ASSOCIAÇÃO EDUCACIONAL DOM BOSCO
CENTRO UNIVERSITÁRIO DOM BOSCO DO RIO DE JANEIRO
CURSO DE GRADUAÇÃO EM SISTEMA DE INFORMAÇÃO

ANA CRISTINA DOS SANTOS ALMEIDA
ANNA CLARA BALIEIRO ALMEIDA DE PAULA
JOÃO PAULO ANDRADE SAMPAIO

CAMALEÃO - SISTEMA DE GESTÃO DA LGPD

RESENDE - RJ
2025

Ana Cristina dos Santos Almeida
Anna Clara Balieiro Almeida De Paula
João Paulo Andrade Sampaio

CAMALEÃO - SISTEMA DE GESTÃO DA LGPD

Trabalho de Conclusão de Curso apresentado ao curso de Sistema de Informação, como requisito parcial para a obtenção do Grau de Bacharel em Sistema de Informação pelo Centro Universitário Dom Bosco do Rio de Janeiro.

Orientador(a): Professora Mônica Mara da Silva

Resende - RJ

2025

Catalogação na fonte
Biblioteca Central da Associação Educacional Dom Bosco – Resende-RJ

A447 Almeida, Ana Cristina dos Santos
Camaleão: sistema de gestão da LGPD / Ana Cristina dos Santos Almeida; Anna Clara Balieiro Almeida de Paula; João Paulo Andrade Sampaio - 2025.
247f.

Orientador: Mônica Mara da Silva
Trabalho de conclusão de curso apresentado como requisito parcial à finalização do curso de Sistemas de Informação do Centro Universitário Dom Bosco do Rio de Janeiro, da Associação Educacional Dom Bosco.

1. Informática. 2. Software. 3. Lei geral de proteção de dados. 4. Proteção de dados. I. Paula, Anna Clara Balieiro Almeida de. II. Sampaio, João Paulo Andrade. III. Silva, Mônica Mara da. IV. Centro Universitário Dom Bosco do Rio de Janeiro. V. Associação Educacional Dom Bosco. VI. Título.

CDU 004.42(043)

Bibliotecária Maria Ismênia de Oliveira – CRB – 7 / 7667

ANA CRISTINA DOS SANTOS ALMEIDA
ANNA CLARA BALIEIRO ALMEIDA DE PAULA
JOÃO PAULO ANDRADE SAMPAIO

CAMALEÃO - SISTEMA DE GESTÃO DA LGPD

Trabalho de Conclusão de Curso apresentado ao curso de Sistema de Informação, como requisito parcial para a obtenção do Grau de Bacharel em Sistema de Informação pelo Centro Universitário Dom Bosco do Rio de Janeiro.

BANCA EXAMINADORA

Prof.: _____

Orientador(a): Prof.(a) Mônica Mara da Silva, M.e.

Prof.: _____

Convidado(a): Prof.(a) Miguel Carlos Damasco dos Santos, M.e.

Prof.: _____

Convidado(a): Prof.(a) Ivan José Vianna de Freitas, Esp.

Resende, 29 de novembro de 2025.

Dedicamos este trabalho, em primeiro lugar, a nós mesmos: Ana Cristina, Anna Clara e João Paulo.

Reconhecemos a nossa coragem de começar, a disciplina para continuar e a força para concluir. Cada um de nós enfrentou obstáculos pessoais, dúvidas, cansaços e até momentos de querer desistir, mas seguimos firmes. Por isso, com muito orgulho, nos abraçamos por tudo o que fomos capazes de construir juntos.

Também dedicamos este trabalho às nossas famílias, que sempre foram nosso apoio incondicional.

A cada palavra de incentivo, gesto de carinho e olhar de confiança, sentimos o quanto somos amados e apoiados. Foram vocês que estiveram por perto mesmo quando tudo parecia distante. Nos ofereceram não apenas apoio material, mas, principalmente, emocional.

Não poderíamos deixar de dedicar este trabalho à nossa professora Mônica, cuja orientação, paciência e incentivo foram fundamentais em toda a nossa trajetória acadêmica. Seu compromisso em ensinar e sua dedicação em nos guiar com firmeza e sabedoria fizeram toda a diferença para que este projeto fosse concluído com êxito.

Este trabalho é resultado de um esforço coletivo. Mesmo sendo escrito por nós, carrega a energia, a presença e o amor daqueles que caminharam conosco — de perto ou de longe. A vocês, nossa eterna gratidão.

Agradecemos primeiramente a Deus, por ter nos sustentado com saúde, sabedoria e fé durante toda essa trajetória.

Agradecemos a nós mesmos, por termos acreditado em nossa capacidade de seguir em frente, mesmo diante das adversidades. Por cada esforço individual e coletivo, por cada momento de companheirismo, e por termos sido suporte uns para os outros quando mais precisamos.

Às nossas famílias, expressamos um agradecimento especial. Vocês foram pilares fundamentais para a realização deste sonho. Obrigado por cada palavra de incentivo, cada gesto de apoio e cada demonstração de amor e paciência ao longo desse processo. Sem vocês, essa conquista não teria o mesmo significado.

Aos professores e orientadores que nos guiaram com sabedoria e nos desafiaram a crescer, deixamos nosso sincero agradecimento. Cada ensinamento contribuiu para que nos tornássemos profissionais mais preparados e pessoas mais conscientes.

Por fim, agradecemos a todos que, de alguma forma, fizeram parte dessa caminhada. Cada presença, palavra, gesto ou silêncio nos fortaleceu. Levar cada um de vocês em nossa memória torna essa conquista ainda mais valiosa.

“A privacidade é o poder de decidir o que os outros sabem sobre você.” — Edward Snowden, ex-analista da NSA e defensor da privacidade digital

RESUMO

Este trabalho trata da crescente relevância da proteção de dados pessoais em um cenário marcado pela transformação digital, com destaque para a Lei Geral de Proteção de Dados (LGPD). A pesquisa analisa os principais conceitos ligados à privacidade, como a definição de dados pessoais e sensíveis, os direitos dos titulares e as responsabilidades legais das organizações, além de discutir a importância da segurança da informação por meio de práticas técnicas e organizacionais. Também é explorado o papel estratégico do Encarregado de Proteção de Dados (DPO), as penalidades previstas em caso de descumprimento e a atuação da Autoridade Nacional de Proteção de Dados (ANPD), estabelecendo conexões entre a LGPD e metas globais, como a Agenda 2030 da ONU. Como aplicação prática, foi desenvolvido um sistema web voltado ao gerenciamento e controle de documentos, com o objetivo de auxiliar empresas na adequação à LGPD. O projeto envolveu etapas de planejamento, levantamento de requisitos, definição de arquitetura, desenvolvimento e testes, além da elaboração de estratégias de implantação, suporte e treinamento de usuários. Foram utilizadas tecnologias como Django, *SQLite*, Node.js, *JavaScript*, *FlutterFlow* e CSS, apoiadas por ferramentas de versionamento e desenvolvimento colaborativo, como GitHub e Visual Studio Code. Conclui-se que a integração entre tecnologia e legislação, quando aplicada de forma responsável, constitui uma importante aliada na proteção de dados pessoais. O sistema desenvolvido demonstra que é possível unir inovação e conformidade legal para promover maior segurança, eficiência e confiança na relação entre organizações e usuários.

Palavras-chave: Proteção de Dados; LGPD; Privacidade; Segurança da Informação; Transformação Digital; Sistema Web.

ABSTRACT

This work addresses the growing relevance of personal data protection in a context marked by digital transformation, with emphasis on Brazil's General Data Protection Law (LGPD). The research analyzes the main concepts related to privacy, such as the definition of personal and sensitive data, data subject rights, and the legal responsibilities of organizations. It also discusses the importance of information security through technical and organizational practices. Furthermore, the strategic role of the Data Protection Officer (DPO), the penalties for noncompliance, and the activities of the National Data Protection Authority (ANPD) are explored, establishing connections between the LGPD and global goals such as the United Nations 2030 Agenda. As a practical application, a web-based system was developed for document management and control, aimed at assisting companies in achieving LGPD compliance. The project involved stages of planning, requirements gathering, architecture definition, development, and testing, in addition to designing deployment, support, and user training strategies. Technologies such as Django, SQLite, Node.js, JavaScript, FlutterFlow, and CSS were used, supported by version control and collaborative development tools like GitHub and Visual Studio Code. It is concluded that the integration of technology and legislation, when applied responsibly, represents an important ally in personal data protection. The developed system demonstrates that it is possible to combine innovation and legal compliance to promote greater security, efficiency, and trust in the relationship between organizations and users.

Keywords: Data Protection; LGPD; Privacy; Information Security; Digital Transformation; Web System.

LISTA DE FIGURAS

Figura 1 - Indústria, Inovação e Infraestrutura....35
Figura 2 - Paz Justiça e Instituições Eficazes....35
Figura 3: Tela de Login....38
Figura 4: Tela de Home....39
Figura 5: Tela de DPO....40
Figura 6: Tela de Formulário de Atividades....41
Figura 7: Tela de Dashboard....42
Figura 8: Tela de Dashboard....42
Figura 9: Tela de Dashboard....43
Figura 10: Tela de Dashboard....43
Figura 11: Tela de Inventário de Dados....44
Figura 12: Cadastro de Usuário....45
Figura 13: Tela Lista Inventários....46
Figura 14: Tela de Avaliação de Risco....47
Figura 15: Figura 15: Tela de Ranking de Riscos....48
Figura 16: Tela de Controle de Plano de Ação....49
Figura 17: Tela de Ações de Monitoramento....50
Figura 18: Tela de Cadastro de Nova Ação de Monitoramento....51
Figura 19: Tela de Edição de Ação de Monitoramento....52
Figura 20: Tela de Controle de Incidentes....53
Figura 21: Tela de Cadastro de Incidente....54
Figura 22: Tela de Edição de Incidente....55
Figura 23: Tela de Heatmap de Risco....56
Figura 24: Tela Calendário de Eventos....56
Figura 25: Tela Visualização Anual do Calendário de Eventos....57
Figura 26: Visualização Semanal do Calendário de Eventos....58
Figura 27: Tela de Login (Versão Mobile)....59
Figura 28: Tela Recuperação de Senha (Versão Mobile)....60
Figura 29: Tela Home (Versão Mobile)....61
Figura 30: Menu Lateral (Versão Mobile)....62
Figura 31: Tela do Encarregado de Proteção de Dados (Versão Mobile)....63
Figura 32: Tela de Checklist (Versão Mobile)....64
Figura 33: Tela de Cadastro de Usuário (Versão Mobile)....65

Figura 34: Tela de Perfil do Usuário (Versão Mobile)....66
Figura 35: Logotipo Camaleão....70
Figura 36: Logo Django....71
Figura 37: Logo SQLite....72
Figura 38: Logo CSS....72
Figura 39: Logo Git Hub....73
Figura 40: Logo Visual Studio Code....74
Figura 41: Logo Node JS....74
Figura 42: Logo JavaScript....75
Figura 43: Github....85
Figura 44: Arquitetura de Implantação....104
Figura 45: Diagrama de Casos de Uso....112
Figura 46: Diagrama de Classes de Dados....145
Figura 47: Gerir Usuários (Diagrama de Atividades)....146
Figura 48: Fazer Login/Logout (Diagrama de Atividades)....147
Figura 49: Gerir Perfil do Usuário (Diagrama de Atividades)....148
Figura 50: Visualizar Informações do DPO (Diagrama de Atividades)....149
Figura 51 Gerir Documentos LGPD (Diagrama de Atividades)....150
Figura 52: Gerir Inventário de Dados (Diagrama de Atividade)....151
Figura 53: Gerir Riscos - Matriz de Riscos LGPD (Diagrama de Atividades)....152
Figura 54: Gerir Planos de Ação (Diagrama de Atividades)....153
Figura 55: Gerir Monitoramentos (Diagrama de Atividades)....154
Figura 56: Gerir Incidentes(Diagrama de Atividades)....155
Figura 57: Visualizar Mapa de Calor de Riscos (Diagrama de Atividades)....156
Figura 58: Gerir Checklist de Conformidade LGPD (Diagrama de Atividades)....157
Figura 59: Gerir Calendári (Diagrama de Atividades)....158
Figura 60: Registrar e Consultar Atividade de Login e Operações do Usuário (Diagrama de Atividades)....159
Figura 61: Visualizar Dashboard....160
Figura 62: Visualizar Notificações e Alertas de Prazo e Segurança(Diagrama de Atividades)....161
Figura 63: Gerar Relatórios de Conformidade (Diagrama de Atividades)....162
Figura 64: Gerir Usuário....163
Figura 65: Login/Logout....164

Figura 66: Gerir Perfil 165
Figura 67: Página do Encarregado (DPO) 166
Figura 68: Gerir Documentos 167
Figura 69: Gerir Inventário de Dados (Figura 1) 168
Figura 70: Gerir Inventário de Dados (Figura 2) 168
Figura 71: Gerir Riscos (Figura 1) 169
Figura 72: Gerir Riscos (Figura 2) 169
Figura 73: Gerir Plano de Ação (Figura 1) 170
Figura 74: Gerir Plano de Ação(Figura 2) 170
Figura 75: Gerir Monitoramento(Figura 1) 171
Figura 76: Gerir Monitoramento(Figura 2) 171
Figura 77: Gerir Incidentes (Figura 1) 172
Figura 78: Gerir Incidentes (Figura 2) 172
Figura 79: Visualizar Heatmap 173
Figura 80: Gerir Checklist(Figura 1) 174
Figura 81: Gerir Checklist(Figura 2) 174
Figura 82: Gerir Calendário(Figura 1) 175
Figura 83: Gerir Calendário(Figura 2) 175
Figura 84: Registrar e consultar logs de ações dos usuários 176
Figura 85: Visualizar Dashboard 177
Figura 86: Visualizar Dashboard 178
Figura 87: Visualizar Notificações 179
Figura 88: Visualizar Notificações 180
Figura 89: Gerar Relatórios 181
Figura 90: Diagrama de Entidade e Relacionamento 182
Figura 91: Autenticar Usuário 207
Figura 92: Visualizar Heatmap 208
Figura 93: Gerir Checklist 209
Figura 94: Gerir Calendário 210
Figura 95: Visualizar Dashboard 211
Figura 96: Visualizar Notificações 212
Figura 97: Gerar Relatórios 213
Figura 98: Visualizar / Monitorar Ações dos Usuários 214
Figura 99: Tela Cadastro de Usuário 215

Figura 100: Página de Login 216
Figura 101: Página Login Esqueceu senha 216
Figura 102: Página de Redefinição de Senha 217
Figura 103: Página Principal 217
Figura 104: Tela Menu lateral 218
Figura 105: Página de Perfil 218
Figura 106: Página Edição Perfil 219
Figura 107: Página Checklist 219
Figura 108: Página de Novo item do Checklist 220
Figura 109: Página do Encarregado (DPO) 220
Figura 110: Página Atividades da LGPD 221
Figura 111: Página Nova Atividade LGPD 222
Figura 112: Página Cadastro de Inventário de Dados (Parte 1) 222
Figura 113: Página Cadastro de Inventário de Dados (Parte 2) 223
Figura 114: Página Cadastro de Inventário de Dados (Parte 3) 223
Figura 115: Página Lista de Inventário 224
Figura 116: Página Avaliação de Risco 225
Figura 117: Página Cadastro de Risco 225
Figura 118: Página Ranking de Risco 226
Figura 119: Página Controle de Plano de Ação 226
Figura 120: Página Incluir Complemento da Controle de Ação 227
Figura 121: Página Controle de Ações, editar e Excluir 227
Figura 122: Página Controle Plano Ação, Excluir Complemento 228
Figura 123: Página Controle Plano de Ação, Adicionando Complemento Pós Exclusão 228
Figura 124: Página Ações de Monitoramento 229
Figura 125: Página Adição Nova Ação Monitoramento 229
Figura 126: Controle de Incidentes 230
Figura 127: Página Novo Incidente 230
Figura 128: Página Heatmap 231
Figura 129: Página Heatmap Gráfico 232
Figura 130: Dashboard de Conformidade LGPD 232
Figura 131: Página Dashboards Riscos 233
Figura 132: Página Dashboard Ações 233

Figura 133: Página Dashboards Incidentes 234
Figura 134: Página Dashboards Acessos e Usuários 234
Figura 135: Página Dashboards Índice de maturidade 235
Figura 136: Página Calendário.....235
Figura 137: Página Calendário Semanal.....236
Figura 138: Página Calendário Anual.....236
Figura 139: Página de Novo Evento Calendário 237
Figura 140: Página Login Mobile.....238
Figura 141: Página Recuperação Senha Login Mobile 239
Figura 142: Página Home Mobile.....240
Figura 143: Página Menu Lateral 241
Figura 144: Página Perfil Usuário Mobile 242
Figura 145: Página Cadastro de Usuário Mobile.....243
Figura 146: Página Checklist Mobile.....244
Figura 147: Página Atividades Mobile 245
Figura 148: Página Encarregado de Dados (DPO) Mobile.....246

LISTA DE TABELAS

Tabela 1: Tabela Nome e Função 66
Tabela 2: Necessidade de Hardware 86
Tabela 3: Necessidade de Software 86
Tabela 4: Necessidade de Pessoas 87
Tabela 5: Lista de Testes 87
Tabela 6: Caso de teste CT001 88
Tabela 7: Caso de teste CT002 88
Tabela 8: Caso de teste CT003 89
Tabela 9: Caso de Teste CT004 89
Tabela 10: Caso de Teste CT005 89
Tabela 11: Caso de Teste CT006 90
Tabela 12: Caso de Teste CT007 90
Tabela 13: Caso de Teste CT008 90
Tabela 14: Caso de Teste CT009 91
Tabela 15:Caso de Teste CT010 91
Tabela 16: Caso de Teste CT011 91
Tabela 17: Caso de Teste CT012 92
Tabela 18: Caso de Teste CT013 92
Tabela 19: Caso de Teste CT014 92
Tabela 20: Caso de Teste CT015 92
Tabela 21: Tabela 21: Caso de Teste CT016 93
Tabela 22: Tabela 21: Caso de Teste CT017 93
Tabela 23: Tabela 21: Caso de Teste CT018 93
Tabela 24: Tabela 21: Caso de Teste CT019 94
Tabela 25: Caso de Teste CT020 94
Tabela 26: Caso de Teste CT021 94
Tabela 27: Caso de Teste CT022 95
Tabela 28: Caso de Teste CT023 95
Tabela 29: Caso de Teste CT024 95
Tabela 30: Caso de Teste CT025 96
Tabela 31: Caso de Teste CT026 96
Tabela 32: Caso de Teste CT027 96

Tabela 33: Dicionário de dados (Tabela: Incidentes)..... 184
Tabela 34: Dicionário de dados (Tabela: Monitoramentos) 185
Tabela 35: Dicionário de dados (Tabela: ChecklistLGPD)..... 187
Tabela 36: Dicionário de dados (Tabela: DocumentosLGPD) 189
Tabela 37: Dicionário de dados (Tabela: RiskLevelBand) 190
Tabela 38: Dicionário de dados (Tabela: Risk)..... 191
Tabela 39: Dicionário de dados (Tabela: User) 193
Tabela 40: Dicionário de dados (Tabela: InventarioDados)..... 194
Tabela 41: Dicionário de dados (Tabela: Relatorios)..... 198
Tabela 42: Dicionário de dados (Tabela: CalendarEvent) 199
Tabela 43: Dicionário de dados (Tabela: ControlEffectivenessItem) 200
Tabela 44: Dicionário de dados (Tabela: ImpactItem) 201
Tabela 45: Dicionário de dados (Tabela: LikelihoodItem)..... 202
Tabela 46: Dicionário de dados (Tabela: Notificacoes) 203
Tabela 47: Dicionário de dados (Tabela: AlertasSeguranca) 204
Tabela 48: Dicionário de dados (Tabela: UserActivityLog)..... 205

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
API	Application Programming Interface (Interface de Programação de Aplicações)
CPF	Cadastro de Pessoas Físicas
CRM	Customer Relationship Management (Gestão de Relacionamento com o Cliente)
CSS	Cascading Style Sheets (Folhas de Estilo em Cascata)
DPO	Data Protection Officer (Encarregado de Proteção de Dados)
ERP	Enterprise Resource Planning (Planejamento de Recursos Empresariais)
GDPR	General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados – União Europeia)
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
HTML	HyperText Markup Language (Linguagem de Marcação de Hipertexto)
HTTP/HTTPS	HyperText Transfer Protocol (Secure)
LGPD	Lei Geral de Proteção de Dados
MoSCoW	Técnica de priorização: Must, Should, Could, Won't
RF	Requisito Funcional
RG	Registro Geral
RNF	Requisito Não Funcional
SaaS	Software as a Service (Software como Serviço)
SQL	Structured Query Language (Linguagem de Consulta Estruturada)
TCC	Trabalho de Conclusão de Curso
URL	Uniform Resource Locator (Endereço na Web)

SUMÁRIO

1 INTRODUÇÃO 19
2 LEGISLAÇÃO GLOBAL DE PROTEÇÃO DE DADOS 21
2.1 CONCEITO DE DADOS PESSOAIS E DADOS SENSÍVEIS 21
2.2 O CENÁRIO BRASILEIRO ANTES DA LGPD 22
2.2.1 A Criação e Implementação da LGPD 23
2.2.2 Princípios e Diretrizes da LGPD 23
2.2.3 Princípios do Tratamento de Dados (Art. 6º Da LGPD) 24
2.2.4 Bases Legais para o Tratamento de Dados 24
2.2.5 Direitos dos Titulares de Dados 25
2.3 IMPACTOS DA LGPD NO SETOR PÚBLICO E PRIVADO 26
2.3.1 Obrigações das Empresas e Organizações 28
2.3.2 O Papel do Encarregado de Proteção de Dados (DPO) 28
2.3.3 Penalidades e Sanções em Caso de Descumprimento 29
2.4 SEGURANÇA DA INFORMAÇÃO E MEDIDAS TÉCNICAS NA LGPD ... 30
2.4.1 Criptografia, Anonimização e Pseudonimização de Dados 30
2.4.2 Gestão de Riscos e Plano de Resposta a Incidentes 31
2.4.3 Boas Práticas e Conformidade com a LGPD 32
2.5 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS 32
2.6 AGENDA 2030 33
3 ESPECIFICAÇÃO DO SISTEMA 36
3.1 DESCRIÇÃO DO(S) PROBLEMA(S) 36
3.2 PROPOSTA DE SOLUÇÃO WEB 37
3.3 PROPOSTA DE SOLUÇÃO MOBILE 58
3.4 PARTICIPANTES DO PROJETO 66
3.5 USUÁRIOS PARTICIPANTES (ATORES) 66
3.6 NECESSIDADES DOS USUÁRIOS 67
3.7 REQUISITOS FUNCIONAIS 67
3.8 REQUISITOS NÃO FUNCIONAIS 68
3.9 ARQUITETURA ESTRUTURAL DO SISTEMA 69
3.10 LOGOTIPO 69

3.11 TECNOLOGIAS E FERRAMENTAS UTILIZADAS 70
3.11.1 Django 71
3.11.2 SQLite 71
3.11.3 CSS 72
3.11.4 GitHub 73
3.11.5 Visual Studio Code 73
3.11.6 Node.js 74
3.11.7 JavaScript 75
3.12 DEPENDÊNCIAS 75
3.13 REFERÊNCIAS (PARA O LEVANTAMENTO INICIAL) 75
3.14 APROVAÇÕES 76
4 ESTRATÉGIAS DE RISCO 78
4.1 LISTA DE RISCOS 78
4.2 PRIORIZAÇÃO DOS RISCOS 79
4.3 PLANOS DE MITIGAÇÃO 80
4.4 PLANOS DE CONTINGÊNCIA 81
5 GERENCIAMENTO DE CONFIGURAÇÃO 84
5.1 PLANO DE GERENCIAMENTO DE CONFIGURAÇÃO 84
5.2 REPOSITÓRIO 85
6 ESTRATÉGIA DE TESTES 86
6.1 TESTES DE UNIDADE AUTOMATIZADOS 86
6.2 TESTES DE VALIDAÇÃO 87
6.2.1 Teste Web 88
6.2.2 Teste Mobile 97
7 ESTRATÉGIA DE IMPLANTAÇÃO E SUPORTE 104
7.1 NECESSIDADES DE IMPLANTAÇÃO 104
7.1.1 Arquitetura de implantação 104
7.1.2 Configuração dos servidores 105
7.1.3 Configuração dos clientes 106
7.1.4 Infraestrutura necessária 106
7.2 CRONOGRAMA DE TREINAMENTOS 107
8 CONCLUSÃO 108
8.1 IMPLEMETAÇÕES FUTURAS 109
REFERÊNCIAS 110

APÊNDICE A: DIAGRAMA DE CASOS DE USO 112
APÊNDICE B: DESCRIÇÕES DE CASOS DE USO 113
APÊNDICE C: DIAGRAMA DE CLASSES DE DADOS.....144
APÊNDICE D: DIAGRAMA DE ATIVIDADES.....146
APÊNDICE E: DIAGRAMA DE SEQUÊNCIA 163
APÊNDICE F: DIAGRAMA DE ENTIDADE E RELACIONAMENTO .182
APÊNDICE G: DICIONÁRIO DE DADOS.....183
MANUAL DO USUÁRIO WEB.....215
MANUAL DO USUÁRIO MOBILE 238

1 INTRODUÇÃO

A sociedade atual é cada vez mais digital, na qual praticamente todas as atividades desde fazer compras até estudar ou acessar serviços públicos envolvem o uso de dados pessoais. Esses dados, que antes eram vistos apenas como informações comuns de cadastro, hoje têm grande valor estratégico para empresas e governos. Ao mesmo tempo, esse cenário traz preocupações importantes: a privacidade das pessoas, o risco de vazamentos, a exposição indevida de informações e a necessidade de garantir que esses dados sejam utilizados de forma correta e transparente.

