INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIAS E TECNOLOGIA DO AMAZONAS
CAMPUS MANAUS CENTRO DEPARTAMENTO ACADÊMICO DE INFORMAÇÃO E COMUNICAÇÃO CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

DPOHub: uma ferramenta para auxiliar o controle de práticas e ocorrências na gestão de privacidade de dados pessoais.

Vinícius Martins Neves

Manaus - 2024
AM

Vinícius Martins Neves

DPOHub: uma ferramenta para auxiliar o controle de práticas e ocorrências na gestão de privacidade de dados pessoais.

“Trabalho de Conclusão de Curso apresentado à banca examinadora Curso Superior de Tecnologia de Desenvolvimento de Software do Instituto Federal de Educação, Ciências e Tecnologia do Amazonas – IFAM Campus Manaus - Centro, como requisito para o cumprimento da disciplina TCC II – Projeto de Software”

Orientador: Prof Dr Renildo Viana Azevedo

Manaus - 2024

AM

Biblioteca do IFAM – Campus Manaus Centro

N518d Neves, Vinícius Martins.
DPOHub: uma ferramenta para auxiliar o controle de práticas e ocorrências na gestão de privacidade de dados pessoais / Vinícius Martins Neves. – Manaus, 2023.
79 p. : il. color.

Monografia (Tecnologia em Análise e Desenvolvimento de Sistemas). – Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, *Campus* Manaus Centro, 2023.
Orientador: Prof. Dr. Renildo Viana Azevedo

1. Desenvolvimento de sistemas. 2. Ferramenta de controle. 3. LGPD. 4. Privacidade. I. Azevedo, Renildo Viana. (Orient. II. Instituto Federal de Educação, Ciência e Tecnologia do Amazonas. III. Título.

CDD 005.3

Elaborada por Márcia Auzier CRB 11/597

RESUMO

Este projeto trata do desenvolvimento de um sistema web que auxilie o encarregado de dados em suas atividades de gerenciamento de práticas e ocorrências. O sistema contém funcionalidades que facilitam a administração de ocorrências e suas soluções, bem como práticas a serem adotadas pelos diferentes setores que compõem uma organização. Portanto, foi desenvolvida uma aplicação web que notifica *e-mails* de acordo com seus respectivos conjuntos de práticas e auxilia o gerenciamento do atendimento de ocorrências, fornecendo alertas via *e-mail* sobre movimentações e detalhamento de resolução dela para consulta posterior.

Palavras-Chave: LGPD, Encarregado de Dados, Privacidade, Notificação, Ocorrência.

ABSTRACT

This project deals with the development of a web system that assists data managers in their practice and occurrence management activities. The system contains features that facilitate the management of incidents and their solutions, as well as practices to be adopted by the different sectors that make up an organization. Therefore, a web application was developed that notifies e-mails according to their respective sets of practices and helps manage incident response, providing alerts via e-mail about movements and details of their resolution for later consultation.

Keywords: LGPD, Data Controller, Privacy, Notification, Occurrence.

SUMÁRIO

INTRODUÇÃO 1
PROBLEMATIZAÇÃO 2
JUSTIFICATIVA 3
OBJETIVOS 4
Objetivo Geral 4
Objetivos Específicos 4
VISÃO GERAL 4
CAPÍTULO 1 - FUNDAMENTAÇÃO TEÓRICA 5
1.1 PROGRAMA DE GOVERNANÇA EM PRIVACIDADE 9
1.2 SERVIÇOS DE NOTIFICAÇÃO (*E-MAIL*) 13
1.3 WEBSOCKET 14
1.4 MICROSSERVIÇOS 15
1.5 TECNOLOGIAS UTILIZADAS 16
1.5.1 Java 16
1.5.2 Framework Angular 17
1.5.3 MySQL / MariaDB 18
CAPÍTULO 2 - PLANEJAMENTO DO PROJETO DPOHUB 18
2.1 INTRODUÇÃO 18
2.1.1 Operador 19
2.1.2 Encarregado de Dados ou Data Protection Officer (DPO) 19
2.2 DIAGRAMA DE CASOS DE USO 21
2.2.1 Gerenciamento de Práticas 21
2.2.2 Ocorrência Externa 33
2.2.3 Ocorrências 38
2.3 MODELO DE NEGÓCIOS (BPMN) 47

2.3.1 Gerenciamento de Práticas 47
2.3.2 Gerenciamento de Ocorrências 48
2.4 PROTÓTIPOS 49
2.4.1 Gerenciamento de Práticas 49
2.4.3 Gerenciamento de Ocorrências 51
CAPÍTULO 3 - IMPLEMENTAÇÃO DO PROJETO DPOHUB 52
3.1 INTRODUÇÃO 52
3.2 ARQUITETURA 52
3.3 DIAGRAMA DE CLASSES 53
3.4 DIAGRAMA DE ESTADO (OCORRÊNCIA) 55
3.5 DIAGRAMAS DE SEQUÊNCIA 56
3.5.1 Ocorrência 56
3.5.2 Prática 57
3.6 DIAGRAMA DE IMPLEMENTAÇÃO 58
3.7 TELAS 59
3.7.1 Gerenciamento de Práticas 59
3.7.2 Gerenciamento de Ocorrências 60
4 CONSIDERAÇÕES FINAIS 68
5 REFERÊNCIAS 69

ÍNDICES

FIGURAS

Figura 1 - Atores da LGPD 9
Figura 2 - Princípios da LGPD 10
Figura 3 - Marcos de Conformidade com a LGPD 12
Figura 4 - Encarregado - Nomeação 12
Figura 5 - Encarregado - Atividades 13
Figura 6 - Diferença entre WebSocket e REST 15
Figura 7 - Controle de Práticas 49
Figura 8 - Controle de Práticas (Detalhes) 49
Figura 9 - Controle de Conjuntos de Práticas 50
Figura 10 - Controle de Conjuntos de Práticas (Detalhes) 50
Figura 11 - Controle de Ocorrências 51
Figura 12 - Controle de Ocorrências (Detalhes) 51
Figura 13 - Sistemas Monolíticos e Microsserviços 53
Figura 14 - Formulário de Conjunto 59
Figura 15 - Formulário de Conjunto - Editar e-mails 59
Figura 16 - Formulário de Prática 60
Figura 17 - Cadastro de Ocorrência - Externo 61
Figura 18 - Cadastro de Ocorrência - Externo - Notificação 61
Figura 19 - Cadastro de Ocorrência 62
Figura 20 - Cadastro de Ocorrência - Notificação 63
Figura 21 - Edição de Ocorrência - Notificação 63
Figura 22 - Detalhamento - DPO 64
Figura 23 - Detalhamento - Operador 64
Figura 24 - Concluído 65

Figura 25 - Concluído - Notificação 65
Figura 26 - Validação Pendente - Detalhamento 66
Figura 27 - Ocorrências Inválidas - Invalidada.....66
Figura 28 - Ocorrências Inválidas - Detalhamento.....67

DIAGRAMAS

Diagrama 1 - Casos de Uso - Gerenciamento de Práticas 21
Diagrama 2 - Casos de Uso - Usuário Externo.....33
Diagrama 3 - Casos de Uso - Ocorrências 38
Diagrama 4 - Diagrama de Classes.....54
Diagrama 5 - Diagrama de Estado (Ocorrência).....55
Diagrama 6 - Diagrama de Sequência - Ocorrência 56
Diagrama 7 - Diagrama de Sequência - Prática 57
Diagrama 8 - Diagrama de Implementação 58

MODELOS

Modelo 1 - Gerenciamento de Práticas.....47
Modelo 2 - Gerenciamento de Ocorrências 48

QUADROS

Quadro 1 – Cadastro de conjunto de práticas 22
Quadro 2 - Atualizar conjunto de práticas.....24
Quadro 3 - Deletar conjunto de práticas 25
Quadro 4 - Criar práticas 27
Quadro 5 - Atualizar práticas 28
Quadro 6 - Deletar práticas.....30
Quadro 7 - Configurar intervalo de notificação 31
Quadro 8 - Cadastrar ocorrência 33
Quadro 9 - Validar ocorrência.....35

Quadro 10 - Consultar ocorrência.....36
Quadro 11 - Cadastrar ocorrência 39
Quadro 12 - Atualizar ocorrência 40
Quadro 13 - Movimentar ocorrência 42
Quadro 14 - Invalidar ocorrência 43
Quadro 15 - Adicionar comentário 45

INTRODUÇÃO

Na década de 1970, foram criadas as primeiras leis europeias direcionadas à proteção dos dados pessoais e garantia da privacidade na Internet. Na década de 1980, houve a unificação das normas entre países europeus para desenvolvimento e melhoria delas.

Com foco em estabelecer normas mais eficazes no mundo digital, a União Europeia desenvolveu a GDPR (*General Data Protection Regulation*), que estabelece regras a serem observadas quanto à coleta, armazenamento e manipulação de dados.

No Brasil, a Constituição Federal Brasileira de 1988, artigo 5º, tratava de forma geral sobre a proteção de dados pessoais e privacidade, e em 1996, com a lei 9.296, passou a referenciar a proteção do titular de dados, especificamente, nos meios de comunicação. Em 1993, o CDC (Código de Defesa do Consumidor) estabeleceu normas de como as empresas devem tratar os dados de titulares e garantir o fácil acesso aos mesmos, bem como exigir que o titular esteja ciente do registro de seus dados.

Até 2018, no Brasil, a lei que regulamentava a Internet era o Marco Civil da Internet (Lei 12.965/2014), que garante o direito à liberdade de expressão, privacidade e acesso à informação. Em 2018, o Brasil criou a Lei 13.709 (Lei Geral de Proteção de Dados - LGPD), uma lei fortemente embasada na GDPR, que visa a regulamentação da coleta, armazenamento, processamento e manipulação de dados de forma geral, ou seja, por meios eletrônicos ou não, por empresas privadas, públicas e pessoas físicas, dentro e fora do Brasil.

No Brasil, o controle dos processos envolvidos na regulamentação da LGPD é exercido por diversos órgãos, dentre eles, podemos destacar a Autoridade Nacional de Proteção de Dados (ANPD) que, de acordo com o artigo 55-J tem o papel de verificar se as empresas estão adequando-se às normas estabelecidas pela LGPD, disponibilizar informações necessárias para que sejam claras para as empresas, órgãos e pessoas físicas. Promover atividades que melhorem ou desenvolvam novos processos, bem como garantir o acesso da população ao devido conhecimento de seus direitos e deveres.

A adequação à LGPD precisa de um time especializado em tratamento de dados, composto por operador e encarregado, que, devido ao volume de informações necessárias para desenvolver suas atividades, envolverá diversos documentos, tornando-se de grande importância ferramentas auxiliares no gerenciamento das atividades desenvolvidas, com foco naquelas realizadas pelo encarregado de dados.

PROBLEMATIZAÇÃO

Com a entrada da LGPD em vigor em 2020, tornou-se necessário a regulamentação de órgãos e empresas até o prazo final de 31 de julho de 2021, sob pena de sanções que variam de advertência a multa de 2% do faturamento, limitado a R$ 50 milhões de reais.

A adequação de uma empresa à LGPD envolve a manipulação de diversos documentos de especificações de armazenamento, controle, processamento e finalidade dos dados, medidas e práticas para prevenir, sanar possíveis lacunas de segurança da informação e comunicação com titulares.

Em levantamento de julho de 2021 realizado pela *BluePex Cybersecurity*[1] em conjunto com 200 gestores de PMEs (Pequena e Média Empresa), somente 4% dos entrevistados consideravam-se aderentes à lei. No mesmo levantamento, publicado em 23 de março de 2022, houve um salto para 15%. Vale ressaltar que, apesar de ter sido um aumento significativo, é uma quantidade muito pequena se comparada às 8,5 milhões de PMEs existentes.

De acordo com a “Pesquisa sobre a LGPD no mercado brasileiro” desenvolvida pela Alvarez & Marsal, HLFMap, Privacy Tools, Serur Advogados e ABNT[2] em conjunto com 366 participantes com perfis diferenciados, destas, somente 9,8% consideram estar completamente, ou quase, em conformidade com a LGPD.

Segundo relatório do Fórum Econômico Mundial, 95% dos problemas de segurança cibernética são causados por descuido humano, sendo 43% de ameaças

[1] **Bluepex Cybersecurity:** é uma empresa com foco em pesquisa antimalware com sede em São Paulo, e com atuação global.

[2] **ABNT (Associação Brasileira de Normas Técnicas):** tem como objetivo, disseminar, através de documentos normativos e avaliação de conformidade, a sistematização do conhecimento da sociedade brasileira.

internas, criando um cenário ainda mais adequado para atuação de cibercriminosos, justificando a necessidade de programas de conscientização dentro das organizações controladoras de dados.

As empresas/organizações precisam tratar com maior prioridade a adequação à LGPD. Porém, os dados informados reforçam que ainda há uma quantidade enorme de empresas, órgãos públicos e atividades desenvolvidas por pessoas físicas que manipulam dados pessoais, e que apesar dos desafios de adaptação estarem diretamente relacionados à forma como os dados são manipulados por uma empresa e o tamanho dela, não deve ser desconsiderada a importância do gerenciamento das práticas que devem ser adotadas para o cumprimento dos princípios da LGPD.

JUSTIFICATIVA

Com a implementação da LGPD em 2018, a adoção de práticas que promovam a proteção de dados, bem como de medidas preventivas, tornou-se essencial para que uma organização se adeque não somente às exigências e princípios de tal lei, mas também de normas internacionais que tratam de adequação de proteção de dados pessoais.

Com a fiscalização exercida pela ANPD, torna-se necessário a elaboração de documentos que possuam detalhamento de práticas adotadas para garantir a segurança da informação e de atividades de tratamento de dados, bem como seus riscos e ações de mitigação e/ou prevenção. Como resultado, são gerados diversos arquivos que precisam ser atualizados conforme necessidade, seja por solicitação do órgão fiscalizador, de titulares de dados ou de mudanças internas do controlador.

O sistema a ser desenvolvido neste trabalho terá como finalidade auxiliar o DPO no controle de práticas a serem adotadas no tratamento de dados e no atendimento de comunicação entre controlador, ANPD e/ou titular de dados, bem como gerenciar estas informações visando armazenamento e acessibilidade.

Com a centralização de informações voltadas à LGPD, a empresa poderá oferecer respostas ágeis às ocorrências, seja por parte de titulares de dados ou mesmo solicitações por agentes da ANPD.

O controle de práticas adotadas por todos que compõem um sistema também é extremamente importante e merece atenção, portanto, o sistema também será capaz de realizar esse gerenciamento.

OBJETIVOS

Objetivo Geral

Desenvolver um sistema para auxiliar o encarregado de dados em suas atividades de controle de práticas e de comunicação entre controlador de dados, titular de dados e ANPD. Estas ocorrências deverão ser armazenadas em forma de discussões que deverão ser atualizadas até o fechamento da ocorrência.

Objetivos Específicos

- Desenvolver aplicação *front-end* para acesso ao portal;
- Desenvolver aplicação *back-end* para resposta a requisições e execução de serviço de notificação;
- Integrar aplicações e banco de dados utilizando a estrutura de microsserviços.

VISÃO GERAL

Ao final do desenvolvimento do projeto, a solução possibilitará o cadastro de ocorrências por encarregado de dados e por usuários externos (sem login), com validação automática e manual, respectivamente, bem como a movimentação delas, por encarregado e operadores. A solução também possibilitará que o encarregado exerça o gerenciamento de práticas que deverão ser atribuídas à grupos de pessoas.

O *e-mail* será utilizado como meio de atualização de estado de ocorrências e práticas, portanto, será implementado um serviço de comunicação para garantir o funcionamento correto de envio de automático de *e-mails*.

CAPÍTULO 1 - FUNDAMENTAÇÃO TEÓRICA

A aplicação DPOHub, a ser desenvolvida neste projeto, visa garantir ao encarregado de dados, o gerenciamento de práticas e ocorrências de forma centralizada, oferecendo também a possibilidade de consulta à ocorrência por parte de um usuário externo, seja o titular de dados ou um agente da ANPD.

Também haverá o serviço de notificação que será responsável por realizar a notificação por e-mail sobre atualizações em ocorrências para todos os e-mails associados à mesma, bem como notificações periódicas para e-mails de acordo com seus respectivos conjuntos de práticas.

Para este projeto, foram necessárias pesquisas sobre: serviços de notificação, paradigmas de programação e microsserviços. Com essas pesquisas, encontramos as tecnologias mais adequadas para o funcionamento do sistema, sendo elas: Java, *Spring Boot*, *Spring Security*, Framework Angular e MariaDB.

O artigo "*The Right To Privacy*" de 1890 aborda a importância do direito das pessoas ao direito de "estar sozinho" como citado por Thomas M. Cooley na obra *"A Treatise on the Law of Torts or the Wrongs Which Arise Independence of Contracts*" de 1879, reforçando a ideia de que era necessário a existência de leis que protejam não somente os bens e a pessoa fisicamente, mas que também protejam o direito à privacidade dela. A obra também já cita situações presentes ainda nos dias de hoje, inclusive sobre os malefícios sobre uma pessoa devido a divulgação de sua vida privada. Um exemplo presente no artigo é o fato de na época em que foi escrito já haver casos em que jornais e revistas obtinham lucros em cima de imagens de pessoas, sem o consentimento necessário.

O livro "*LGPD: muito além da Lei: Uma análise do direito em conjunto com a segurança da informação*" aborda de forma prática como as leis devem ser aplicadas para garantir o direito à privacidade, conforme as obras referenciadas anteriormente, reforçando a necessidade da adequação de órgãos e empresas, públicas e privadas, ao tratamento de dados dos titulares. É também reforçada mesmo que de forma involuntária o atraso do Brasil em relação à Europa quanto ao artigo 12 da Declaração Universal dos Direitos Humanos, incorporada no ano de 1948 visando globalizar a política de direito à privacidade.

O livro também reforça a importância que os dados possuem, fazendo parte da evolução da sociedade e do ser humano, ressaltando os benefícios e malefícios que o acesso à informação viabiliza e que foram fortalecidos com a Revolução Industrial 4.0. Se por um lado essa acessibilidade traz vantagens, como trabalho remoto, acesso rápido a informações e comunicação instantânea, por outro, também traz problema afetando a saúde e privacidade das pessoas devido à exposição ao excesso de informação e risco de invasão de privacidade.

Uma preocupação mais recente em relação à privacidade, é o uso de redes sociais que muitos não percebem, mas não são gratuitas pois ao utilizá-las nós estamos permitindo que utilizem nossos dados como um negócio lucrativo. O livro cita a frase de Andrew Lewis que coloca a ideia de negócio dessas empresas de forma explícita: *"se você não paga pelo produto, você é o produto"*.

Como informado no livro, de acordo com relatório de 2019 do site *We Are Social*, o Brasil ficou em segundo lugar entre os países que passaram mais tempo utilizando redes sociais, com média diária de 3 horas e 34 minutos, portanto podemos identificar a necessidade da adoção de medidas mais seguras e transparentes de proteção de dados. Para reforçar tal necessidade, é citado casos como o vazamento de dados de 30 milhões de usuários do Facebook e o caso do Google+ que, em primeiro caso, teve mais de 500 mil perfis afetados, e no segundo, houve mais de 50 milhões.

Em 2014, entrou em vigor a Lei do Marco Civil da Internet, que visava atribuir direitos e deveres no mundo virtual no Brasil, que até então era considerada terra sem lei, no entanto não eram suficientes para garantir a proteção dos dados pessoais. Em 2018, com a criação GDPR na Europa, sob forte influência desta, o Brasil desenvolveu a LGPD que visa garantir que a proteção de dados seja cumprida, de forma transparente, independentemente do cenário em que os dados são manipulados. Vale ressaltar que tal lei rege sobre dados não anonimizados ou pseudonimizados, ou seja, que não seja possível identificar o titular do dado. O livro também ressalta a importância do direito ao esquecimento e como ele deve ser interpretado, uma vez que não justifica a censura ou qualquer atitude que comprometa o acesso à informação.

