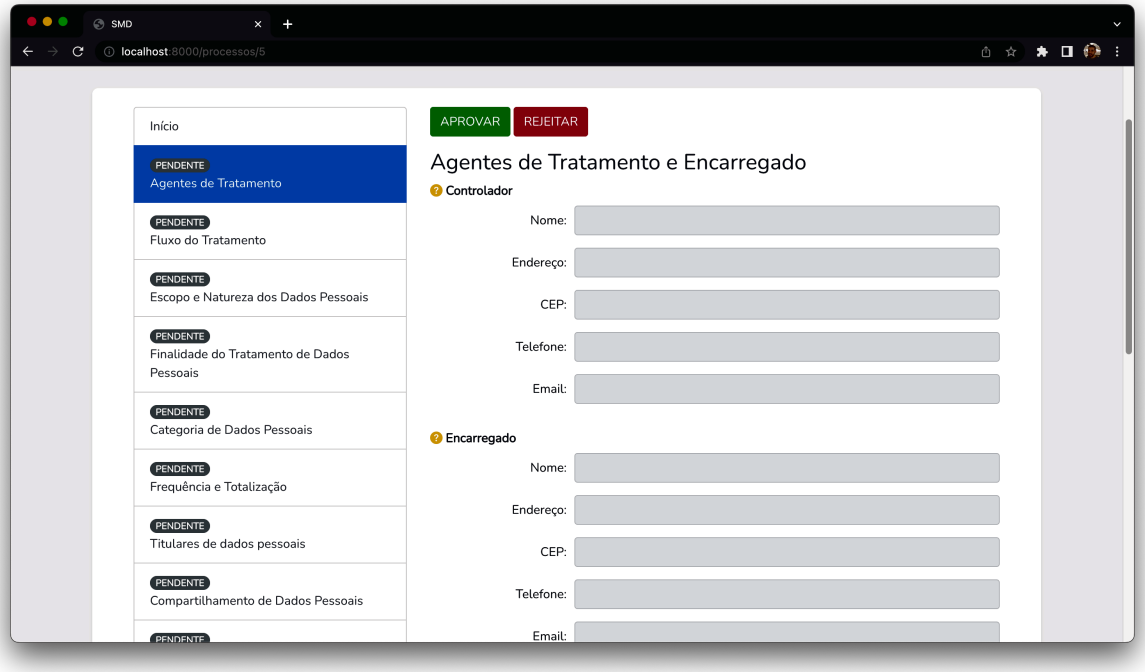

Figura 51: Seção de um IDP quando o processo está em análise

- Ao Aprovar uma seção, a label de “Aprovado” aparece junto ao título da seção. Enquanto o processo estiver em análise, é possível rejeitar a seção (Figura 52):

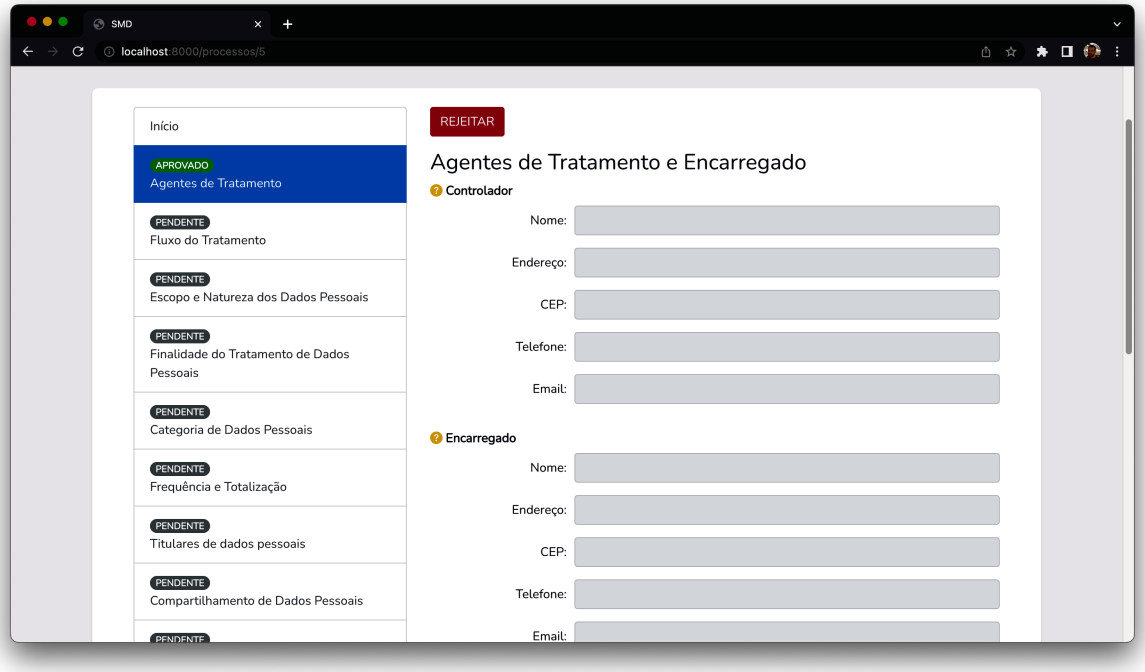

Figura 52: Seção aprovada de um IDP quando um processo está em análise

- Caso o analista decida por rejeitar, é necessário escrever uma mensagem para o

Operador que irá corrigir (Figura 53):