Foi diante desse desafio que o Brasil criou a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), inspirada em legislações internacionais como o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR), da União Europeia. Essa lei europeia tem como objetivo proteger os dados pessoais dos cidadãos e garantir maior transparência e controle sobre o tratamento dessas informações. De forma semelhante, a LGPD brasileira busca proteger os direitos dos cidadãos, estabelecendo regras claras para a coleta, o armazenamento e o uso de dados pessoais. No entanto, muitas instituições ainda enfrentam dificuldades para se adequar, seja pela complexidade da legislação, seja pela falta de ferramentas que facilitem a aplicação das regras no dia a dia.

Este trabalho nasce justamente dessa necessidade: desenvolver um sistema de apoio à gestão da conformidade com a LGPD, capaz de auxiliar instituições — em especial no ambiente acadêmico, devido à grande quantidade de dados pessoais sensíveis de alunos, professores e colaboradores que essas instituições tratam diariamente — a organizar suas informações de forma segura, transparente e eficiente. O sistema proposto inclui funcionalidades como inventário de dados, matriz de riscos, checklist de conformidade, controle de documentos e geração de relatórios, tudo voltado para apoiar a tomada de decisão e fortalecer a cultura da proteção de dados.

O Sistema Camaleão foi desenvolvido nas versões web e mobile, de forma integrada e sincronizada. A versão web concentra as funcionalidades administrativas e de gestão, permitindo o cadastro, a edição e o acompanhamento de informações relacionadas à conformidade com a LGPD, por meio de módulos como Inventário de Dados, Matriz e Ranking de Riscos, Planos de Ação, Monitoramentos, Incidentes,

Checklist de Conformidade, Calendário, Dashboard e Documentos LGPD. Já a versão mobile tem como objetivo oferecer mobilidade e praticidade no acesso às informações, possibilitando que o usuário visualize indicadores, receba notificações de prazos e alertas de segurança, além de registrar incidentes e monitoramentos de forma rápida. Ambas as plataformas compartilham o mesmo banco de dados, garantindo sincronização em tempo real, controle de permissões e rastreamento das ações dos usuários, o que reforça a confiabilidade e a eficiência do sistema.

A importância desta pesquisa está em unir teoria e prática. De um lado, o estudo discute a evolução da proteção de dados, os fundamentos legais da LGPD e os impactos dessa legislação. De outro, apresenta uma solução tecnológica concreta, que responde às demandas atuais de governança e segurança da informação. Assim, o trabalho não apenas analisa o tema, mas também propõe caminhos para que organizações se adequem à lei e fortaleçam a confiança nas relações digitais.

Para tornar a leitura mais clara, este TCC foi dividido em capítulos. O Capítulo 2 apresenta o histórico da proteção de dados, as legislações internacionais que serviram de referência e o cenário brasileiro até a criação da LGPD, abordando seus princípios, direitos e impactos. O Capítulo 3 descreve a especificação do sistema desenvolvido, detalhando o problema, a proposta de solução, os requisitos e as tecnologias utilizadas, como Django, SQLite, Node.js, JavaScript, CSS, GitHub e Visual Studio Code. O Capítulo 4 aborda as estratégias de risco, enquanto o Capítulo 5 trata do gerenciamento de configuração e do uso do repositório para controle de versões. O Capítulo 6 apresenta a estratégia de testes aplicada ao sistema e o Capítulo 7 descreve a estratégia de implantação e suporte. Por fim, o Capítulo 8 traz as conclusões, destacando as contribuições alcançadas e as possibilidades de aprimoramento futuro.

2 LEGISLAÇÃO GLOBAL DE PROTEÇÃO DE DADOS

O GDPR representa um divisor de águas no cenário internacional. Sua aprovação em 2016 e entrada em vigor em 2018 estabeleceram um conjunto de regras abrangentes e rigorosas, que passaram a valer não apenas para organizações situadas na União Europeia, mas também para qualquer entidade estrangeira que ofereça bens ou serviços a cidadãos europeus (UNIÃO EUROPEIA, 2016, p. 101). Essa característica de extraterritorialidade conferiu ao GDPR uma dimensão global, fazendo com que empresas do mundo inteiro precisassem adaptar suas práticas para manter relações comerciais com países europeus.

Inspirada por esse modelo, a LGPD foi aprovada no Brasil em 2018 e entrou em vigor em 2020. Embora possua particularidades adaptadas ao contexto nacional, sua estrutura guarda forte semelhança com o regulamento europeu, refletindo o movimento global de harmonização normativa e buscando inserir o Brasil em padrões internacionais de privacidade (CAVALCANTI, 2020, p. 93). Dessa forma, a LGPD fortaleceu a segurança jurídica, aumentou a confiança em transações digitais e posicionou o país de forma mais competitiva no cenário econômico global.

2.1 CONCEITO DE DADOS PESSOAIS E DADOS SENSÍVEIS

A LGPD trouxe clareza e precisão conceitual ao diferenciar dados pessoais de dados sensíveis. Dados pessoais são todas as informações que permitem identificar, direta ou indiretamente, uma pessoa natural. Exemplos incluem nome, CPF, RG, endereço residencial, número de telefone e e-mail. São informações amplamente utilizadas em cadastros, contratos e serviços de comunicação e, por essa razão, devem ser tratadas conforme os princípios de necessidade e transparência, evitando coleta ou uso excessivo (BRASIL, 2018, p. 37).

Já os dados sensíveis abrangem informações que, caso expostas, podem gerar riscos de discriminação, constrangimento ou violação de direitos fundamentais. Entre eles estão: origem racial ou étnica, convicções religiosas, opiniões políticas, dados de saúde, vida sexual, filiação sindical e dados biométricos. O tratamento desses dados exige proteção especial e só é permitido em situações restritas, como mediante consentimento explícito do titular ou quando necessário para o cumprimento de

obrigações legais, políticas públicas ou preservação da vida e integridade física (BRASIL, 2018, p. 38).

Essa distinção é essencial para garantir que as organizações tratem os dados com proporcionalidade e responsabilidade. Enquanto dados pessoais comuns já exigem cuidados, as sensíveis demandam salvaguardas adicionais, de modo a assegurar que não sejam utilizados de forma abusiva ou discriminatória (VIOLA; LEAL, 2020, p. 64).

2.2 O CENÁRIO BRASILEIRO ANTES DA LGPD

Antes da criação da LGPD em 2018, a realidade brasileira era marcada por uma legislação fragmentada, sem foco exclusivo na privacidade e no uso de informações pessoais. A Constituição Federal de 1988 assegurava o direito à intimidade e à vida privada, mas de forma genérica, sem detalhar critérios para a coleta, armazenamento ou compartilhamento de dados. O Código de Defesa do Consumidor, por sua vez, abordava a proteção de dados apenas em situações relacionadas às relações de consumo, não abrangendo a totalidade das práticas que envolvem o tratamento de informações pessoais (SOUZA, 2019, p. 54).

Outro marco importante foi o Marco Civil da Internet (Lei nº 12.965/2014), considerado a “Constituição da Internet” no Brasil. Essa legislação trouxe princípios como a neutralidade da rede, a privacidade e a proteção dos registros digitais, mas ainda não estabelecia diretrizes completas sobre o uso de dados fora do ambiente *online*. Assim, cidadãos permaneciam expostos a práticas abusivas de coleta e uso de informações, muitas vezes sem consentimento ou transparência. Empresas também se viam diante de um cenário de insegurança jurídica, com regras dispersas e pouco objetivas sobre o correto tratamento de dados pessoais (MENEZES, 2020, p. 77).

Com a crescente digitalização e a influência internacional, especialmente do GDPR da União Europeia, tornou-se evidente que o Brasil necessitava de uma legislação moderna, abrangente e alinhada às melhores práticas globais. Foi nesse contexto que surgiu a LGPD, estabelecendo regras claras para garantir a proteção da privacidade dos cidadãos e a segurança no uso de suas informações (BRASIL, 2018, p. 19).

2.2.1 A Criação e Implementação da LGPD

A aprovação da LGPD, em 14 de agosto de 2018, representou um divisor de águas na regulamentação da privacidade no Brasil. Inspirada no GDPR europeu, que havia entrado em vigor em 2018, a LGPD buscou não apenas modernizar o ordenamento jurídico nacional, mas também alinhar o país a padrões internacionais de proteção de dados (MENEZES, 2020, p. 83; ALMEIDA, 2019, p. 64).

O artigo 3º da LGPD estabelece que a lei se aplica a qualquer operação de tratamento de dados realizada no território nacional ou destinada a indivíduos localizados no Brasil, independentemente da sede da organização. Essa abrangência garante que tanto empresas nacionais quanto estrangeiras respeitem as normas brasileiras ao ofertar bens ou serviços no país (BRASIL, 2018, p. 22; VIEIRA, 2019, p. 117).

Para garantir sua efetiva aplicação, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por regulamentar, fiscalizar e aplicar sanções. A partir de 2020, empresas e órgãos públicos precisaram revisar suas práticas, adotar políticas de privacidade mais rigorosas, nomear o Encarregado de Proteção de Dados (DPO) e implementar medidas técnicas de segurança, como criptografia. (GONÇALVES, 2020, p. 42).

A implementação da LGPD, entretanto, não foi apenas normativa. Ela provocou uma verdadeira mudança cultural nas organizações, promovendo a conscientização sobre a importância da privacidade e da ética no tratamento de dados. Ainda assim, sua aplicação tem sido gradual e desafiadora, diante da necessidade de adequação de diferentes setores da economia e da capacidade da ANPD de garantir fiscalização efetiva (SILVA, 2020, p. 102; PEREIRA, 2020, p. 91).

2.2.2 Princípios e Diretrizes da LGPD

A LGPD orienta o tratamento de dados pessoais a partir de princípios fundamentais, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (BRASIL, 2018, p. 30). Esses princípios funcionam como diretrizes que obrigam as organizações a agirem com ética e responsabilidade, limitando a coleta de

informações ao estritamente necessário e garantindo clareza nas finalidades informadas ao titular.

Além disso, a lei estabelece bases legais que legitimam o tratamento de dados. Entre elas, destacam-se: o consentimento do titular; a execução de contratos; o cumprimento de obrigações legais; a proteção da vida ou da integridade física; o legítimo interesse do controlador, desde que não sobreponha os direitos do titular; e a proteção do crédito. Essa estrutura garante equilíbrio entre as necessidades organizacionais e a preservação dos direitos fundamentais (VIOLA; LEAL, 2020, p. 61).

2.2.3 Princípios do Tratamento de Dados (Art. 6º Da LGPD)

Um dos maiores avanços da LGPD foi assegurar aos cidadãos um conjunto de direitos sobre seus dados pessoais. Entre eles, estão: a obtenção de informações sobre os dados que estão sendo tratados, correção de dados incompletos ou desatualizados, exclusão de informações desnecessárias, portabilidade para outros fornecedores de serviços, revogação do consentimento e oposição ao tratamento irregular (BRASIL, 2018, p. 34).

Esses direitos fortalecem a autonomia dos titulares, permitindo maior controle sobre suas informações e garantindo que o uso dos dados seja transparente e responsável. Além disso, contribuem para o fortalecimento da confiança entre sociedade, empresas e governo, em um ambiente digital cada vez mais exigente quanto à proteção da privacidade (VIOLA; LEAL, 2020, p. 66).

2.2.4 Bases Legais para o Tratamento de Dados

A LGPD surgiu como uma resposta à necessidade de garantir mais segurança e transparência no uso das informações pessoais. No mundo digital de hoje, onde os dados são coletados a todo momento, proteger a privacidade dos indivíduos se tornou essencial. A LGPD estabelece bases legais para que esse tratamento ocorra de forma responsável, equilibrando o direito à privacidade com as necessidades das empresas e organizações que utilizam essas informações no dia a dia (BRASIL, 2018).

Uma das principais formas de tratamento permitido pela lei é a autorização do titular. Isso significa que qualquer pessoa tem o direito de decidir se autoriza ou não o

uso de seus dados, desde que essa escolha seja feita de forma livre e informada. Essa liberação pode ser retirada a qualquer momento, garantindo mais controle sobre as informações pessoais. Além disso, quando há um contrato em vigor, o uso dos dados se justifica para garantir a prestação de serviços ou o cumprimento de obrigações assumidas entre as partes (VIOLA; LEAL, 2020).

Outra situação em que o tratamento de dados é permitido ocorre quando há uma exigência legal ou regulatória, como no caso de registros fiscais e trabalhistas. Em emergências, como atendimentos médicos ou ações humanitárias, a lei também autoriza o uso dessas informações para preservar vidas. O interesse legítimo do controlador pode ser outra justificativa, desde que respeite os direitos do titular e não cause prejuízos (BRASIL, 2018).

A proteção do crédito é um exemplo prático da aplicação da LGPD, pois permite a análise financeira para concessão de empréstimos e financiamentos. O uso de dados também é essencial em disputas judiciais, garantindo que os envolvidos tenham disponibilidade dos dados essenciais para defender seus direitos. Além disso, o setor público pode utilizar esses registros para executar políticas sociais e administrativas, desde que isso ocorra de forma responsável e transparente. A lei ainda permite o uso de dados para pesquisas científicas, históricas ou estatísticas, desde que medidas de segurança sejam aplicadas para preservar a identidade dos indivíduos (VIOLA; LEAL, 2020).

2.2.5 Direitos dos Titulares de Dados

A LGPD foi criada para garantir maior segurança e transparência no uso das informações pessoais, oferecendo aos cidadãos um controle efetivo sobre seus dados. Por meio da LGPD, os titulares têm direitos que lhes permitem acessar, corrigir, excluir ou impedir o tratamento de suas informações quando julguem necessário, reforçando a proteção da privacidade e o uso responsável dos dados (BRASIL, 2018).

Entre os principais direitos previstos está o direito de consulta aos dados pessoais, que possibilita ao indivíduo solicitar a qualquer empresa ou órgão público detalhes sobre quais dados estão sendo coletados, de que forma são usados e com quem são compartilhados. Caso haja alguma informação incorreta, o titular pode solicitar a retificação para corrigir ou atualizar esses dados. Além disso, a exclusão

permite que os titulares requisitem a eliminação das informações quando não forem mais necessárias para a finalidade inicial da coleta (VIOLA; LEAL, 2020).

Outro direito fundamental é a revogação da permissão a qualquer momento. Caso o titular tenha permitido o uso de seus dados para uma finalidade específica e depois decida retirar essa permissão, a empresa deve interromper o tratamento dessas informações, salvo em casos excepcionais previstos na lei. Também está assegurado o direito à portabilidade, que permite a transferência segura dos dados para outro fornecedor, facilitando o controle do titular sobre suas informações (BRASIL, 2018).

A LGPD ainda prevê o direito à oposição, que possibilita ao titular contestar o tratamento dos dados caso este ocorra de forma inadequada ou sem base legal. A lei contempla ainda mecanismos como a ocultação dos dados, bloqueio ou eliminação dos dados quando houver uso indevido ou excessivo. Para garantir ainda mais transparência, os titulares devem ser informados sobre a possibilidade de não fornecer autorização e as consequências dessa escolha (VIOLA; LEAL, 2020).

O respeito a esses direitos é fundamental para que a LGPD cumpra seu propósito de proteger a privacidade dos cidadãos e fomentar um ambiente digital mais ético e seguro. Empresas e instituições precisam implementar medidas que assegurem a eficiência no atendimento às solicitações dos titulares, fortalecendo a confiança e a transparência na relação entre organizações e indivíduos.

2.3 IMPACTOS DA LGPD NO SETOR PÚBLICO E PRIVADO

A LGPD trouxe mudanças significativas tanto para o setor público quanto para o privado, estabelecendo regras claras sobre o tratamento de dados pessoais. Com a crescente digitalização e o uso intensivo de dados, a implementação da LGPD tornou-se essencial para garantir a privacidade e a segurança dos cidadãos. Empresas e órgãos governamentais precisaram se adaptar para atender às novas exigências, promovendo maior transparência e responsabilidade na gestão de dados (BRASIL, 2018).

No setor privado, a LGPD impactou diretamente empresas de todos os portes, exigindo que revisassem suas políticas de coleta, armazenamento e compartilhamento de dados pessoais. Organizações que utilizam dados para suas operações, como ecommerces, bancos e prestadoras de serviços, passaram a adotar

medidas para garantir a conformidade com a lei. O consentimento dos titulares tornou-se um requisito fundamental, e práticas como a mascaramento dos dados e a implementação de políticas de segurança se tornaram indispensáveis. Além disso, a necessidade de nomeação de um Encarregado de Proteção de Dados, conhecido internacionalmente como Data Protection Officer (DPO), trouxe um novo desafio, exigindo profissionais qualificados para garantir a adequação das empresas às exigências da LGPD (VIOLA; LEAL, 2020).

Já no setor público, a lei trouxe desafios adicionais, pois órgãos governamentais lidam com grandes volumes de informações sensíveis. A LGPD determinou que os dados dos cidadãos devem ser tratados com o mesmo nível de proteção exigido das empresas privadas, obrigando a administração pública a aprimorar suas práticas de segurança da informação. Além disso, a transparência na coleta e no uso de dados tornou-se uma exigência, garantindo que os cidadãos saibam como suas informações estão sendo utilizadas pelos governos municipais, estaduais e federal (BRASIL, 2018).

Um dos impactos mais relevantes da LGPD é a mudança na cultura organizacional. Tanto no setor público quanto no privado, houve a necessidade de educar colaboradores sobre boas práticas no uso de dados, minimizando riscos de vazamentos e acessos indevidos. Empresas privadas que descumprem a LGPD estão sujeitas a sanções aplicadas pela ANPD, incluindo advertências, multas, publicização da infração e restrições operacionais. No caso dos órgãos e entidades da administração pública, embora não estejam sujeitos a multas, eles podem sofrer outras sanções previstas na lei, como advertência, publicização da infração, bloqueio ou eliminação de dados pessoais, além de responsabilização administrativa pelos órgãos de controle. Para as empresas privadas, a exposição negativa decorrente de incidentes de segurança pode ainda afetar a reputação e a confiança dos clientes, resultando em prejuízos financeiros e institucionais (VIOLA; LEAL, 2020).

A adequação à LGPD não deve ser vista apenas como uma obrigação legal, mas como um passo fundamental para fortalecer a confiança entre cidadãos, empresas e governo. A segurança no tratamento de informações é um elemento essencial para um ambiente digital mais ético e confiável, garantindo que a privacidade seja respeitada em todas as esferas da sociedade.

2.3.1 Obrigações das Empresas e Organizações

O DPO é figura central na governança da LGPD. Previsto no artigo 41 da lei, ele atua como elo entre a organização, os titulares dos dados e a ANPD, sendo responsável por orientar colaboradores, receber demandas, supervisionar processos internos e garantir conformidade legal (BRASIL, 2018, p. 46).

Além disso, o DPO colabora na elaboração de relatórios de impacto, promove ações de conscientização e atua como consultor estratégico dentro da organização. Sua presença contribui para o fortalecimento da transparência e da confiança entre as partes, consolidando a privacidade como um valor organizacional (DONEDA, 2021, p. 115).

2.3.2 O Papel do Encarregado de Proteção de Dados (DPO)

Com a entrada em vigor da LGPD (Lei nº 13.709/2018), tornou-se obrigatória a presença do DPO. Essa figura foi instituída para atuar como elo entre os titulares de dados, as organizações que realizam o tratamento e a ANPD, sendo considerada essencial para assegurar a conformidade e a transparência no uso das informações pessoais (BRASIL, 2018, p. 46).

O DPO possui atribuições amplas e estratégicas. É responsabilidade desse profissional orientar a instituição sobre as melhores práticas de governança, monitorar os procedimentos internos, supervisionar o cumprimento da LGPD e garantir que os direitos dos titulares sejam efetivamente respeitados. Além disso, cabe ao encarregado receber reclamações, pedidos de informações e solicitações de exercício de direitos, funcionando como ponto de contato direto com a ANPD (SENAC, 2021, p. 58).

Mais do que um cargo administrativo, o encarregado exerce um papel educativo e preventivo. Entre suas atribuições, destacam-se a promoção de treinamentos, o estímulo à cultura organizacional de proteção de dados e o apoio na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), quando necessário. Dessa maneira, o DPO contribui para que a privacidade seja incorporada ao cotidiano das organizações não apenas como obrigação legal, mas como valor ético e diferencial competitivo (DONEDA, 2021, p. 115).

É relevante mencionar que, embora a LGPD estabeleça a obrigatoriedade dessa função, a própria ANPD admite flexibilizações para determinados segmentos, como micro e pequenas empresas, que podem adotar modelos simplificados de adequação. Ainda assim, a presença do encarregado permanece central para o fortalecimento da governança de dados no Brasil, promovendo transparência, responsabilidade e confiança nas relações entre empresas, governo e sociedade (ANPD, 2022, p. 40).

Por fim, é importante esclarecer um ponto frequentemente mal interpretado: a LGPD não prevê aplicação de multas a órgãos públicos, uma vez que as penalidades financeiras — multa simples e multa diária — previstas nos incisos II e III do art. 52 da LGPD são restritas às pessoas jurídicas de direito privado. Para entidades públicas, aplicam-se outras formas de sanção, como advertência, publicização da infração e adoção de medidas corretivas, preservando-se o interesse público e a continuidade do serviço.