Com a LGPD, os controladores de dados passam a ser responsabilizados de forma mais clara sobre a necessidade do cuidado de tratar e conscientizar os titulares de dados como seus dados são tratados, sob pena de multa em caso de descumprimento. Como exemplo, em 2019 o PROCON[3] de São Paulo multou o Google em R$ 9.964.615,17 e a Apple em R$ 7.744.320,00 por conta da disponibilização do aplicativo FaceApp sem informação de Políticas de Privacidade sobre o tratamento dos dados dos usuários.

Com a implementação da GDPR na União Europeia exigindo que países do exterior adotassem leis equivalentes para garantir o nível de proteção de dados, o Brasil em especial visto que outros países da América do Sul já possuíam leis para tal finalidade, e que também era uma exigência para compor a OCDE[4], normas que garantem a proteção de dados. Um dos incentivos fornecidos pela UE[5], para países que adotassem leis rígidas para garantir o nível adequado de proteção de dados, é a transferência com menos burocracias de dados pessoais oriundos do EEE[6]. Mesmo com a LGPD, até o momento não foi definido se o Brasil é considerado adequado, sendo necessária que empresas de países que façam parte da Decisão de Adequação da UE precisem realizar medidas adicionais de segurança para transferência de dados para o Brasil, a Lego é o exemplo citado de empresa que precisa adotar medidas adicionais de segurança para operar no país através da Regra Vinculativa.

Para garantir que a LGPD será aplicada corretamente, é necessário entender o conceito de *Privacy by Design* e *Privacy by Default*. Este primeiro conceito visa estabelecer que o produto/serviço deve ser desenvolvido já com a garantia da proteção de dados em mente, e o segundo conceito visa garantir que o produto/serviço possui configurações de privacidade que por padrão já sejam preenchidas de forma que garanta a melhor proteção de dados possível.

[3] **PROCON (Departamento Estadual de Proteção e Defesa do Consumidor):** é um órgão público que atua na mediação de conflitos entre consumidores, empresas e prestadores de serviços.

[4] **OCDE (Organização para a Cooperação e Desenvolvimento Econômico):** dedica-se à promoção de padrões internacionais em questões econômicas, financeiras, comerciais, sociais e ambientais.

[5] **UE (União Europeia):** é uma união política e econômica composta por 27 países do continente europeu.

[6] **EEE (Espaço Econômico Europeu):** acordo de livre comércio composto pelos 27 países da EU mais Noruega, Islândia e Liechtenstein.

Um dos procedimentos a serem realizados para o controle de atividades de risco em relação ao tratamento de dados pessoais é a elaboração do documento RIPD[7] que deve ser composto por tais atividades, finalidade, riscos e medidas protetivas em relação às mesmas. A necessidade de elaboração do RIPD pode variar de acordo com a interpretação do ANPD, mas de forma geral toda empresa/órgão que trate dados que possam gerar situações de risco para a privacidade dos titulares de dados.

Com a criação da LGPD, 2 posições no mercado de trabalho se tornaram necessárias, são elas:

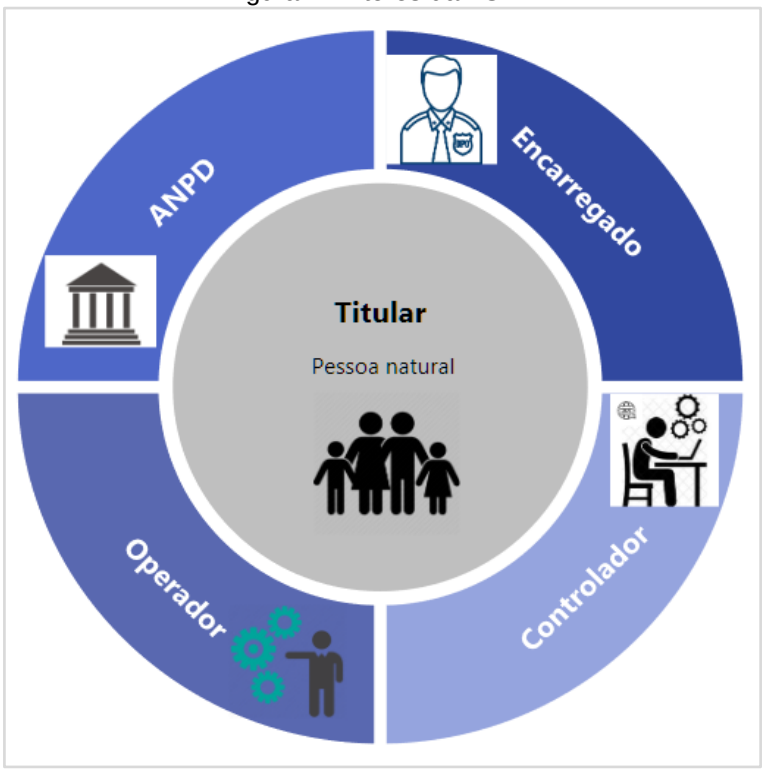
1. **Operador:** é responsável por exercer atividades de tratamento dos dados pessoais em nome do controlador.

2. **Data Protection Officer (DPO):** conhecido como Encarregado de Proteção de Dados. De acordo com a LGPD, no Brasil o Controlador de Dados pode ser obrigado a indicá-lo e disponibilizar publicamente a identidade e informações de contato do mesmo para consulta. Suas atividades são compostas do gerenciamento das medidas a serem adotadas para garantir que a LGPD seja implementada corretamente na empresa/órgão e manter contato com titulares de dados e órgãos fiscalizadores como a ANPD.

Essas duas novas posições de mercado, respondem ao “Controlador” que é responsável por garantir a proteção de dados dos titulares durante todo o ciclo de vida dos mesmos em sua posse, sendo responsabilizado pelas medidas necessárias para a proteção de dados, assim como as consequências do mau tratamento. A Figura 1 representa essa relação entre os titulares de dados e os demais atores da LGPD.

[7] **RIPD (Relatório de Impacto à Proteção de Dados Pessoais):** trata-se de um documento composto por descrição de processos de tratamento de dados, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Figura 1 - Atores da LGPD



Fonte: Secretaria de Governo Digital, 2020.

1.1 PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

De acordo com o Programa de Governança em Privacidade, – representado na Figura 2 – elaborado pelo governo brasileiro, a LGPD foi composta a partir de 10 princípios, são eles:

1. **Finalidade:** estabelecer de forma direta e clara para o titular dos dados, como eles serão tratados;

2. **Adequação:** garantir que o tratamento dos dados está sendo realizado de forma condizente com a finalidade informada ao titular de dados;

3. **Necessidade:** limitar o tratamento ao mínimo necessário para realização da finalidade;

4. **Livre Acesso:** garantir consulta livre e fácil de informações relacionadas ao tratamento de dados;

5. **Qualidade dos Dados:** garantir que os titulares possam consultar, alterar ou excluir seus dados, se necessário, bem como atualizar os mesmo para cumprir a finalidade;

6. **Transparência:** garantir que as informações sobre tratamento de dados sejam claras, acessíveis e precisas.

7. **Segurança:** adotar técnicas e práticas para garantir a segurança da informação e proteção dos dados pessoais;

8. **Prevenção:** adotar medidas preventivas em caso de danos a privacidade dos dados pessoais;

9. **Não Discriminação:** impedir a utilização dos dados para atos discriminatórios ou abusivos;

10. **Responsabilização e Prestação de Contas:** comprovar adoção de medidas que atendam os requisitos da LGPD e seus princípios.

Figura 2 - Princípios da LGPD

Fonte: Secretaria de Governo Digital, 2020.

Seguindo estes princípios, o processo de conformidade com a LGPD pode ser subdividido em etapas estabelecidas de acordo com um diagnóstico inicial de como a organização se encontra em relação a mesma, como podemos ver na Figura 3, sendo

repetidos tantas vezes quanto for necessário, de acordo com o diagnóstico diferencial. As etapas podem ser:

1. **Diagnóstico Inicial:** trata-se do diagnóstico que definirá as etapas que deverão ser seguidas para garantir a conformidade com a LGPD;

2. **Programa de Privacidade:** conscientizar a organização sobre a necessidade da adoção da LGPD, e atividades a serem realizadas, de acordo com o Projeto de Adequação;

3. **Inventário de Tratamento de Dados:** levantamento das operações de tratamento de dados pessoais, acompanhadas de avaliação de acordo com a LGPD;

4. **Termos de Uso e Políticas de Privacidade:** elaborar, revisar e atualizar termos e políticas referente ao tratamento de dados, com intuito de conscientizar os titulares;

5. **Riscos de Segurança e Privacidade:** identificar e mitigar riscos existentes em todo o ciclo de vida do tratamento de dados;

6. **Adequação de Contratos:** elaborar, revisar e atualizar contratos, com intuito de garantir o processo de adequação do tratamento de dados de acordo com os princípios estabelecidos pela LGPD;

7. **Relatório de Impacto de Proteção de Dados:** elaborar documentação descritiva de atividades de tratamento de dados, seus riscos, medidas preventivas e salvaguardas;

8. **Resposta à Incidentes:** elaboração de um plano de resposta em caso de incidentes, incluindo a comunicação dos titulares de dados e a ANPD.

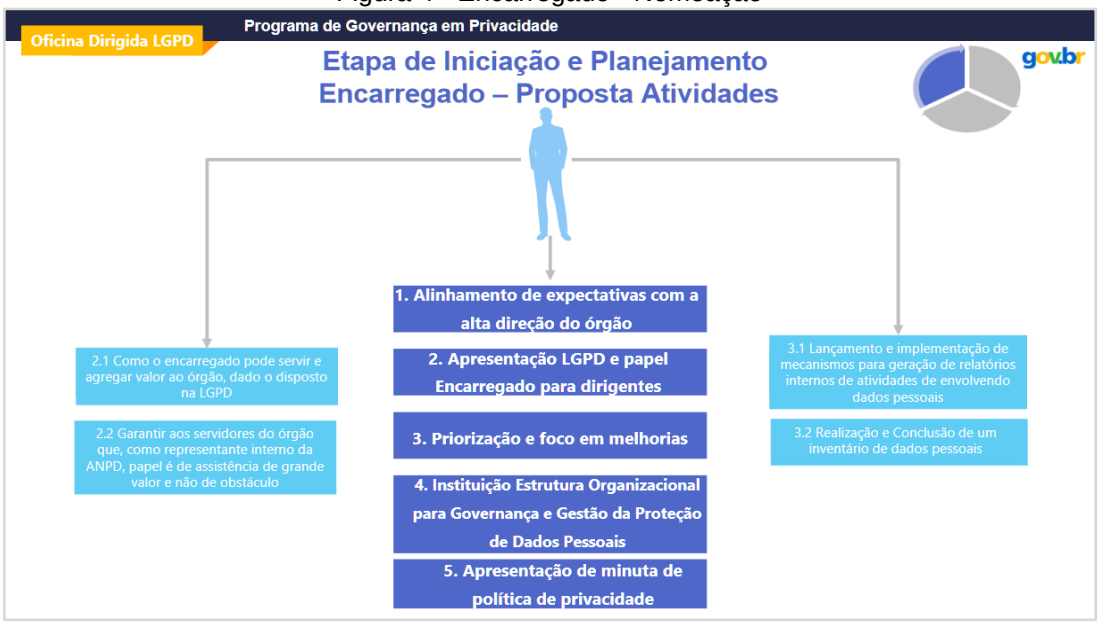
9. **Diagnóstico Diferencial:** é realizado ao final das etapas anteriores, para identificar possíveis medidas e/ou tratamentos que precisam ser inseridos ou ajustados, e ao final desta etapa, se necessário, as etapas anteriores são realizadas novamente com intuito de obter adequação à LGPD.

Figura 3 - Marcos de Conformidade com a LGPD

Fonte: Secretaria de Governo Digital, 2020.

Em todas as etapas deverá estar presente o controlador ou DPO, que deverá ser indicado no início do Projeto de Adequação. Portanto, como representado na Figura 4, é necessário que o encarregado tenha conhecimento de todos os processos organizacionais, ou o máximo possível. E que possua autonomia, independência e apoio da organização para realizar seu trabalho que deverá ser documentado e posteriormente enviado para ANPD com intuito de obter aprovação de adequação à LGPD.

Figura 4 - Encarregado - Nomeação

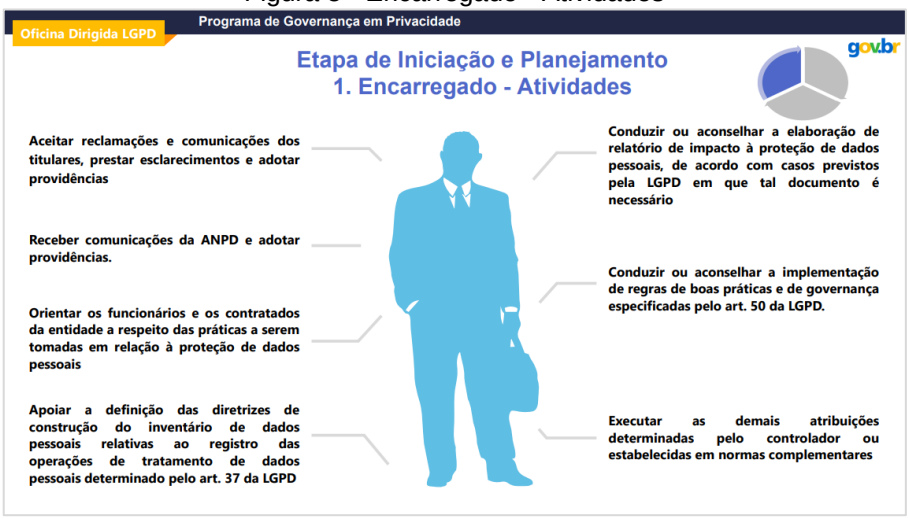


Fonte: Secretaria de Governo Digital, 2020.

Podemos destacar dentre as responsabilidades especificadas pelo governo ao encarregado de dados, conforme Figura 5:

- Atender reclamações e comunicações de titulares de dados;
- Prestar esclarecimentos;
- Adotar providências;
- Orientar funcionários e contratados sobre práticas a serem adotadas.

Figura 5 - Encarregado - Atividades



Fonte: Secretaria de Governo Digital, 2020.

1.2 SERVIÇOS DE NOTIFICAÇÃO (*E-MAIL*)

A necessidade de manter logs e registros de eventos de um sistema é um processo complexo que envolve grande cautela para evitar uma possível sobrecarga tanto de processamento quanto de armazenamento, e uma das alternativas complementares que auxiliam esse processo é a notificação por *e-mail*, que inclusive mantém suas características auditáveis (KLEPPMAN, 2017).

O correio eletrônico é uma tecnologia de mensagens assíncronas. A pessoa que você está tentando alcançar não precisa estar disponível naquele instante. Ela receberá sua mensagem na próxima vez que verificar seu *e-mail*. Este simples fato permite que quase todos os internautas enviem uma mensagem para qualquer outra pessoa a qualquer momento. O correio eletrônico é usado em empresas, departamentos governamentais, universidades, escolas, residências, quiosques e em laptops móveis, pagers e assistentes digitais pessoais. Enquanto a Web distribui informações, o *e-mail* nos mantém em contato uns com os outros (WOOD, 1999).

O termo “aviso” refere-se a capacidade de um sistema de monitoramento detectar e notificar os operadores sobre eventos relevantes que indicam uma grande mudança de estado. A notificação é conhecida como aviso e é uma mensagem simples que pode assumir diversos formatos, como *e-mail*, *SMS*, mensagem instantânea (IM) ou ligação telefônica (LIGUS, 2013).

Entende-se que a utilização do *e-mail* é a melhor alternativa para um serviço de notificação periódico das práticas e pontual para movimentações de ocorrências devido à sua capacidade de trabalho em diversos dispositivos, pela não necessidade de que o usuário do *e-mail* esteja ativo no momento da notificação, e pela natureza auditável do *e-mail* que permite.

1.3 WEBSOCKET

De acordo com Rishti Gupta, *WebSockets* são conexões bidirecionais entre clientes e servidores que permitem comunicação em tempo real, ou seja, a troca de dados é instantânea permitindo menor tempo de resposta em aplicações, diferente da conexão comum de requisição-resposta como as implementações de *REST APIs*[8].

Um arquivo ou banco de dados é suficiente para conectar cliente e servidores: o servidor gera um evento e então cada cliente realiza uma consulta periódica por novos eventos desde a última consulta. No entanto, ao utilizar a técnica de *polling*[9], essas interações tornam-se mais custosas, sendo mais vantajosa a utilização de técnicas que permitam a notificação imediata do evento (KLEPPMAN, 2017).

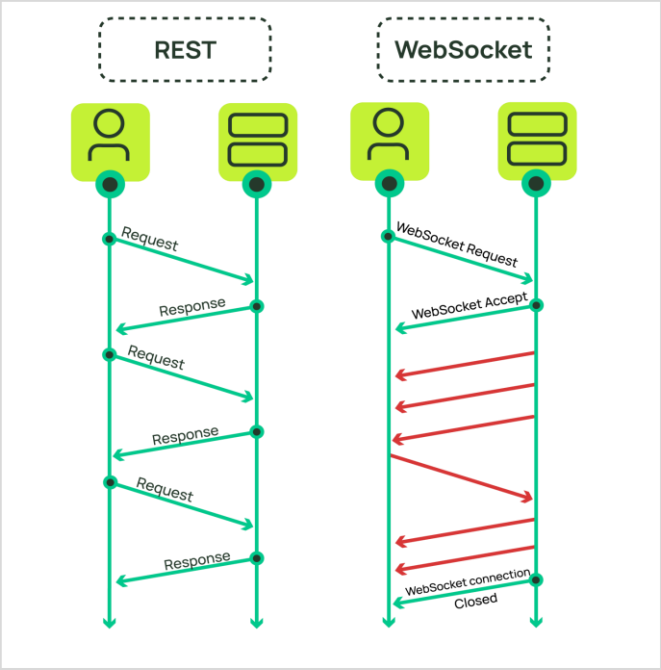
O *WebSocket* reduz a latência porque, uma vez estabelecida a conexão *WebSocket*, o servidor pode enviar mensagens assim que estiverem disponíveis. Por exemplo, diferentemente do *polling*, o *WebSocket* faz uma única requisição. O servidor não precisa esperar por uma requisição do cliente. De forma similar, o cliente pode enviar mensagens ao servidor a qualquer momento. Esta única requisição reduz muito o tempo em relação ao *polling*, que envia requisições intervaladas,

[8] **REST API:** um serviço disponibilizado remotamente, capaz de transmitir dados, realizando requisições HTTP/HTTPS.

[9] **Polling:** é um processo de obtenção de dados baseado em entrada/saída, onde torna-se necessário o envio constante requisições (entradas).

independentemente se há mensagens disponíveis (WANG, SALIM, MOSKOVITS. 2013), conforme representado na Figura 6.

Figura 6 - Diferença entre WebSocket e REST



Fonte: Moment, Rishti Gupta

A utilização do *WebSocket* faz-se necessária na implementação do projeto devido o módulo de *chat* para garantir que haja comunicação efetiva entre os envolvidos sem que cause grande impacto no resto do sistema.

1.4 MICROSSERVIÇOS

Microsserviços são um tipo de arquitetura de desenvolvimento de software que estrutura uma aplicação como uma coleção de serviços pequenos e autônomos, cada um executando um único processo e comunicando-se através de mecanismos leves (CLEDUPE, 2024).

Cada serviço é focado em realizar uma função de negócio específica, é desenvolvido de forma independente por uma pequena equipe, e pode ser implantado, atualizado, escalado e reiniciado de forma independente dos outros serviços (CLEDUPE, 2024).

Em contraste com a arquitetura monolítica, onde todos os componentes de uma aplicação são interdependentes e compilados como uma única unidade, os microsserviços são independentes e podem ser gerenciados separadamente. Isso

traz vantagens significativas em termos de escalabilidade, flexibilidade e agilidade, permitindo que as equipes de desenvolvimento adaptem e evoluam partes da aplicação sem impactar o sistema como um todo (CLEDUPE, 2024).