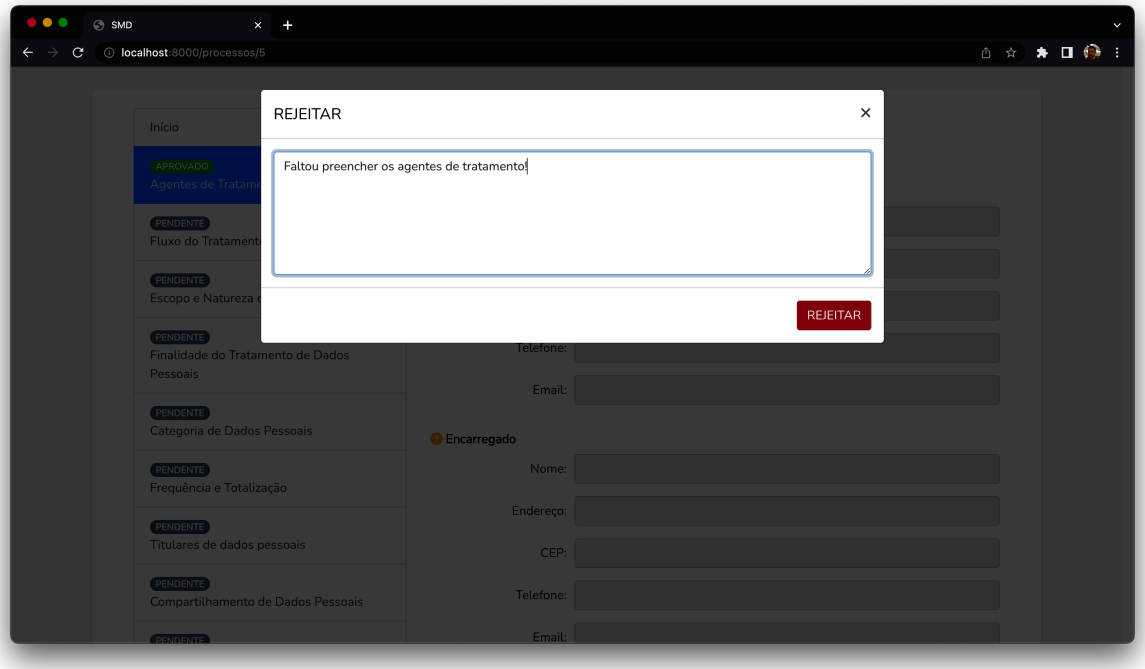

Figura 53: Formulário para rejeitar uma seção do IDP

- A mensagem aparece no topo da seção. Enquanto o processo estiver em análise é possível mudar a mensagem ou aprovar (Figura 54):

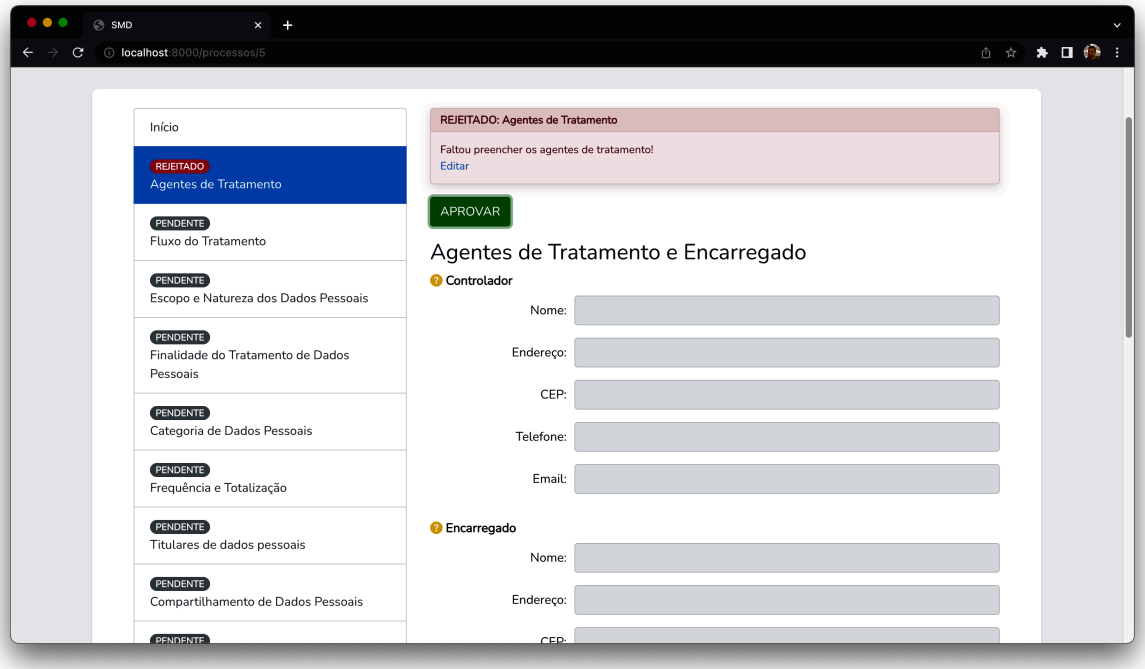

Figura 54: Seção rejeitada do IDP de um processo em análise

- Todas as mensagens de erro aparecem no topo da seção de Início do IDP. Ao clicar em visualizar, aparece a seção da mensagem de erro (Figura 55):

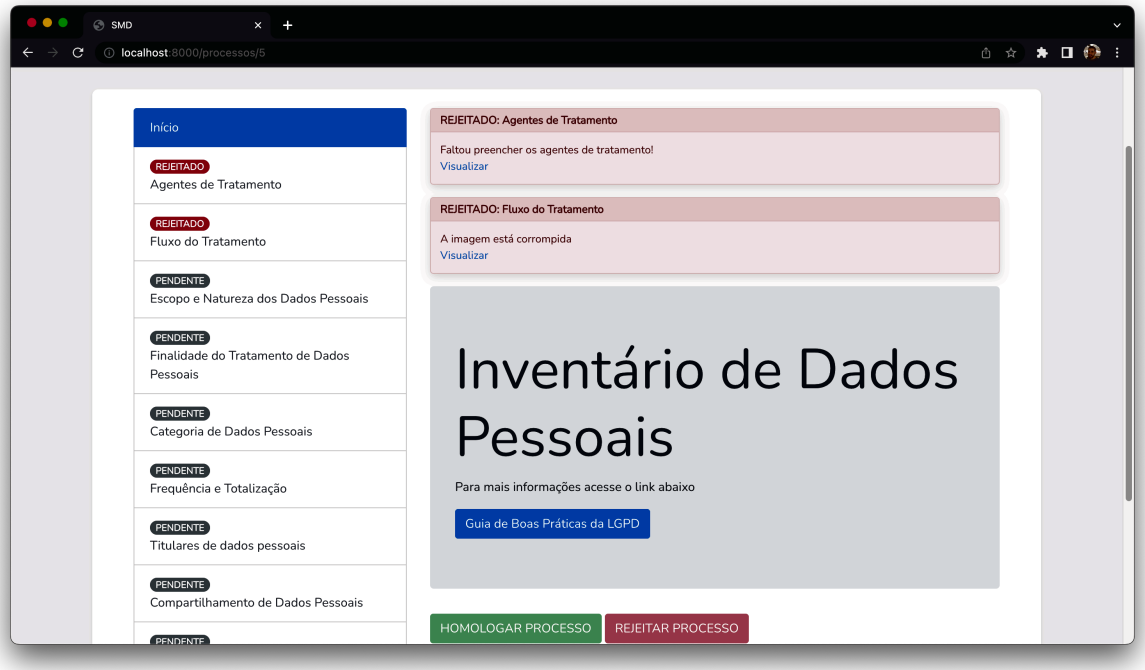

Figura 55: Tela inicial do IDP de um processo em análise com duas seções rejeitadas

4.7.3 IDP Pronto

- Uma vez que todas as seções tenham sido aprovadas e/ou rejeitadas, o processo fica em status de “Pronto”, o que significa que ele está pronto para ser rejeitado ou aprovado.