2.3.3 Penalidades e Sanções em Caso de Descumprimento

O descumprimento da LGPD pode acarretar uma série de penalidades às organizações que realizam o tratamento de dados de forma irregular, colocando em risco os direitos dos titulares. A ANPD é o órgão responsável por fiscalizar e aplicar sanções administrativas, conforme previsto no Capítulo VIII da lei (BRASIL, 2018).

As sanções podem variar de acordo com a gravidade da infração e com a reincidência da conduta, sendo aplicadas após processo administrativo que assegure o direito à ampla defesa e ao contraditório. Entre as penalidades previstas pela LGPD, destacam-se:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples de até 2% do faturamento da empresa, limitada a R$ 50 milhões por infração;
- Multa diária, enquanto persistir a infração;
- Publicização da infração, após devidamente apurada e confirmada;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais objeto da infração.

Além dessas, a ANPD também pode recomendar medidas técnicas e administrativas a serem adotadas pelas organizações para evitar futuras infrações.

A aplicação das sanções considera critérios como a natureza e a gravidade da infração, a boa-fé do infrator, a repetição da conduta e o grau do dano causado (ANPD, 2022).

Cabe ressaltar que as sanções administrativas não excluem a possibilidade de responsabilização civil, penal ou mesmo em outras esferas regulatórias. Ou seja, uma organização que infringe a LGPD pode ser acionada judicialmente pelos titulares afetados e sofrer outras consequências legais, como a obrigação de indenizar danos morais e materiais.

Dessa forma, as penalidades previstas pela LGPD reforçam a importância de uma cultura organizacional voltada à proteção de dados, promovendo responsabilidade, conformidade e respeito aos direitos dos cidadãos no ambiente digital.

2.4 SEGURANÇA DA INFORMAÇÃO E MEDIDAS TÉCNICAS NA LGPD

A segurança da informação é um dos eixos centrais da LGPD, pois garante a integridade, a confidencialidade e a disponibilidade dos dados tratados por organizações públicas e privadas. A lei determina que os agentes de tratamento adotem medidas técnicas e administrativas adequadas ao contexto, levando em conta a natureza dos dados, os riscos envolvidos e o porte da instituição (BRASIL, 2018, p. 55). Essa abordagem flexível permite que tanto grandes corporações quanto pequenas empresas implementem estratégias proporcionais às suas realidades, mas igualmente comprometidas com a proteção da privacidade.

Entre as medidas técnicas destacam-se mecanismos como criptografia, autenticação multifatorial, pseudonimização de dados, que reduzem o impacto de incidentes de segurança. Já no campo administrativo, a LGPD incentiva a criação de políticas internas de governança, treinamentos periódicos para colaboradores e auditorias regulares, fortalecendo a cultura organizacional de proteção de dados (SENAC, 2021, p. 29; DONEDA, 2021, p. 123).

A adoção de tais medidas não apenas cumpre exigências legais, mas também fortalece a reputação das organizações, que passam a ser vistas como confiáveis e responsáveis na gestão das informações de clientes, usuários e cidadãos.

2.4.1 Criptografia, Anonimização e Pseudonimização de Dados

A LGPD incentiva o uso de recursos tecnológicos que elevam o nível de proteção de dados. A criptografia é amplamente utilizada para tornar ilegíveis os dados em trânsito ou armazenados, impedindo o acesso por agentes não autorizados. Já a anonimização elimina ou altera identificadores de forma irreversível, permitindo o uso das informações para pesquisas e estatísticas sem comprometer a identidade dos titulares. A pseudonimização, por sua vez, substitui dados identificadores por códigos ou chaves que dificultam a associação direta com a pessoa, mas permitem a reidentificação em situações autorizadas (BRASIL, 2018, p. 59; DONEDA, 2021, p. 129).

Essas técnicas não apenas reforçam a conformidade com a LGPD, mas também reduzem os riscos de discriminação, fraude e exposição indevida. Sua utilização demonstra maturidade na gestão de dados e compromisso ético das organizações com a proteção da privacidade.

2.4.2 Gestão de Riscos e Plano de Resposta a Incidentes

A gestão de riscos e a elaboração de planos de resposta a incidentes são componentes essenciais da segurança da informação e da conformidade com a LGPD. Esses mecanismos visam identificar, avaliar e mitigar vulnerabilidades relacionadas ao tratamento de dados pessoais, além de preparar a organização para agir de maneira eficaz diante de falhas ou ameaças que comprometam a privacidade e a integridade das informações (BRASIL, 2018).

A gestão de riscos envolve um processo contínuo de mapeamento das atividades de tratamento de dados, análise de possíveis impactos e probabilidades de ocorrência de incidentes, e a definição de controles preventivos. Essa prática permite que a organização compreenda seus pontos críticos, adote medidas de proteção adequadas e mantenha uma postura proativa frente às obrigações legais. A LGPD estabelece que os agentes de tratamento devem adotar boas práticas de governança e segurança que considerem os riscos envolvidos nas operações realizadas (ANPD, 2022).

Por sua vez, o plano de resposta a incidentes consiste em um conjunto de procedimentos estruturados para lidar com eventos que possam afetar a segurança dos dados, como vazamentos, acessos não autorizados, falhas sistêmicas, ou ataques cibernéticos. O plano deve incluir etapas como a detecção do incidente, a

contenção dos danos, a investigação das causas, a comunicação aos titulares e à ANPD, bem como ações corretivas para evitar recorrências (CERT.br, 2021).

A existência de um plano de resposta eficaz demonstra a maturidade da organização em relação à proteção de dados e reduz significativamente os impactos legais, financeiros e reputacionais de um eventual incidente. Além disso, a transparência na comunicação com os titulares afetados e com a ANPD é um dos requisitos legais previstos pela LGPD, especialmente nos casos em que houver risco ou dano relevante aos direitos dos titulares (BRASIL, 2018).

Portanto, a gestão de riscos e os planos de resposta a incidentes são práticas indispensáveis para uma política robusta de segurança da informação, contribuindo para a prevenção de falhas, a manutenção da conformidade e a proteção efetiva dos dados pessoais sob responsabilidade da organização.

2.4.3 Boas Práticas e Conformidade com a LGPD

A conformidade com a LGPD exige mais do que o cumprimento mínimo da legislação. Envolve a adoção de boas práticas organizacionais, como mapeamento dos fluxos de dados, definição de políticas claras de privacidade, controle de acessos, treinamentos periódicos e realização de RIPD, quando necessário (SENAC, 2021, p. 63; ANPD, 2022, p. 49).

Tais práticas podem ser reforçadas por frameworks internacionais de segurança, como a ISO/IEC 27001, que padroniza processos e amplia a governança de riscos. Ao adotar essas medidas, as organizações demonstram responsabilidade social e comprometimento ético, fortalecendo sua imagem e a confiança de clientes, parceiros e cidadãos.

2.5 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A ANPD é o órgão responsável por zelar pela proteção de dados pessoais e garantir o cumprimento da LGPD no Brasil. Sua criação foi prevista no artigo 55-A da LGPD, por meio da Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, que lhe conferiu autonomia técnica para atuar como entidade central na regulamentação, fiscalização e orientação sobre o tema (BRASIL, 2019).

A ANPD exerce funções regulatórias, normativas, fiscalizatórias e sancionatórias. Entre suas principais atribuições estão: editar normas e diretrizes para a aplicação da LGPD; fiscalizar e aplicar sanções em casos de descumprimento; promover ações de conscientização e educação sobre proteção de dados; elaborar relatórios sobre o panorama da privacidade no país; e analisar incidentes de segurança envolvendo dados pessoais, podendo instaurar investigações e exigir medidas corretivas (ANPD, 2022).

A autoridade também atua como canal institucional para o exercício dos direitos dos titulares de dados — como acesso, correção, exclusão, portabilidade e oposição ao tratamento de informações pessoais — e orienta os agentes de tratamento por meio de guias, boas práticas e diretrizes técnicas aplicáveis a diferentes setores da economia e da administração pública.

Sua estrutura organizacional é composta pelo Conselho Diretor, órgão máximo decisório, e por setores técnicos e administrativos que atuam de forma integrada. Conta ainda com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, de caráter consultivo, responsável por contribuir para o desenvolvimento da política nacional de proteção de dados (BRASIL, 2019).

Dessa forma, a ANPD desempenha papel fundamental na consolidação de uma cultura de respeito à privacidade no Brasil, servindo como elo entre os direitos dos titulares, as obrigações das organizações e a promoção da confiança digital no país.

2.6 AGENDA 2030

A Agenda 2030 é um compromisso global firmado pelos Estados-membros da Organização das Nações Unidas (ONU), que estabelece 17 Objetivos de Desenvolvimento Sustentável (ODS), com metas a serem alcançadas até o ano de 2030. Esses objetivos visam promover o desenvolvimento social, econômico e ambiental de forma integrada e sustentável, com foco na erradicação da pobreza, na redução das desigualdades e na promoção da paz, justiça e instituições eficazes.

O sistema desenvolvido para a gestão da conformidade com a LGPD se alinha diretamente com alguns desses objetivos, especialmente com o ODS 16 – Paz, Justiça e Instituições Eficazes, que inclui, entre suas metas, o fortalecimento das instituições para garantir o acesso à informação, a proteção de dados pessoais e o respeito aos direitos fundamentais.

Ao contribuir para a organização e controle do tratamento de dados pessoais em conformidade com a LGPD, o sistema promove a transparência, a responsabilização e o acesso à informação de forma segura, todos princípios alinhados à meta 16.10 da Agenda 2030: "Assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais."

Além disso, o projeto também se relaciona com o ODS 9 – Indústria, Inovação e Infraestrutura, ao utilizar tecnologias modernas para propor uma solução digital segura e eficiente, fomentando a inovação e a transformação digital no setor da governança de dados.

Por meio do desenvolvimento de um sistema que respeita os direitos dos titulares de dados, promove a cultura de proteção de dados e apoia a atuação do DPO, o projeto contribui para uma sociedade mais justa, ética e tecnicamente preparada para os desafios do mundo digital, em total consonância com os princípios da Agenda 2030.

A Figura 1 destaca o ODS 9 – Indústria, Inovação e Infraestrutura, evidenciando a importância do uso de tecnologias modernas e soluções digitais eficientes para promover o desenvolvimento sustentável. No contexto do sistema de gestão da LGPD, o ODS 9 está diretamente relacionado à inovação e à transformação digital, mostrando como a implementação de ferramentas tecnológicas seguras e eficientes contribui para a melhoria da infraestrutura de governança de dados e para a promoção de práticas digitais responsáveis.

Figura 1 - Indústria, Inovação e Infraestrutura

Fonte: Rede ODS Brasil

A Figura 2 destaca o ODS 16 – Paz, Justiça e Instituições Eficazes, enfatizando a importância do fortalecimento das instituições e da promoção de processos transparentes e responsáveis. No contexto do sistema de gestão da LGPD, o ODS 16 está relacionado à proteção de dados pessoais, à garantia do acesso à informação e ao respeito aos direitos fundamentais, demonstrando como a implementação de soluções digitais seguras contribui para instituições mais eficientes, éticas e alinhadas às exigências legais.

Figura 2 - Paz Justiça e Instituições Eficazes

Fonte: CT Agenda

3 ESPECIFICAÇÃO DO SISTEMA

Este trabalho tem como objetivo o desenvolvimento de uma aplicação web especializada no suporte às atividades do DPO, figura central na estrutura de governança estabelecida pela legislação brasileira de proteção de dados. Diante da crescente complexidade das exigências normativas e da responsabilidade atribuída a esse profissional na supervisão do tratamento de informações pessoais, torna-se essencial a adoção de ferramentas tecnológicas que garantam maior eficiência, segurança e organização na gestão documental e processual.

A proposta consiste na criação de um sistema que possibilite o armazenamento, a categorização, o acompanhamento e a atualização de documentos relevantes — como termos de consentimento, relatórios de impacto, políticas internas, registros de operações e comunicações com a autoridade reguladora. Ao centralizar essas informações de maneira estruturada, a aplicação facilitará o atendimento aos princípios de transparência, accountability e segurança, otimizando a atuação do DPO no monitoramento da conformidade organizacional exigida pelo marco legal vigente.

Além disso, busca-se reduzir riscos jurídicos e operacionais decorrentes da má gestão de dados, bem como fortalecer uma cultura institucional mais consciente e madura quanto à proteção de informações pessoais.

3.1 DESCRIÇÃO DO(S) PROBLEMA(S)

No contexto da adequação à LGPD, muitas organizações ainda encontram sérios desafios na gestão documental, sobretudo pela falta de padronização e centralização dos processos. Em grande parte das empresas, informações fundamentais para demonstrar conformidade são mantidas em planilhas isoladas, documentos físicos ou ferramentas genéricas que não contemplam as exigências específicas da legislação. Esse cenário resulta em processos morosos, suscetíveis a falhas e de difícil rastreabilidade, o que compromete não apenas a eficiência operacional, mas também a transparência e a confiabilidade dos dados tratados.

A ausência de mecanismos integrados impacta diretamente atividades cruciais, como a elaboração de relatórios de impacto, o controle de solicitações de titulares de dados, o registro de incidentes de segurança e a comprovação das medidas adotadas para proteção das informações. Essas lacunas fragilizam a atuação do DPO,

responsável por supervisionar a aplicação da LGPD dentro da organização, além de expor a empresa a riscos de sanções da ANPD, perdas financeiras e danos à reputação.

Nesse cenário, torna-se evidente a necessidade de investir em soluções tecnológicas que automatizem, organizem e consolidem os processos documentais relacionados à LGPD. O desenvolvimento de uma aplicação web específica para essa finalidade representa um avanço estratégico, pois oferece maior agilidade, confiabilidade e segurança no tratamento das informações, além de possibilitar a criação de registros auditáveis e alinhados às boas práticas de governança de dados. Mais do que cumprir uma obrigação legal, essa abordagem fortalece a cultura de conformidade e evidencia a valorização dos dados pessoais como ativos críticos no ambiente digital contemporâneo.

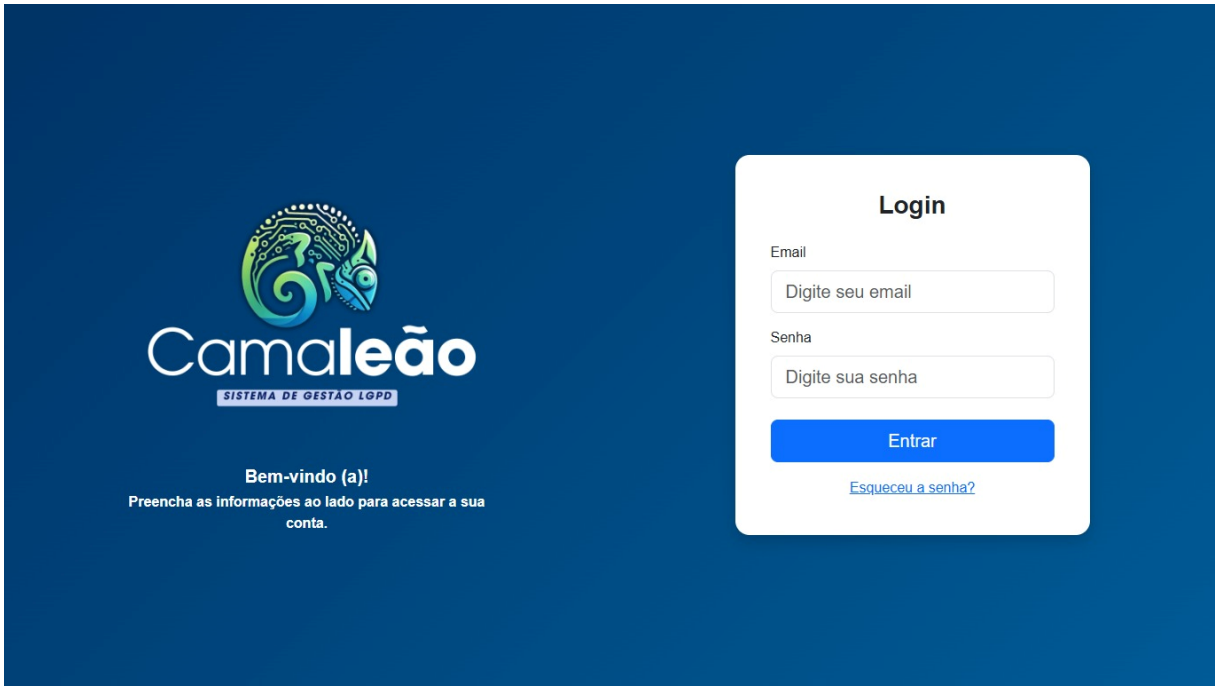
3.2 PROPOSTA DE SOLUÇÃO WEB

A solução proposta consiste em uma aplicação web que oferece uma integração centralizada dos documentos relacionados à proteção de dados pessoais, permitindo o acesso, a edição e a exclusão de informações de forma ágil, segura e controlada. A plataforma, denominada de Camaleão, foi idealizada para otimizar os processos de gestão documental, garantindo padronização, rastreabilidade e integridade das informações.

Por meio de uma interface intuitiva e recursos funcionais, o sistema Camaleão proporciona ao DPO um controle eficiente, preciso e transparente sobre todas as atividades vinculadas à coleta, ao tratamento e ao uso de dados pessoais no ambiente organizacional. A ferramenta visa assegurar a conformidade com os princípios e exigências da LGPD, ao mesmo tempo em que promove maior governança, responsabilidade e segurança no manejo das informações sensíveis. Abaixo, estão listadas as telas fundamentais que estruturam o sistema:

A Figura 3 apresenta a tela de login de gestão da LGPD, que representa a porta de entrada para os usuários. Essa interface foi desenvolvida com foco na simplicidade e na segurança, permitindo que apenas usuários autenticados tenham acesso às funcionalidades internas. Além disso, a tela de login reforça os princípios de proteção de dados ao exigir credenciais individuais, garantindo a rastreabilidade das ações realizadas dentro do sistema e assegurando a conformidade com a legislação vigente.

Figura 3: Tela de Login

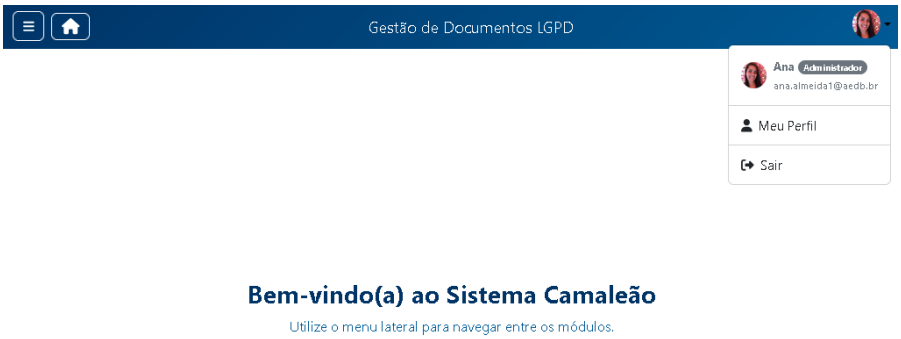


Fonte: Elaboração Própria

A Figura 4 apresenta a tela principal do sistema Camaleão, que funciona como um painel centralizado de acesso às principais funcionalidades do sistema. Nela, o usuário encontra módulos essenciais para a conformidade com a LGPD, como informações de DPO e forma de contato, Monitoramento, Checklist, Documentos, Dashboard, Inventário de Dados, Matriz de Risco, Relatórios e Notificações.

A interface foi desenvolvida com foco na usabilidade e segurança, oferecendo uma navegação simples e organizada. Dessa forma, a tela principal reflete a proposta do sistema de disponibilizar uma ferramenta intuitiva e confiável, que apoia a gestão e o controle das informações conforme os princípios da LGPD.

Figura 4: Tela de Home



Fonte: Elaboração Própria

A Figura 5 apresenta a tela de informações e contato do DPO, função prevista pela LGPD como elo entre o controlador, os titulares de dados e a ANPD. Nessa interface, são exibidos de forma clara os dados do profissional designado, como nome, e-mail institucional, telefone, data de nomeação, validade da designação e cargo na organização.

A centralização dessas informações reforça a transparência e a conformidade legal, garantindo um canal de comunicação acessível entre os usuários e o DPO. Dessa forma, a funcionalidade contribui para o cumprimento das obrigações previstas na LGPD e fortalece a confiança dos titulares no processo de governança e proteção de dados adotado pela instituição.

Figura 5: Tela de DPO

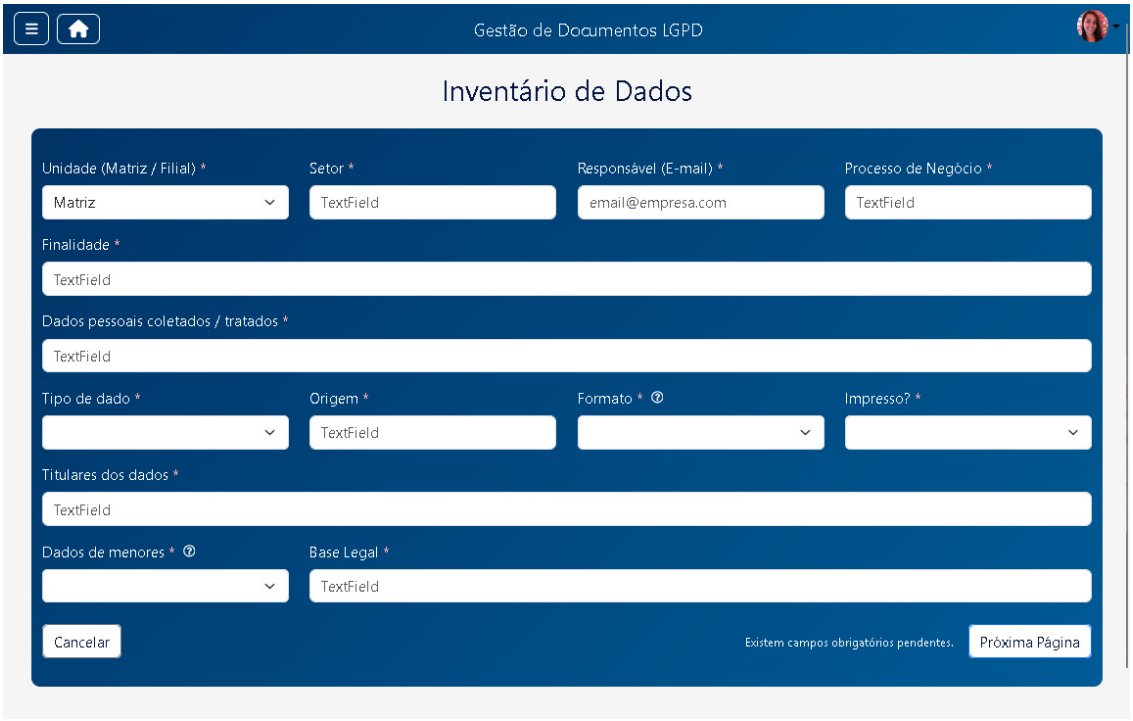
Fonte: Elaboração Própria

A Figura 6 apresenta a tela do Formulário de Atividades, que tem papel central na gestão da conformidade com a LGPD. Nessa interface, são registradas e acompanhadas as atividades de gerenciamento relacionadas à privacidade e proteção de dados pessoais, garantindo maior controle e organização das ações adotadas pela instituição.