Microsserviços representam uma abordagem poderosa e flexível para o desenvolvimento de software, oferecendo vantagens significativas em termos de escalabilidade, resiliência e agilidade. No entanto, sua implementação requer cuidadosa consideração dos desafios inerentes e um compromisso com as melhores práticas e ferramentas adequadas. Na medida em que as tecnologias evoluem e as organizações buscam maior eficiência e capacidade de resposta, os microsserviços continuam a ser uma escolha arquitetônica cada vez mais popular (CLEDUPE, 2024).

O desenvolvimento de microsserviços pode ser facilitado por uma série de tecnologias e frameworks, cada um com suas características específicas que podem ajudar no enfrentamento dos desafios comuns encontrados neste estilo arquitetural. A escolha da tecnologia certa depende de uma variedade de fatores, incluindo a compatibilidade com o ecossistema existente, a experiência da equipe, a comunidade de apoio e as características de desempenho (CLEDUPE, 2024).

1.5 TECNOLOGIAS UTILIZADAS

1.5.1 Java

1.5.1.1 Spring

O *Spring* é um projeto com diversos plugins minimalistas no que diz respeito à implementação e manutenção de suas funcionalidades, capaz de ser utilizada para desenvolvimento de aplicações web, mobile e JEE (COSMINA, 2023).

O *Spring Framework* é baseado no princípio de inversão de controle (Inversion of Control - IoC), uma técnica que externaliza a criação e gerenciamento de dependências de componentes. Esse princípio no qual componentes genéricos reutilizáveis são usados para controlar a execução de códigos, faz com que o *Spring* seja um gerenciador de dependências.

A utilização do projeto *Spring* é justificada pelo minimalismo na intervenção, a partir de implementações customizadas por parte do programador, no funcionamento

do software a ser desenvolvido, possibilitando a entrega de uma base de códigos minimizada de acordo com as possibilidades oferecidas pelo *Spring*.

1.5.1.1.1 Spring Boot

O *Spring Boot* foi lançado e se tornou um dos projetos *Spring* mais utilizados. Desenvolvedores da Pivotal (empresa responsável pelo framework *Spring*) identificaram alguns tipos de projetos sendo construídos e então criaram aplicações de exemplo, chamados *template*, usando padrões de dependências de componentes, bem como configurações automáticas. Estes *templates* são modelados de acordo com conjunto de projetos iniciais do *Spring Boot* (COSMINA, 2023).

O *Spring Boot* será utilizado para realizar o gerenciamento das dependências necessárias para o funcionamento das funcionalidades de *e-mail*, *API REST*, *WebSocket* e banco de dados.

1.5.1.1.2 Spring Security

O *Spring Security* é o projeto que oferece a possibilidade de trabalhar com a segurança de aplicações de forma simples, englobando tanto autorização quanto autenticação (COSMINA, 2023).

Sua utilização possibilitará uma implementação simplificada de controle de acesso e de requisições, que deverão ser constantemente validadas de acordo com a função de cada usuário.

1.5.2 Framework Angular

O Angular é uma plataforma de desenvolvimento *open-source* escrita em TypeScript[10] que consiste em pequenos subsistemas, incluindo um framework JavaScript, uma linha de comando, um serviço de linguagem, e uma rica coleção de bibliotecas *first-party* (sem necessidade de instalação) (BAMPAKOS, DEELEMAN. 2023).

O uso desse *framework* é indicado principalmente por sua robustez, tanto no que diz respeito ao ecossistema de desenvolvimento fornecido à quem o utilizará quanto sua elevada utilização em projetos no mundo todo. Estatisticamente, mais de

[10] TypeScript: um conjunto de utilitários, adicional à linguagem de programação JavaScript.

2500 projetos dentro da Google utilizam o Angular, e mais de 1.5 milhões de desenvolvedores preferem sua utilização (BAMPAKOS, DEELEMAN. 2023).

Portanto, podemos concluir que a utilização do Angular é recomendada tanto por produtividade quanto pelo suporte oferecido pela vasta comunidade. O ecossistema do *framework* fornece acesso direto às bibliotecas necessárias para aplicações básicas, ao mesmo tempo que também suporta a instalação de novas dependências em conjunto com o gerenciador de pacotes de escolha do desenvolvedor, oferecendo um ambiente de desenvolvimento robusto e dinâmico.

1.5.3 MySQL / MariaDB

O MySQL é um banco de dados relacional, *multithread*, *open-source*, escalável e com capacidade de lidar com dezenas de milhares de tabelas e bilhões de registros, bem como apresentam ótimo desempenho para base de dados menores, fazendo sua utilização conveniente a empresas pequenas ou projetos amadores (DYER, 2015).

Uma pesquisa com testes controlados, que envolvia diversos bancos de dados, identificou que o MariaDB foi capaz de processar 61% mais ordens que o MySQL, sendo o mais eficiente da pesquisa (MITCHELL, 2023).

Considerando que o MariaDB é um *fork*[11] do próprio MySQL, este primeiro foi escolhido para compor o projeto deste trabalho, por tratar-se de um banco de dados totalmente *open-source*, ao contrário do MySQL que após sua venda à *Oracle*, passou a ter funcionalidades proprietárias. Mesmo com essa diferença, ambos têm suas vantagens em determinados cenários, porém, de forma geral, o MariaDB é capaz de atender as demandas que o projeto necessitará.

CAPÍTULO 2 - PLANEJAMENTO DO PROJETO DPOHUB

2.1 INTRODUÇÃO

A proposta leva em consideração que o encarregado de dados e operador necessitam centralizar suas atividades em um único sistema capaz de facilitar a

[11] Fork: na engenharia de software, é a duplicação de um projeto já existente, para desenvolvimento de uma variante do próprio, sem afetá-lo diretamente.

colaboração entre ambos na solução de conflitos. E, apenas para o encarregado, auxiliar na atividade de conscientização dos diversos setores que podem compor uma organização, através do gerenciamento de conjuntos de práticas a serem adotadas.

2.1.1 Operador

Na versão deste trabalho, o operador deverá ser capaz de atuar na solução de ocorrências, interagindo através de comentários na seção de discussão da ocorrência. No entanto, o operador não poderá alterar o estado da ocorrência, por exemplo, mudar para concluído, ou em andamento.

2.1.2 Encarregado de Dados ou Data Protection Officer (DPO)

2.1.2.1 Gerenciamento de Práticas

O sistema deve permitir que o DPO possa cadastrar e editar práticas e conjuntos, sendo que cada conjunto poderá conter uma relação de 0 a N práticas associadas, a mesma regra se aplica a relação com *e-mails*.

O serviço de notificação será configurado pelo encarregado para efetuar notificações periódicas informando as respectivas práticas do conjunto ao qual um *e-mail* está associado. Também deverá ser possível que o encarregado configure o intervalo, em dias, que deverá ocorrer essa notificação.

2.1.2.2 Gerenciamento de Ocorrências

O encarregado deverá cadastrar ocorrências, que serão automaticamente validadas pelo sistema, para que a mesma possa ser resolvida externamente (sem envolvimento da aplicação). A ocorrência também poderá ser cadastrada por um usuário externo (ex.: titular de dados), nesse caso, necessitando de validação, ou invalidação, manual por parte do encarregado de dados.

O serviço de notificação deverá notificar os *e-mails* associados à ocorrência quando houver cadastro ou atualização da mesma, importante ressaltar que o encarregado sempre deverá ser notificado, enquanto um operador só será notificado se for associado à ocorrência pelo encarregado.

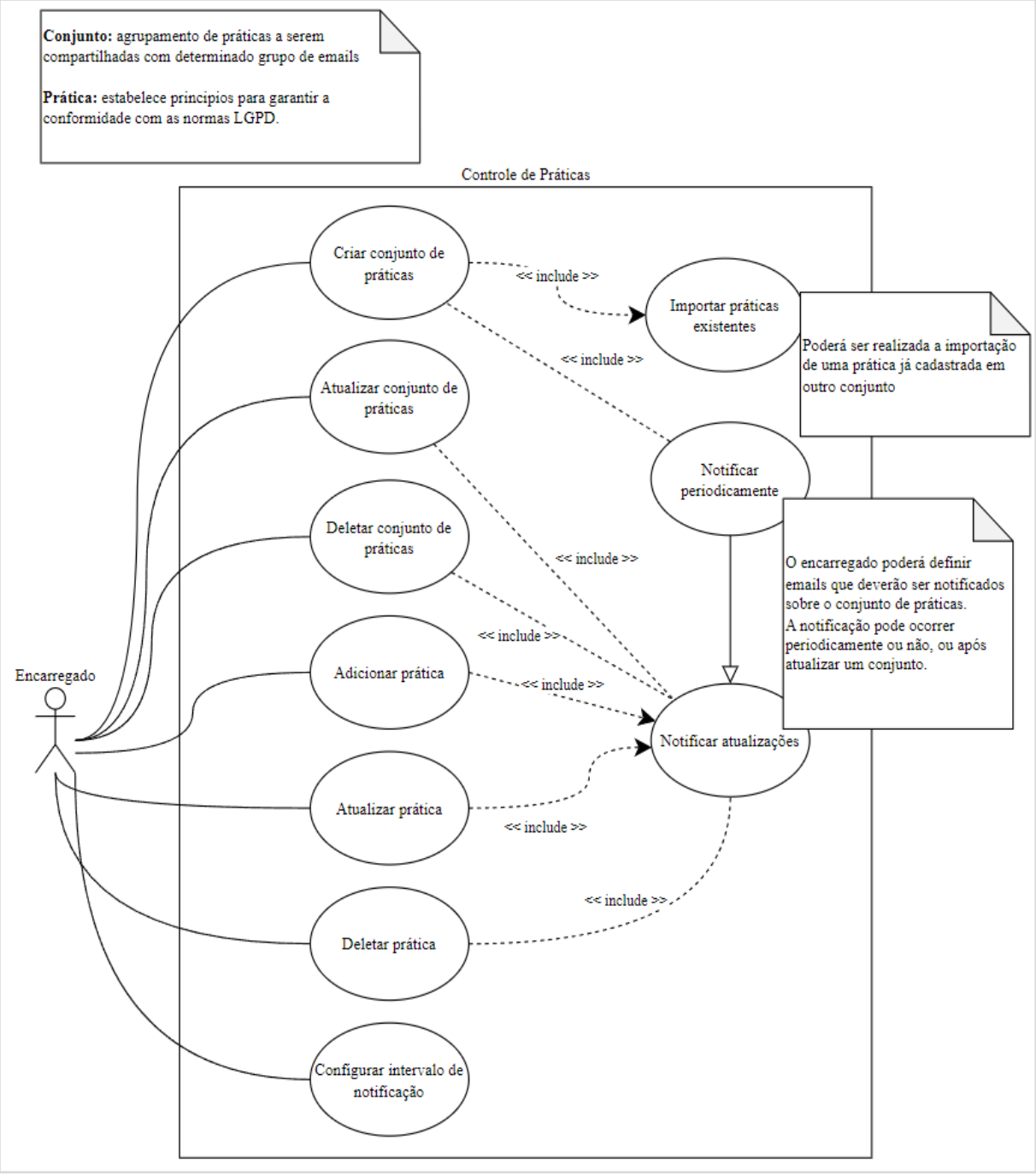
O encarregado de dados poderá atualizar o estado da ocorrência, interagir na discussão e, se necessário, invalidar uma ocorrência mesmo que já tenha sido validada, sendo uma alternativa para não haver exclusão de ocorrência. Para o estado de “concluído”, aplica-se a necessidade de preencher o campo de “solução”, que poderá ser consultado futuramente para casos de ocorrências semelhantes.

2.2 DIAGRAMA DE CASOS DE USO

2.2.1 Gerenciamento de Práticas

Este módulo do sistema, deve permitir que o encarregado possa criar práticas e conjuntos que poderão ser associados à *e-mails* que serão notificados periodicamente, conforme Diagrama 1.

Diagrama 1 - Casos de Uso - Gerenciamento de Práticas



Fonte: De autoria própria.

Quadro 1 – Cadastro de conjunto de práticas

UC001	Cadastrar conjunto de práticas
Objetivo	Realizar cadastro de conjunto de práticas
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	N/A
Pós-condições	1. Os *e-mails* são devidamente notificados periodicamente sobre seus conjuntos associados.
	2. O conjunto criado é exibido na listagem de conjuntos.
	3. Conjunto é disponibilizado para associação durante cadastro de prática.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de conjuntos.	
	2. Exibir página com listagem de conjuntos e botão de cadastrar conjunto.
3. Clica no botão de cadastrar conjunto.	
	4. Exibir janela modal com campos a serem preenchidos e botão para associar *e-mails* ao conjunto.

5. Preencher os campos e clicar no botão para associar *e-mails*.	
	6. Exibir modal para associar *e-mails* ao conjunto.
7. Associar e-mails ao conjunto e clicar para fechar o modal de *e-mails*.	
	8. Fechar o modal de *e-mails* e focar no modal com os campos preenchidos no passo 5.
9. Associar as práticas listadas na parte inferior do modal.	
10. Clicar no botão de cadastrar.	
	11. Cadastrar conjunto de práticas
	12. Notificar sucesso ou falha do cadastro.
	13. Notificar *e-mails* associados ao conjunto sobre as práticas associadas.
Cenários alternativos	1. O encarregado pode cancelar o cadastro a qualquer momento.
Regras de negócio	1. Campos obrigatórios: título e descrição.
	2. Campos opcionais: associação de *e-mails* e práticas.
	3. O sistema deve destacar os campos obrigatórios vazios e emitir o aviso: Formulário Inválido. “Verifique os campos destacados“.

Fonte: De autoria própria.

Quadro 2 - Atualizar conjunto de práticas

UC002	Atualizar conjunto de práticas
Objetivo	Realizar atualização de conjunto de práticas
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possuir conjunto criado
Pós-condições	1. Os *e-mails* são devidamente notificados periodicamente sobre seus conjuntos associados.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de conjuntos.	
	2. Exibir página com listagem de conjuntos e botão de detalhamento para cada registro da tabela.
3. Clica no botão de detalhamento do conjunto na tabela.	
	4. Exibir janela modal com campos preenchidos com os dados atuais e botão de *e-mails* associados.
5. Editar os campos e clicar no botão para associar *e-mails*.	
	6. Exibir modal para atualizar *e-mails* ao conjunto.
7. Atualizar *e-mails* do conjunto e clicar	

para fechar o modal de *e-mails*.	
	8. Fechar o modal de *e-mails* e focar no modal com os campos pré-preenchidos, ou editados no passo 5.
9. Editar as práticas associadas na parte inferior do modal	
10. Clicar no botão de salvar.	
	11. Atualizar conjunto de práticas.
	12. Notificar sucesso ou falha do cadastro.
	13. Notificar *e-mails* associados ao conjunto sobre as práticas associadas.
Cenários alternativos	1. O encarregado pode cancelar a edição a qualquer momento.
Regras de negócio	1. Campos obrigatórios: título e descrição.
	2. Campos opcionais: associação de *e-mails* e práticas.
	3. O sistema deve destacar os campos obrigatórios vazios e emitir o aviso: “Formulário Inválido. Verifique os campos destacados“.

Fonte: De autoria própria.

Quadro 3 - Deletar conjunto de práticas

UC003	Deletar conjunto de práticas
Objetivo	Realizar exclusão de conjunto de práticas
Ator principal	Encarregado de dados

Ator secundário	N/A
Pré-condições	1. Já possui um conjunto criado.
Pós-condições	1. Conjunto não é mais listado.
	2. Conjunto não é mais listado para associação com práticas.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de conjuntos.	
	2. Exibir página com listagem de conjuntos e botão de exclusão para cada registro da tabela.
3. Clica no botão de exclusão do conjunto na tabela.	
	4. Exclusão é realizada.
	5. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Sucesso. Conjunto excluído com sucesso”
Regras de negócio	1. Conjunto não deve mais estar disponível para consulta.
	2. Os *e-mails* associados ao conjunto excluído não receberão mais notificações relacionadas ao mesmo.

Fonte: De autoria própria.

Quadro 4 - Criar práticas

UC004	Criar práticas
Objetivo	Realizar cadastro de novas práticas
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	N/A
Pós-condições	1. A prática é exibida na listagem de práticas.
	2. A prática é disponibilizada para associação com conjuntos.
	3. A prática faz parte das notificações dos conjuntos associados.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de conjuntos.	
	2. Exibir página com listagem de conjuntos e botão de cadastro de nova prática.
3. Clica no botão de cadastro.	
	4. Exibir o modal com os campos: título, descrição e tabela de conjuntos para associação.
5. Preencha os campos e associe os conjuntos desejados para a prática.	

6. Clique no botão “Cadastrar”.	
	7. Cadastrar a nova prática.
	8. Notificar ao encarregado com a seguinte mensagem: “Sucesso. Prática cadastrada com sucesso”
Regras de negócio	1. Campos obrigatórios: título e descrição.
	2. Campos opcionais: conjuntos associados.
	3. A prática deve estar presente na notificação de atualização dos conjuntos associados durante cadastro.

Fonte: De autoria própria.

Quadro 5 - Atualizar práticas

UC005	Atualizar práticas
Objetivo	Realizar atualização de práticas
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possuir prática criada
Pós-condições	N/A
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de práticas.	

	2. Exibir página com listagem de práticas e botão de detalhamento para cada registro da tabela.
3. Clica no botão de detalhamento da prática na tabela.	
	4. Exibir janela modal com campos preenchidos com os dados atuais e conjuntos associados.
5. Editar os campos.	
6. Editar os conjuntos associados na parte inferior do modal	
7. Clicar no botão de salvar.	
	8. Atualizar prática e conjuntos associados.
	9. Notificar sucesso ou falha do cadastro.
	10. Notificar *e-mails* associados à conjuntos afetados pela atualização da prática.
Cenários alternativos	1. O encarregado pode cancelar a edição a qualquer momento.
Regras de negócio	1. Campos obrigatórios: título e descrição.
	2. Campos opcionais: associação de conjuntos.
	3. O sistema deve destacar os campos obrigatórios vazios e emitir o aviso: “Formulário Inválido. Verifique os campos destacados“.

Fonte: De autoria própria.

Quadro 6 - Deletar práticas

UC006	Deletar práticas
Objetivo	Realizar exclusão de práticas
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possui um conjunto criado.
Pós-condições	1. A prática não é mais listada.
	1. A prática não é mais listada para associação com conjuntos.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de práticas.	
	2. Exibir página com listagem de práticas e botão de exclusão para cada registro da tabela.
3. Clica no botão de exclusão da prática na tabela.	
	4. Exclusão é realizada.
	5. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Sucesso. Prática excluída com sucesso”
	6. Notificar *e-mails* associados à conjuntos afetados pela atualização da prática.

Regras de negócio	1. A prática não deve mais estar disponível para consulta.
	2. Os *e-mails* associados ao conjunto excluído não receberão mais notificações relacionadas ao mesmo.

Fonte: De autoria própria.

Quadro 7 - Configurar intervalo de notificação

UC007	Configurar intervalo de notificação
Objetivo	Configurar o intervalo, em dias, na qual as notificações devem ocorrer
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Período inicial de 90 dias.
Pós-condições	N/A
Ações do encarregado	**Ações do sistema**
1. Acessar tela de configurações de práticas.	
	2. Exibir página de configuração.
3. Alterar o valor do intervalo.	
4. Salvar valor alterado.	
	5. Salvar o novo valor do intervalo.