- Quando um processo possui um ou mais seções rejeitadas, a única opção disponível é Rejeitar o processo(Figura 56):

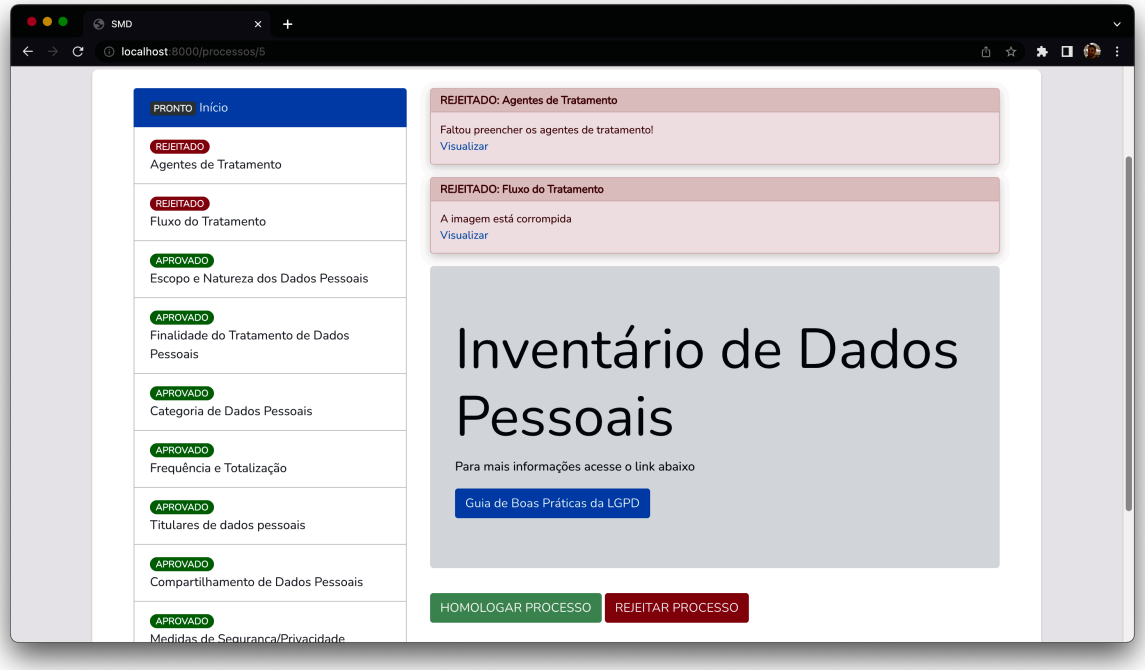

Figura 56: IDP em estado de “pronto”, com todas as seções analisadas

- O projeto tendo sido rejeitado, ele retorna para status “Pendente”, e a opção de “Solicitar Análise” reaparece (Figura 57):

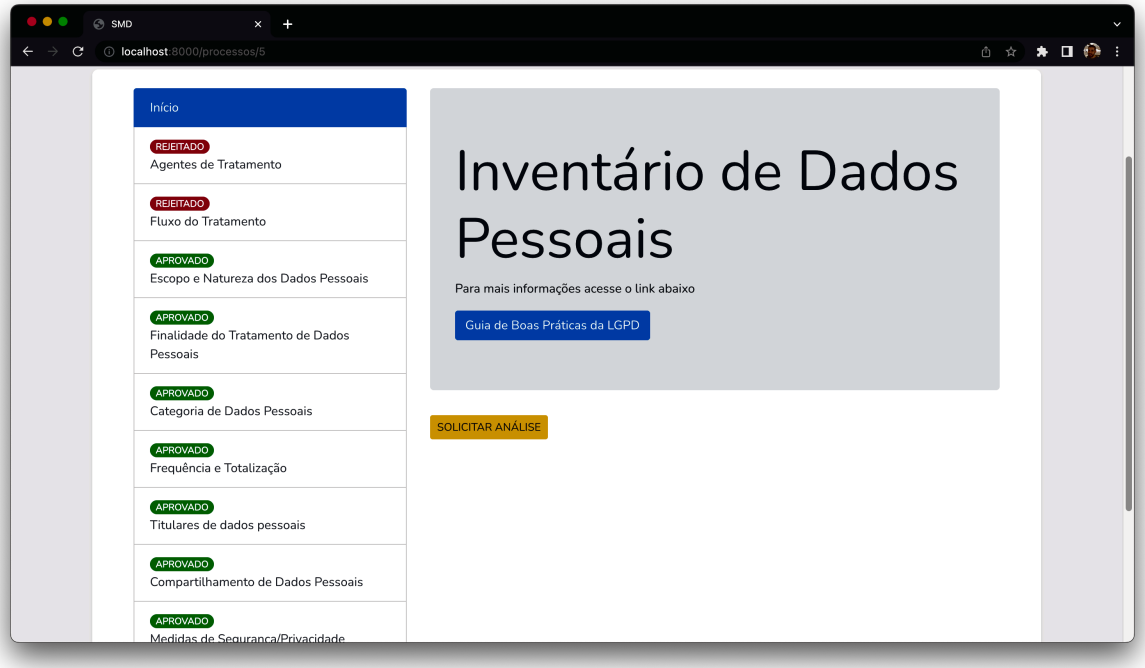

Figura 57: Tela inicial do IDP de um processo com status pendente

- Ainda em “Pendente”, apenas as seções rejeitadas estão disponíveis para serem

editadas. Todas as outras ficam apenas em modo de visualização, com os formulários desabilitados (Figura 58):