O formulário reúne campos essenciais, como atividade de gerenciamento, base legal correspondente (com referência aos artigos da Lei nº 13.709/2018), evidência documental, data de revisão, classificação, status e ações. Essa estrutura possibilita o monitoramento e a rastreabilidade das medidas implementadas, assegurando que todas as obrigações legais estejam devidamente documentadas.

Dessa forma, a funcionalidade contribui para uma gestão eficiente e transparente, fortalecendo a governança de dados pessoais e oferecendo suporte prático ao DPO e demais responsáveis pelo acompanhamento da adequação da organização à LGPD.

Figura 6: Tela de Formulário de Atividades

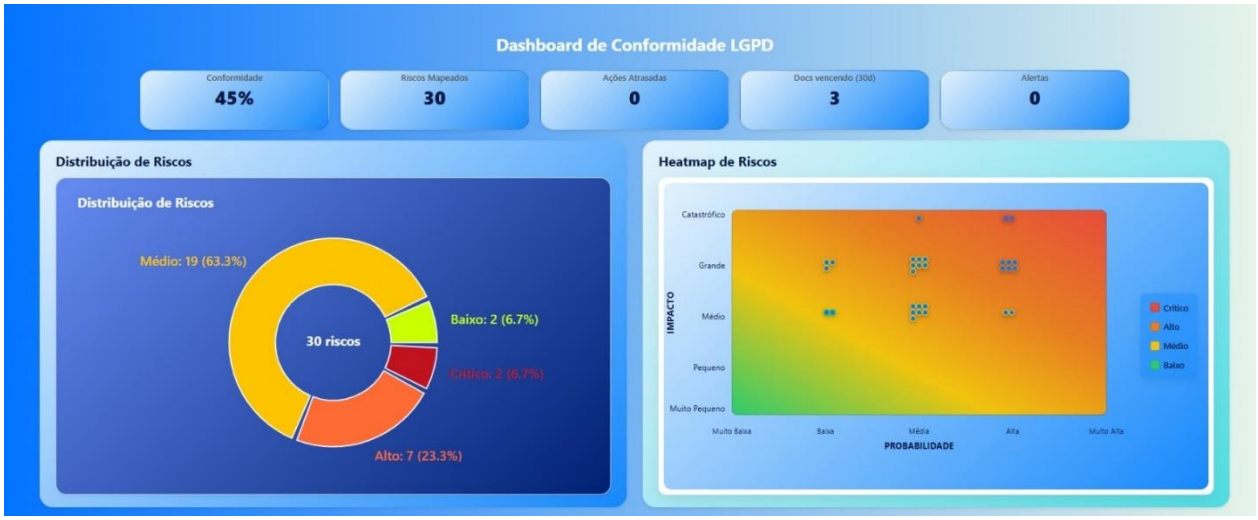


Fonte: Elaboração Própria

Das Figuras 7 até 10, apresentam as telas de Dashboard, que funcionam como o painel central de monitoramento do sistema. Seu objetivo é reunir, em um único espaço, as informações mais relevantes para o acompanhamento das atividades ligadas à conformidade com a LGPD. Os gráficos e indicadores exibidos permitem uma análise rápida e visual sobre o andamento dos processos, oferecendo ao DPO e aos gestores uma visão clara do nível de conformidade, do status das tarefas realizadas e dos pontos que precisam de maior atenção.

Além disso, o Dashboard facilita a identificação de tendências, gargalos e oportunidades de melhoria, uma vez que concentra dados que podem ser utilizados para a tomada de decisões estratégicas. Essa funcionalidade é essencial para garantir que a organização mantenha um controle contínuo sobre suas práticas de proteção de dados, promovendo eficiência, transparência e proatividade na gestão das informações.

Figura 7: Tela de Dashboard

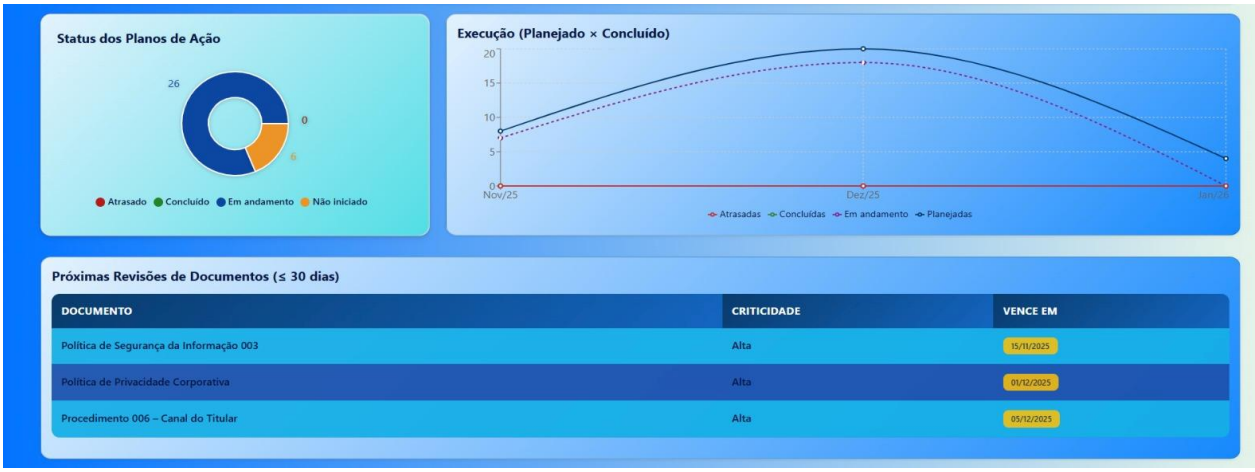


Fonte: Elaboração Própria

Figura 8: Tela de Dashboard

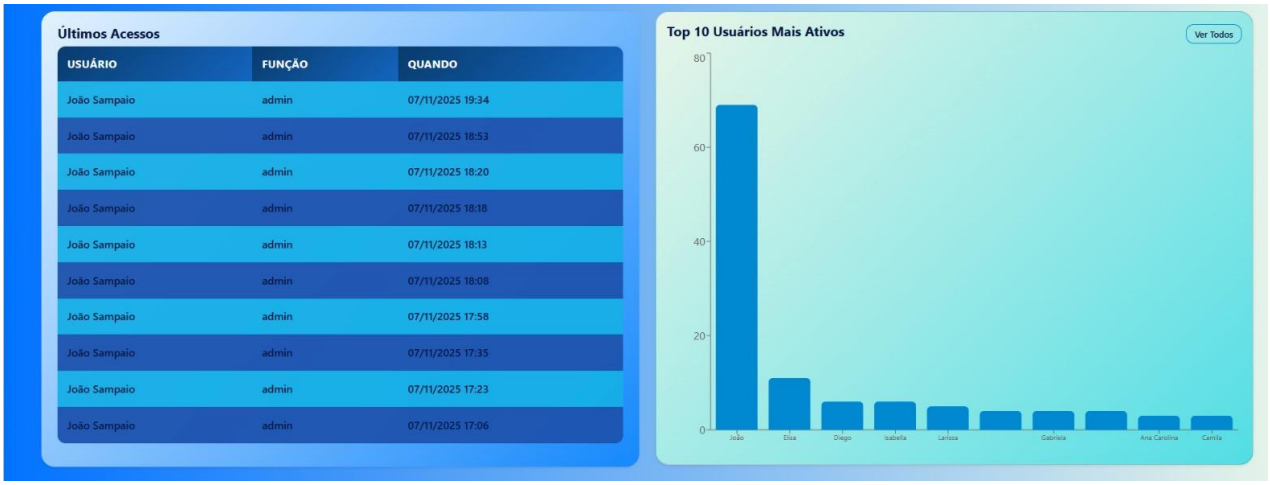
Fonte: Elaboração Própria

Figura 9: Tela de Dashboard



Fonte: Elaboração Própria

Figura 10: Tela de Dashboard



Fonte: Elaboração Própria

A Figura 11 apresenta a tela de cadastro do Inventário de Dados do sistema Camaleão. Nessa interface, o usuário registra informações sobre cada processo de tratamento de dados pessoais, incluindo unidade, setor responsável, e-mail do responsável e processo de negócio. O formulário também solicita dados como finalidade do tratamento, tipos e origem dos dados, formato de armazenamento, presença de registros físicos, identificação dos titulares e base legal conforme a LGPD. Ao final, os botões “Cancelar”, “Salvar” e “Próxima Página” permitem gerenciar o preenchimento do inventário de forma prática e padronizada. Essa estrutura facilita o controle e a rastreabilidade das informações tratadas pela organização.

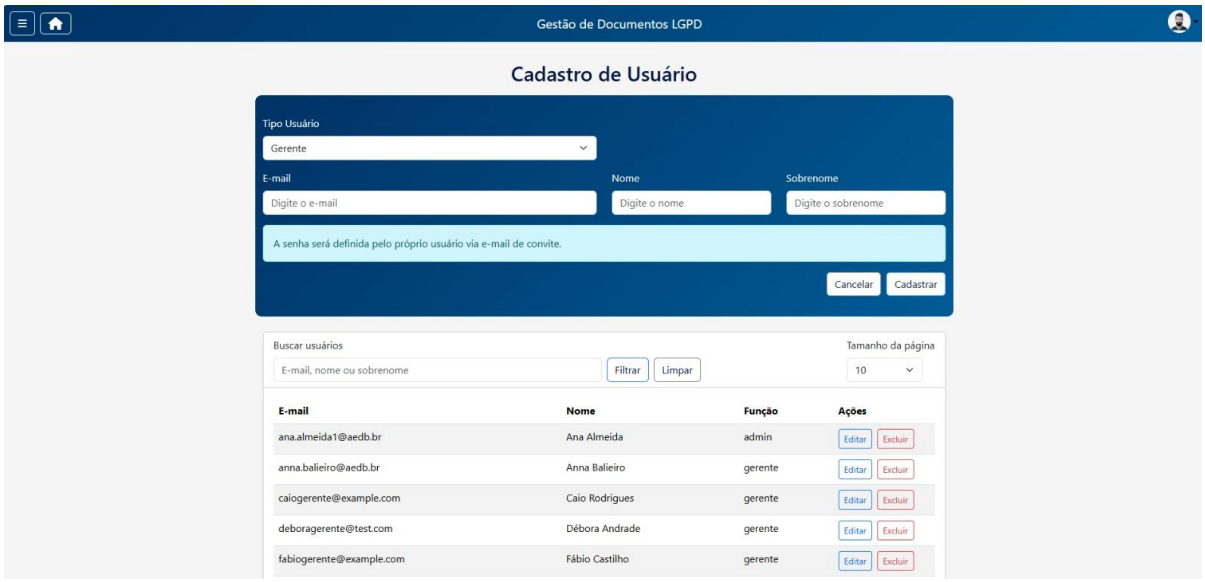
Figura 11: Tela de Inventário de Dados

Fonte: Elaboração Própria

A Figura 12 apresenta a tela de Cadastro de Usuário do sistema Camaleão, utilizada para registrar e gerenciar os perfis que têm acesso à plataforma. De forma simples e intuitiva, o sistema permite selecionar o tipo de usuário (como gerente ou administrador) e preencher informações básicas, como nome, sobrenome e e-mail. Em seguida, o sistema informa que a senha será criada pelo próprio usuário, que receberá um convite por e-mail, garantindo maior segurança no processo de autenticação.

Na parte inferior da tela, é exibida uma lista de usuários cadastrados, com informações como e-mail, nome, função e opções para editar ou excluir registros, além de filtros e campo de busca para facilitar a gestão. Essa funcionalidade contribui para uma administração eficiente e segura dos acessos, reforçando a governança e a proteção dos dados pessoais no ambiente do sistema Camaleão.

Figura 12: Cadastro de Usuário

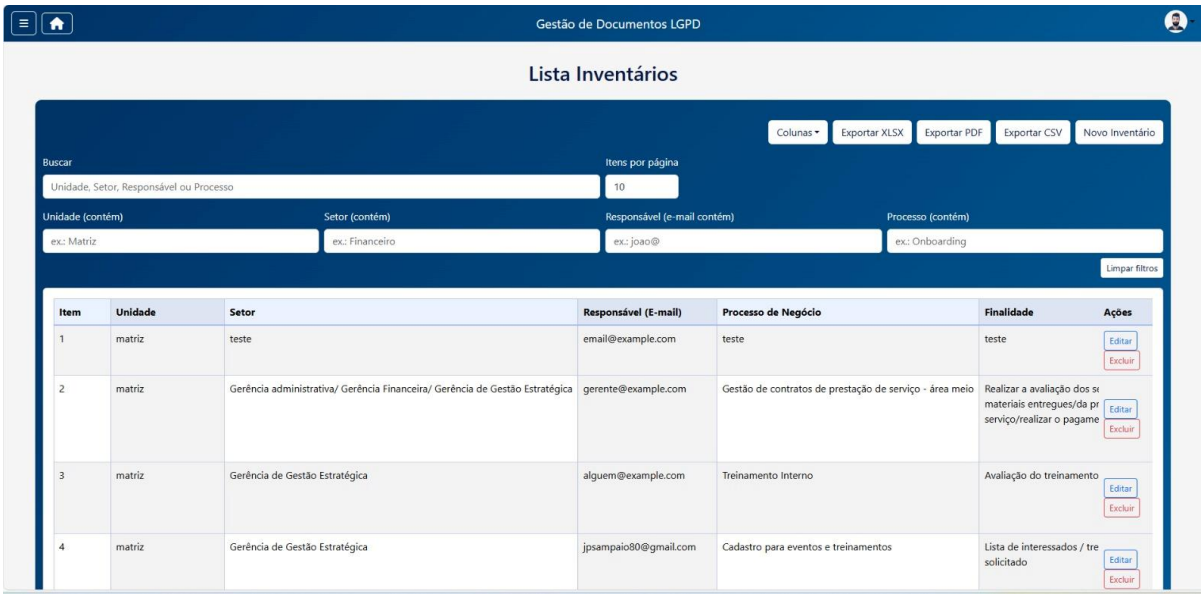


Fonte: Elaboração Própria

A Figura 13 apresenta a tela de Lista de Inventários do sistema Camaleão. Nela, é possível visualizar todos os inventários de tratamento de dados previamente cadastrados pela organização. A interface dispõe de uma barra de pesquisa e filtros específicos para facilitar a localização dos registros, permitindo filtrar por unidade, setor, responsável e processo de negócio. Também há opções de exportação dos dados em diferentes formatos (XLSX, PDF e CSV), bem como o botão para criação de um novo inventário.

Logo abaixo, encontra-se a tabela de inventários, organizada em colunas que exibem informações como unidade, setor, responsável, processo de negócio e finalidade do tratamento. Na coluna final, são disponibilizadas ações de edição e exclusão, que permitem a manutenção contínua dos registros. A distribuição dos elementos na tela prioriza a clareza e a acessibilidade das informações, oferecendo ao usuário uma visualização estruturada e alinhada às boas práticas de gestão de dados pessoais.

Figura 13: Tela Lista Inventários

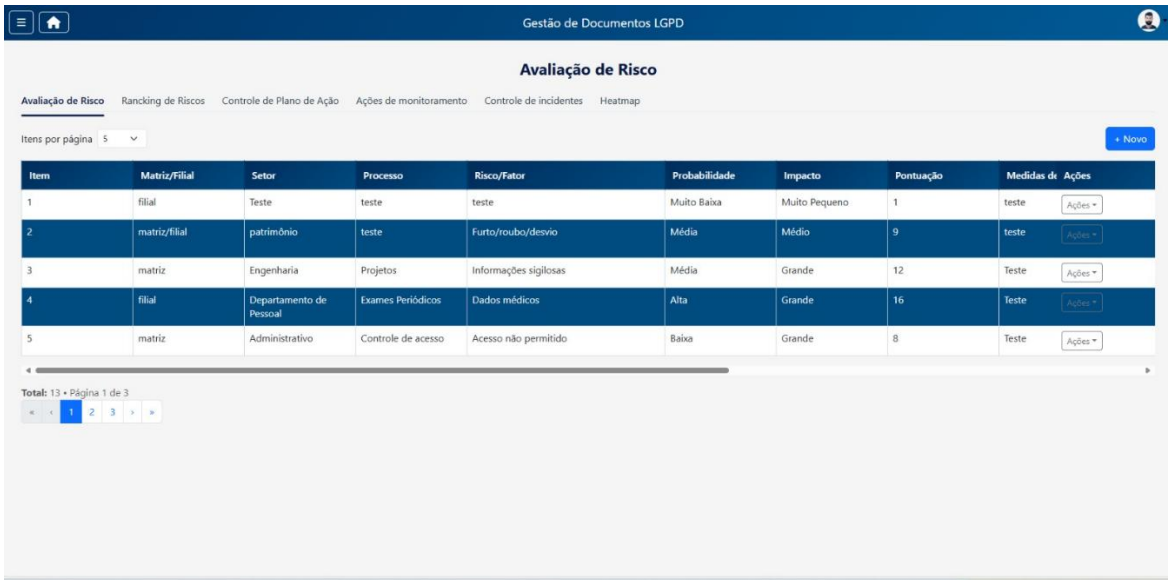


Fonte: Elaboração Própria

A Figura 14 apresenta a tela de Avaliação de Risco do sistema Camaleão, onde são exibidos os riscos identificados no contexto organizacional. No topo, o menu de navegação permite acessar módulos relacionados, como Ranking de Riscos, Plano de Ação, Ações de Monitoramento, Controle de Incidentes e Heatmap, facilitando a continuidade do processo de gestão.

A tabela central organiza os riscos em colunas que indicam unidade, setor, processo, fator de risco, probabilidade, impacto e a pontuação resultante. Cada registro possui um menu de ações para edição ou acompanhamento, enquanto o botão “+ Novo” permite cadastrar novos riscos. A interface prioriza clareza e objetividade, apoiando a análise e tomada de decisão.

Figura 14: Tela de Avaliação de Risco

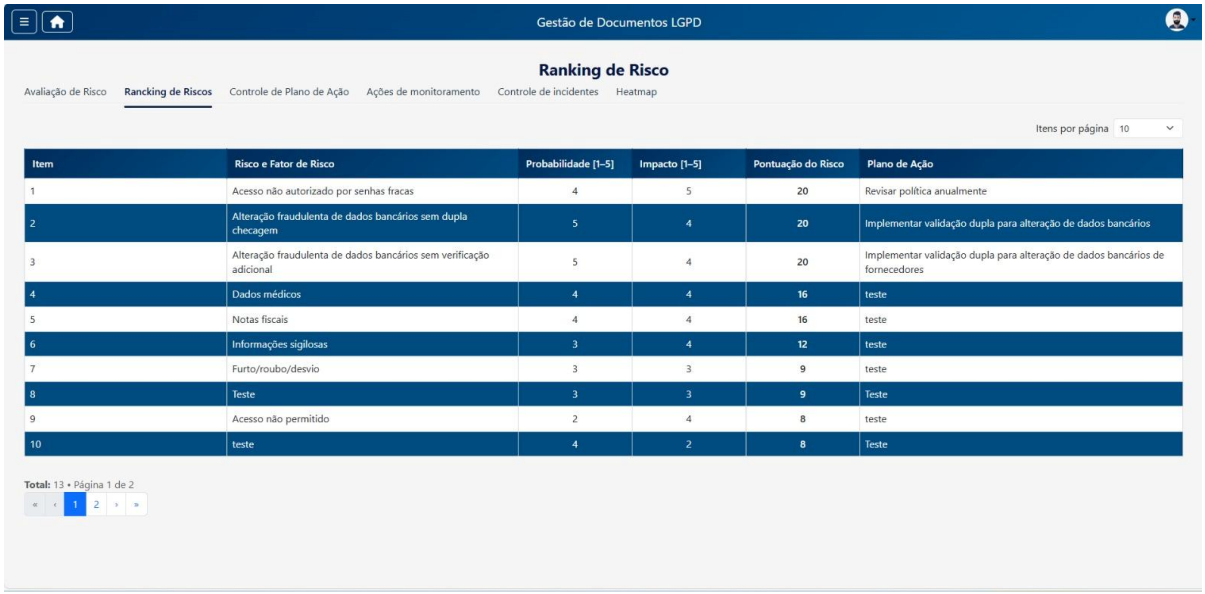


Fonte: Elaboração Própria

A Figura 15 apresenta a tela de Ranking de Riscos do sistema Camaleão, utilizada para exibir a priorização dos riscos identificados na organização. Nessa visualização, os riscos são classificados de acordo com suas pontuações, resultado da combinação entre os níveis de probabilidade e impacto atribuídos durante a avaliação. O objetivo é facilitar a identificação daqueles que exigem maior atenção e definição de medidas de tratamento.

A tabela central organiza os dados em colunas que mostram o risco, sua probabilidade, impacto e a pontuação final, além do plano de ação associado. Essa disposição permite que o usuário compare rapidamente a criticidade entre diferentes situações e direcione esforços para mitigação conforme a gravidade. A interface mantém um layout limpo, alinhado à navegação contínua do módulo de gestão de riscos, favorecendo análise e tomada de decisão.

Figura 15: Figura 15: Tela de Ranking de Riscos



Fonte: Elaboração Própria

A Figura 16 apresenta a tela de Controle de Plano de Ação do sistema Camaleão, utilizada para acompanhar e gerenciar as medidas definidas para mitigação dos riscos identificados. Essa interface permite ao usuário visualizar, de forma centralizada, quais ações estão associadas a cada risco, bem como os setores responsáveis e os processos envolvidos. O menu superior mantém a navegação contínua entre os módulos de gestão de riscos, facilitando a progressão natural da análise.

A tabela exibe informações como unidade, setor proprietário, processo, plano de ação adicional e responsável pela execução. Na última coluna, o menu de ações permite editar ou atualizar o andamento de cada medida. A estrutura da tela foi planejada para garantir clareza e rastreabilidade, possibilitando que a organização monitore o cumprimento das ações e avance em direção à redução de vulnerabilidades relacionadas à proteção de dados pessoais.

Figura 16: Tela de Controle de Plano de Ação

Fonte: Elaboração Própria

A Figura 17 apresenta a tela de Ações de Monitoramento do sistema Camaleão, utilizada para registrar e acompanhar atividades contínuas de verificação relacionadas à conformidade e à gestão de riscos. Nesta interface, cada ação corresponde a um procedimento de monitoramento planejado, incluindo informações sobre o requisito ou framework de referência, o escopo da atividade, a data prevista para realização, o critério adotado para avaliação e o responsável pela execução.

A tabela organiza os dados de forma padronizada, permitindo identificar com clareza o andamento das ações e eventuais deficiências constatadas durante auditorias e revisões internas. Na última coluna, o menu de ações possibilita a atualização ou edição dos registros, assegurando a manutenção contínua das informações. Assim, a tela apoia o acompanhamento sistemático das medidas de conformidade, fortalecendo a governança e a rastreabilidade dos processos de proteção de dados pessoais.