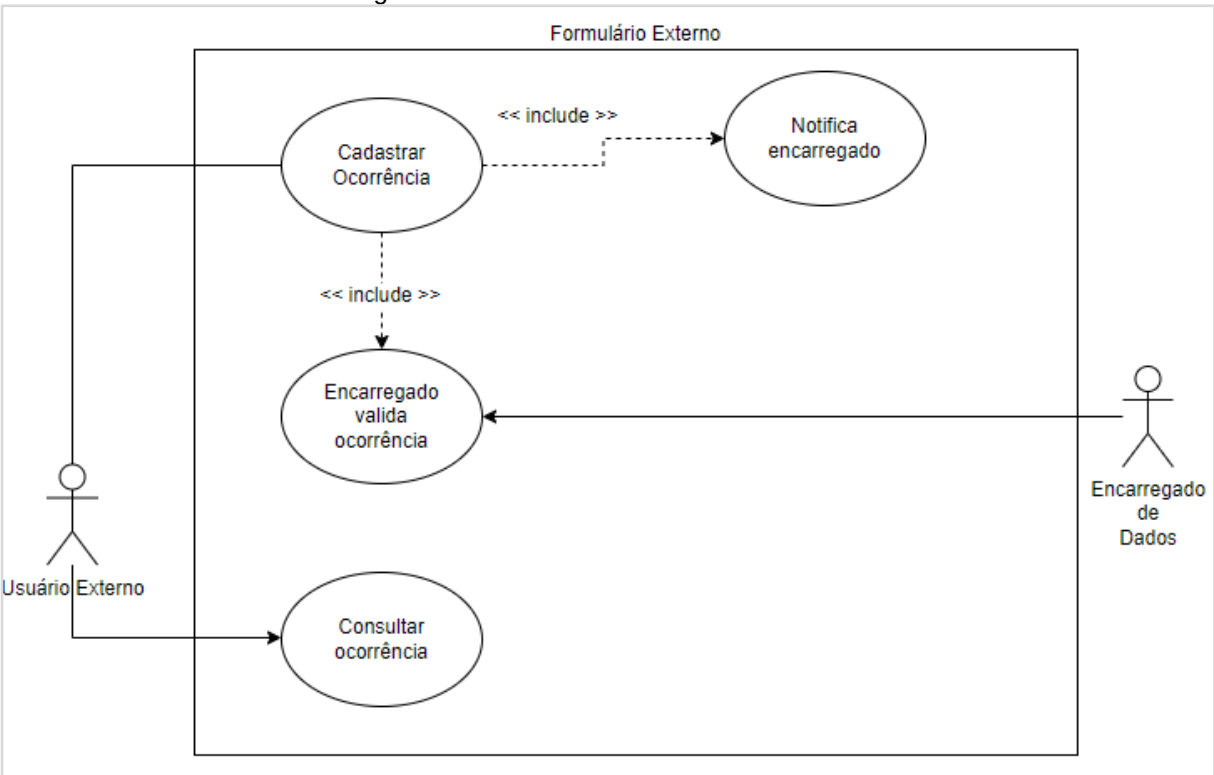
	6. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Sucesso. Notificação será enviada a cada **X** dias”. Obs: **X** é o número definido pelo encarregado de dados.
Regras de negócio	1. O valor padrão inicial é de 90 dias.
	2. Exibir valor padrão, ou último valor preenchido pelo encarregado de dados.

Fonte: De autoria própria.

2.2.2 Ocorrência Externa

O cadastro externo de ocorrências deve permitir que usuários possam, sem a necessidade de *login*, cadastrar ocorrências que deverão ser validadas, ou invalidadas, pelo encarregado de dados. E o sistema deverá notificar os envolvidos em cada uma dessas etapas.

Diagrama 2 - Casos de Uso - Usuário Externo



Fonte: De autoria própria.

Quadro 8 - Cadastrar ocorrência

UC008	Cadastrar ocorrência
Objetivo	Como usuário externo, gostaria de criar uma ocorrência sem que seja necessário efetuar login
Ator principal	Usuário externo
Ator secundário	N/A

Pré-condições	N/A
Pós-condições	1. É possível consultar a ocorrência pelo número fornecido via *e-mail*.
Ações do encarregado	**Ações do sistema**
1. Acessar página externa, sem necessidade de login.	
	2. Exibir página externa para consulta e cadastro de ocorrências.
3. Preencher campos.	
4. Clicar em “cadastrar”.	
	5. Cadastrar a ocorrência.
	6. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Ocorrência cadastrada. Entraremos em contato o mais breve possível”.
	7. Notificar ao encarregado de dados sobre a nova ocorrência cadastrada.
	8. Notificar ao usuário externo sobre o número da nova ocorrência cadastrada.
Regras de negócio	1. Campos obrigatórios: nome completo, *e-mail*, título, descrição, tipo de ocorrência.
	2. Se um dos campos obrigatórios não estiver preenchido, exibir o seguinte aviso: “Formulário Inválido. Verifique os

	campos destacados”
	3. O usuário deve aceitar as políticas de privacidade antes de poder cadastrar ocorrência.

Fonte: De autoria própria.

Quadro 9 - Validar ocorrência

UC009	Validar ocorrência
Objetivo	Como encarregado de dados, gostaria de validar uma ocorrência cadastrada por usuário externo, para que possa prosseguir com a solução.
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Existir ocorrência cadastrada por usuário externo.
Pós-condições	1. Ocorrência é listada na lista de ocorrências do encarregado e operador.
Ações do encarregado	**Ações do sistema**
1. Acessar página de validações pendentes.	
	2. Exibir página de validações pendentes.
	3. Listar ocorrências pendentes de validação.
	4. Exibir ícone de detalhamento em cada registro da tabela.

5. Clicar no ícone de detalhamento.	
	6. Exibir modal para validação ou invalidação da ocorrência, com detalhamento da mesma.
7. Clicar no botão “validar” ou “invalidar”.	
	8. Notificar ao encarregado sobre a validação ou invalidação da ocorrência.
	9. Notificar usuário externo sobre a atualização da ocorrência.
Regras de negócio	1. Notificar usuário externo, informando se a mesma foi invalidada.
	2. Somente o encarregado pode validar/invalidar uma ocorrência.

Fonte: De autoria própria.

Quadro 10 - Consultar ocorrência

UC010	Consultar ocorrência
Objetivo	Como usuário externo, gostaria de consultar uma ocorrência sem que seja necessário efetuar login
Ator principal	Usuário externo
Ator secundário	N/A
Pré-condições	1. Ocorrência deve existir.
Pós-condições	N/A

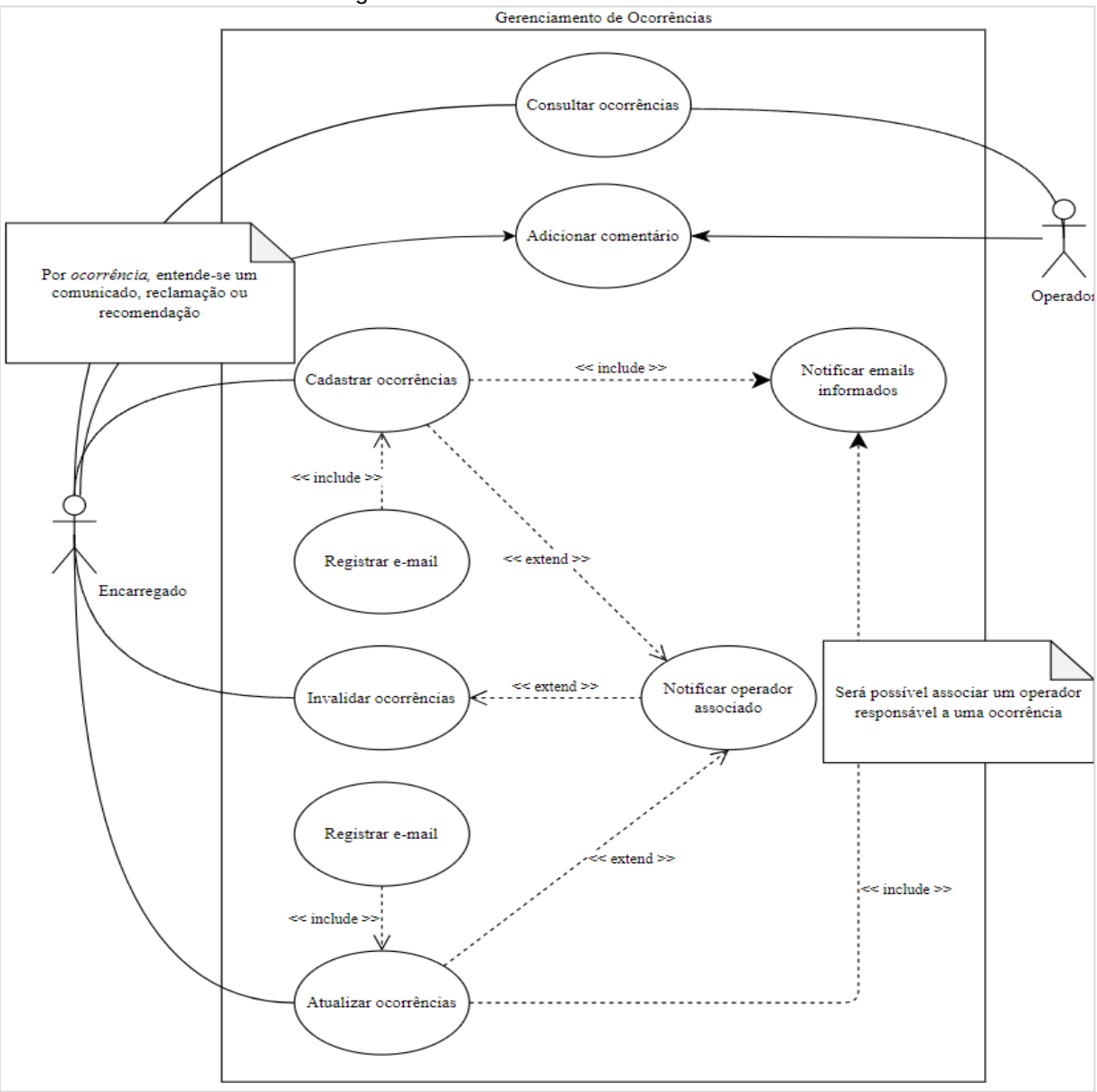
Ações do encarregado	Ações do sistema
1. Acessar página externa, sem necessidade de login.	
	2. Exibir página externa para consulta e cadastro de ocorrências.
3. Preencher o campo.	
4. Clicar em “consultar”.	
	5. Exibir modal com o estado da ocorrência.
Regras de negócio	1. Habilitar botão “consultar” somente se o preenchimento for numérico.
	2. Caso não funcione a consulta, deve ser exibida a seguinte mensagem: “Ocorrência não encontrada. Erro na consulta da ocorrência”

Fonte: De autoria própria.

2.2.3 Ocorrências

O módulo de ocorrências deve disponibilizar as funcionalidades de cadastro, edição, atualização de estado, validação e invalidação de ocorrências para o encarregado de dados. Enquanto as funcionalidades de envio de comentários na seção de discussão e visualização de detalhamento da ocorrência, devem ser disponibilizadas tanto para o encarregado quanto para o operador. Também é necessário que o sistema notifique os *e-mails* associados à ocorrência que sofra uma alteração de estado, não sendo necessário a notificação de comentários, conforme Diagrama 3.

Diagrama 3 - Casos de Uso - Ocorrências



Fonte: De autoria própria.

Quadro 11 - Cadastrar ocorrência

UC011	Cadastrar ocorrência
Objetivo	Como encarregado de dados, gostaria de criar uma ocorrência.
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	N/A
Pós-condições	1. Ocorrência é exibida na listagem de ocorrências.
	2. *E-mails* associados a ocorrências atualizadas devem ser notificados.
Ações do encarregado	**Ações do sistema**
1. Acessar página de listagem de ocorrências.	
2. Clicar no botão “cadastrar”.	
	3. Exibir modal de cadastro de nova ocorrência.
4. Preencher os campos.	
5. Clicar no botão “cadastrar”.	
	6. Cadastrar ocorrência.
	7. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Sucesso. Ocorrência

	cadastrada com sucesso”.
	8. Serviço de notificação comunica aos *e-mails* definidos sobre o número da nova ocorrência cadastrada.
Cenários alternativos	1. O Operador será notificado somente se for associado.
Regras de negócio	1. Campos obrigatórios: título, descrição, tipo de ocorrência, prioridade e progresso.
	2. Se um dos campos obrigatórios não estiver preenchido, exibir o seguinte aviso: “Formulário Inválido. Verifique os campos destacados”
	3. *E-mails* especificados no campo “*e-mails*” devem receber um *e-mail* automático referente a nova consulta cadastrada, e o número da própria.
	4. Somente encarregado de dados poderá cadastrar ocorrência internamente.

Fonte: De autoria própria.

Quadro 12 - Atualizar ocorrência

UC012	Atualizar ocorrência
Objetivo	Realizar atualização de ocorrência
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possuir ocorrência cadastrada.
Pós-condições	1. Os *e-mails* associados são devidamente notificados.

Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de ocorrências.	
	2. Exibir página com listagem de ocorrências e botão de edição para cada registro da tabela.
3. Clica no botão de edição da ocorrência na tabela.	
	4. Exibir janela modal com campos preenchidos com os dados atuais.
5. Editar os campos.	
6. Clicar no botão “salvar”.	
	7. Atualizar ocorrência.
	1. Se sucesso, exibir a seguinte mensagem: “Sucesso. Ocorrência atualizada com sucesso”
	8. Notificar *e-mails* associados à ocorrência sobre a atualização.
Cenários alternativos	1. O encarregado pode cancelar a edição a qualquer momento.
	2. O Operador será notificado somente se for associado.
Regras de negócio	1. Campos obrigatórios: título, descrição, tipo de ocorrência, prioridade e progresso.

	2. Se um dos campos obrigatórios não estiver preenchido, exibir o seguinte aviso: “Formulário Inválido. Verifique os campos destacados”
	3. *E-mails* associados devem receber um *e-mail* automático referente à atualização da ocorrência, e o número da própria.
	4. Somente encarregado de dados poderá editar ocorrência.

Fonte: De autoria própria.

Quadro 13 - Movimentar ocorrência

UC013	Movimentar ocorrência
Objetivo	Realizar movimentação de ocorrência
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possuir ocorrência cadastrada.
Pós-condições	2. Os *e-mails* associados são devidamente notificados.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de ocorrências.	
	2. Exibir página com listagem de ocorrências e botão de detalhamento para cada registro da tabela.
3. Clica no botão de detalhamento da ocorrência na tabela.	

	4. Exibir janela modal com detalhes da ocorrência.
5. Alterar o estado da ocorrência.	
	6. Atualizar ocorrência.
	2. Se sucesso, exibir a seguinte mensagem: “Sucesso. Ocorrência atualizada com sucesso”
	7. Notificar *e-mails* associados à ocorrência sobre a atualização.
Cenários alternativos	1. O Operador será notificado somente se for associado.
	2. O encarregado pode adicionar comentários na seção de discussão da ocorrência.
	3. Se a ocorrência for alterada para o estado de “concluída”, deve ser exigido o preenchimento do campo “solução”.
	4. Somente encarregado de dados pode alterar o estado de uma ocorrência.
Regras de negócio	1. *E-mails* associados devem receber um *e-mail* automático referente à movimentação da ocorrência, e o número da própria.
	2. Ao concluir a especificação da solução, exibir a mensagem: “Sucesso. Ocorrência atualizada com sucesso”

Fonte: De autoria própria.

Quadro 14 - Invalidar ocorrência

UC014	Invalidar ocorrência

Objetivo	Realizar invalidação de ocorrência
Ator principal	Encarregado de dados
Ator secundário	N/A
Pré-condições	1. Já possui ocorrência cadastrada.
Pós-condições	1. Ocorrência não é mais listada.
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de ocorrências.	
	2. Exibir página com listagem de ocorrência e botão de invalidação para cada registro da tabela.
3. Clicar no botão de invalidação da ocorrência na tabela.	
	4. Invalidar ocorrência.
	5. Sistema notifica encarregado sobre sucesso de exclusão com a seguinte mensagem: “Sucesso. Ocorrência invalidada com sucesso”
Cenários alternativos	1. O Operador será notificado somente se associado.
Regras de negócio	5. Conjunto não deve mais estar disponível para consulta.
	6. Os *e-mails* associados à ocorrência devem ser notificados sobre a invalidação.

	7. Ocorrência deve ser definida como concluída.
	8. Somente encarregado de dados pode invalidar uma ocorrência.

Fonte: De autoria própria.

Quadro 15 - Adicionar comentário

UC015	Adicionar comentário
Objetivo	Adicionar comentário à seção de “discussão” da ocorrência
Ator principal	Encarregado de dados e Operador
Ator secundário	N/A
Pré-condições	1. Já possui ocorrência cadastrada.
Pós-condições	N/A
Ações do encarregado	**Ações do sistema**
1. Acessar a listagem de ocorrências.	
	2. Exibir página com listagem de ocorrência e botão de detalhamento para cada registro da tabela.
3. Clicar no botão de detalhamento da ocorrência na tabela.	
	4. Exibir modal de detalhamento da ocorrência.
5. Escrever mensagem e clicar no botão de “enviar”.	

	6. Salvar mensagem no banco de dados.
	7. Enviar mensagens pela comunicação via *WebSocket*.
	8. Exibir mensagem enviada/recebida pelo *WebSocket*.

Fonte: De autoria própria.

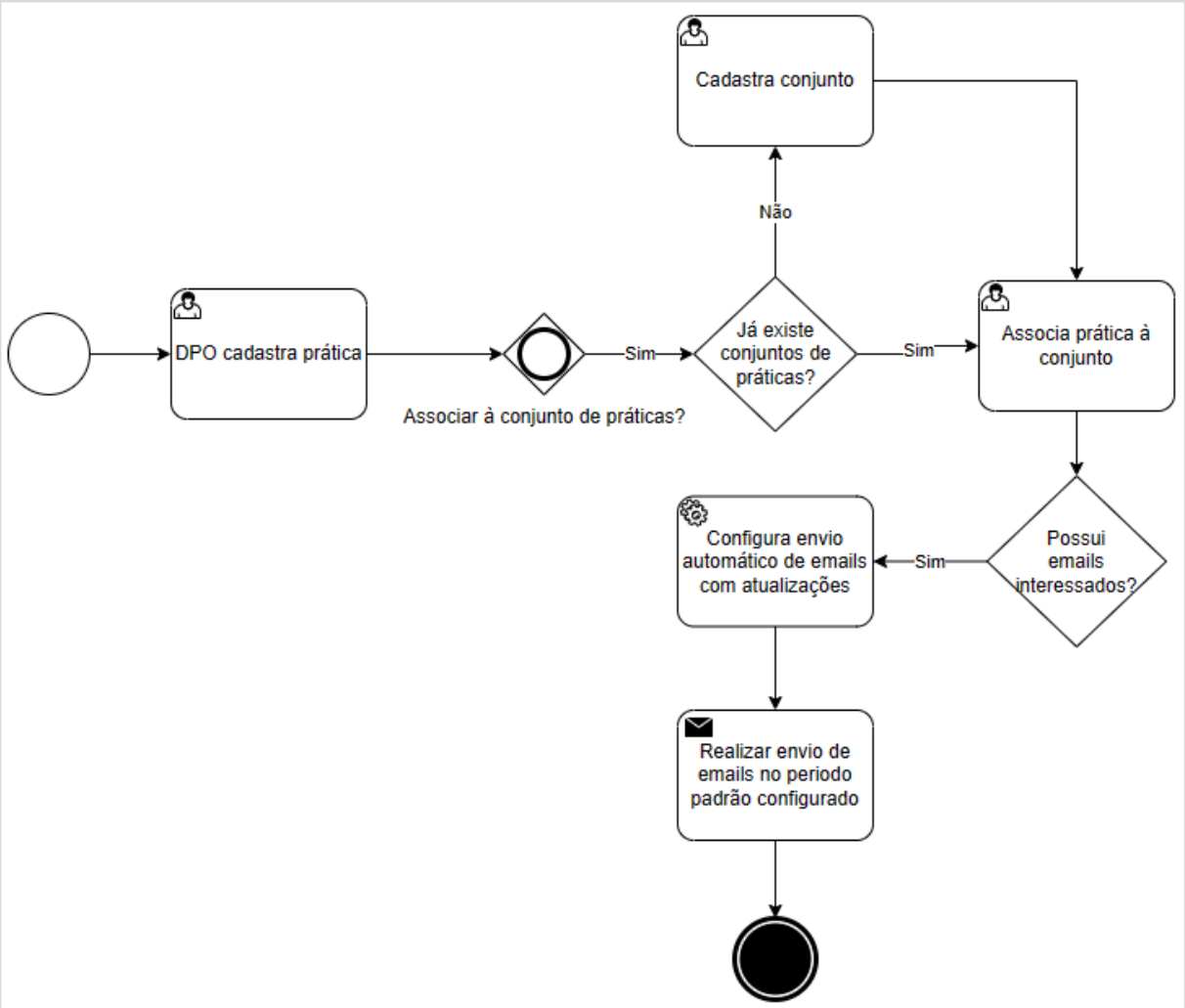
2.3 MODELO DE NEGÓCIOS (BPMN)

2.3.1 Gerenciamento de Práticas

Conforme o Modelo 1, o sistema deve oferecer ao encarregado, a capacidade de cadastrar práticas, optando, ou não, pela associação à um conjunto já existente, do contrário, o encarregado poderá cadastrar a prática para associação posterior à um conjunto.