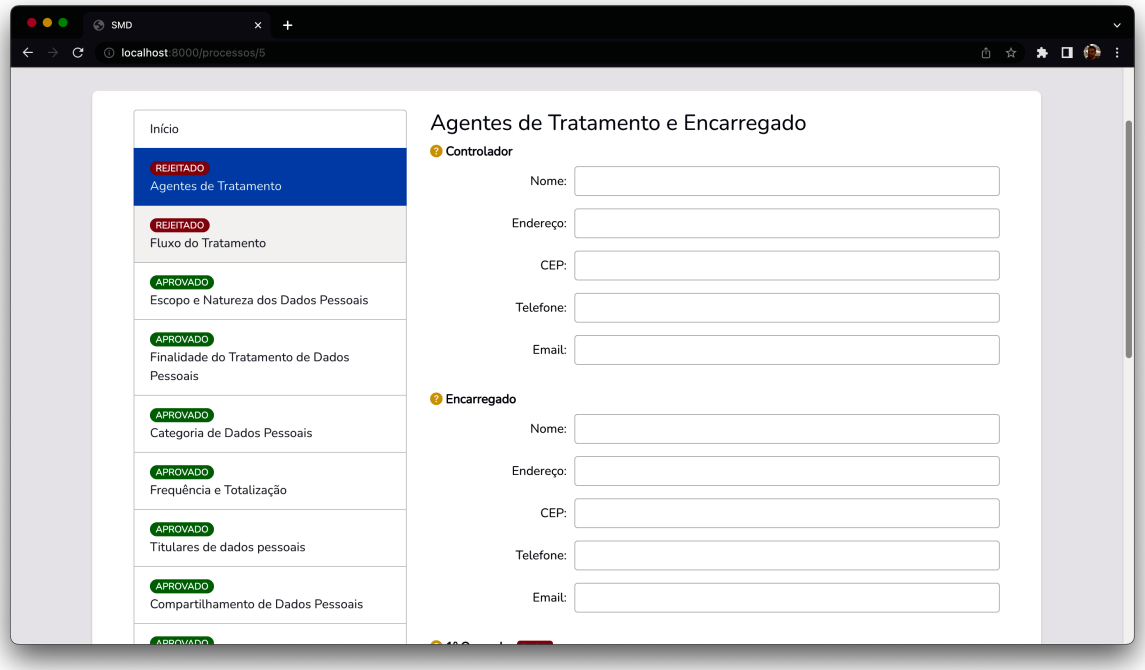

Figura 58: Tela de cadastro de agentes de tratamento e encarregado. Essa seção foi rejeitada em sua última análise

- Uma vez que todas as seções tenham sido individualmente aprovadas, o a opção de homologar o processo fica disponível enquanto que a de rejeitar fica desabilitada (Figura 59):

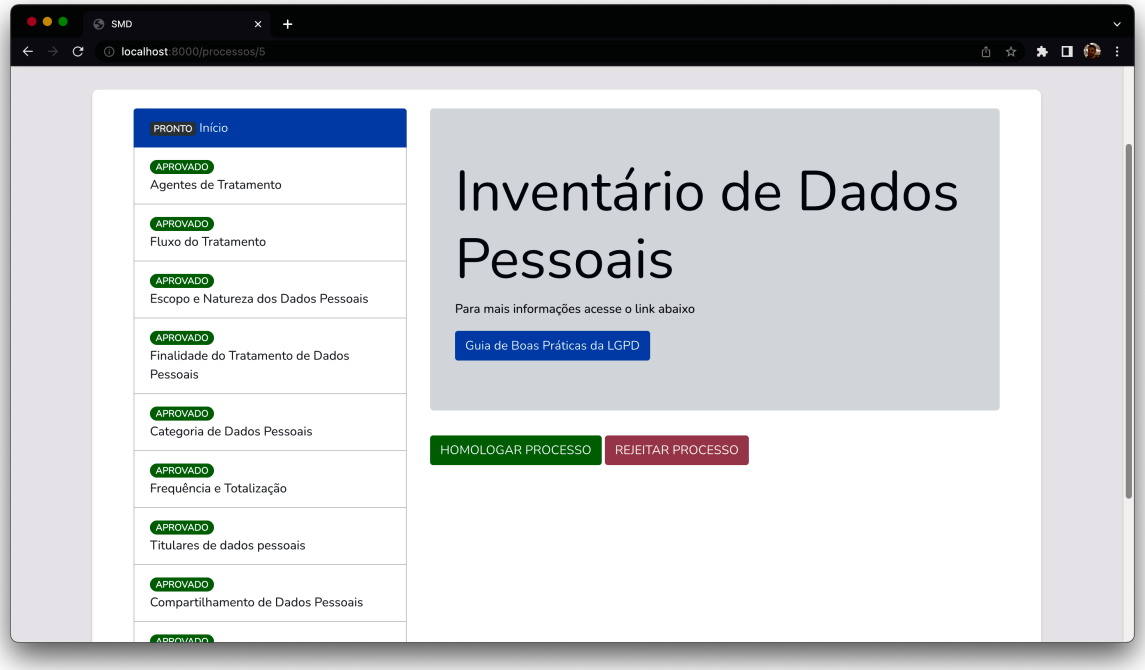

Figura 59: Tela inicial do IDP de um processo cujas seções foram todas aprovadas

- O projeto estando em status de “Homologado”, a opção de solicitar análise reaparece e fica novamente disponível (Figura 60):