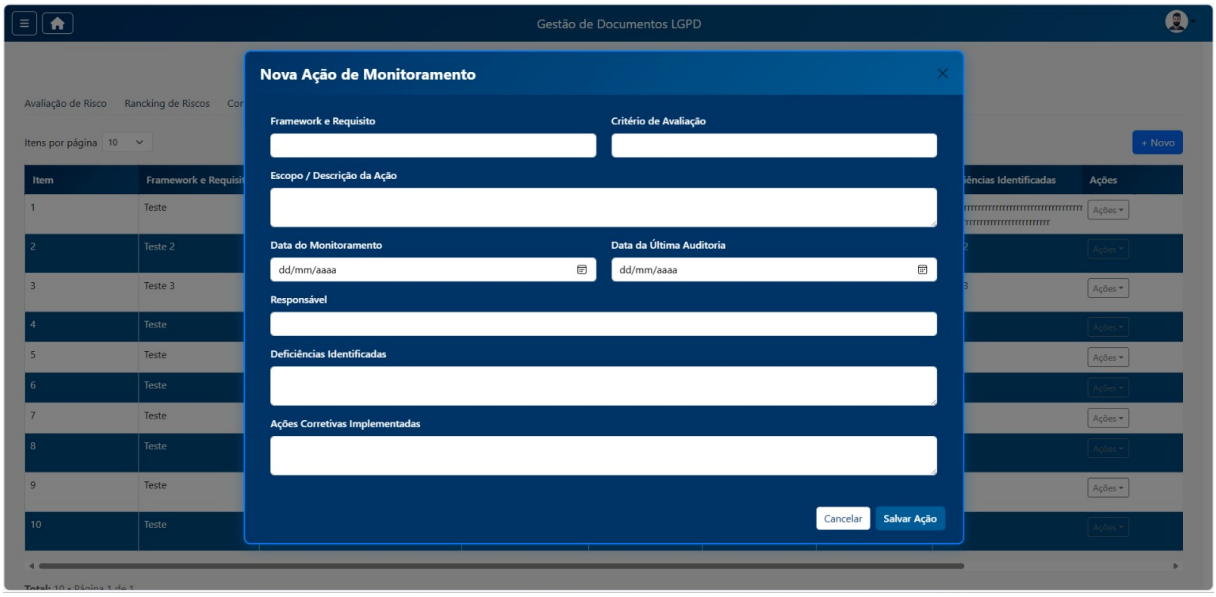
Figura 17: Tela de Ações de Monitoramento

Fonte: Elaboração Própria

A Figura 18 apresenta a tela de Cadastro de Nova Ação de Monitoramento do sistema Camaleão, exibida em formato de janela modal. Nessa interface, o usuário pode registrar atividades de monitoramento relacionadas à conformidade e gestão de riscos, preenchendo campos como framework ou requisito de referência, descrição do escopo, critérios de avaliação, datas de monitoramento e auditoria e o responsável pela execução.

O formulário também permite registrar deficiências identificadas e ações corretivas adotadas, garantindo rastreamento e documentação completa do processo. Ao final, o usuário pode salvar ou cancelar o cadastro. Essa funcionalidade promove a padronização e o controle das evidências de conformidade, fortalecendo a governança e o acompanhamento contínuo das práticas de proteção de dados pessoais.

Figura 18: Tela de Cadastro de Nova Ação de Monitoramento

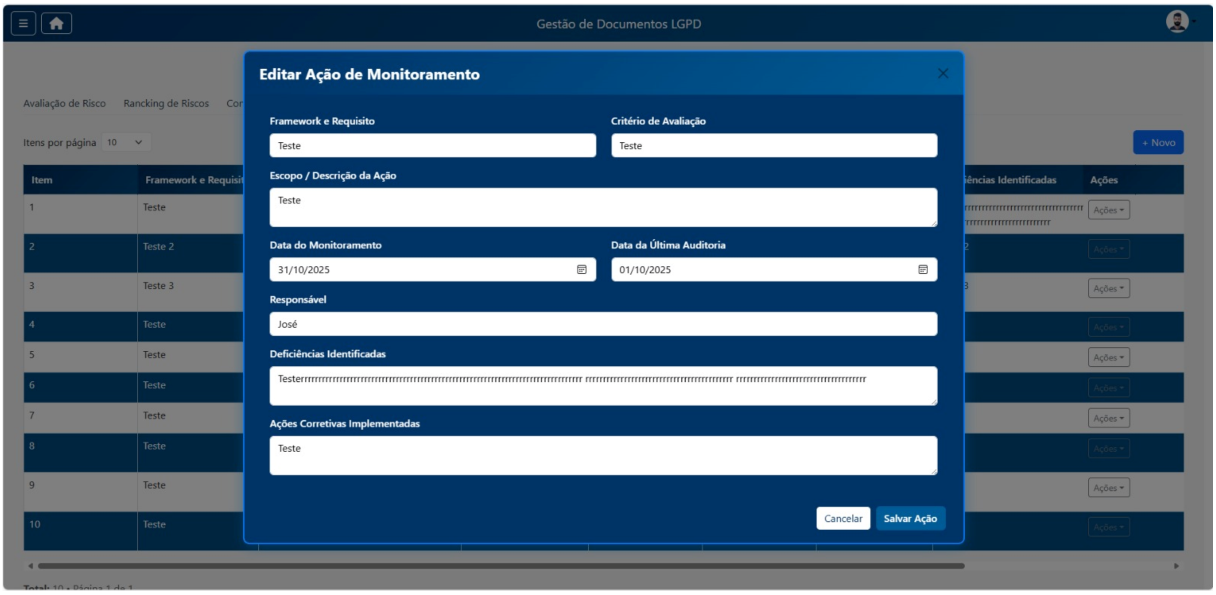


Fonte: Elaboração Própria

A Figura 19 apresenta a tela de Edição de Ação de Monitoramento do sistema Camaleão. Essa interface é apresentada em formato de janela modal e permite ao usuário atualizar registros previamente cadastrados referentes às atividades de monitoramento contínuo da conformidade. O formulário disponibiliza campos para revisão do framework ou requisito utilizado como referência, descrição da ação, critério de avaliação adotado, datas de monitoramento e da última auditoria, além do responsável pela execução.

Também são possíveis ajustes quanto às deficiências identificadas e às ações corretivas já implementadas, garantindo que o histórico de monitoramento permaneça fiel ao que foi constatado durante a execução das auditorias internas. Ao final da edição, o usuário pode salvar as alterações ou cancelar a operação. Essa funcionalidade assegura a manutenção e a rastreabilidade das evidências de conformidade, reforçando a governança e o acompanhamento estruturado do programa de proteção de dados pessoais.

Figura 19: Tela de Edição de Ação de Monitoramento



Fonte: Elaboração Própria

A Figura 20 apresenta a tela de Controle de Incidentes do sistema Camaleão, responsável pelo registro, acompanhamento e tratamento de eventos que possam representar violação, falha ou risco à proteção de dados pessoais. Por meio dessa interface, o usuário pode visualizar os incidentes já registrados, identificando detalhes como número do registro, descrição, fonte do incidente, data de ocorrência e responsável pela análise.

A tabela organiza os incidentes de forma cronológica e inclui ainda informações sobre a data de conclusão da análise, a ação recomendada e eventuais recomendações adicionais. Na coluna final, o menu de ações permite editar ou atualizar o andamento de cada registro. A presença do botão “+ Novo” possibilita o cadastro de novos incidentes, assegurando que todos os eventos relevantes sejam documentados de maneira estruturada. Essa tela contribui para a rastreabilidade, transparência e contínua melhoria dos processos de segurança da informação e conformidade com a LGPD.

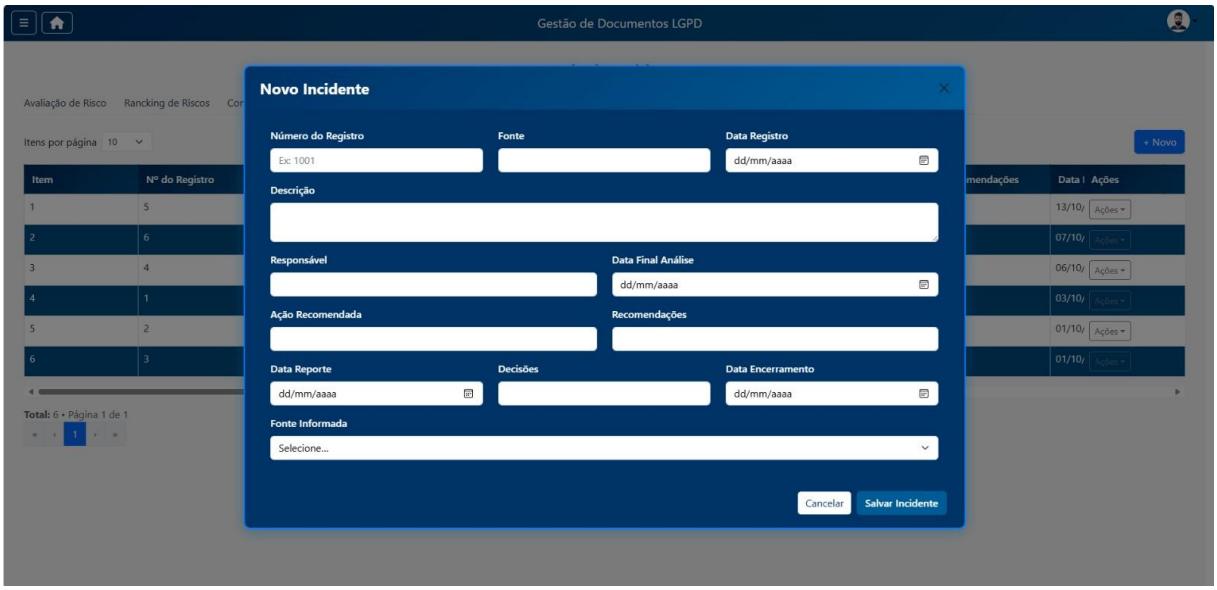
Figura 20: Tela de Controle de Incidentes

Fonte: Elaboração Própria

A Figura 21 exibe a interface destinada ao registro de novos incidentes no sistema Camaleão. Nessa tela, o usuário pode inserir informações detalhadas sobre o evento ocorrido, assegurando a rastreabilidade e o acompanhamento adequado das medidas corretivas. São disponibilizados campos como *Número do Registro*, *Fonte*, *Data de Registro* e *Descrição*, que permitem caracterizar o incidente de forma clara e objetiva.

Além disso, é possível indicar o *Responsável* pela análise, a *Data Final da Análise*, bem como registrar as *Ações Recomendadas*, *Recomendações*, *Decisões* e *Datas de Reporte* e *Encerramento*. O campo *Fonte Informada* possibilita selecionar a origem da notificação, garantindo a padronização dos registros. Ao final, os botões Salvar Incidente e Cancelar permitem confirmar ou abortar o processo de criação do registro. Essa estrutura contribui para um gerenciamento sistemático e transparente dos incidentes relacionados à proteção de dados pessoais.

Figura 21: Tela de Cadastro de Incidente

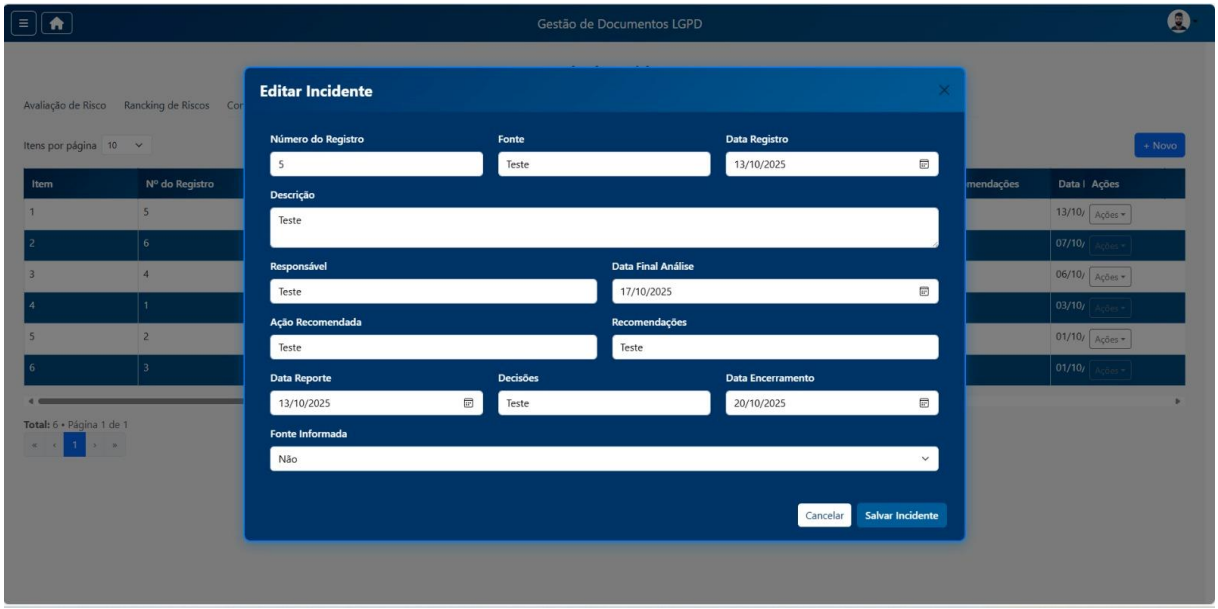


Fonte: Elaboração Própria

A Figura 22 apresenta a tela de edição de incidentes do sistema Camaleão. Essa interface foi desenvolvida para permitir ao usuário revisar e atualizar as informações previamente cadastradas sobre um incidente, garantindo a consistência e a integridade dos registros ao longo de todo o processo de tratamento.

A estrutura do formulário mantém o mesmo padrão visual da tela de criação, dispondo de campos como *Número do Registro*, *Fonte*, *Data de Registro*, *Descrição*, *Responsável*, *Ação Recomendada*, *Recomendações*, *Decisões*, além das *Datas de Reporte, Análise* e *Encerramento*. O campo *Fonte Informada* permite definir a origem da notificação do incidente, assegurando maior rastreabilidade. Ao final da tela, os botões Salvar Incidente e Cancelar possibilitam confirmar as alterações realizadas ou desistir da edição, promovendo controle e transparência na gestão dos registros de incidentes relacionados à proteção de dados pessoais.

Figura 22: Tela de Edição de Incidente



Fonte: Elaboração Própria

A Figura 23 apresenta o *Heatmap de Risco* do sistema Camaleão, uma ferramenta visual que consolida a relação entre a probabilidade e o impacto dos riscos identificados na organização. Cada ponto exibido no gráfico representa um risco real cadastrado no sistema, permitindo a análise de sua criticidade de forma intuitiva e comparativa.

Na parte superior da tela, são exibidos indicadores quantitativos que resumem a distribuição dos riscos conforme sua classificação: *Crítico*, *Alto*, *Médio* e *Baixo*. Abaixo, o mapa de calor evidencia graficamente essas proporções, utilizando um gradiente de cores que vai do verde (baixo risco) ao vermelho (crítico). Essa visualização facilita a priorização das ações de mitigação e o acompanhamento contínuo da eficácia dos controles implementados, contribuindo para uma gestão de riscos mais estratégica e alinhada à conformidade com a LGPD.

Figura 23: Tela de Heatmap de Risco

Fonte: Elaboração Própria

A Figura 24 apresenta a visualização anual do módulo de calendário do sistema Camaleão. Essa interface exibe de forma organizada os doze meses do ano, permitindo ao usuário consultar de maneira panorâmica todos os períodos e datas disponíveis para o registro de atividades, auditorias ou monitoramentos. A disposição em blocos mensais facilita o planejamento estratégico e a identificação de períodos de maior demanda, contribuindo para uma gestão eficiente das ações relacionadas à conformidade co a LGPD.

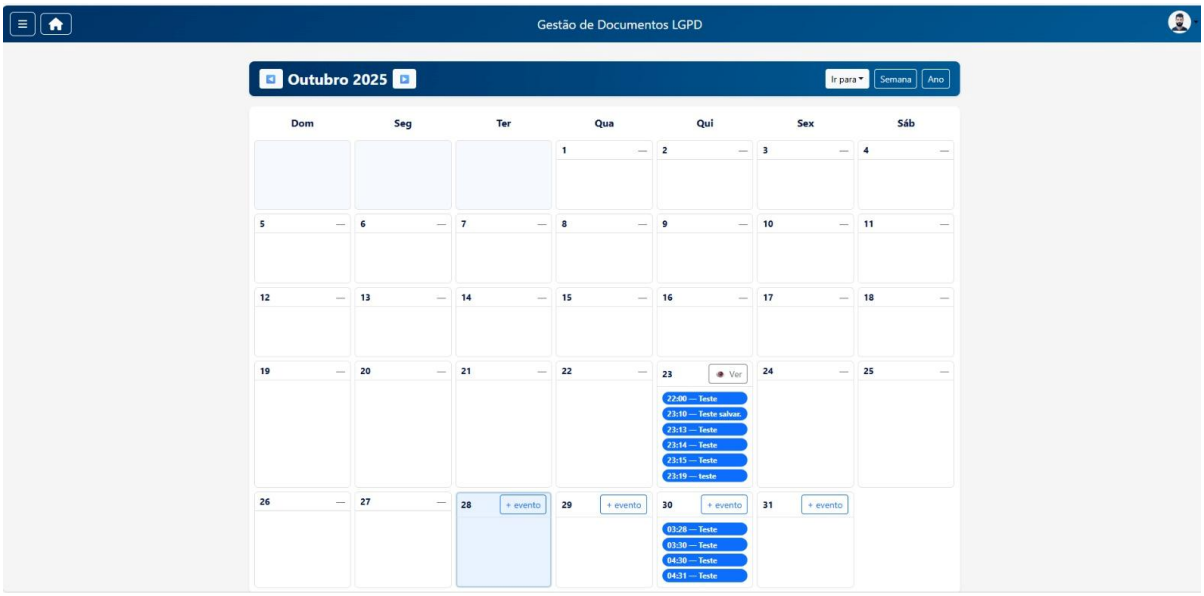
Figura 24: Tela Calendário de Eventos

Fonte: Elaboração Própria

A Figura 25 mostra a visualização mensal do calendário, que oferece uma perspectiva detalhada das atividades e compromissos agendados. O usuário pode

navegar entre os meses por meio dos botões de controle e visualizar, em cada dia, os eventos cadastrados no sistema. Essa visualização favorece o acompanhamento das tarefas de curto prazo, permitindo a adição de novos eventos, a edição de registros existentes e o monitoramento contínuo das ações programadas no contexto da governança de dados pessoais.

Figura 25: Tela Visualização Anual do Calendário de Eventos



Fonte: Elaboração Própria

A Figura 26 ilustra a visualização semanal do calendário, que possibilita um controle mais minucioso das atividades planejadas. Nessa perspectiva, cada dia da semana é apresentado com os eventos associados, acompanhados de seus respectivos horários. O usuário pode incluir novos compromissos por meio da opção + evento, garantindo o registro preciso das ações realizadas. Essa funcionalidade apoia o gerenciamento operacional das rotinas relacionadas à proteção de dados, assegurando maior rastreabilidade e cumprimento dos prazos estabelecidos nos planos de conformidade da LGPD.

Figura 26: Visualização Semanal do Calendário de Eventos

Fonte: Elaboração Própria

3.3 PROPOSTA DE SOLUÇÃO MOBILE

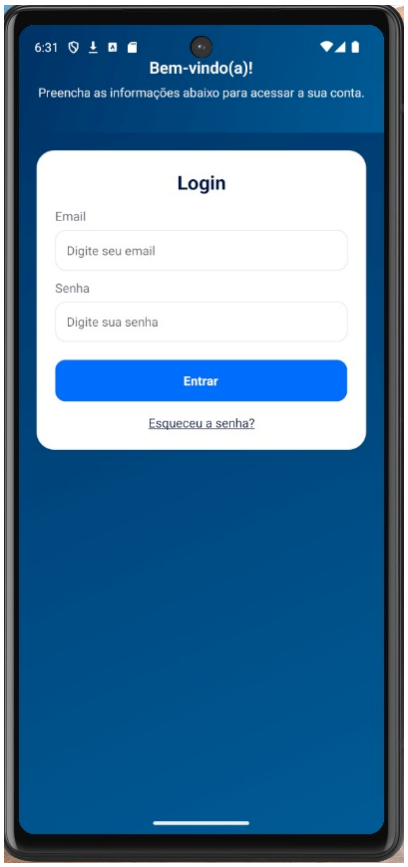
A solução proposta é uma aplicação web responsiva com versão mobile, desenvolvida para centralizar e gerenciar documentos relacionados à proteção de dados pessoais. A plataforma permite acesso, edição e exclusão de informações de forma ágil, segura e controlada, a partir de qualquer dispositivo. Seu objetivo é otimizar a gestão documental, garantindo padronização, rastreabilidade e integridade das informações.

Com interface adaptada a dispositivos móveis, menus simplificados e componentes otimizados, o sistema oferece ao DPO e demais usuários um controle eficiente e transparente das atividades de tratamento de dados pessoais. Dessa forma, é possível registrar inventários, consultar documentos, acompanhar prazos e monitorar ações diretamente pelo celular, promovendo mobilidade, governança e segurança no cumprimento da LGPD.

A Figura 27 apresenta a tela de login da versão mobile do sistema. Nessa interface, o usuário é recebido com uma mensagem de boas-vindas e orientado a inserir suas credenciais para acessar a aplicação. São disponibilizados dois campos de entrada: um para digitar o endereço de e-mail e outro para informar a senha. Abaixo dos campos, encontra-se o botão “Entrar”, que realiza a autenticação no sistema. Há ainda a opção “Esqueceu a senha?”, que permite ao usuário iniciar o processo de recuperação de acesso, caso seja necessário. O layout foi projetado com foco na simplicidade, legibilidade e usabilidade em dispositivos móveis, utilizando contraste

adequado entre fundo e componentes, centralização dos elementos e uma hierarquia visual clara, o que facilita a interação rápida e segura pelo usuário.

Figura 27: Tela de Login (Versão Mobile)



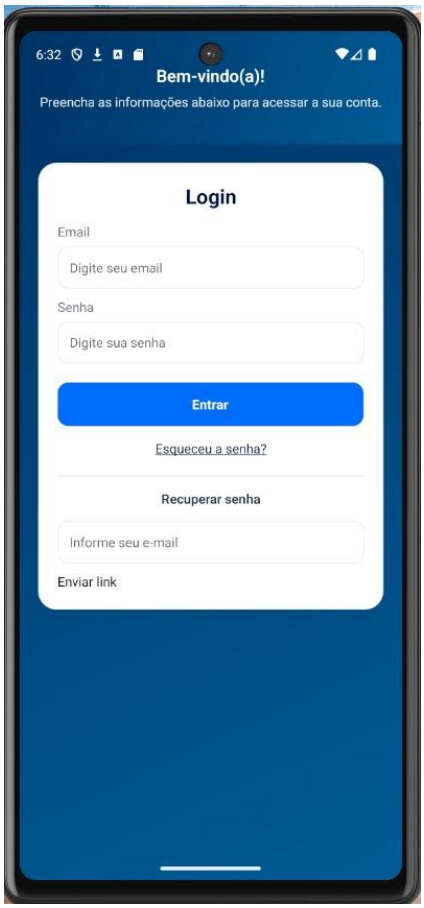
Fonte: Elaboração Própria

A Figura 28 apresenta a tela de recuperação de senha da versão mobile do sistema Camaleão. Após selecionar a opção “Esqueceu a senha?”, o usuário é direcionado para essa interface, onde pode iniciar o procedimento de redefinição de acesso. A tela mantém a estrutura visual simples, com campos centralizados e texto instrutivo claro, preservando a identidade visual da aplicação. Inicialmente, exibem-se os campos de login, seguidos pela área dedicada exclusivamente à recuperação de senha.