Os conjuntos de práticas devem possuir *e-mails* interessados, sendo estes, os destinatários dos envios automáticos, e periódicos, relacionado à seus respectivos conjuntos.

Modelo 1 - Gerenciamento de Práticas



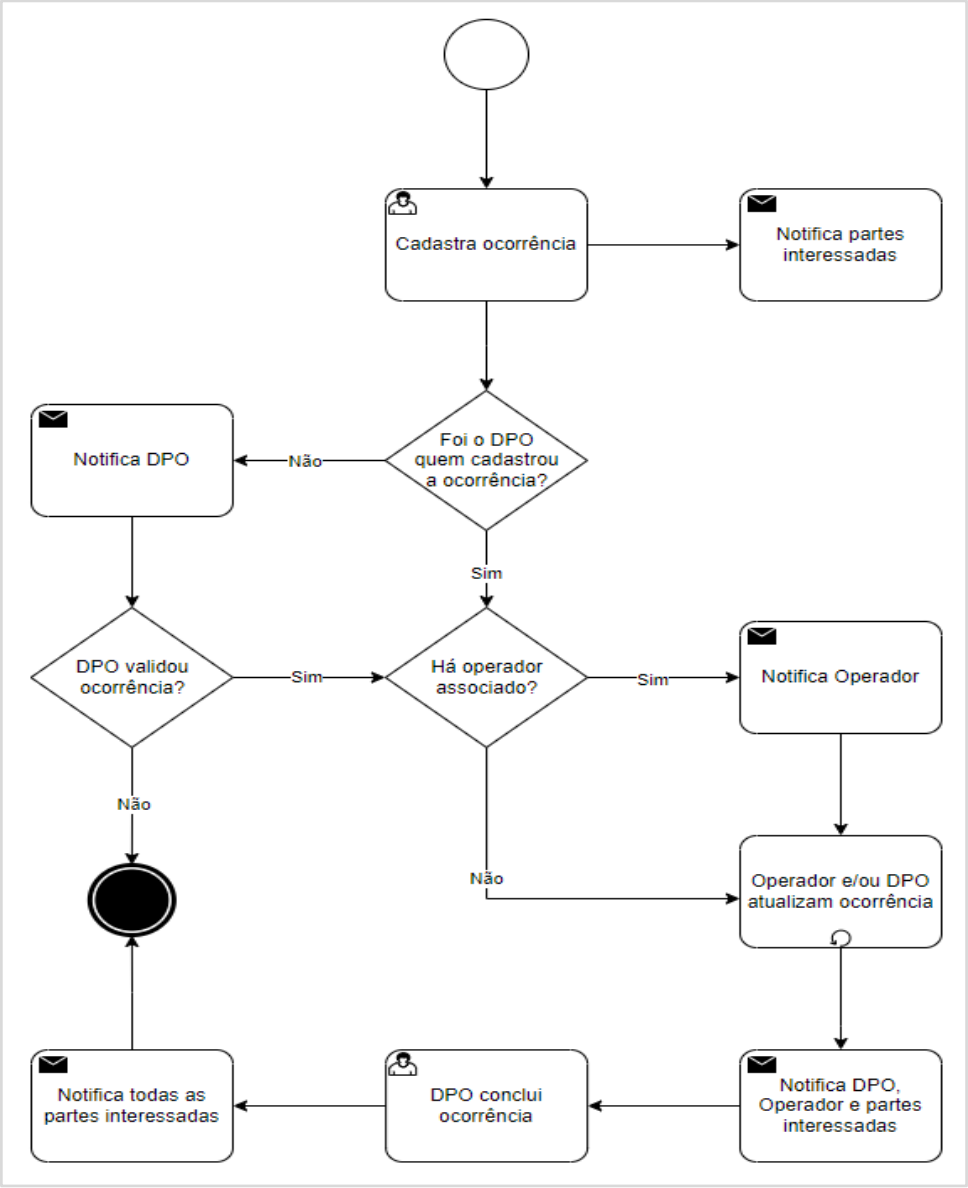
Fonte: De autoria própria.

2.3.2 Gerenciamento de Ocorrências

Conforme o Modelo 2, o módulo de gerenciamento de ocorrências deve permitir um usuário do sistema, seja o encarregado ou um usuário externo, cadastre uma ocorrência. Caso o cadastro tenha sido realizado por um usuário externo, o encarregado será notificado, e deverá validar a mesma, sendo automaticamente validada se for cadastrada pelo próprio encarregado.

Todos os *e-mails* associados (encarregado, operador, quando definido, e terceiros definidos pelo encarregado) serão notificados quando houver atualização do estado da ocorrência, inclusive em sua conclusão.

Modelo 2 - Gerenciamento de Ocorrências



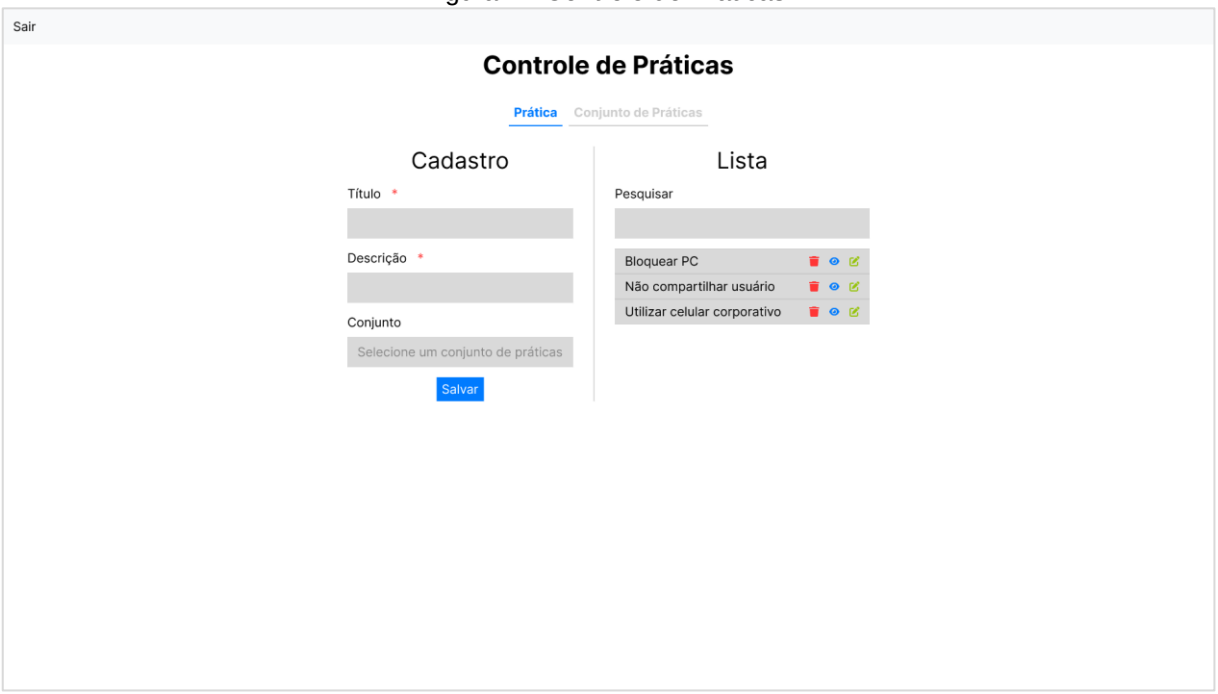
Fonte: De autoria própria.

2.4 PROTÓTIPOS

2.4.1 Gerenciamento de Práticas

2.4.1.1 Controle de Práticas

Figura 7 - Controle de Práticas



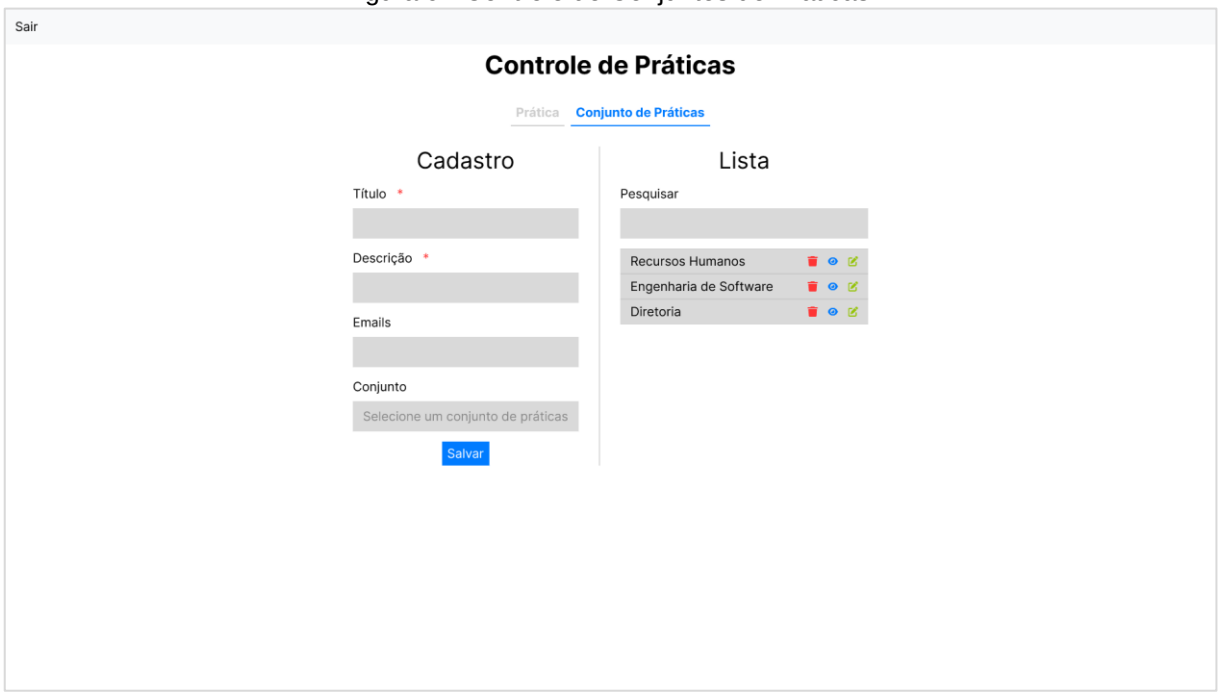
Fonte: De autoria própria.

Figura 8 - Controle de Práticas (Detalhes)

Fonte: De autoria própria.

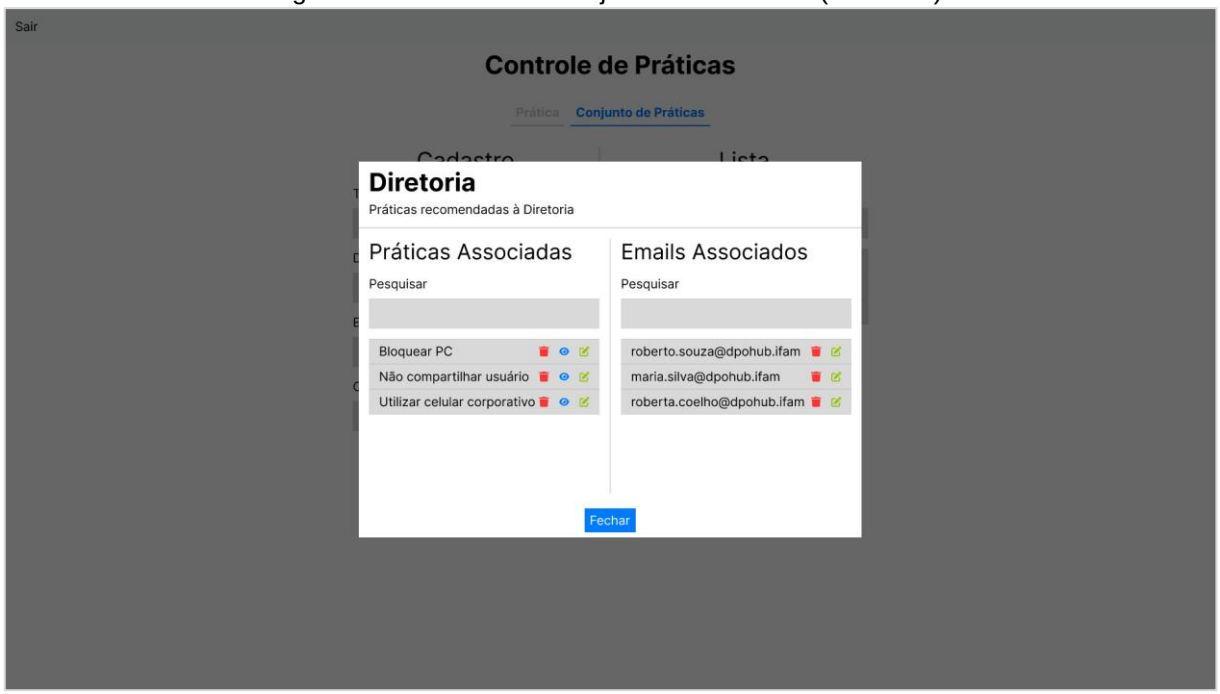
2.4.1.2 Controle de Conjuntos de Práticas

Figura 9 - Controle de Conjuntos de Práticas



Fonte: De autoria própria

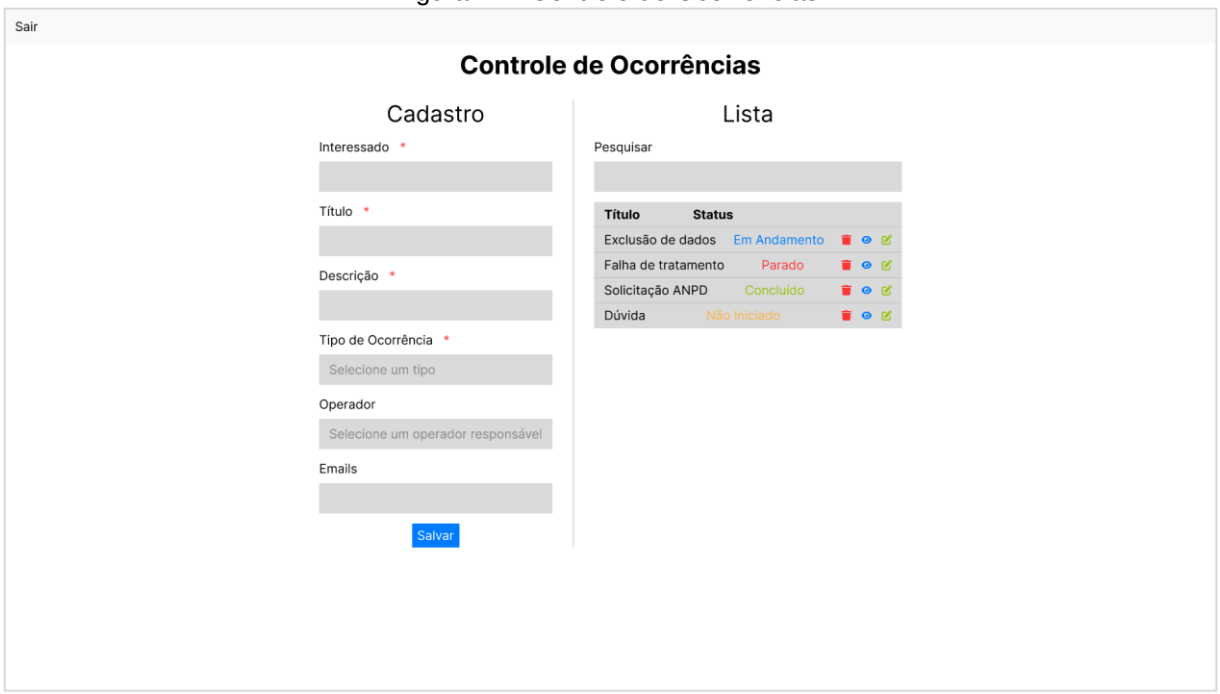
Figura 10 - Controle de Conjuntos de Práticas (Detalhes)



Fonte: De autoria própria.

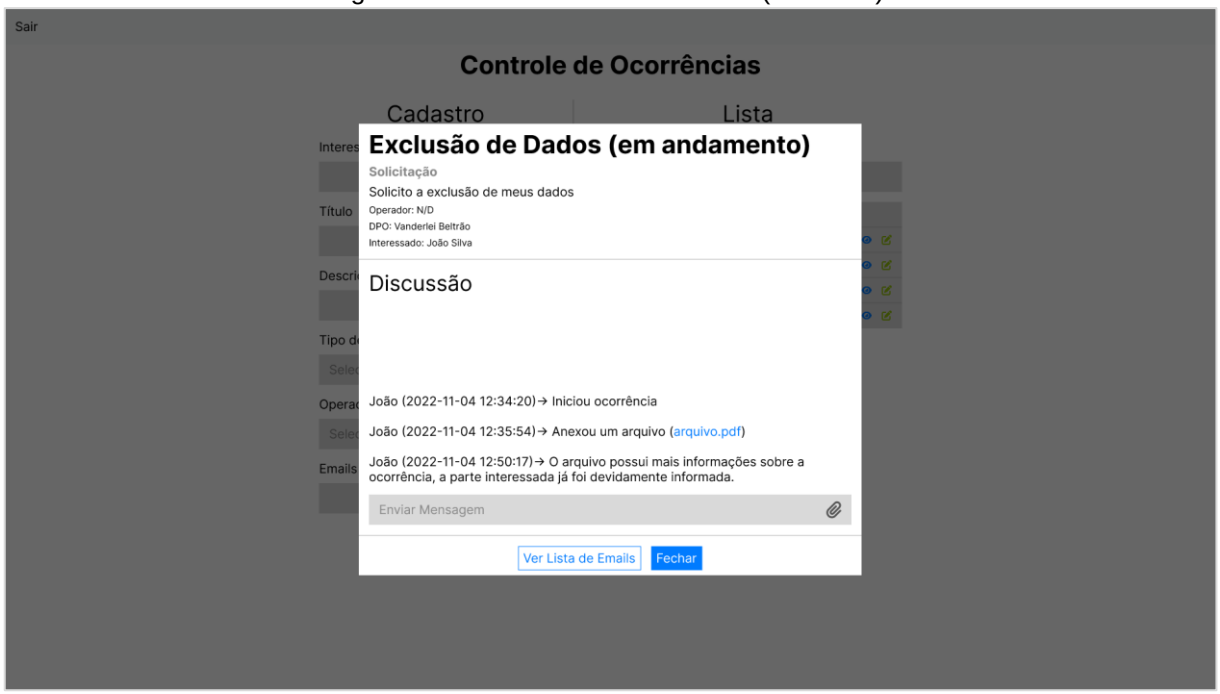
2.4.3 Gerenciamento de Ocorrências

Figura 11 - Controle de Ocorrências



Fonte: De autoria própria.

Figura 12 - Controle de Ocorrências (Detalhes)



Fonte: De autoria própria.

CAPÍTULO 3 - IMPLEMENTAÇÃO DO PROJETO DPOHUB

3.1 INTRODUÇÃO

Foram realizadas pesquisas para entender qual a melhor forma de implementação do sistema, chegando à conclusão de que utilizar o conjunto de microsserviços, *Java Spring* no *back-end*, Angular no *front-end* e MariaDB como banco de dados seria uma alternativa viável por tratar-se de um sistema complexo, justificando a necessidade de um planejamento cuidadoso para utilização de tecnologias que auxiliem no desenvolvimento e manutenção do projeto.