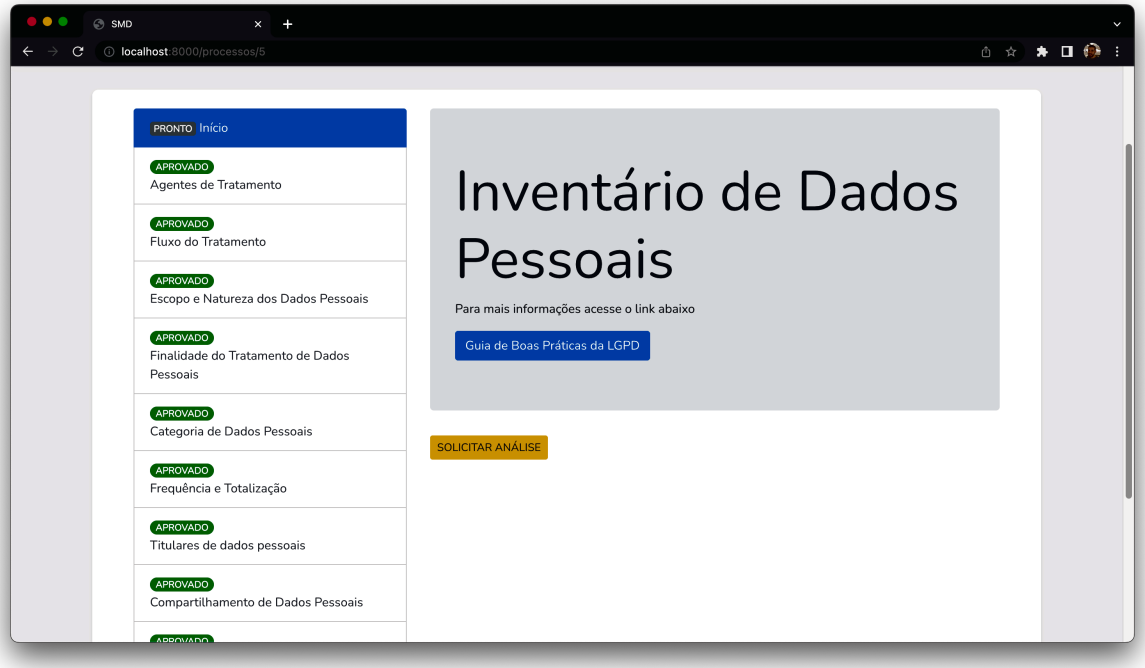

Figura 60: Tela inicial de um IDP cujo processo possui status de “homologado”

- Tela de listagem de processos com um processo homologado (Figura 61):

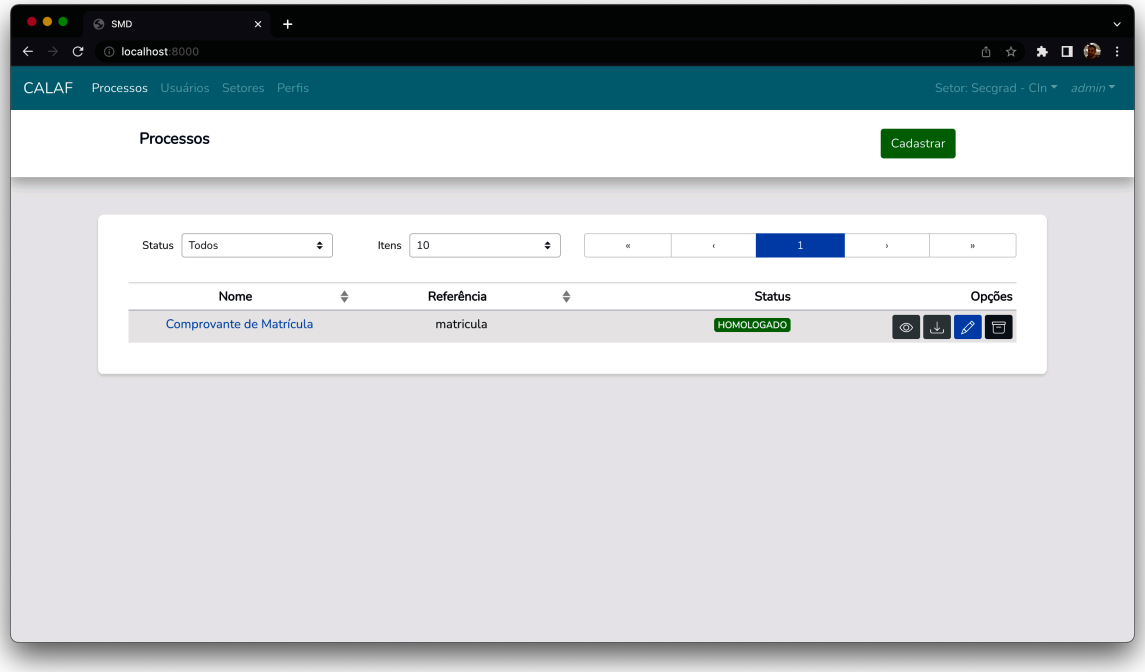

Figura 61: Processo homologado

4.7.4 Arquivar/Desarquivar Processo

- A qualquer momento é possível arquivar um processo clicando na opção “Arquivar” da tela de listagem de processos (Figura 62):

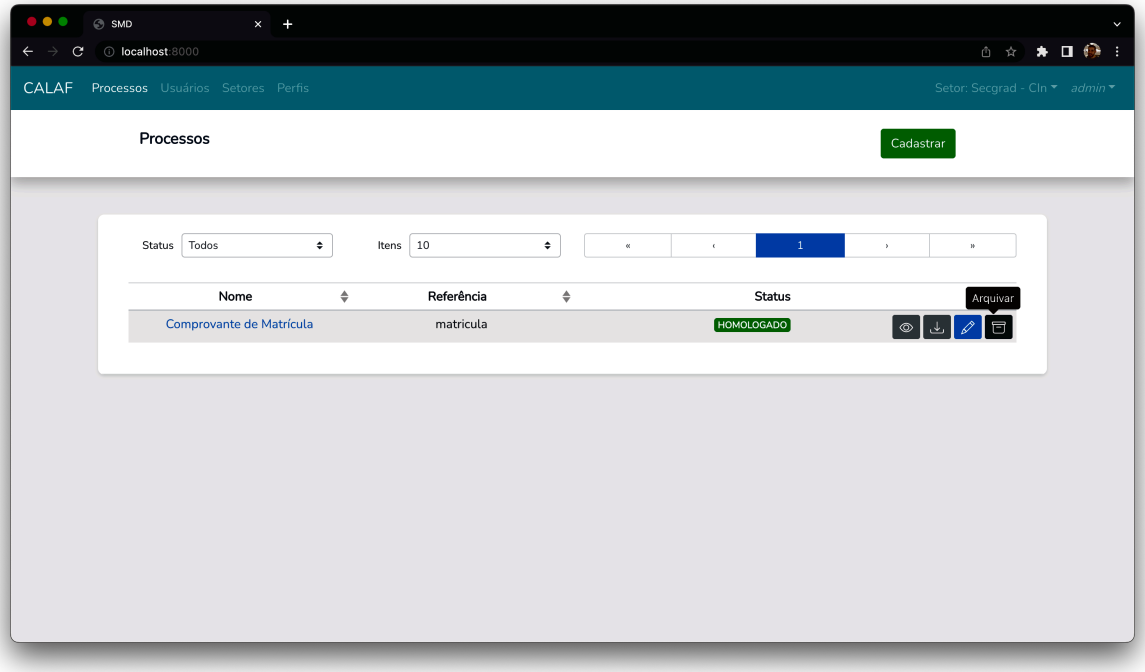

Figura 62: Botão de arquivar processo em destaque

- Para listar os processos arquivados, é necessário filtrar o status por “Arquivado”. A qualquer momento é possível desarquivar um processo arquivado clicando no botão de “Desarquivar” (Figura 63):