Nessa seção, o usuário encontra um campo para inserção do endereço de e-mail e o botão “Enviar link”, responsável por encaminhar uma mensagem contendo orientações para redefinir a senha. A interface foi planejada de forma a garantir clareza, acessibilidade e usabilidade em dispositivos móveis, permitindo que o processo seja realizado de forma ágil, segura e sem a necessidade de suporte técnico

adicional. Essa abordagem contribui para uma experiência fluida e contínua no acesso ao sistema.

Figura 28: Tela Recuperação de Senha (Versão Mobile)



Fonte: Elaboração Própria

A Figura 29 apresenta a tela inicial (Home) da versão mobile do sistema Camaleão. Após realizar o login, o usuário é direcionado para esta interface, onde é saudado pelo sistema e tem acesso rápido às principais funcionalidades. O layout apresenta uma organização em blocos, com ícones e rótulos descritivos que facilitam a identificação visual de cada módulo. A paleta de cores em tons de azul reforça a identidade visual da aplicação, ao mesmo tempo em que confere um aspecto de segurança e confiança, características importantes para um sistema voltado à proteção de dados pessoais.

Na parte central da tela, são exibidos os atalhos para os módulos: Encarregado, Monitoramento, Checklist, Documentos, Dashboards, Inventário de Dados, Matriz de Risco e Relatórios. Essa disposição em grade favorece a navegação por toque,

permitindo que o usuário acesse todas as funções de maneira prática e intuitiva em dispositivos móveis. O design responsivo assegura que os elementos se ajustem de forma adequada às dimensões da tela, garantindo boa legibilidade e usabilidade mesmo em smartphones com diferentes resoluções.

Figura 29: Tela Home (Versão Mobile)

Fonte: Elaboração Própria

A Figura 30 apresenta o menu lateral da versão mobile do sistema Camaleão. Esse menu pode ser acessado a partir do ícone localizado no canto superior esquerdo da tela inicial, abrindo uma área deslizante que ocupa parte da lateral do dispositivo. Na parte superior do menu, são exibidos o nome do usuário e o e-mail associado ao seu perfil, juntamente com a indicação do tipo de permissão atribuída (por exemplo, Administrador), reforçando a identificação e o nível de acesso do usuário dentro da aplicação.

Abaixo da identificação, são listados os módulos disponíveis no sistema, organizados em formato de lista, com ícones representativos ao lado de cada item para facilitar a navegação visual. Entre as opções disponíveis encontram-se: Dashboards, Relatórios, Checklist, Notificação, Encarregado, Monitoramento,

Documentos, Inventário de Dados, Lista de Inventários, Matriz de Risco, Cadastro de Usuário e Meu Perfil. O menu lateral facilita o acesso rápido às funcionalidades principais, permitindo que o usuário transite entre as áreas da aplicação de maneira prática e eficiente, mantendo a experiência intuitiva e adequada ao uso em dispositivos móveis.

Figura 30: Menu Lateral (Versão Mobile)

Fonte: Elaboração Própria

A Figura 31 apresenta a tela referente ao Encarregado de Proteção de Dados (DPO) na versão mobile do sistema Camaleão. Nessa tela, o usuário pode visualizar de forma clara e objetiva as informações institucionais do profissional responsável pela comunicação com titulares de dados e com a ANPD. A área de destaque apresenta a foto do DPO, seu nome completo e a identificação de seu papel, reforçando a transparência e a formalidade das informações exibidas.

Logo abaixo, são apresentados os dados de contato e informações essenciais, incluindo e-mail, número de telefone, data de nomeação e período de validade da designação como DPO. O layout utiliza cartões com bordas arredondadas e contraste adequado, proporcionando boa legibilidade e organização visual, especialmente em dispositivos móveis. Essa estrutura favorece o acesso rápido às informações

relevantes, reforçando o papel do sistema no apoio à governança, rastreabilidade e conformidade com a LGPD.

Figura 31: Tela do Encarregado de Proteção de Dados (Versão Mobile)

Fonte: Elaboração Própria

A Figura 32 apresenta a tela de Checklist de Itens da LGPD na versão mobile do sistema Camaleão. Essa interface permite ao usuário acompanhar e registrar o andamento das atividades relacionadas à adequação organizacional à LGPD. No topo da tela, é possível selecionar a quantidade de itens exibidos por página e cadastrar novos registros por meio do botão “+ Novo”. Em seguida, são apresentados os itens do checklist em formato de cartões, cada um contendo título, descrição e breve contextualização sobre sua importância no processo de conformidade.

Cada item possui um controle de situação, representado por um seletor que permite marcar a atividade como concluída ou pendente, além do botão “Ações”, que oferece opções de gerenciamento ou edição. O layout prioriza a legibilidade e o uso eficiente do espaço em dispositivos móveis, organizando as informações de forma clara e segmentada. Essa abordagem facilita o acompanhamento progressivo das

etapas de conformidade, apoiando o DPO e demais responsáveis na manutenção da governança e monitoramento contínuo das obrigações previstas na LGPD.

Figura 32: Tela de Checklist (Versão Mobile)

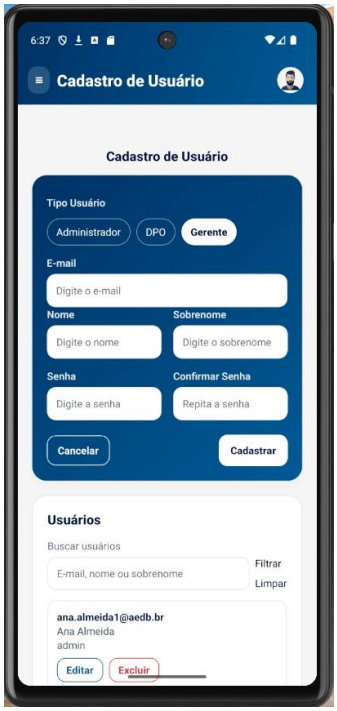
Fonte: Elaboração Própria

A Figura 33 apresenta a tela de Cadastro de Usuário na versão mobile do sistema Camaleão. Essa interface permite a criação e gerenciamento de contas de acesso, sendo fundamental para o controle de permissões e níveis hierárquicos dentro da aplicação. No topo da tela, o usuário pode selecionar o tipo de perfil a ser atribuído ao novo usuário, como Administrador, DPO ou Gerente. Abaixo, encontram-se os campos destinados ao preenchimento de informações essenciais para o cadastro, incluindo e-mail, nome, sobrenome, senha e confirmação de senha, acompanhados dos botões “Cancelar” e “Cadastrar” para controle das ações.

Na parte inferior da tela, é exibida uma lista dos usuários já cadastrados no sistema, com um campo de busca que permite filtrar registros por e-mail, nome ou sobrenome. Cada usuário listado apresenta opções de Editar e Excluir, permitindo ajustes e remoção conforme necessário. O layout foi organizado de modo a garantir clareza e fluidez durante o uso em dispositivos móveis, mantendo campos bem

distribuídos, boa legibilidade e acessibilidade por toque. Essa estrutura reforça a governança de acessos e contribui diretamente para a segurança da informação, requisito essencial no contexto da LGPD.

Figura 33: Tela de Cadastro de Usuário (Versão Mobile)



Fonte: Elaboração Própria

A Figura 34 apresenta a tela de Perfil do Usuário na versão mobile do sistema de Gestão de Documentos LGPD. Essa interface permite ao usuário visualizar suas informações pessoais e funcionais cadastradas no sistema. A tela exibe a imagem de perfil, seguida do endereço de e-mail associado à conta, acompanhado da indicação de que esse campo não pode ser alterado por motivos de segurança e controle interno. Logo abaixo, é apresentada a função atribuída ao usuário dentro do sistema, como, por exemplo, administrador, DPO ou gerente.

A interface também disponibiliza o botão “Editar”, que permite ao usuário realizar ajustes em dados que são autorizados para modificação, como troca de foto ou atualização de informações complementares. O layout prioriza simplicidade e clareza, com componentes bem distribuídos e contraste adequado para leitura em telas menores, garantindo boa experiência de uso em dispositivos móveis. Essa tela contribui para manter a identidade de acesso e reforça o controle de permissões e perfis, aspectos fundamentais para governança e segurança no ambiente da LGPD.

Figura 34: Tela de Perfil do Usuário (Versão Mobile)

Fonte: Elaboração Própria

3.4 PARTICIPANTES DO PROJETO

Os participantes deste projeto são compostos pelo grupo de estudantes responsáveis pelo desenvolvimento da aplicação e pela professora Mônica, que atua como orientadora do trabalho, acompanhando e validando as etapas do processo.

Tabela 1: Tabela Nome e Função

Nome	Função
Ana Cristina	Front-End
Anna Clara	Documentação
João Sampaio	Full Stack
Mônica Mara	Orientadora

Fonte: Elaboração Própria

3.5 USUÁRIOS PARTICIPANTES (ATORES)

Os usuários participantes deste projeto são compostos pelo administrador do sistema, pelo DPO e pelos gerentes de setores, os quais interagirão com a plataforma conforme suas funções e responsabilidades na organização.

3.6 NECESSIDADES DOS USUÁRIOS

Os usuários do sistema apresentam necessidades distintas de acordo com suas funções e responsabilidades. O administrador do sistema necessita de recursos que permitam o gerenciamento de cadastros, a definição de permissões de acesso, a configuração e a manutenção da plataforma, além do monitoramento constante da segurança e da integridade das informações. O DPO, por sua vez, demanda funcionalidades voltadas ao acompanhamento da conformidade com a LGPD, incluindo a centralização de relatórios sobre o tratamento de dados pessoais, a gestão de solicitações dos titulares, o controle de incidentes de segurança e a disponibilização de evidências necessárias para auditorias e comunicações com a ANPD. Já os gerentes de setores, enquanto usuários finais, necessitam de ferramentas que possibilitem o registro e a atualização de informações relacionadas ao tratamento de dados em suas áreas, o acesso a relatórios e indicadores de apoio à gestão, além de recursos que favoreçam respostas ágeis às solicitações do DPO ou da administração, sempre por meio de uma interface intuitiva, acompanhada de notificações e alertas que facilitem o uso no cotidiano organizacional.

3.7 REQUISITOS FUNCIONAIS

Para garantir que o sistema Camaleão atenda às necessidades específicas da gestão de proteção de dados conforme a LGPD, foram definidos diversos requisitos funcionais essenciais. Esses requisitos estabelecem as funcionalidades que permitirão uma operação eficiente, segura e alinhada às responsabilidades do DPO e demais usuários envolvidos. A seguir, estão listadas as principais funcionalidades que compõem o escopo do sistema:

- RF01 – Permitir o cadastro de Administrador.
- RF02 – Permitir o cadastro do DPO.
- RF03 – Permitir o cadastro de Gerentes dos setores.
- RF04 – Poder inserir documentos.

- RF05 – Gerenciar documentos.
- RF06 – Disponibilizar um formulário para gerar o relatório de inventário de dados pessoais.
- RF07 – Disponibilizar um formulário para gerar a matriz de riscos e as ações de mitigação.
- RF08 – Apresentar um dashboard com gráficos e indicadores relacionados à LGPD.
- RF09 – Registrar logs de acessos e ações realizadas por cada usuário.
- RF10 – Emitir alertas automáticos sobre vencimento de documentos e eventos importantes (como auditorias).
- RF11 – Disponibilizar uma página com as informações e forma de contato do DPO.
- RF12 – Permitir que usuários possam cadastrar documentos, conforme seu nível de permissão.
- RF13 – Permitir a edição de documentos, conforme o nível de permissão do usuário.
- RF14 – Permitir a exclusão de registros, conforme o nível de permissão do usuário.
- RF15 – Permitir o controle de permissões conforme o papel do usuário na gestão da LGPD.
- RF16 – Enviar e-mail automático ao criar um usuário no sistema.
- RF17 – Permitir o login de usuários cadastrados, validando credenciais de acesso.
- RF17 – Permitir o login de usuários cadastrados, validando credenciais de acesso.
- RF18 – Permitir o logout do sistema, encerrando a sessão de forma segura.
- RF19 – Permitir a definição, e redefinição de senha de acesso.
- RF20 – Permitir a edição de perfil do usuário (alteração de nome, e-mail, senha e foto de perfil).
- RF21 – Permitir a inserção de novos itens no checklist de conformidade.
- RF22 – Permitir a edição de itens do checklist, possibilitando atualizar descrições, responsáveis, status conforme necessidade.

3.8 REQUISITOS NÃO FUNCIONAIS

Além dos requisitos funcionais, o sistema deve atender a requisitos não funcionais que garantem sua qualidade, segurança e usabilidade. Esses critérios são fundamentais para assegurar que a aplicação seja confiável, eficiente e fácil de usar,

proporcionando uma experiência satisfatória para todos os usuários. A seguir, estão descritos os principais requisitos não funcionais do sistema:

- RNF01 – O sistema deve implementar controle de acesso seguro baseado em papéis.
- RNF02 – Os registros de atividades (logs) devem ser protegidos contra alterações e acessos não autorizados.
- RNF03 – Alertas e notificações devem ser enviadas com antecedência adequada para garantir ações preventivas.
- RNF04 – A interface deve ser intuitiva e facilitar o uso por diferentes perfis de usuário.
- RNF05 – O sistema será uma aplicação web para desktop.

3.9 ARQUITETURA ESTRUTURAL DO SISTEMA

O projeto será desenvolvido em uma única instância, na versão web, com foco no gerenciamento e controle de documentos relacionados à conformidade com a LGPD.

A versão web consistirá em um sistema acessível via navegador, restrito apenas a usuários com níveis específicos de permissão. Seu propósito principal será centralizar o gerenciamento de documentos e informações relacionadas à proteção de dados pessoais, conforme as diretrizes da LGPD. O sistema permitirá o controle de acessos, a rastreabilidade das ações realizadas e a supervisão do ciclo de vida dos dados.

3.10 LOGOTIPO

O logotipo do sistema foi desenvolvido com base no conceito de adaptabilidade, um princípio fundamental tanto no contexto organizacional quanto na conformidade legal. A ideia central é que, assim como na natureza a evolução e a sobrevivência estão diretamente relacionadas à capacidade de se adaptar, no cenário corporativo, especialmente no que diz respeito à proteção de dados, essa flexibilidade é essencial. A escolha do camaleão como símbolo principal reforça essa mensagem. O camaleão é um animal conhecido por sua habilidade de mudar de cor e se adequar ao ambiente,

com mecanismo de defesa contra predadores, conferindo-lhe maior chance de sobrevivência, o que o torna uma representação ideal da constante transformação exigida por um ambiente regulatório em evolução, como o da LGPD.

Ele transmite visualmente a capacidade do sistema de se ajustar rapidamente às novas diretrizes legais, às necessidades específicas de cada organização e às mudanças nos processos internos. Além disso, o design do logotipo foi pensado para comunicar versatilidade e agilidade, duas qualidades essenciais para qualquer solução voltada à gestão da privacidade e da segurança da informação. A proposta visual busca estabelecer uma conexão entre a inovação tecnológica e o compromisso com a conformidade legal, transmitindo confiança, dinamismo e prontidão para enfrentar os desafios atuais e futuros no tratamento de dados pessoais. Dessa forma, o logotipo não é apenas um elemento estético, mas também um símbolo da missão do sistema Camaleão: ser uma ferramenta eficaz, adaptável e segura para auxiliar empresas no cumprimento da LGPD, promovendo a cultura da proteção de dados desde o design até a execução

Figura 35: Logotipo Camaleão

Fonte: Elaboração Própria

3.11 TECNOLOGIAS E FERRAMENTAS UTILIZADAS

As tecnologias utilizadas no desenvolvimento da aplicação são: Django (Python), SQLite (para testes), PostgreeSQL (para prdoduçao), HTML, CSS, JavaScript, Vite (React), Git, GitHub, VS Code, FlutterFlow e Node.js.

3.11.1 Django

A linguagem principal utilizada no *backend* foi o Python, por meio do framework Django. Ele é conhecido por sua robustez, segurança e rapidez no desenvolvimento de aplicações web. Foi utilizado para implementar toda a lógica de negócios da aplicação, como o cadastro e gerenciamento de procedimentos, riscos e ações de mitigação, além de fornecer rotas e recursos para o *frontend*. Foi escolhido por oferecer um conjunto completo de funcionalidades integradas, como ORM, sistema de autenticação e proteção contra vulnerabilidades comuns.

Figura 36: Logo Django

Fonte: Django Community

3.11.2 SQLite

Foi utilizado o SQLite para o armazenamento dos dados durante o desenvolvimento e etapas de teste. Por ser leve, sem necessidade de servidor e com integração nativa ao Django, ele se mostrou ideal para persistir informações como usuários, checklists da LGPD e planos de ação, facilitando o desenvolvimento e testes locais.

Figura 37: Logo SQLite

Fonte: SQLite Logotipo

3.11.3 CSS

O CSS *(Cascading Style Sheets)* foi utilizado para definir a aparência e o layout das páginas do sistema, permitindo a criação de uma interface limpa, moderna e responsiva. Com ele, foi possível personalizar cores, tipografias, espaçamentos e o posicionamento dos elementos, garantindo uma melhor experiência visual ao usuário. Além disso, o CSS contribuiu para a adaptação do sistema a diferentes dispositivos, como computadores, tablets e celulares.

Figura 38: Logo CSS

Fonte: Css Logo PNG Vectors

3.11.4 GitHub

O controle de versões do sistema foi realizado utilizando o Git, com os repositórios hospedados no GitHub. Essa combinação possibilitou o gerenciamento eficiente do código-fonte e favoreceu a colaboração entre os membros da equipe. Além disso, o uso do Git garantiu o registro detalhado das alterações realizadas, permitindo rastrear modificações, corrigir falhas e implementar melhorias de forma organizada e segura. O GitHub complementou esse processo ao oferecer recursos como *branches*, *issues* e *pull requests*, que facilitaram a revisão do código e tornaram o desenvolvimento mais estruturado e transparente.

Figura 39: Logo Git Hub

Fonte: GitHub, 2008

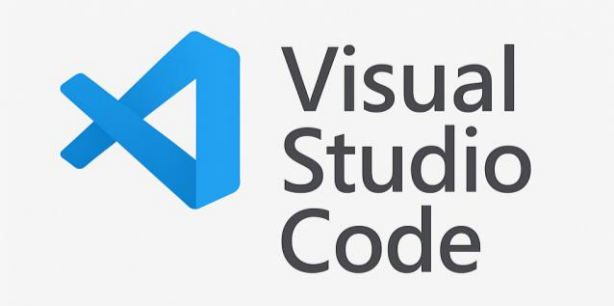
3.11.5 Visual Studio Code

O editor de código escolhido para o desenvolvimento do sistema foi o Visual Studio Code (VS Code). Essa escolha se mostrou bastante adequada, pois o VS Code alia leveza e rapidez a uma interface intuitiva, o que facilitou seu uso durante todas as etapas do projeto. Além disso, trata-se de uma ferramenta altamente personalizável, permitindo a instalação de diversas extensões que atenderam de forma específica às necessidades da equipe.

Entre os recursos mais utilizados, destacaram-se o controle de versão integrado, que facilitou a interação com os repositórios no GitHub, o depurador, que

auxiliou na identificação e correção de erros, e as sugestões inteligentes de código, que aumentaram a produtividade e reduziram falhas comuns durante a implementação. O suporte a múltiplas linguagens também foi um diferencial importante, permitindo que diferentes partes do sistema fossem desenvolvidas dentro do mesmo ambiente.

Figura 40: Logo Visual Studio Code

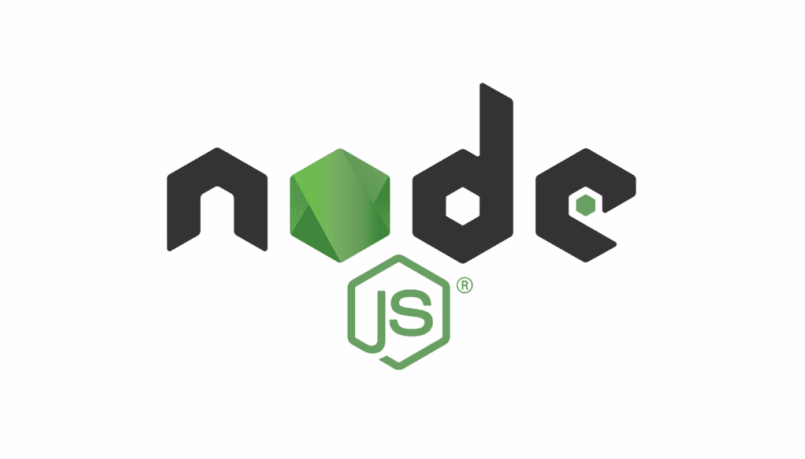


Fonte: StickPNG

3.11.6 Node.js

Por fim, a tecnologia Node.js também foi empregada, de forma complementar, para testes e possíveis integrações com APIs REST em tempo real. Node.js é um ambiente de execução de JavaScript no lado do servidor, conhecido por sua alta performance e capacidade de lidar com múltiplas requisições simultaneamente. Sua utilização foi útil para situações em que a performance assíncrona era essencial.

Figura 41: Logo Node JS



Fonte: NODE JS, 2024

3.11.7 JavaScript

O JavaScript foi responsável por tornar a aplicação interativa e dinâmica. Ele permitiu a criação de funcionalidades como a validação de formulários, atualização automática de conteúdo sem recarregar a página (usando requisições assíncronas), exibição de mensagens instantâneas ao usuário e navegação mais fluida. Essa linguagem é essencial no desenvolvimento web moderno e foi fundamental para proporcionar uma experiência de uso mais eficiente e agradável no sistema voltado à gestão da LGPD.

Figura 42: Logo JavaScript

Fonte: JavaScript, 2011

3.12 DEPENDÊNCIAS

Para o funcionamento adequado do sistema, será necessário o uso das ferramentas utilizadas no desenvolvimento e manutenção, além de acesso à internet para a operação e validação das funcionalidades.

3.13 REFERÊNCIAS (PARA O LEVANTAMENTO INICIAL)

No cenário atual, as pequenas empresas enfrentam desafios significativos no que diz respeito à adequação à LGPD. Em geral, essas organizações não dispõem da mesma estrutura, recursos financeiros ou equipes especializadas que empresas de maior porte possuem para gerir a conformidade legal e a segurança da informação.

Muitas vezes, os processos relacionados ao tratamento de dados pessoais são realizados de maneira manual, descentralizada ou com o uso de ferramentas genéricas, como planilhas e arquivos físicos, o que aumenta a probabilidade de erros, inconsistências e falhas de segurança.

Essa realidade evidencia a necessidade da adoção de sistemas específicos para o controle da LGPD, que possibilitem a centralização das informações, a padronização de procedimentos, a rastreabilidade das operações e o monitoramento contínuo do uso dos dados pessoais. Um sistema desse tipo contribui para a redução de riscos, para a prevenção de incidentes de segurança e para a resposta rápida a solicitações dos titulares de dados, além de facilitar a geração de relatórios e a comprovação de conformidade em auditorias.

Portanto, investir em uma solução tecnológica voltada ao controle da LGPD representa não apenas uma obrigação legal, mas também uma estratégia de fortalecimento institucional. Para as pequenas empresas, em especial, trata-se de uma oportunidade de alinhar-se às exigências regulatórias, assegurar a integridade das informações e promover maior confiança junto a clientes, parceiros e ao mercado em geral.

3.14 APROVAÇÕES

Após a fase de levantamento de requisitos, foram elaborados protótipos funcionais da aplicação, com o objetivo de representar visualmente as funcionalidades previstas no sistema. Esses protótipos permitiram simular a navegação e a experiência do usuário, facilitando a compreensão da proposta por parte do cliente e demais envolvidos.