Para testes durante o desenvolvimento do sistema, foram utilizados 4 *e-mails* com propósitos diferentes:

- **Serviço de notificação:** responsável por realizar os envios de *e-mails* automáticos (remetente padrão do serviço de notificação);
- **Encarregado de dados:** representa o *e-mail* utilizado pelo encarregado de dados;
- **Operador:** representa o operador que poderá ser associado à uma ocorrência.
- **Usuário Externo:** representa o usuário que poderá cadastrar e consultar ocorrências sem a necessidade de realizar *login*.

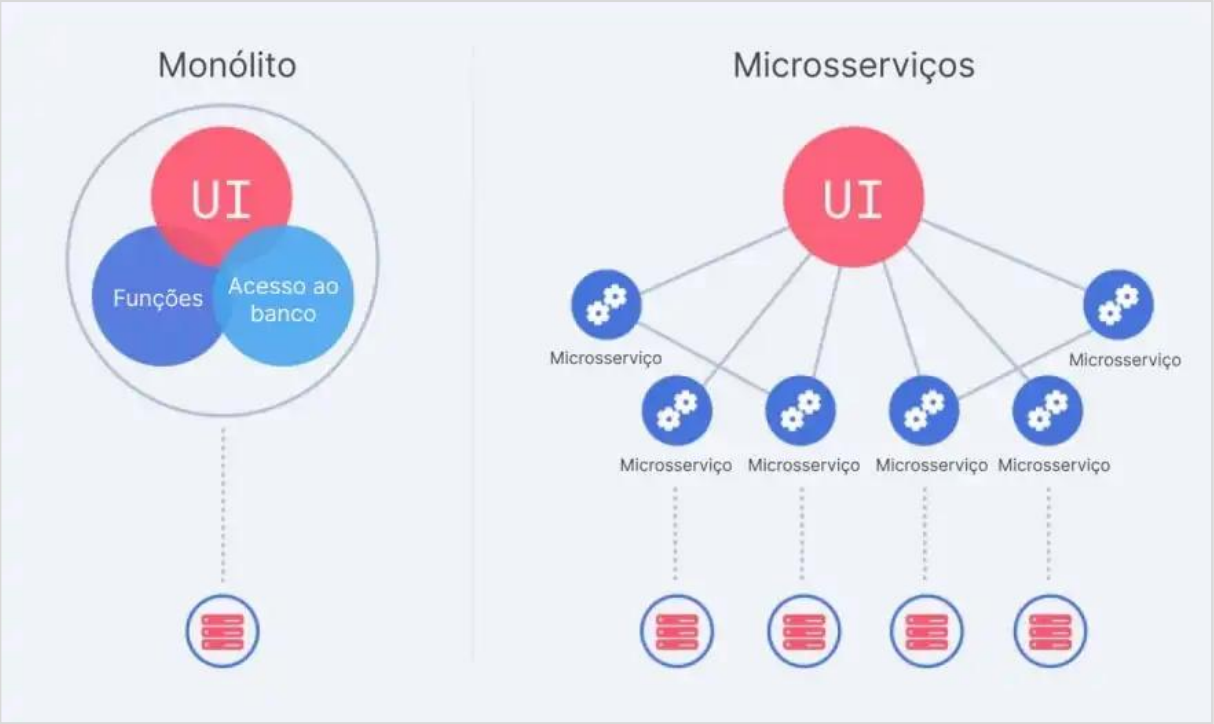
3.2 ARQUITETURA

O projeto é desenvolvido levando em consideração o conceito de microsserviços, em que o funcionamento do sistema não se dá de forma centralizada como os sistemas monolíticos onde todo o seu desenvolvimento é realizado em um único ambiente, por muitas vezes ocasionando falhas críticas nos processos mais importantes a partir de simples mau funcionamento de um único componente.

Na Figura 13, podemos observar a diferença entre os sistemas monolíticos e microsserviços, onde o primeiro funciona como um único projeto que engloba diversos componentes responsáveis por manter o sistema funcionando, enquanto o segundo representa um desenvolvimento descentralizado e autônomo, garantindo, ao final do projeto, a resiliência e manutenibilidade do sistema.

SOLICITAÇÃO ELETRÔNICA nº 630/2025 PROT/CMC (1603741) 23042.000492/2025-17 pg. 65

Figura 13 - Sistemas Monolíticos e Microsserviços



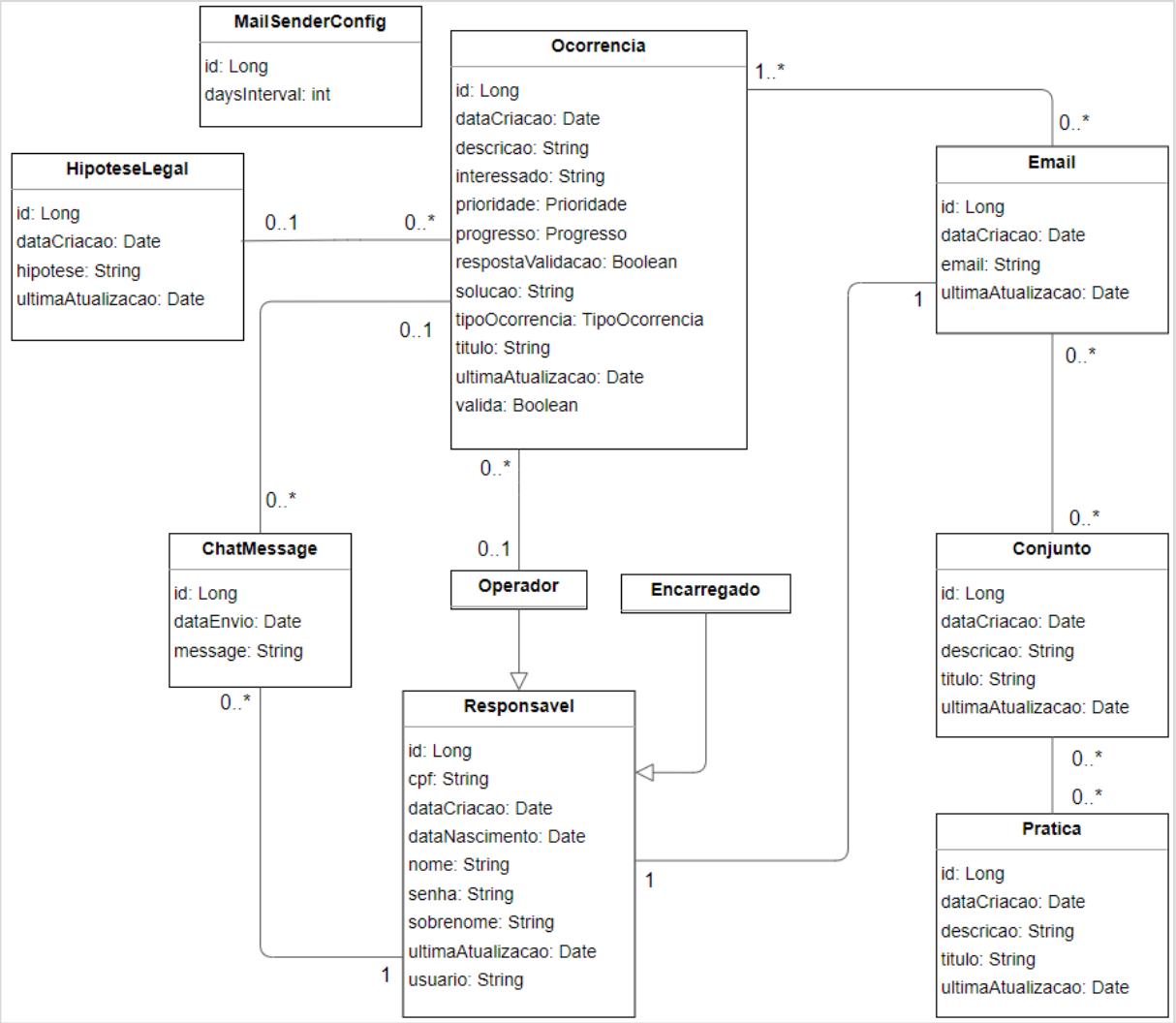
Fonte: DIO, Weslley Prado, 2023.

3.3 DIAGRAMA DE CLASSES

No Diagrama 6, temos a representação das classes que compõem o sistema e suas relações, podemos destacar:

- **Ocorrencia:** pode estar associada à 0 ou N *e-mails*, sem contar o do encarregado e o do operador que, de forma automática, são relacionados pelo próprio sistema. Também pode estar associada à 0 ou N mensagens (ChatMessage). Também é possível definir a hipótese legal.
- **Conjunto:** representa os conjuntos de práticas. Pode estar associado à 0 ou N práticas, e 0 ou N *e-mails*.
- **Responsavel:** classe abstrata que representa encarregado e operador. Deve ser associada à 1 *e-mail* e pode ter 0 ou N mensagens associadas;
    - **Operador:** estende a classe **Responsavel** e pode estar associado a 0 ou N ocorrências;
    - **Encarregado:** estende a classe **Responsavel**.

Diagrama 4 - Diagrama de Classes

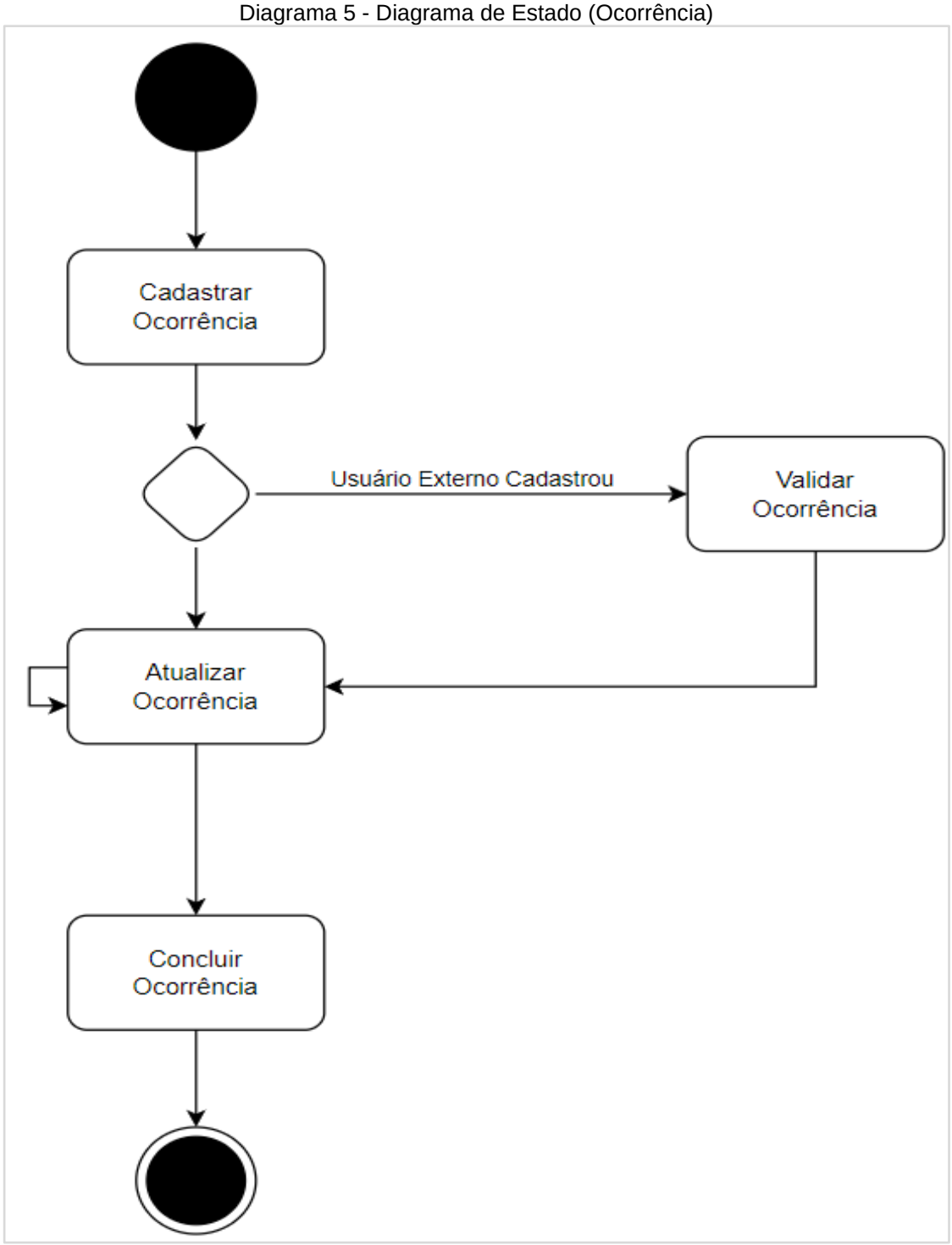


Fonte: De autoria própria.

3.4 DIAGRAMA DE ESTADO (OCORRÊNCIA)

Conforme o Diagrama 7, o estado inicial de uma ocorrência cadastrada pelo encarregado de dados, deve ser automaticamente definido como “validado”, por outro lado, se for cadastrada por um usuário externo, o encarregado deve validar manualmente a ocorrência.

Diagrama 5 - Diagrama de Estado (Ocorrência)



Fonte: De autoria própria.

3.5 DIAGRAMAS DE SEQUÊNCIA

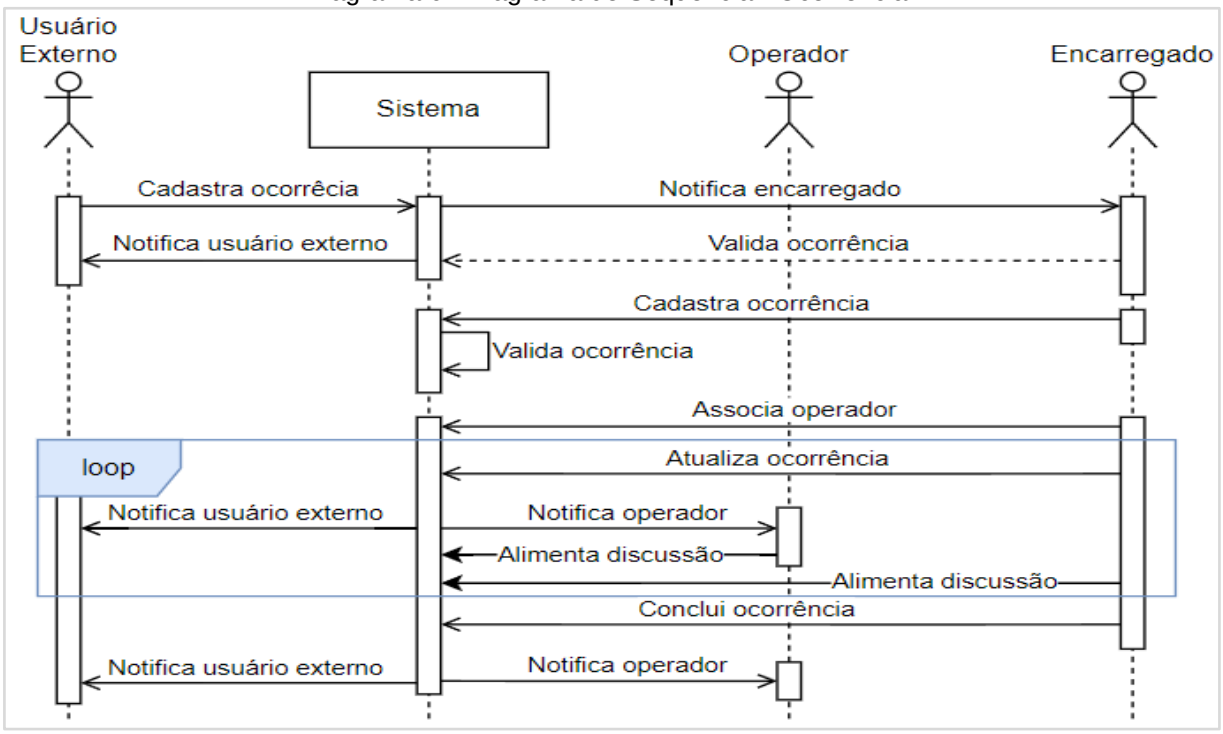
3.5.1 Ocorrência

Como representado no Diagrama 8, quando o cadastro de uma ocorrência for realizado por um usuário externo, o encarregado deve ser notificado, e após validação manual dele, o usuário externo deve ser notificado por *e-mail*. Porém, se o próprio encarregado tiver cadastrado a ocorrência, então o sistema deve, automaticamente, validar a ocorrência.

Durante cadastro, ou edição, de uma ocorrência, o encarregado poderá associar um operador que auxiliará na resolução da ocorrência, e ao ser associado, o operador deverá ser notificado por *e-mail*.

A ocorrência poderá ser atualizada pelo encarregado conforme o necessário, e o sistema deverá notificar todos os *e-mails* associados à ocorrência, incluindo quando for realizada a conclusão da própria. A ocorrência também deve disponibilizar a seção de discussão para que sejam registradas as mensagens enviadas por operador e encarregado.

Diagrama 6 - Diagrama de Sequência - Ocorrência



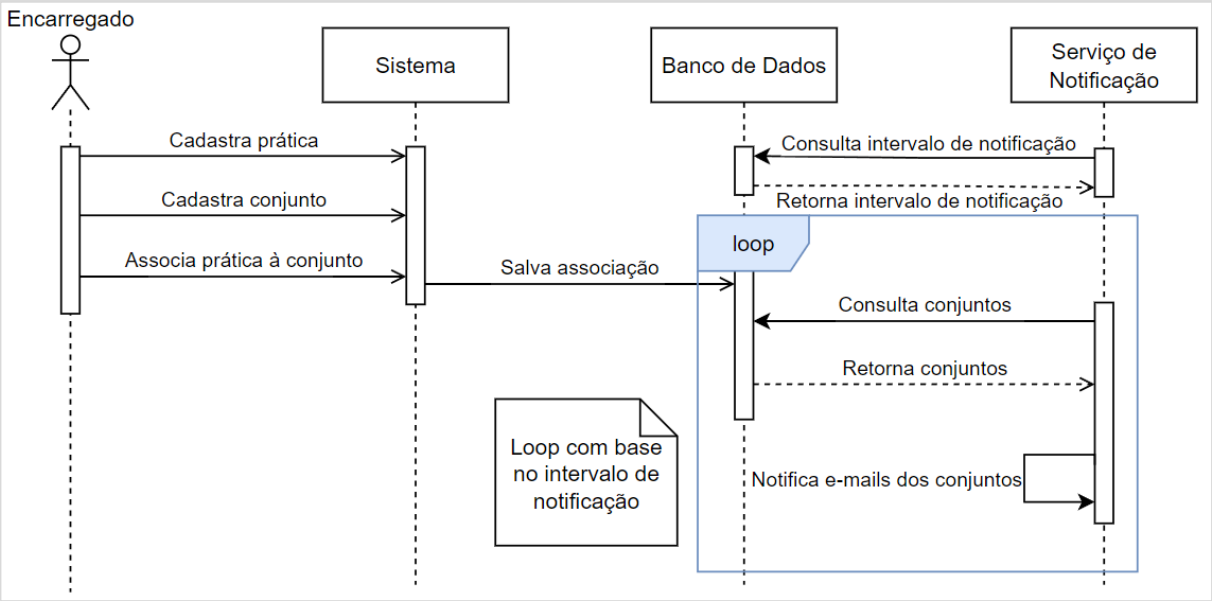
Fonte: De autoria própria.

3.5.2 Prática

Conforme Diagrama 9, o serviço de notificação consulta automaticamente o intervalo de notificação ao iniciar o servidor, e atualiza sempre que o encarregado altera esse período.

Ao cadastrar uma prática, o encarregado poderá associar a um conjunto já existente, ou associar posteriormente ao cadastro da prática. O sistema deverá consultar os conjuntos e, conforme o período configurado, notificar os respectivos *e-mails* associados.