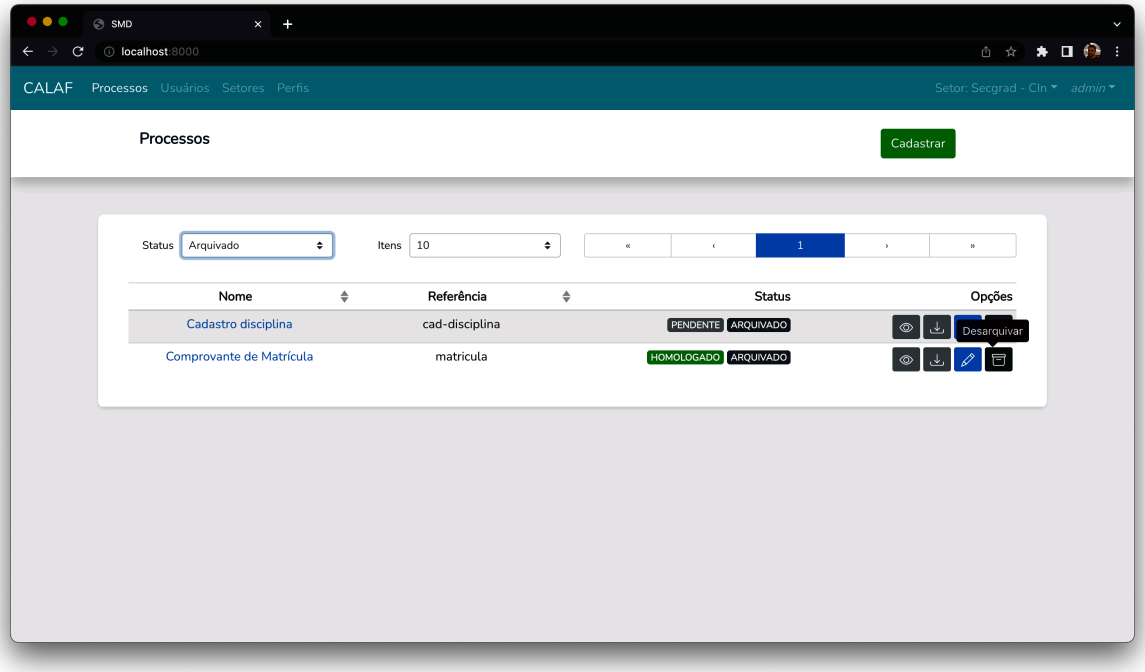

Figura 63: Botão de desarquivar processo em destaque

4.7.5 Gerar PDF do Processo

- É possível visualizar o PDF do processo clicando na opção “Download PDF” (Figura 64):

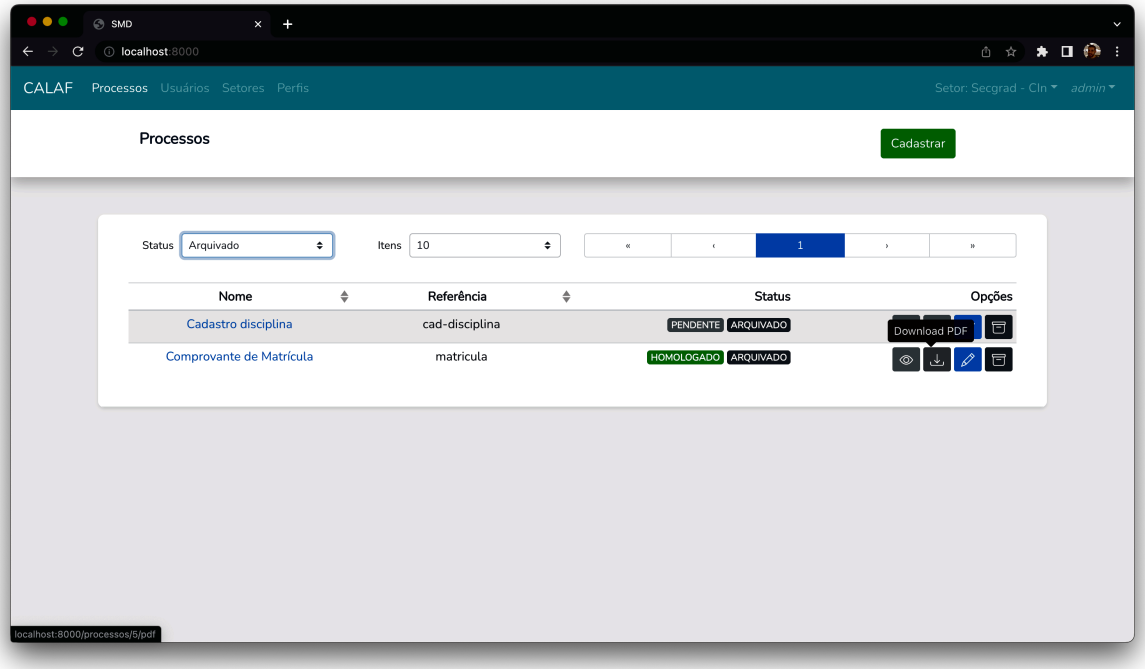

Figura 64: Botão de gerar PDF em destaque

- PDF de um processo homologado (Figura 65):