Os protótipos foram apresentados em reuniões de validação com o cliente, proporcionando um momento crucial para a análise da interface, dos fluxos de navegação e das funcionalidades planejadas. Esse processo teve como finalidade garantir que o desenvolvimento estivesse alinhado às expectativas e às necessidades reais do cliente. Com base no feedback recebido, foram realizados ajustes e melhorias, promovendo maior precisão no direcionamento do projeto e evitando retrabalho em fases posteriores.

Além das validações com o cliente, o projeto passou por três seminários acadêmicos ao longo do desenvolvimento, com apresentação parcial de resultados e

etapas concluídas. Cada seminário contou com a participação de bancas avaliadoras, que contribuíram com sugestões técnicas, observações metodológicas e críticas construtivas. Essas contribuições foram fundamentais para o aprimoramento contínuo do projeto.

O processo de orientação também foi essencial durante todas as etapas, com encontros frequentes entre o orientador e o discente para revisão das entregas, acompanhamento da evolução do sistema e orientação técnica e acadêmica. A soma das validações com o cliente, os seminários, as bancas e as orientações resultaram em um desenvolvimento mais sólido, alinhado aos requisitos propostos e fundamentado em boas práticas de engenharia de software.

4 ESTRATÉGIAS DE RISCO

4.1 LISTA DE RISCOS

Todo projeto de desenvolvimento de software está sujeito a riscos que podem comprometer seu andamento, sua viabilidade e, principalmente, a entrega de valor ao usuário final. No caso específico deste sistema, voltado à gestão de documentos e conformidade com a LGPD, é fundamental identificar e analisar os principais riscos que podem surgir durante o ciclo de vida do projeto. A antecipação desses riscos permite planejar ações preventivas, reduzir impactos negativos e garantir maior segurança no uso da solução.

A seguir, estão listados os principais riscos identificados:

1. Inserção de dados imprecisos: Usuários do sistema podem cadastrar documentos ou informações incorretas, o que compromete a conformidade com a LGPD e dificulta auditorias.
2. Interrupção na coleta de dados: a indisponibilidade de conexão com a internet nos dispositivos utilizados pode ocasionar falhas na captura e no registro das informações, comprometendo a continuidade e a confiabilidade dos dados armazenados no sistema.
3. Software não otimizado: Um software com falhas de desempenho afeta diretamente a experiência do usuário, podendo ser um fator decisivo na escolha por soluções concorrentes.
4. Baixa participação de usuários: Um mercado saturado, o software incompleto ou concorrentes mais baratos e com mais funcionalidades podem reduzir a adesão de usuários.
5. Mercado consolidado: Entrar em um mercado já dominado por soluções reconhecidas pode dificultar a aceitação do sistema, caso ele não ofereça diferenciais claros em funcionalidades ou preço.
6. Servidor não suportar acessos simultâneos: Em cenários de muitos acessos, o servidor pode não suportar a carga, resultando em lentidão ou indisponibilidade do sistema.
7. Tecnologia perder o suporte: Há risco de que tecnologias utilizadas se tornem obsoletas, mudem suas políticas de uso ou passem a cobrar por recursos antes gratuitos.

8. Internet indisponível: Como o sistema depende de conectividade, a falta de internet inviabiliza o uso adequado durante períodos offline.
9. Invasão e vazamento de dados: Vulnerabilidades de segurança ou ataques direcionados podem resultar em acesso indevido às informações, com sérias consequências legais e financeiras.
10. Projeto atrasar: Falhas no planejamento ou imprevistos técnicos podem estender o cronograma além do previsto.
11. Custos acima do previsto: Despesas adicionais não previstas podem surgir durante o desenvolvimento ou manutenção, comprometendo o orçamento.
12. Falha de integração com outros sistemas: Problemas de compatibilidade podem prejudicar a comunicação entre a solução e plataformas externas, afetando a automação e o fluxo de informações.
13. Perda de dados durante migração: A transferência de dados de sistemas anteriores para o novo pode falhar, gerando perda de informações importantes e até prejuízos irreparáveis.
14. Capacitação insuficiente dos usuários: A falta de treinamento adequado pode limitar o uso do sistema, levando a erros recorrentes e reduzindo a eficiência da operação.
15. Dependência de fornecedor externo: O uso de recursos ou serviços de terceiros pode tornar o sistema vulnerável a mudanças externas de contrato, suporte ou custos.

4.2 PRIORIZAÇÃO DOS RISCOS

Para a elaboração da matriz de riscos, foi realizada uma reunião entre os integrantes do projeto, na qual foram identificados e discutidos os principais riscos associados ao desenvolvimento e à utilização do sistema. Cada participante atribuiu, de forma individual, uma estimativa de probabilidade de ocorrência e o respectivo impacto de cada risco, permitindo a construção de uma média para fins de priorização e análise.

4.3 PLANOS DE MITIGAÇÃO

Ao longo da análise de riscos do projeto, foram identificadas diversas situações que podem comprometer o desempenho, a adesão dos usuários e a conformidade legal do sistema. Diante disso, torna-se essencial estabelecer planos de mitigação para reduzir a probabilidade de ocorrência desses riscos ou minimizar seus impactos caso aconteçam. A seguir, apresentam-se os principais riscos levantados e as respectivas estratégias de mitigação:

1. Inserção de dados imprecisos: Implementar validações nos formulários, avisos de confirmação e revisão de dados.
2. Interrupção na coleta de dados**:** para mitigar esse risco, recomenda-se implementar mecanismos de armazenamento temporário das informações em modo offline, permitindo que os dados sejam registrados localmente e sincronizados automaticamente com o sistema assim que a conexão à internet for restabelecida. Além disso, a utilização de provedores de internet redundantes ou conexões alternativas pode aumentar a disponibilidade e reduzir a probabilidade de falhas prolongadas.
3. Software não otimizado: Testes de desempenho e melhorias contínuas na performance do sistema.
4. Baixa participação dos usuários: Divulgar os benefícios do sistema, como rastreabilidade e conformidade com a LGPD.
5. Mudanças na legislação: Acompanhamento contínuo das atualizações legais e manutenções programadas no sistema.
6. Servidor não suportar acessos simultâneos: Uso de servidores em nuvem com escalabilidade automática.
7. Tecnologia perder suporte: Priorizar tecnologias com comunidade ativa e suporte de longo prazo.
8. Internet indisponível: Adotar armazenamento temporário local com sincronização posterior.
9. Invasão e vazamento de dados: Implementar criptografia, autenticação forte e política de segurança da informação.
10. Projeto atrasar: Aplicar metodologias ágeis com entregas incrementais e acompanhamento constante.

11. Custos acima do previsto: Monitorar orçamento regularmente e manter reserva financeira para imprevistos.
12. Falha de integração com outros sistemas: Realizar testes de integração antecipados e usar APIs padronizadas.
13. Perda de dados durante migração: Fazer backup completo antes da migração e testes em ambiente controlado.
14. Capacitação insuficiente dos usuários: Desenvolver treinamentos práticos, materiais de apoio e reciclagens periódicas.
15. Dependência de fornecedor externo: Firmar contratos claros, prever SLA e manter plano de contingência para suporte alternativo.

4.4 PLANOS DE CONTINGÊNCIA

Os planos de contingência têm como objetivo estabelecer medidas específicas a serem executadas caso os riscos identificados se concretizem, garantindo a continuidade das operações do sistema, minimizando impactos negativos e assegurando conformidade com a legislação vigente, em especial a LGPD.

1. Inserção de dados imprecisos: Permitir a revisão e correção de informações por usuários autorizados, mantendo um registro detalhado de todas as alterações realizadas. Essa medida garante a rastreabilidade e reduz o impacto de erros no banco de dados, preservando a confiabilidade das informações.
2. Interrupção na coleta de dados: Em caso de falha de conexão, os dados serão armazenados localmente em modo offline e sincronizados automaticamente quando a internet for restabelecida. Como alternativa, poderá ser utilizada conexão móvel para garantir a continuidade do processo.
3. Software não otimizado: Coletar feedback contínuo dos usuários sobre desempenho, executar ajustes corretivos e aplicar melhorias de performance. Essa ação busca manter o sistema funcional, eficiente e confiável, mesmo diante de falhas de performance.
4. Baixa participação dos usuários: Implementar ações de incentivo, como reconhecimento interno, notificações periódicas e melhorias na interface para facilitar a navegação. Essas medidas aumentam o engajamento e garantem que os usuários participem ativamente do sistema.

5. Mudanças na legislação: Manter a equipe técnica preparada para implementar alterações rápidas, atualizando o sistema conforme novas exigências legais. Também é importante comunicar de forma imediata os usuários sobre mudanças que impactem processos ou regras internas.
6. Sobrecarga do servidor: Ativar recursos emergenciais, como servidores auxiliares ou balanceamento de carga, garantindo que o sistema continue disponível e funcionando normalmente mesmo em picos de acesso.
7. Obsolescência tecnológica: Planejar a migração para tecnologias substitutas antes que o suporte das atuais seja descontinuado, assegurando compatibilidade e continuidade operacional, sem interrupção das atividades.
8. Indisponibilidade de internet: Habilitar modo offline seguro, com cache temporário dos dados, permitindo que o usuário continue operando normalmente. Os dados são sincronizados automaticamente assim que a conexão é restabelecida, garantindo integridade e continuidade das informações.
9. Invasão e vazamento de dados: Acionar imediatamente os protocolos de resposta a incidentes, realizar análise forense detalhada, comunicar autoridades competentes e informar os usuários afetados conforme exige a LGPD. Além disso, reforçar medidas de segurança para prevenir novos incidentes.
10. Atraso no cronograma do projeto: Replanejar atividades, redefinir prioridades e ajustar prazos das entregas críticas. Essa ação busca minimizar o impacto do atraso e garantir que os objetivos essenciais do projeto sejam cumpridos.
11. Erro na integração com outros sistemas: Implementar processos de verificação e validação contínua da integração, permitindo a identificação rápida de inconsistências e correções imediatas, garantindo a continuidade das operações entre sistemas.
12. Perda de dados por falha do banco: Restaurar informações a partir de backups regulares, realizar monitoramento contínuo da integridade dos dados e implementar medidas preventivas adicionais, evitando perdas significativas e interrupções das operações.
13. Falha de autenticação ou segurança: Aplicar bloqueios temporários, revisar permissões e reforçar medidas de proteção de acesso, garantindo que apenas

usuários autorizados possam operar o sistema e protegendo dados sensíveis de acessos indevidos.

14. Problemas de compatibilidade de dispositivos: Disponibilizar ajustes de software, alternativas de acesso ou versões compatíveis com diferentes dispositivos, garantindo que todos os usuários consigam utilizar o sistema de forma eficiente, independentemente do equipamento.
15. Resistência à mudança por parte dos usuários: Promover comunicação direcionada, treinamento personalizado, suporte contínuo e acompanhamento próximo dos usuários, facilitando a adaptação às novas funcionalidades e garantindo o uso correto do sistema.

5 GERENCIAMENTO DE CONFIGURAÇÃO

Para o versionamento e gerenciamento do projeto, estão sendo utilizados o Git e GitHub.

5.1 PLANO DE GERENCIAMENTO DE CONFIGURAÇÃO

O gerenciamento de configuração do projeto Camaleão tem como objetivo garantir o controle, a organização e a rastreabilidade de todas as modificações realizadas ao longo do desenvolvimento, assegurando que cada entrega seja devidamente documentada e validada antes de sua disponibilização. Para isso, foram adotadas práticas de controle de versão e acompanhamento de tarefas que mantiveram a consistência entre os módulos Web, Backend e Aplicativo Mobile.

GitHub foi utilizado como repositório central do código-fonte, permitindo versionamento e colaboração estruturada entre os membros da equipe. A organização do desenvolvimento ocorreu por meio de branches específicas, como main para a versão estável, feature/ para novas funcionalidades e fix/ para correções, garantindo que implementações fossem desenvolvidas de forma isolada antes da integração ao projeto principal. Todas as alterações passaram por pull requests, possibilitando validação prévia, revisão de código e registro das justificativas das modificações. Também foi adotado um padrão de mensagens de commit para facilitar o entendimento histórico da evolução do sistema.

Paralelamente, o Trello foi utilizado para o gerenciamento visual das atividades, permitindo acompanhar o progresso em tempo real. O quadro foi estruturado em etapas que representavam o fluxo de trabalho, passando de “A Fazer” para “Em Progresso”, “Aguardando Validação” e “Concluído”. Cada cartão representava uma atividade ou entrega, contendo descrição, responsáveis, prazos, checklists e comentários de acompanhamento. As etiquetas foram empregadas para classificar o tipo de tarefa — como desenvolvimento, documentação ou testes — tornando o processo mais transparente e organizado.

A integração entre GitHub e Trello permitiu alinhamento contínuo da equipe quanto ao que estava sendo desenvolvido, testado e entregue, evitando retrabalhos e assegurando a rastreabilidade das decisões. Dessa forma, o gerenciamento de configuração contribuiu para a evolução controlada do projeto, preservando a

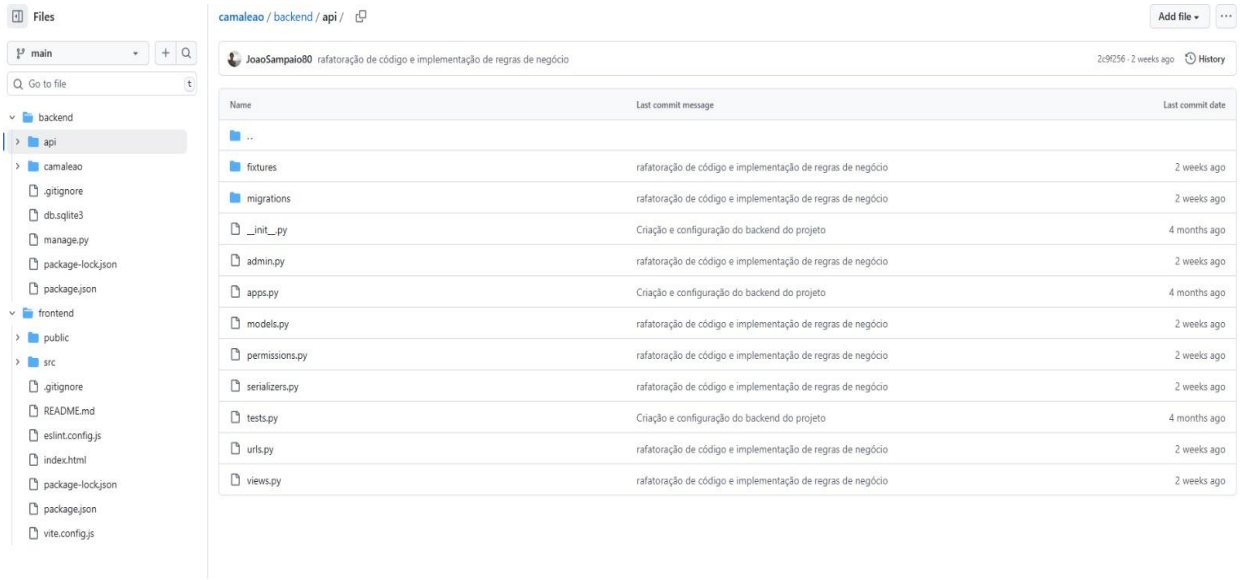
integridade do código e garantindo consistência nas entregas durante todas as etapas do TCC.

5.2 REPOSITÓRIO

No desenvolvimento do sistema voltado à gestão da conformidade com a LGPD, utilizou-se a plataforma GitHub como principal ferramenta de versionamento e colaboração. O ambiente, baseado no sistema de controle de versões Git, possibilitou armazenar, gerenciar e acompanhar a evolução do código-fonte de maneira organizada e segura. Cada alteração realizada no projeto foi registrada, permitindo rastrear modificações, identificar eventuais falhas e reverter para versões anteriores sempre que necessário.

Além disso, o uso do GitHub favoreceu a integração contínua entre os desenvolvedores e proporcionou um processo de trabalho mais estruturado, aumentando a confiabilidade do sistema e a transparência do seu histórico de alterações. Esses aspectos se mostraram essenciais para um projeto que envolve requisitos de segurança, governança e rastreabilidade, características fundamentais em iniciativas relacionadas à conformidade com a legislação de proteção de dados.

Figura 43: Github



Fonte: Elaboração Própria

6 ESTRATÉGIA DE TESTES

A estratégia de testes adotada no desenvolvimento do sistema buscou garantir sua confiabilidade e conformidade com a LGPD. Foram realizados testes unitários, para validar o funcionamento de componentes isolados, e testes de integração, assegurando a comunicação correta entre os módulos. Também foram aplicados testes funcionais e de usabilidade, a fim de verificar se as funcionalidades atendiam aos requisitos e se a interface oferecia boa experiência ao usuário. Por fim, considerando a natureza sensível dos dados tratados, foram conduzidos testes de segurança, voltados à prevenção de falhas e acessos indevidos. Essa abordagem contribuiu para a entrega de uma aplicação robusta e alinhada às boas práticas de proteção de dados.

6.1 TESTES DE UNIDADE AUTOMATIZADOS

O capítulo de testes apresenta de forma detalhada os procedimentos realizados na aplicação desenvolvida, descrevendo os métodos adotados, os resultados esperados e as condições necessárias para a execução adequada de cada teste. O objetivo foi validar o correto funcionamento das funcionalidades propostas, assegurando que o sistema atenda aos requisitos de conformidade com a LGPD.

A seguir, são apresentadas as tabelas que descrevem os requisitos de hardware, software e pessoas envolvidos no processo de testes.

Tabela 2: Necessidade de Hardware

Tipo de Hardware	Detalhamento	Forma de Disponibilização	Data Limite
Smartphone	Android 8 ou superior	Pessoal	15/08/2025
Computador	Windows 10 ou superior	Pessoal	15/08/2025

Fonte: Elaboração Própria

Tabela 3: Necessidade de Software

Tipo de Software	Detalhamento	Forma de Disponibilização	Data Limite

Navegador Web	Google Chrome, versão 127 ou superior	Pessoal	15/08/2025
Navegador Web	Mozilla Firefox, versão 129 ou superior	Pessoal	15/08/2025
Navegador Web	Microsoft Edge, versão 127 ou superior	Pessoal	15/08/2025
Navegador Web	Opera, versão 112 ou superior	Pessoal	15/08/2025

Fonte: Elaboração Própria

Tabela 4: Necessidade de Pessoas

Papel	Envolvimento Estimado	Período de Envolvimento no Projeto
João Sampaio (Web)	25 horas	14/08/2025 a 12/09/2025
Ana Cristina (Mobile)	20 horas	14/08/2025 a 12/09/2025
Anna Clara (Doc)	30 Horas	14/08/2025 a 12/09/2025

Fonte: Elaboração Própria

6.2 TESTES DE VALIDAÇÃO

Abaixo está a lista dos testes realizados na aplicação, descrevendo os métodos utilizados e apresentando os resultados esperados e as necessidades primárias atendidas para que os testes ocorram como planejado.

Tabela 5: Lista de Testes

Caso de Uso/Requisito	Tipo de Teste	Caso de Teste	Ator
Cadastro de usuário	Funcional	CT001	Usuário
Cadastro de DPO	Funcional	CT002	Admin
Login de usuário	Segurança	CT003	Usuário
Login de administrador	Segurança	CT004	Admin
Recuperação de senha	Segurança	CT005	Usuário
Exibir Dashboard	Funcional	CT006	Usuário
Cadastrar atividade	Funcional	CT007	Usuário
Editar atividade	Funcional	CT008	Usuário
Excluir atividade	Funcional	CT009	Usuário

Visualizar atividade	Funcional	CT010	Usuário
Checklist – incluir item	Funcional	CT011	Admin
Checklist – marcar item concluído	Funcional	CT012	Usuário
Inventário – cadastrar processo	Funcional	CT013	Usuário
Inventário – editar processo	Funcional	CT014	Usuário
Inventário – excluir processo	Funcional	CT015	Usuário
Inventário – exportar relatório	Funcional	CT016	Admin
Matriz de Risco – cadastrar risco	Funcional	CT017	Usuário
Matriz de Risco – editar risco	Funcional	CT018	Usuário
Matriz de Risco – excluir risco	Funcional	CT019	Usuário
Matriz de Risco – heatmap	Funcional	CT020	Admin
Matriz de Risco – plano de ação	Funcional	CT021	Usuário
Usuários – cadastrar administrador	Funcional	CT022	Admin
Usuários – cadastrar gerente	Funcional	CT023	Admin
Usuários – editar usuário	Funcional	CT024	Admin
Usuários – excluir usuário	Funcional	CT025	Admin
Configurações – alterar senha	Segurança	CT026	Usuário
Configurações – alterar tema	Usabilidade	CT027	Usuário
Configurações – editar perfil	Funcional	CT028	Usuário
Logout – usuário	Segurança	CT029	Usuário

Fonte: Elaboração Própria

6.2.1 Teste Web

A seguir, são apresentados os testes realizados na aplicação web, descrevendo os métodos utilizados, os resultados esperados e as necessidades primárias que devem ser atendidas para que os testes ocorram conforme o planejado.

Tabela 6: Caso de teste CT001

Caso Nº	CT001
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se o sistema realiza o cadastro de usuários corretamente.
Entradas	Nome, E-mail, Senha, Telefone
Passos	1. Acessar tela de cadastro. 2. Preencher todos os campos obrigatórios. 3. Clicar em ‘Cadastrar’. 4. Aguardar mensagem de confirmação.
Comportamento Esperado	Usuário cadastrado com sucesso.

Fonte: Elaboração Própria

Tabela 7: Caso de teste CT002

Caso Nº	CT002

Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se o sistema realiza o cadastro de DPO corretamente.
Entradas	Nome, E-mail, Tipo de Usuário
Passos	1. Acessar tela de cadastro. 2. Preencher todos os campos obrigatórios. 3. Clicar em ‘Cadastrar’. 4. Aguardar mensagem de confirmação.
Comportamento Esperado	DPO cadastrado com sucesso e exibido na tela de Cadastro.

Fonte: Elaboração Própria

Tabela 8: Caso de teste CT003

Caso Nº	CT003
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Verificar autenticação de login de usuário.
Entradas	E-mail e senha válidos
Passos	1. Acessar tela de login. 2. Inserir credenciais válidas. 3. Clicar em 'Entrar'. 4. Aguardar redirecionamento.
Comportamento Esperado	Usuário autenticado e redirecionado a tela principal.

Fonte: Elaboração Própria

Tabela 9: Caso de Teste CT004

Caso Nº	CT004
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Verificar login de administrador com credenciais válidas.
Entradas	E-mail e senha de administrador
Passos	1. Acessar tela de login. 2. Inserir credenciais do administrador. 3. Clicar em 'Entrar'. 4. Aguardar redirecionamento.
Comportamento Esperado	Usuário autenticado e redirecionado a tela principal.

Fonte: Elaboração Própria

Tabela 10: Caso de Teste CT005

Caso Nº	CT005
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Verificar recuperação de senha.
Entradas	E-mail cadastrado
Passos	1. Acessar tela de login. 2. Clicar em 'Esqueceu a senha'. 3. Informar e-mail válido. 4. Confirmar solicitação. 5. Verificar recebimento do link no e-mail.

Comportamento Esperado	Sistema envia link seguro de redefinição de senha, válido por 72h.