Diagrama 7 - Diagrama de Sequência - Prática



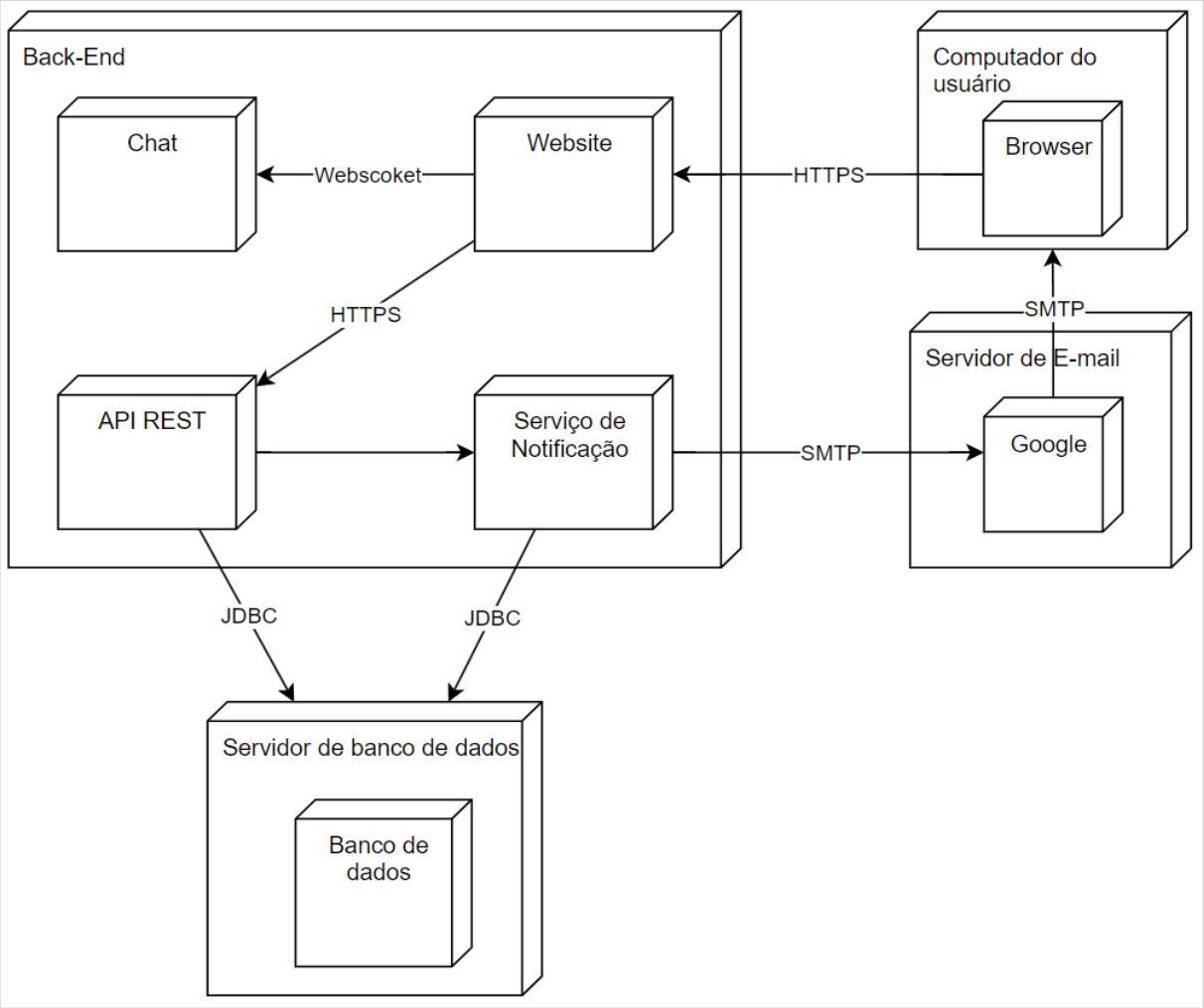
Fonte: De autoria própria.

3.6 DIAGRAMA DE IMPLEMENTAÇÃO

A implementação da arquitetura de microsserviços, em que os componentes são separados para garantir que um componente não interfira nas atribuições de outros componentes, em caso de problemas técnicos. Esse é um primeiro passo para garantir a resiliência do sistema que, deve ser apoiada por uma infraestrutura robusta.

O Diagrama 10 representa a implementação realizada no DPOHub, onde são especificados os componentes e a forma como comunicam-se, por exemplo: o usuário utilizará o browser para se conectar através de HTTPS[12] ao *Website*, que por sua vez, comunica-se por *WebSocket* ao componente de *Chat*, e HTTPS à *API REST*.

Diagrama 8 - Diagrama de Implementação



Fonte: De autoria própria.

[12] **HTTPS (HypeText Transfer Protocol Secure):** o Protocolo de Transferência de HiperTexto Seguro é versão criptografa do HTTP é o principal protocolo de comunicação entre usuário e *websites*.

3.7 TELAS

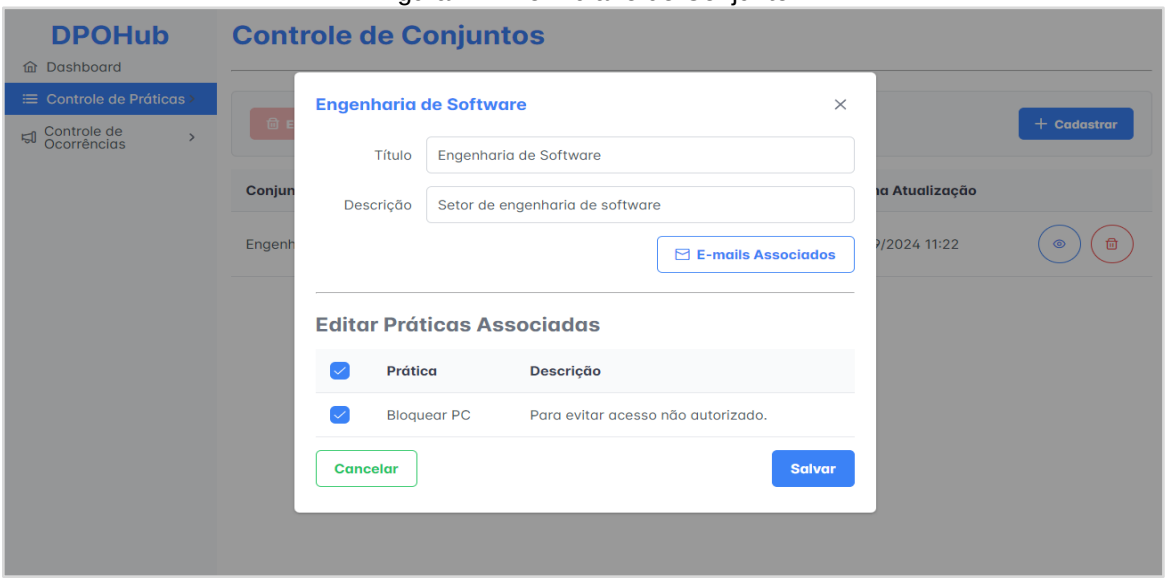
3.7.1 Gerenciamento de Práticas

3.7.1.1 Controle de Conjuntos

3.7.1.1.1 Formulário de Conjunto

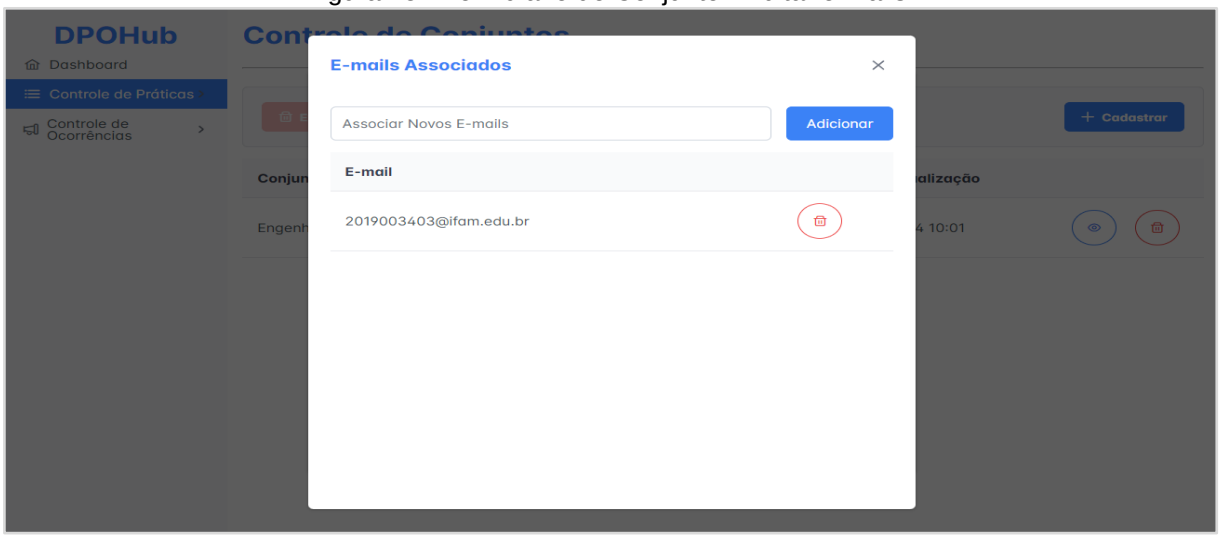
A Tela 1 representa o cadastro de um conjunto, e pode ser acessado na página de listagem de conjuntos. Enquanto a Tela 2, representa a associação de *e-mails* ao conjunto. Através deste formulário, acessível pela tela de listagem de conjuntos, é possível cadastrar e editar conjuntos.

Figura 14 - Formulário de Conjunto



Fonte: De autoria própria

Figura 15 - Formulário de Conjunto - Editar e-mails



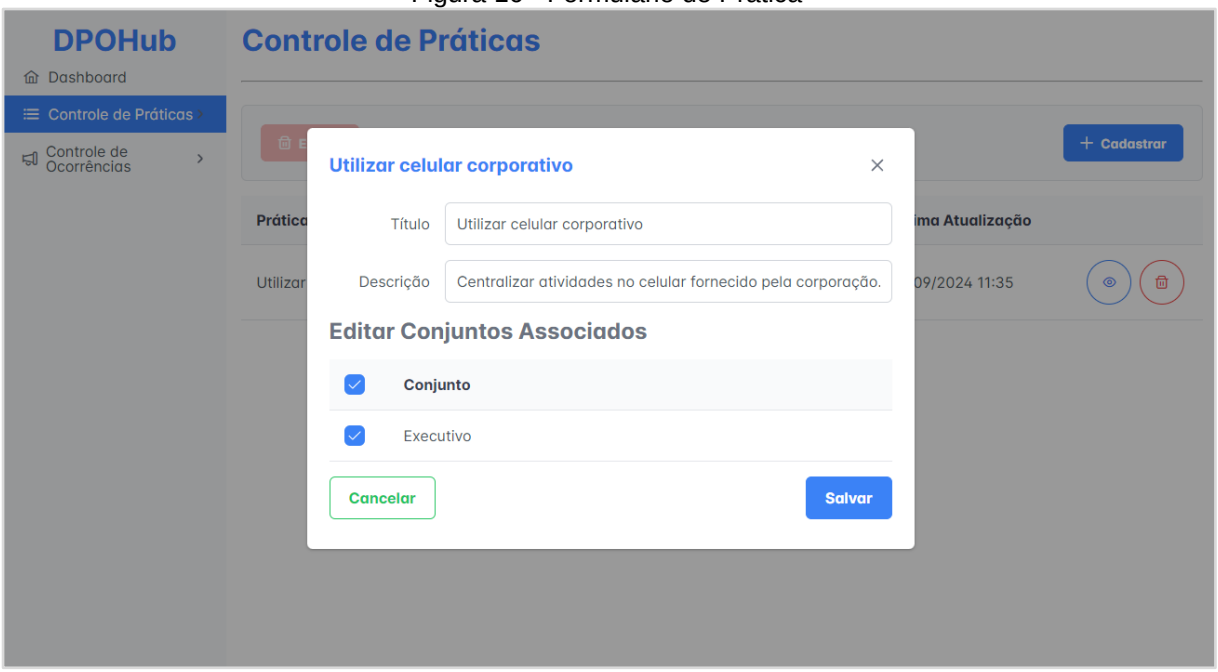
Fonte: De autoria própria

3.7.1.2 Controle de Práticas

3.7.1.2.1 Formulário de Prática

A Tela 3 representa o cadastro de um conjunto, e pode ser acessado na página de listagem de conjuntos. Através deste formulário, acessível pela tela de listagem de práticas, é possível cadastrar e editar práticas.

Figura 16 - Formulário de Prática



Fonte: De autoria própria.

3.7.2 Gerenciamento de Ocorrências

3.7.2.1 Externo (Usuário Externo)

3.7.2.1.1 Cadastro de Ocorrência

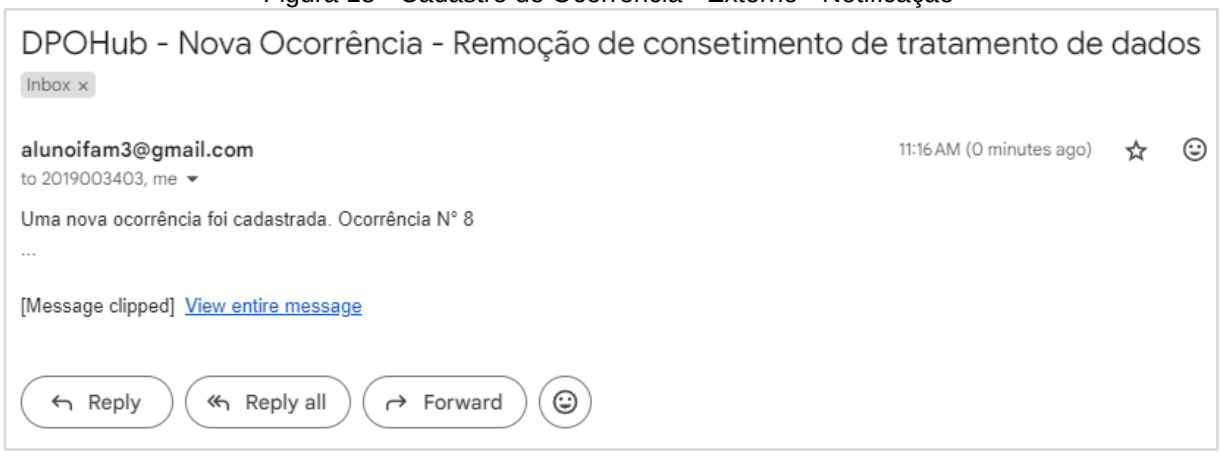
Uma página externa é disponibilizada para permitir cadastro e consulta de ocorrências, sem necessidade de realizar *login*.

Figura 17 - Cadastro de Ocorrência - Externo

Fonte: De autoria própria.

Após cadastro de ocorrência pelo usuário externo, será enviada uma notificação para o encarregado de dados e o próprio usuário, conforme Tela 5.

Figura 18 - Cadastro de Ocorrência - Externo - Notificação



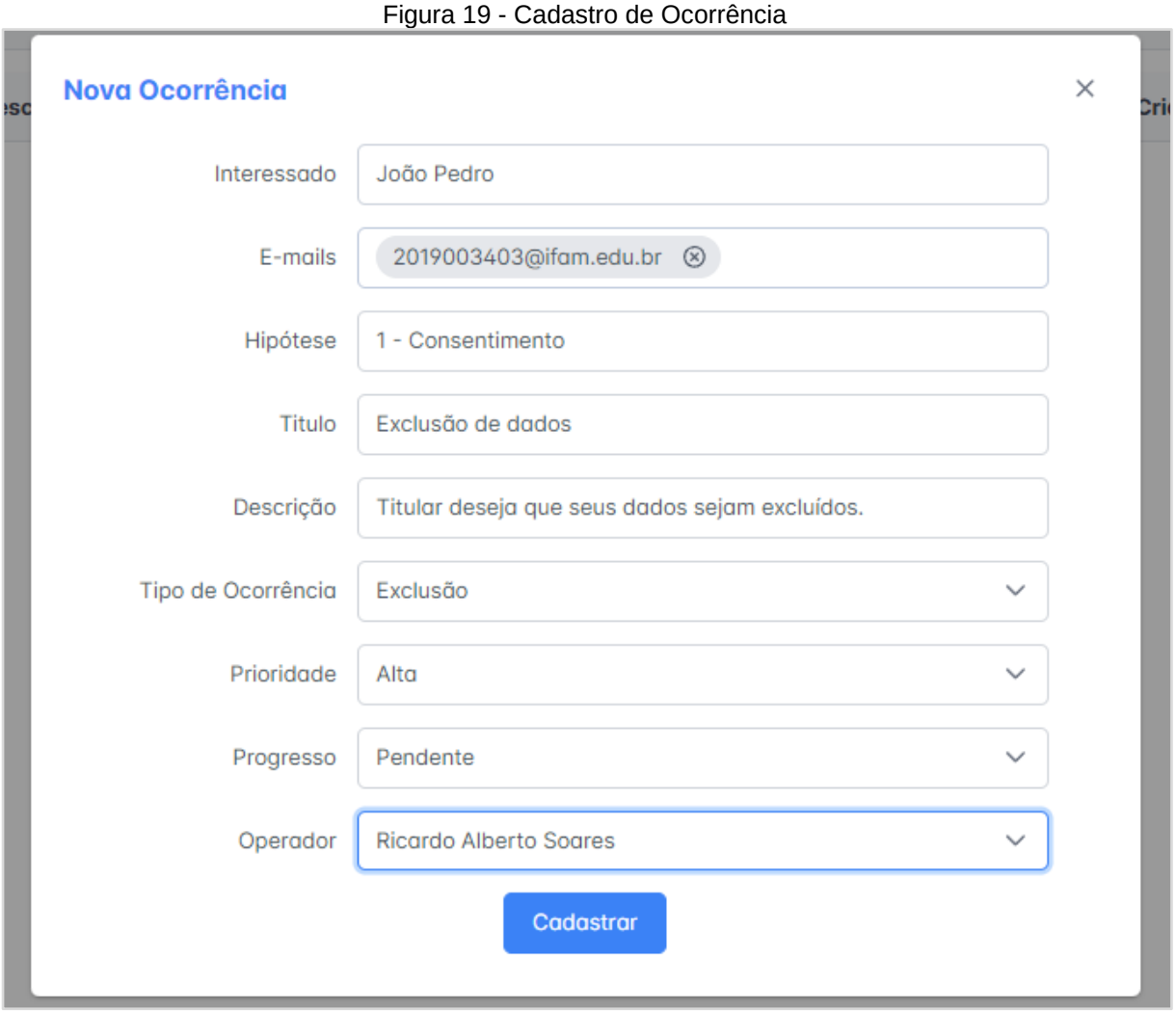
Fonte: De autoria própria.

3.7.2.2 Interno (Encarregado de dados e Operador)

3.7.2.2.1 Formulário de Ocorrência

A Tela 6, disponível somente para o encarregado de dados, representa a tela de cadastro e edição de ocorrência, onde é possível definir todos os dados necessário e, inclusive, indicar operador responsável.

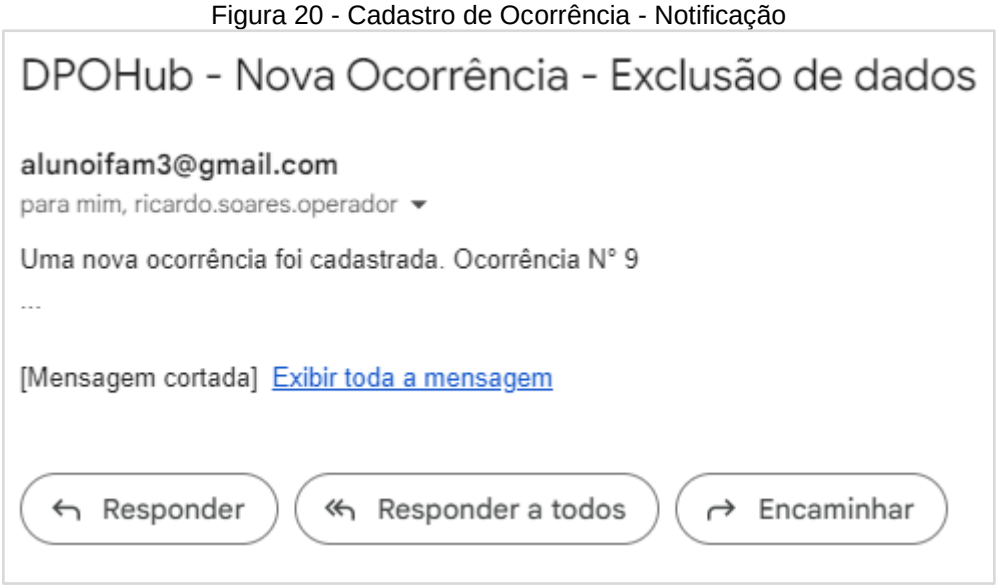
Figura 19 - Cadastro de Ocorrência



Fonte: De autoria própria.