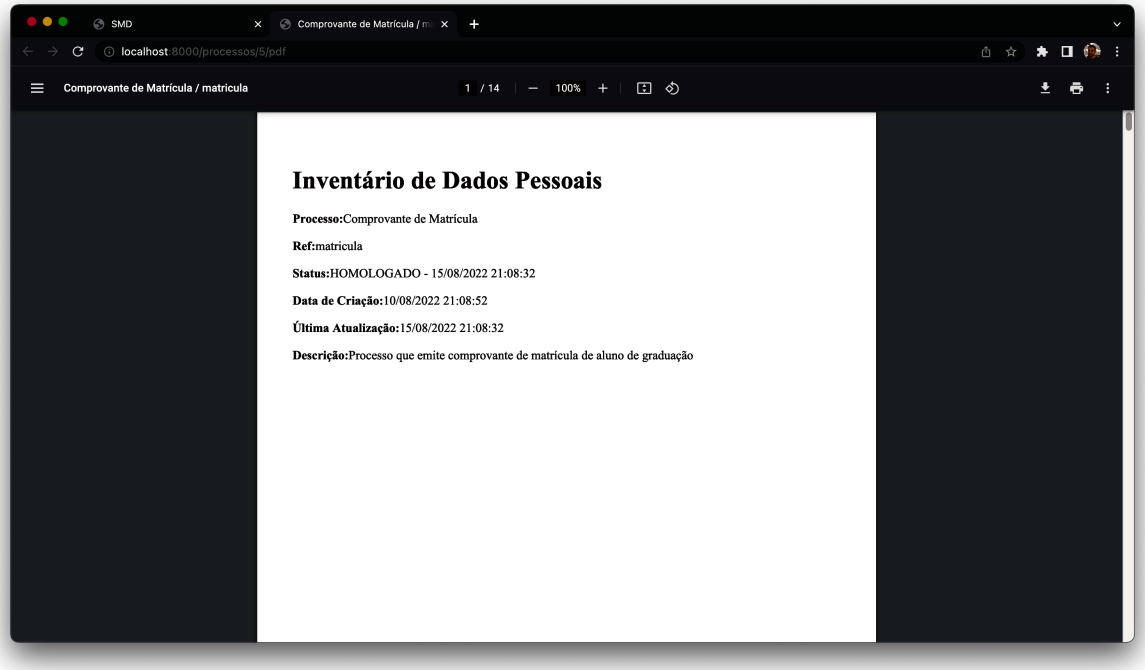

Figura 65: PDF do Inventário de Dados Pessoais

5

CONCLUSÃO

5.1 CONSIDERAÇÕES FINAIS

Com o levantamento bibliográfico realizado neste estudo, foi possível conhecer os principais aspectos dos temas Privacidade, Lei Geral de Proteção de Dados, Processos e Inventário de Dados Pessoais. Como foi visto, o cuidado com a privacidade tem sido uma preocupação crescente, ao longo dos anos, de autoridades de diversos países. Uma das formas de violação de privacidade se dá por meio da divulgação não autorizada de informações ou mesmo pelo vazamento de dados, os quais podem ocorrer durante o tratamento de dados por entidades públicas ou privadas. Logo, pode-se considerar a preocupação com a privacidade como uma prerrogativa para o tratamento de dados, a fim de evitar qualquer contravenção legal, uma vez que a mesma pode ser garantida com regulamentação do acesso às informações que as organizações detêm controle.

Uma importante regulamentação que surgiu nos últimos anos foi a General Data Protection Regulation (GDPR) na União Europeia (UE), com o esforço do partido *The Greens* no intuito de melhorar o tratamento de dados pessoais. A GDPR foi importante não só para a UE, mas, também, para outros países que tiveram que se adaptar criando legislações ao mesmo nível da europeia caso quisessem manter relações comerciais com os países deste bloco. No Brasil, surgiu então, Lei Geral de Proteção de Dados Pessoais (LGPD) que possui, naturalmente, bastante semelhança à GDPR.

A LGPD traz algumas determinações como a criação de um órgão chamado de Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e garantir o cumprimento das normas da dessa lei. Como visto, a ANPD está sob comando do Poder Executivo, o que

pode comprometer a parcialidade do bloco. Esta mesma lei define, ainda, os responsáveis pelo tratamento dos dados, conhecidos como os agentes de tratamentos. São eles: (1) controlador, responsável pela coleta de dados e decidir como se dará o tratamento de dados e qual a finalidade; (2) o encarregado, responsável por intermediar a comunicação entre o controlador, titular dos dados e a ANPD; por fim, o (3) operador, pessoa física ou jurídica que de fato irá tratar os dados. Quanto ao tratamento de dados, o operador deve, antes de tudo, se certificar de que há uma base legal que permita o tratamento. Para isso, a LGPD elenca algumas hipóteses de tratamento.

A qualquer momento a ANPD pode exigir um relatório de uma entidade que trata dados chamado de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Documento este que serve para analisar se o tratamento de dados realizado pela entidade está em conformidade com a LGPD. Para produzir este documento, a Secretaria de Governo Digital (SGD) sugere a elaboração de um Inventário de Dados Pessoais (IDP), que se trata de um mapeamento de dados do processo de negócio em que há tratamento de dados pessoais. Portanto, o IDP serve para documentar o tratamento que ocorre dentro de um processo ou serviço de uma empresa, órgão público, etc.

Para a elaboração do IDP, a SGD disponibiliza um template em formato de planilha de dados para que o operador possa preenche-la de forma a documentar todo o tratamento de dados que se dá em um ou mais processos de negócio. Contudo, verifica-se que a utilização de uma planilha para esta atividade pode ocasionar em dificuldade para manutenção e aumentar as chances de erros, visto a necessidade de operação manual constante. Além disso, é uma prática que impede a colaboração, visto que manter um arquivo único compartilhado por diversas pessoas aumenta a chance de perda do trabalho além de não garantir a qualidade das informações, pois fica suscetível ao erro humano na hora de preencher os dados. A falta de um sistema específico para realizar o mapeamento de dados é a grande motivação para a elaboração deste trabalho.