Ao efetuar o cadastro de uma ocorrência, é enviado o *e-mail* de notificação para todos envolvidos, conforme Tela 7, também é enviada a notificação de atualização de ocorrência, conforme Tela 8.

Figura 20 - Cadastro de Ocorrência - Notificação



Fonte: De autoria própria.

Figura 21 - Edição de Ocorrência - Notificação

Fonte: De autoria própria.

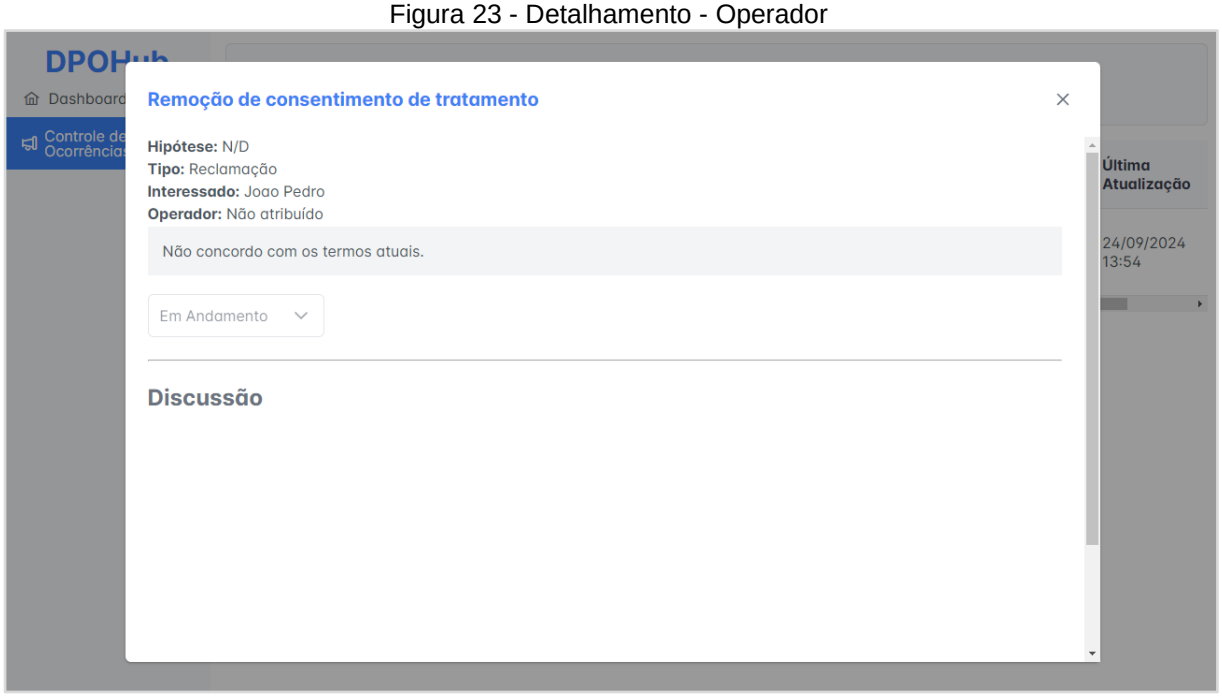
3.7.2.2.2 Movimentação de Ocorrência

A tela de detalhamento disponibiliza a alteração de estado da ocorrência e lista de *e-mails* associados somente para o DPO, enquanto a discussão, bem como informações sobre a ocorrência, é disponibilizada tanto para o encarregado quanto para o operador, de acordo com Tela 9 e Tela 10.

Figura 22 - Detalhamento - DPO

Fonte: De autoria própria.

Figura 23 - Detalhamento - Operador

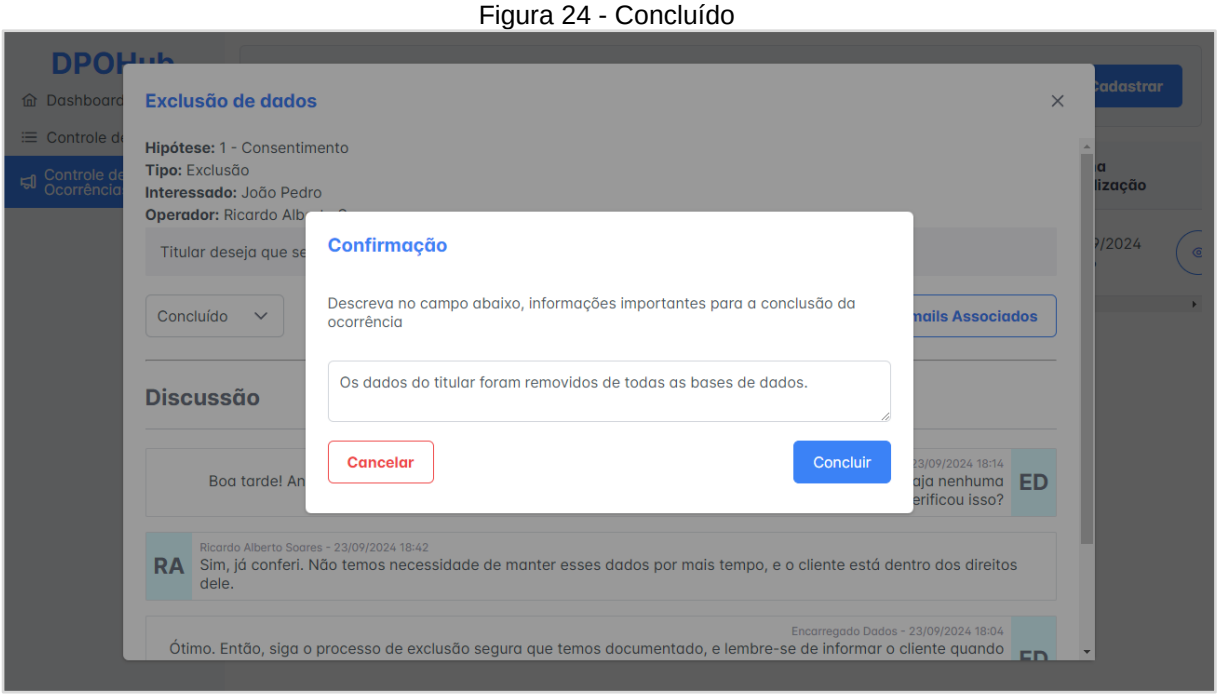


Fonte: De autoria própria.

3.7.2.2.3 Conclusão de Ocorrência

A Tela 11, trata-se da solicitação de confirmação, exibida quando o encarregado de dados alterar o estado da ocorrência para “concluído”, onde será necessário preencher um campo de resolução da ocorrência para, utilizando um campo de pesquisa, consulta posterior.

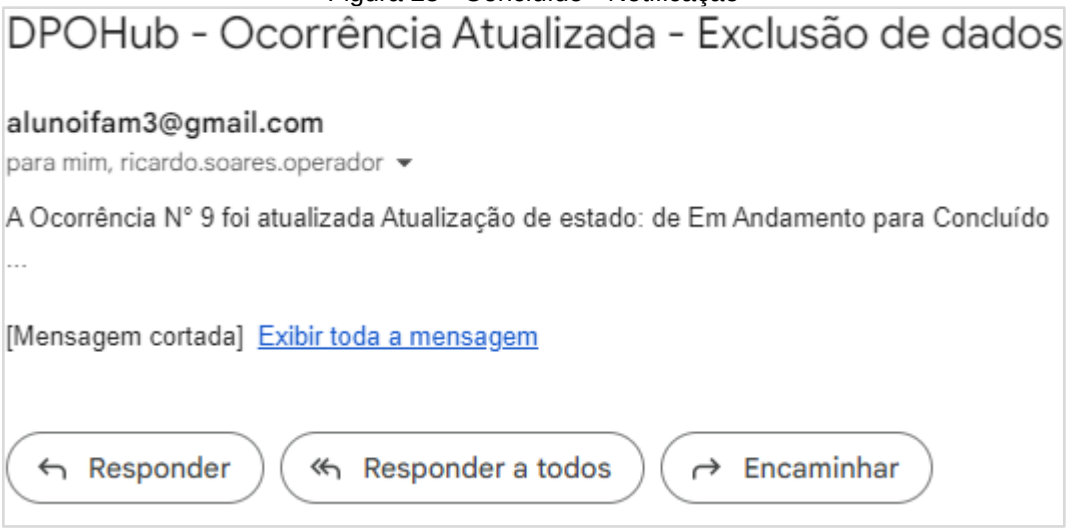
Figura 24 - Concluído



Fonte: De autoria própria.

Assim como todas as atualizações de estado da ocorrência, os *e-mails* serão notificados sobre a conclusão da própria, conforme Tela 12.

Figura 25 - Concluído - Notificação

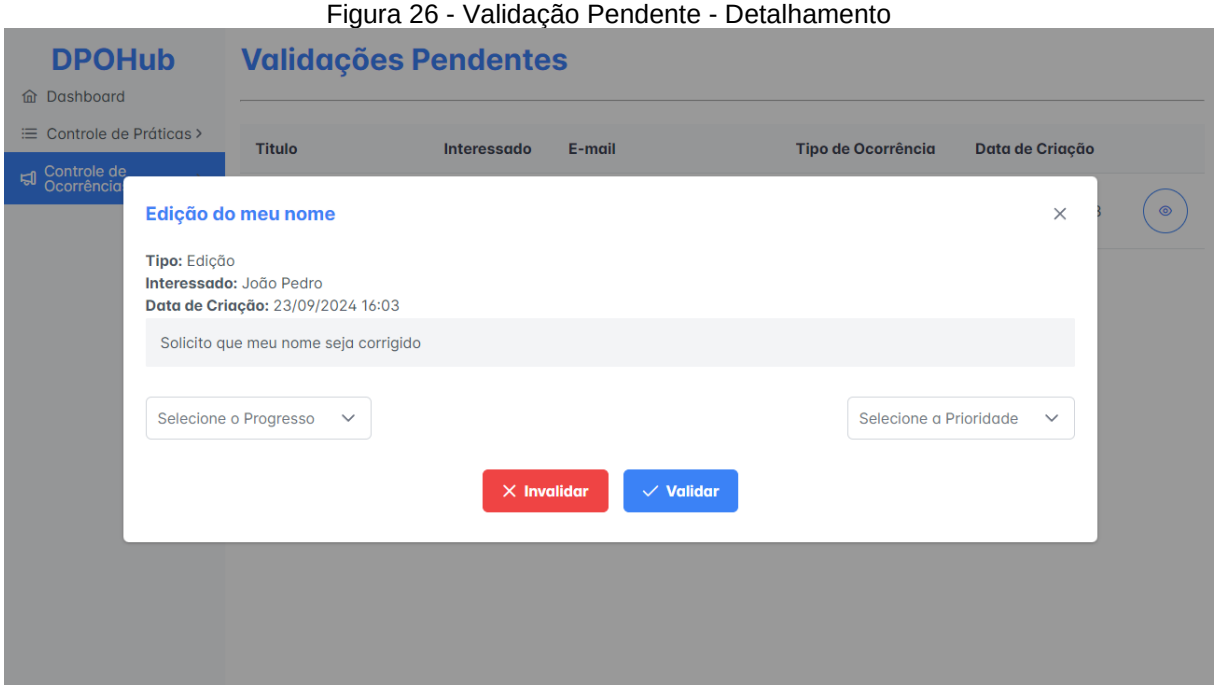


Fonte: De autoria própria.

3.7.2.2.4 Validações

Quando um usuário externo cadastra uma ocorrência, o encarregado de dados é notificado por *e-mail* e a ocorrência passa a estar disponível na tela de consulta de ocorrências com validação pendente, conforme Tela 13.

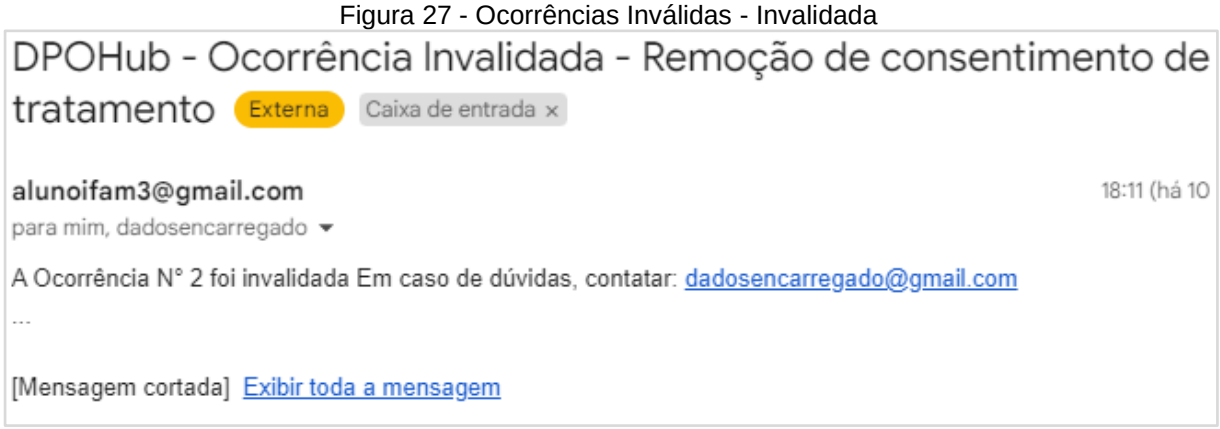
Figura 26 - Validação Pendente - Detalhamento



Fonte: De autoria própria.

Caso a ocorrência seja invalidada pelo encarregado, o usuário externo será notificado, informando-o sobre a invalidação e fornecendo o *e-mail* do encarregado, conforme Tela 14.

Figura 27 - Ocorrências Inválidas - Invalidada



Fonte: De autoria própria.

Após invalidação de uma ocorrência externa, o encarregado poderá, se necessário, consultar a ocorrência para validação na tela de anteriormente ocorrências invalidadas, conforme Tela 15.

Figura 28 - Ocorrências Inválidas - Detalhamento

Fonte: De autoria própria.

4 CONSIDERAÇÕES FINAIS

Desde o planejamento do projeto DPOHub, foi necessário cautela para decisão das tecnologias a serem utilizadas, de forma a evitar tornar o projeto desnecessariamente grande e custoso tanto de desenvolvimento quanto de manutenção. Dessa forma foi possível realizar implementações consistentes utilizando a arquitetura de microsserviços, e apesar de alguns descuidos iniciais que causaram problemas de duplicação de código, a modularidade e reutilização de código tanto do Java Spring quanto do Angular possibilitaram refatorações que apresentaram diminuição considerável de códigos repetidos.

Mesmo com a adoção da arquitetura de microsserviços, para amenizar a quantidade de serviços independentes, foi unificado o serviço de notificação com o servidor de API REST, visto a possibilidade de ineficiência que a máquina a ser utilizada para executar os softwares separados poderia apresentar.

Neste trabalho realizado, o DPOHub foi capaz de atender o proposto através do desenvolvimento de um sistema com foco em auxiliar, principalmente, o encarregado de dados em 2 atribuições muito importantes e burocráticas que podem exigir um alto esforço de controle através da utilização de planilhas, o gerenciamento de práticas e o gerenciamento de ocorrências.

O módulo de gerenciamento de práticas, incluindo conjuntos, atendeu todos os requisitos propostos de cadastro, edição, exclusão e associação de práticas com conjuntos, e de *e-mails* com conjuntos. A notificação periódica também foi implementada, bem como a configuração do intervalo, em dias, pelo encarregado de dados.

O módulo de gerenciamento de ocorrências também foi implementado conforme o proposto, com exceção da funcionalidade de envio de arquivos pelo *chat* de discussão de ocorrência. O serviço de notificação de criação e atualização de ocorrências para todos os *e-mails* associados a respectiva ocorrência também é realizado.

O formulário para cadastro de ocorrências externas também foi implementado, assim como a consulta de andamento dela, através do número recebido no *e-mail* durante o cadastro. Nesse caso, também foi implementado a necessidade de

validação por parte do encarregado de dados, processo que é automático quando o cadastro da ocorrência é realizado pelo próprio DPO.

O DPOHub poderá ser utilizado para expansão de funcionalidades que auxiliem em outras atividades do encarregado de dados, como geração e formulação de relatórios e capacidades de auditoria.

Também deverá ser implementado um login, que atualmente ocorre de forma estática através de perfis pré-definidos de usuários, sendo um controlador e um encarregado de dados. Outras implementações seriam, - ambas relacionadas à ocorrências – o envio de arquivos no *chat* de discussão de ocorrências e alteração dos campos escritos de “hipótese legal” para campos de opções fechadas (pré-definidas), visto que atualmente é possível a inserção de qualquer valor textual neste campo.

5 REFERÊNCIAS

ALVAREZ & MARSAL. **LGPD no mercado brasileiro**. Novembro de 2021. Disponível em: https://www.alvarezandmarsal.com/sites/default/files/2021-11/E-book%20LGPD%20no%20Mercado%20Brasileiro.pdf. Acesso em: 28 nov. 2024.

BAMPAKOS, Aristeidis. DEELEMAN, Pablo. **Learning Angular: A no-nonsense guide to building web applications with Angular 15, 4th Edition (English Edition)**. [S. l]: Packt Publishing, 2023. E-book Kindle.

BLUEPEX CYBERSECURITY. Pesquisa da BluePex CyberSecurity aponta que apenas 15% das PMEs se consideram preparadas para a LGPD. **TI Inside**. Março, 2022. Disponível em: https://bluepex.com.br/noticias/pesquisa-da-bluepex-cybersecurity-aponta-que-apenas-15-das-pmes-se-consideram-preparadas-para-a-lgpd. Acesso em: 28 nov. 2024.

CLEDUPE, Cleiton. **Microsserviços: Direto ao Ponto**. [S. l]: [s.n.], 2024. E-book Kindle.

COSMINA, Juliana. HARROP, Rob. SCHAEFER, Chris. HO, Clarence. **Pro Spring 6: An In-Depth Guide to the Spring Framework (English Edition)**. [S. l]: Apress, 2023. E-book Kindle.

J. T. DYER, Russell. **Learning MySQL and MariaDB: Heading in the Right Direction with MySQL and MariaDB (English Edition)**. [S. l]: O'Reilly Media, 2015. E-book Kindle.

KLEPPMANN, Martin. **Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems (English Edition)**. [S. l]: O'Reilly Media, 2017. E-book Kindle.

LIGUS, Slawek. **Effective Monitoring and Alerting**. [S. l]: O'Reilly Media, 2012. E-book Kindle.

MITCHELL, Cal. Aurora vs MariaDB vs MySQL performance and cost comparison. **Albatross**. Fevereiro, 2023. Disponível em: https://www.albatrossmigrations.com/blog/aurora-vs-mariadb-vs-mysql. Acesso em: 27 nov. 2024.

WANG, Vanessa. SALIM, Frank. MOSKOVITS, Peter. **The Definitive Guide to HTML5 WebSocket (English Edition)**. [S. l]: Apress, 2013. E-book Kindle.

WOOD, David. **Programming Internet Email: Mastering Internet Messaging Systems (English Edition)**. [S. l]: O'Reilly Media, 1999. E-book Kindle.

WORLD ECONOMIC FORUM. Chapter 3. Digital Dependencies and Cyber Vulnerabilities. **Global Risks Report 2022**. Janeiro, 2022. Disponível em: https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities. Acesso em: 28 nov. 2024.