Para isso, foi desenvolvido um sistema web batizado de Sistema de Mapeamento de Dados (SMD), que serve como ferramenta alternativa para substituir o template do IDP sugerido pela SGD. Nele, é possível cadastrar o processo que se deseja ter o tratamento de dados documentado e, para cada seção do IDP, há uma seção no SMD para que a documentação seja fidedigna ao inventário. É possível também, que diferentes perfis tenham múltiplas permissões em variados setores de uma organização. Um processo pode, a qualquer momento, ser arquivado ou desarquivado, além de pode requisitar a edição e homologação do mesmo. Todas essas

funcionalidades tornam o trabalho bastante colaborativo e diminui a chance de erro humano. Logo, conclui-se que o SMD pode ser uma ferramenta alternativa que permite a substituição do template do Inventário de Dados Pessoais fornecido pela Secretaria de Governo Digital.

Certamente, muitas pessoas se beneficiarão com a utilização do SMD para cumprir a tarefa do Inventário. Isto porque torna-se mais fácil e seguro o preenchimento dos dados do processo, bem como a manutenção e atualização das informações. Os titulares dos dados também se beneficiarão, pois, indiretamente, há menos chances de ocorrer um erro humano no preenchimento das informações do IDP. Em suma, o SMD pode ser de grande utilidade para os órgãos públicos do Brasil dada a sua proposta de substituir um trabalho que hoje é realizado de forma manual.

5.2 TRABALHOS FUTUROS

Como visto, o RIPD é o principal documento que mostra se a organização está em conformidade com a LGPD e pode ser requerido a qualquer momento pela ANPD. Para produzi-lo, a SGD recomenda que se faça a *documentação* dos processos de negócios que realizam tratamento de dados pessoais por meio do IDP. Portanto, para o futuro, seria interessante que a aplicação consiga gerar o RIPD de forma automatizada utilizando as informações que foram preenchidas durante a documentação do IDP pelo Operador. Outro ponto a ser considerado acerca de futuras pesquisas, é a realização de estudos comparativos com outros trabalhos relacionados. Mais especificamente, comparar a aplicação SMD, a qual foi desenvolvida durante este projeto, com outras ferramentas e sistemas que possam realizar o mesmo tipo de atividade. Outra forma de avaliar o SMD é disponibilizando-o para os *stakeholders*. Dessa forma, seria possível realizar testes de usabilidade.

REFERÊNCIAS

[1] Araújo Da Costa Júnior, E., Jéssyka, O. ., & Ferreira Vilela, F. (2020). Análise de conformidade de processos de negócios em relação a LGPD Recife 2020 2.

[2] Brasil (2011). Lei Nº 12.414, de 9 de Junho DE 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 4 de Outubro de 2022.

[3] Brasil (2014). Lei Nº 12.965, de 23 DE Abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 4 de Outubro de 2022.

[4] Brasil (2020). Secretaria de Governo Digital: Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD). 65.

[5] Brasil (2022a). Ministério da Cidadania: Acesso à Informação - LGPD. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em 19 de Julho de 2022.

[6] Brasil (2022b). Ministério da Cidadania: Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em 19 de Julho de 2022.

[7] Brito, Felipe Timbó e Machado, J. C. (2017). Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. *An. da XXXVI Jorn. Atualização em Informática*, (July):91–130.

[8] de Oliveira, A. C. S. (2022). *DPO-Encarregado de dados pessoais-Teoria e Prática*. Saraiva Educação SA.

[9] Erickson, A. (2019). Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. *Brooklyn Journal of International Law*, 44(2):859.

[10] Evan You (2022). VueJS. Disponível em: https://vuejs.org/. Acesso em 4 de Outubro de 2022.

[11] Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Rev. da Fac. Direito, Univ. São Paulo*, 88(0):439.

[12] Goddard, M. (2017). The eu general data protection regulation (gdpr): European regulation that has a global impact. *International Journal of Market Research*, 59(6):703–705.

[13] Hu, R., Wang, Z., Hu, J., Xu, J., & Xie, J. (2008). Agile web development with web framework. In *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 1–4.

[14] iapp (2022). 2022 Privacy Tech Vendor Report. Disponível em: https://iapp.org/media/pdf/resource_center/2022TechVendorReport.pdf. Acesso em 19 de Outubro de 2022.

[15] Jet Brains (2022). PHP Storm Features. Disponível em: https://www.jetbrains.com/phpstorm/features/. Acesso em 4 de Outubro de 2022.

[16] Jones, P. M. (2016). *Modernizing Legacy Applications in PHP*. Packt Publishing Ltd.

[17] Laravel LLC. (2022). Docs - Laravel - The PHP Framework For Web Artisans. Disponível em: `https://laravel.com/docs`. Acesso em 4 de Outubro de 2022.

[18] Machado, D. D. (2021). Guia de Elaboração de Inventário de Dados Pessoais. *Rev. Científica Multidiscip. Núcleo do Conhecimento*, 93–98.

[19] Magacho, B. T. P. & Trento, M. (2021). LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público? *... Rev. Bras. Pesqui. Jurídicas (Brazilian J. Law Res.*, 2(2):7–26.

[20] PHP - A Maneira Errada (2022). Disponível em: `https://phpthewrongway.com/pt_br/`. Acesso em 4 de Outubro de 2022.

[21] PHP - FIG (2022). PHP Framework Interop Group. Disponível em: `https://www.php-fig.org/`. Acesso em 4 de Outubro de 2022.

[22] Pinheiro, P. P. (2020). *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD*. Saraiva Educação SA.

[23] Queiroz, M. J. D. & Motta, G. H. M. B. (2013). Privacidade e Transparência no Setor Público : Um Estudo de Caso da Publicação de Microdados do INEP. 1–4.

[24] Singh, H. & Hassan, S. I. (2015). Effect of solid design principles on quality of software: An empirical assessment. *International Journal of Scientific & Engineering Research*, 6(4).

[25] Squizani, C. & Sarturi Prass, F. (2018). Otimização e automação de processos de negócio com uso da notação BPMN: Um estudo de caso. *Discip. Sci.*, 19(1):69–86.

[26] Tessari, R. (2008). Gestão De Processos De Negócio: Um Estudo De Caso Dda Bpmn Em Uma Empresa Do Setor Moveleiro. 83.

[27] The PHP Group (2022). Manual do PHP. Disponível em: `https://www.php.net/manual/pt_BR/`. Acesso em 4 de Outubro de 2022.

[28] Vieira, T. M. (2007). O direito À privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.

[29] Wang, X. & Zhao, J. (2021). Domain invariant-based spreadsheet debugging. *Proc. - 2021 IEEE/ACM Int. Work. Autom. Progr. Repair, APR 2021*, 1:21–22.