Fonte: Elaboração Própria

Tabela 11: Caso de Teste CT006

Caso Nº	CT006
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar se o usuário consegue acessar o dashboard e visualizar os indicadores.
Entradas	Credenciais de login válidas.
Passos	1. Acessar a tela inicial do sistema no navegador. 2. Informar o e-mail de login no campo correspondente. 3. Informar a senha no campo de senha. 4. Clicar no botão Entrar. 5. Aguardar a validação do sistema e o carregamento da área logada. 6. No menu, clicar na opção Dashboard. 7. Verificar a tela do dashboard carregada.
Comportamento Esperado	O sistema deve exibir corretamente o dashboard com checklist, inventário, riscos e alertas.

Fonte: Elaboração Própria

Tabela 12: Caso de Teste CT007

Caso Nº	CT007
Data	16/09/2025
Testador	Anna
Objetivo do Teste	Validar cadastro de uma nova atividade de tratamento.
Entradas	Descrição da atividade, base legal, evidências.
Passos	1. Acessar o sistema. 2. Inserir login e senha válidos. 3. Clicar em 'Entrar'. 4. Acessar menu ‘Documentos’. 5. Clicar em 'Novo’. 6. Preencher descrição. 7. Selecionar base legal. 8. Adicionar evidências. 9. Conferir dados. 10. Clicar em ‘Criar’. 11. Verificar mensagem de confirmação.
Comportamento Esperado	Atividade cadastrada e exibida na listagem.

Tabela 13: Caso de Teste CT008

Caso Nº	CT008
Data	16/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar edição de atividade existente.
Entradas	Descrição da atividade já cadastrada, novos dados.

Passos	1. Logar no sistema. 2. Acessar menu 'Atividades'. 3. Selecionar atividade existente. 4. Clicar em 'Editar'. 5. Alterar campos necessários. 6. Clicar em 'Salvar Alterações'. 7. Confirmar mensagem de atualização.
Comportamento Esperado	Atividade alterada e exibida na listagem atualizada.

Fonte: Elaboração Própria

Tabela 14: Caso de Teste CT009

Caso Nº	CT009
Data	17/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar exclusão de atividade.
Entradas	Atividade existente.
Passos	1. Logar no sistema. 2. Acessar menu 'Atividades'. 3. Selecionar atividade existente. 4. Clicar em 'Excluir'. 5. Confirmar exclusão. 6. Verificar mensagem do sistema.
Comportamento Esperado	Atividade removida e não deve mais aparecer na listagem.

Fonte: Elaboração Própria

Tabela 15:Caso de Teste CT010

Caso Nº	CT010
Data	17/09/2025
Testador	Anna
Objetivo do Teste	Validar visualização de atividade.
Entradas	Atividade cadastrada.
Passos	1. Logar no sistema. 2. Acessar menu 'Atividades'. 3. Verificar exibição completa das atividades.
Comportamento Esperado	Sistema exibe todas as atividades existentes.

Fonte: Elaboração Própria

Tabela 16: Caso de Teste CT011

Caso Nº	CT011
Data	17/09/2025
Testador	Anna
Objetivo do Teste	Validar inclusão de item no checklist.
Entradas	Descrição do item de checklist.
Passos	1. Logar no sistema. 2. Acessar menu 'Checklist'. 3. Clicar em 'Novo’. 4. Preencher descrição do item. 5. Clicar em ‘Criar’. 6. Confirmar mensagem do sistema.

Comportamento Esperado	Item de checklist incluído e visível na lista.

Fonte: Elaboração Própria

Tabela 17: Caso de Teste CT012

Caso Nº	CT012
Data	17/09/2025
Testador	Anna
Objetivo do Teste	Validar marcação de item de checklist como concluído.
Entradas	Item de checklist existente.
Passos	1. Logar no sistema. 2. Acessar menu 'Checklist'. 3. Selecionar item pendente. 4. Marcar como concluído.
Comportamento Esperado	Item deve aparecer como concluído no checklist.

Fonte: Elaboração Própria

Tabela 18: Caso de Teste CT013

Caso Nº	CT013
Data	17/09/2025
Testador	Anna
Objetivo do Teste	Validar cadastro de processo no inventário de dados.
Entradas	Nome do processo, setor, base legal.
Passos	1. Logar no sistema. 2. Acessar menu 'Inventário de Dados'. 3. Preencher informações obrigatórias 4. Confirmar mensagem do sistema.
Comportamento Esperado	Processo cadastrado e listado no inventário.

Fonte: Elaboração Própria

Tabela 19: Caso de Teste CT014

Caso Nº	CT014
Data	17/09/2025
Testador	Anna
Objetivo do Teste	Validar edição de processo do inventário.
Entradas	Processo existente, novos dados.
Passos	1. Logar no sistema. 2. Acessar menu ‘Lista Inventário'. 3. Selecionar processo existente. 4. Clicar em 'Editar'. 5. Alterar informações necessárias. 6. Clicar em 'Salvar Alterações'. 7. Confirmar mensagem de atualização.
Comportamento Esperado	Processo alterado e exibido atualizado no inventário.

Fonte: Elaboração Própria

Tabela 20: Caso de Teste CT015

Caso Nº	CT015
Data	17/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar exclusão de processo do inventário.

Entradas	Processo existente.
Passos	1. Logar no sistema. 2. Acessar menu ‘Lista Inventário'. 3. Selecionar processo existente. 4. Clicar em 'Excluir'. 5. Confirmar ação. 6. Verificar mensagem do sistema.
Comportamento Esperado	Processo removido e não deve mais aparecer no inventário.

Fonte: Elaboração Própria

Tabela 21: Tabela 21: Caso de Teste CT016

Caso Nº	CT016
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Exportar Relatório
Entradas	Processo existente.
Passos	1. Logar no sistema. 2. Acessar o menu Inventário de Dados. 3. Verificar se há processos cadastrados. 4. Clicar em Exportar no formato desejado (PDF, XLSX, CSV). 5. Abrir o arquivo gerado.
Comportamento Esperado	O sistema deve gerar um relatório fiel aos dados cadastrados no inventário.

Fonte: Elaboração Própria

Tabela 22: Tabela 21: Caso de Teste CT017

Caso Nº	CT017
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar inclusão de um novo risco na matriz de risco.
Entradas	Descrição do risco, impacto, probabilidade.
Passos	1. Logar no sistema. 2. Acessar menu Matriz de Risco. 3. Clicar em Novo. 4. Preencher informações obrigatórias 5. Clicar em Salvar Risco.
Comportamento Esperado	O risco deve ser classificado automaticamente e exibido na matriz.

Fonte: Elaboração Própria

Tabela 23: Tabela 21: Caso de Teste CT018

Caso Nº	CT018
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar edição de risco existente.
Entradas	Risco previamente cadastrado, novos valores de impacto/probabilidade

Passos	1. Logar no sistema. 2. Acessar Matriz de Risco. 3. Selecionar risco existente. 4. Clicar em Editar. 5. Alterar os valores necessários. 6. Confirmar a edição.
Comportamento Esperado	O sistema deve atualizar o risco e recalcular a pontuação.

Fonte: Elaboração Própria

Tabela 24: Tabela 21: Caso de Teste CT019

Caso Nº	CT019
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar exclusão de risco na matriz.
Entradas	Risco previamente cadastrado.
Passos	1. Logar no sistema. 2. Acessar Matriz de Risco. 3. Selecionar risco cadastrado. 4. Clicar em Excluir. 5. Confirmar ação.
Comportamento Esperado	O risco deve ser removido da matriz e da listagem.

Fonte: Elaboração Própria

Tabela 25: Caso de Teste CT020

Caso Nº	CT020
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar se o heatmap exibe os riscos cadastrados.
Entradas	Matriz com múltiplos riscos cadastrados.
Passos	1. Logar no sistema. 2. Acessar Matriz de Risco. 3. Selecionar a aba Heatmap. 4. Visualizar os riscos posicionados no gráfico.
Comportamento Esperado	O sistema deve exibir heatmap com riscos classificados por cores e níveis.

Fonte: Elaboração Própria

Tabela 26: Caso de Teste CT021

Caso Nº	CT021
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar inclusão de plano de ação vinculado a risco.
Entradas	Estratégia de mitigação, responsável, prazo.
Passos	1. Logar no sistema. 2. Acessar Matriz de Risco. 3. Selecionar Controle de Plano de Ação. 4. Clicar em Incluir Complemento. 5. Preencher os campos obrigatórios. 6. Clicar em Salvar.
Comportamento Esperado	O plano de ação deve ser salvo e vinculado ao risco selecionado.

Fonte: Elaboração Própria

Tabela 27: Caso de Teste CT022

Caso Nº	CT022
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar cadastro de um novo usuário com papel de administrador.
Entradas	Nome completo, e-mail válido, senha forte, papel = administrador.
Passos	1. Logar no sistema como administrador. 2. Acessar menu. 3. Clicar em **Cadastrar Usuário**. 4. Preencher o campo **E-mail** com endereço válido. 5. Preencher o campo **Nome**. 6. Criar senha conforme requisitos de segurança. 7. Selecionar papel **Administrador**. 8. Clicar em **Cadastrar**.
Comportamento Esperado	O sistema deve cadastrar o administrador e listá-lo na tabela de usuários.

Fonte: Elaboração Própria

Tabela 28: Caso de Teste CT023

Caso Nº	CT023
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar cadastro de usuário com papel de gerente.
Entradas	Nome completo, e-mail válido, senha forte, papel = gerente.
Passos	1. Logar no sistema. 2. Acessar menu Usuários. 3. Clicar em Cadastrar Usuário. 4. Preencher nome e e-mail. 5. Definir senha. 6. Selecionar papel Gerente. 7. Clicar em **Cadastrar**.
Comportamento Esperado	O sistema cadastra o gerente e o exibe na lista de usuários.

Fonte: Elaboração Própria

Tabela 29: Caso de Teste CT024

Caso Nº	CT024
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar edição de dados de um usuário existente.
Entradas	Usuário cadastrado previamente, novos dados (telefone, papel, senha).
Passos	1. Logar como administrador. 2. Acessar meu perfil. 3. Clicar em Editar. 4. Alterar os campos desejados. 6. Clicar em Salvar Alterações.
Comportamento Esperado	O sistema atualiza os dados do usuário e exibe mensagem de confirmação.

Fonte: Elaboração Própria

Tabela 30: Caso de Teste CT025

Caso Nº	CT025
Data	24/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar exclusão de usuário cadastrado.
Entradas	Usuário existente.
Passos	1. Logar como administrador. 2. Acessar menu Cadastro de Usuários. 3. Selecionar usuário na listagem. 4. Clicar em Excluir. 5. Confirmar ação.
Comportamento Esperado	O sistema remove o usuário e atualiza a listagem.

Fonte: Elaboração Própria

Tabela 31: Caso de Teste CT026

Caso Nº	CT026
Data	26/09/2025
Testador	Anna Clara
Objetivo do Teste	Validar alteração de senha pelo usuário.
Entradas	Senha atual, nova senha.
Passos	1.Logar no sistema. 2.Acessar menu **Meu Perfil**. 3.Selecionar opção **editar**. 4.Informar senha atual. 5.Informar nova senha. 6.Confirmar alteração.
Comportamento Esperado	Sistema deve gerar notificação de incidente e registrá-lo no log.

Fonte: Elaboração Própria

Tabela 32: Caso de Teste CT027

Caso Nº	CT027
Data	03/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar logout de usuário comum.
Entradas	Sessão ativa de usuário.
Passos	1. Logar no sistema como usuário. 2. Navegar pelo sistema. 3. Clicar em Logout.
Comportamento Esperado	Sessão encerrada e redirecionamento para tela de login.

Fonte: Elaboração Própria

6.2.2 Teste Mobile

A seguir, são apresentados os testes realizados na aplicação mobile, descrevendo os métodos empregados, os resultados esperados e as condições necessárias para que os testes sejam executados conforme o planejado.

Caso de Uso/Requisito	Tipo de Teste	Caso de Teste	Ator
Login de usuário	Segurança	CT028	Usuário
Recuperação de senha	Segurança	CT049	Usuário
Exibir tela inicial (Home)	Funcional	CT030	Usuário
Acessar menu lateral	Funcional	CT031	Usuário
Exibir informações do DPO (Encarregado)	Funcional	CT032	Usuário
Visualizar perfil do usuário	Funcional	CT033	Usuário
Editar informações do perfil	Funcional	CT034	Usuário
Cadastrar novo usuário	Funcional	CT035	Admin
Exibir lista de usuários	Funcional	CT036	Admin
Exibir documentos	Funcional	CT037	Usuário
Cadastrar novo documento	Funcional	CT038	Admin
Exibir detalhes de documento (base legal, evidência, status)	Funcional	CT039	Usuário
Exibir notificações	Funcional	CT040	Usuário
Exibir checklist	Funcional	CT041	Usuário
Exibir matriz de risco	Funcional	CT042	Usuário
Exibir relatórios	Funcional	CT043	Admin
Exportar relatórios (PDF/Excel)	Funcional	CT043	Admin
Exibir inventário de dados	Funcional	CT044	Usuário
Cadastrar item de inventário	Funcional	CT045	Usuário

Tabela 33: Caso de Teste CT028

Caso Nº	CT028
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar o login de usuário no aplicativo mobile.
Entradas	E-mail e senha válidos de um usuário cadastrado.
Passos	1. Abrir o aplicativo. 2. Informar e-mail e senha. 3. Clicar em Entrar.
Comportamento Esperado	Sistema autêntica o usuário e redireciona para a tela inicial (Home).

Fonte: Elaboração Própria

Tabela 34: Caso de Teste CT029

Caso Nº	CT029
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar a recuperação de senha.

Entradas	E-mail válido de usuário existente.
Passos	1. Clicar em Esqueceu a senha?. 2. Informar o e-mail cadastrado. 3. Clicar em Enviar link.
Comportamento Esperado	Sistema envia um link de redefinição de senha para o e-mail informado.

Fonte: Elaboração Própria

Tabela 35: Caso de Teste CT030

Caso Nº	CT030
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar exibição da tela inicial (Home).
Entradas	Sessão ativa de usuário logado.
Passos	1. Logar no aplicativo. 2. Acessar a tela Home. 3. Verificar exibição dos ícones e módulos.
Comportamento Esperado	Todos os módulos são exibidos corretamente e funcionam ao toque.

Fonte: Elaboração Própria

Tabela 36: Caso de Teste CT031

Caso Nº	CT031
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar abertura e funcionamento do menu lateral.
Entradas	Sessão ativa.
Passos	1. Logar no aplicativo. 2. Abrir o menu lateral. 3. Acessar diferentes seções.
Comportamento Esperado	Menu lateral exibe todas as opções e redireciona corretamente.

Fonte: Elaboração Própria

Tabela 37: Caso de Teste CT032

Caso Nº	CT032
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar exibição dos dados do Encarregado (DPO).
Entradas	Sessão ativa e dados do DPO cadastrados no backend.
Passos	1. Logar no app. 2. Acessar a tela Encarregado.
Comportamento Esperado	As informações do DPO são exibidas corretamente (nome, e-mail, telefone e validade).

Fonte: Elaboração Própria

Tabela 38: Caso de Teste CT033

Caso Nº	CT033
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar o cadastro de novos usuários.

Entradas	Dados completos: e-mail, nome, sobrenome, senha e tipo de usuário.
Passos	1. Acessar Cadastro de Usuário. 2. Preencher todos os campos obrigatórios. 3. Clicar em Cadastrar.
Comportamento Esperado	Usuário é cadastrado e aparece na lista de usuários.

Fonte: Elaboração Própria

Tabela 39: Caso de Teste CT034

Caso Nº	CT034
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar exibição e atualização do perfil.
Entradas	Sessão ativa, dados de perfil válidos.
Passos	1. Acessar Meu Perfil. 2. Clicar em Editar. 3. Alterar informações e salvar.
Comportamento Esperado	Perfil atualizado e exibido corretamente com nova foto ou dados.

Fonte: Elaboração Própria

Tabela 40: Caso de Teste CT035

Caso Nº	CT035
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar se o administrador consegue cadastrar corretamente um novo usuário pelo aplicativo mobile.
Entradas	Usuário autenticado com perfil Admin e acesso à seção “Usuários”.
Passos	1. Acessar o menu lateral. 2. Selecionar “Usuários”. 3. Clicar no botão “+ Novo Usuário”. 4. Preencher os campos obrigatórios (Nome, E-mail, Função, Senha). 5. Clicar em “Salvar”.
Comportamento Esperado	O sistema exibe mensagem de sucesso e o novo usuário aparece na lista de usuários.

Tabela 41: Caso de Teste CT036

Caso Nº	CT036
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se o aplicativo exibe corretamente a lista de usuários cadastrados no sistema.
Entradas	Usuário autenticado com perfil Admin e acesso à seção “Usuários”.
Passos	1. Acessar o menu lateral. 2. Selecionar “Usuários”.

Comportamento Esperado	A lista de usuários é carregada, exibindo nome, e-mail, função e status de cada registro.

Fonte: Elaboração Própria

Tabela 42: Caso de Teste CT037

Caso Nº	CT037
Data	13/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar se o aplicativo exibe corretamente a lista de documentos cadastrados.
Entradas	Usuário autenticado e documentos previamente cadastrados no sistema.
Passos	1. Acessar o menu lateral. 2. Selecionar “Documentos”.

Fonte: Elaboração Própria

Tabela 43: Caso de Teste CT038

Caso Nº	CT038
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar se o usuário Admin consegue cadastrar corretamente um novo documento no aplicativo mobile.
Entradas	Usuário autenticado como Admin e com acesso à seção “Documentos”.
Passos	1. Acessar o menu lateral. 2. Selecionar “Documentos”. 3. Clicar em “+ Novo”. 4. Preencher os campos obrigatórios (Título, Categoria, Base Legal, Evidência, Data de Revisão). 5. Clicar em “Salvar”.
Comportamento Esperado	O sistema exibe mensagem de sucesso e o novo documento aparece na lista.

Fonte: Elaboração Própria

Tabela 44: Caso de Teste CT039

Caso Nº	CT039
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se os detalhes de um documento são exibidos corretamente ao selecioná-lo na lista.
Entradas	Usuário autenticado e documento existente.
Passos	1. Acessar “Documentos”. 2. Selecionar um documento na lista. 3. Visualizar as informações detalhadas.

Comportamento Esperado	O aplicativo exibe corretamente os campos de base legal, evidência, status e data de revisão.

Fonte: Elaboração Própria

Tabela 45: Caso de Teste CT040

Caso Nº	CT040
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Garantir que o aplicativo exiba corretamente as notificações relacionadas a prazos e documentos.
Entradas	Usuário autenticado e notificações ativas no sistema.
Passos	1. Acessar o menu lateral. 2. Selecionar “Notificações”.
Comportamento Esperado	A tela exibe todas as notificações disponíveis com título, mensagem e data de vencimento.

Fonte: Elaboração Própria

Tabela 46: Caso de Teste CT041

Caso Nº	CT041
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Garantir que o aplicativo exiba corretamente as notificações relacionadas a prazos e documentos.
Entradas	Usuário autenticado e notificações ativas no sistema.
Passos	1. Acessar o menu lateral. 2. Selecionar “Notificações”.
Comportamento Esperado	A tela exibe todas as notificações disponíveis com título, mensagem e data de vencimento.

Fonte: Elaboração Própria

Tabela 47: Caso de Teste CT042

Caso Nº	CT042
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar se a matriz de risco é carregada corretamente, exibindo todos os registros cadastrados.
Entradas	Usuário autenticado e matriz de risco existente no sistema.
Passos	1. Acessar o menu lateral. 2. Selecionar “Matriz de Risco”.
Comportamento Esperado	A matriz é exibida com colunas de probabilidade, impacto, risco total e status residual.

Fonte: Elaboração Própria

Tabela 48: Caso de Teste CT043

Caso Nº	CT043
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se os relatórios de conformidade e risco são exibidos corretamente.

Entradas	Usuário autenticado com relatórios disponíveis no sistema.
Passos	1. Acessar o menu lateral. 2. Selecionar “Relatórios”.
Comportamento Esperado	O aplicativo apresenta a lista de relatórios disponíveis, com nome, tipo e data de geração.

Fonte: Elaboração Própria

Tabela 49: Caso de Teste CT044

Caso Nº	CT044
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar a exportação de relatórios em formatos PDF e Excel pelo aplicativo mobile.
Entradas	Usuário autenticado, relatórios existentes e permissões de exportação habilitadas.
Passos	1. Acessar “Relatórios”. 2. Selecionar um relatório. 3. Tocar em “Exportar”. 4. Escolher formato (PDF ou Excel).
Comportamento Esperado	O sistema gera o arquivo no formato escolhido e disponibiliza o download ou visualização.

Fonte: Elaboração Própria

Tabela 50: Caso de Teste CT045

Caso Nº	CT045
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Verificar se o inventário de dados é exibido corretamente com todas as entradas registradas.
Entradas	Usuário autenticado e inventário de dados existente.
Passos	1. Acessar o menu lateral. 2. Selecionar “Inventário de Dados”.
Comportamento Esperado	O aplicativo exibe lista com processos, titulares, categorias, base legal e status de cada item.

Fonte: Elaboração Própria

Tabela 51: Caso de Teste CT046

Caso Nº	CT046
Data	27/10/2025
Testador	Anna Clara
Objetivo do Teste	Validar o cadastro de um novo item no inventário de dados via aplicativo mobile.
Entradas	Usuário autenticado como Admin e com acesso à seção de inventário.
Passos	1. Acessar “Inventário de Dados”. 2. Tocar em “+ Novo”. 3. Preencher os campos obrigatórios (Processo, Categoria, Titular, Base Legal, Controlador, Operador, etc.). 4. Clicar em “Salvar”.
Comportamento Esperado	O sistema exibe mensagem de sucesso e o novo item é listado no inventário.

Fonte: Elaboração Própria

7 ESTRATÉGIA DE IMPLANTAÇÃO E SUPORTE

Neste capítulo, serão descritas as necessidades essenciais para a implantação do sistema, garantindo seu funcionamento adequado e eficiente. Para que o sistema atenda às expectativas de performance e qualidade, é necessário decidir como será feita a arquitetura de implantação, a configuração dos servidores, a configuração dos clientes, a infraestrutura necessária e definir um cronograma de treinamentos.

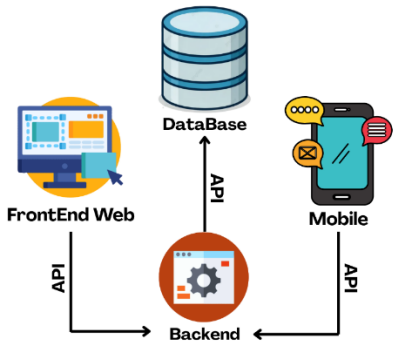
7.1 NECESSIDADES DE IMPLANTAÇÃO

Neste capítulo, são descritas as necessidades essenciais para a implantação do sistema Camaleão, garantindo seu funcionamento adequado, seguro e eficiente. O processo de implantação busca assegurar que a plataforma opere de forma integrada entre os ambientes web e mobile, atendendo aos requisitos de desempenho e qualidade esperados, além de promover a conformidade com os princípios da LGPD.

7.1.1 Arquitetura de implantação

A arquitetura de implantação do sistema Camaleão foi estruturada para integrar os módulos web e mobile de forma segura, escalável e eficiente. O modelo apresentado a seguir demonstra a relação entre os principais componentes da aplicação, incluindo o frontend, o backend, o banco de dados e os serviços externos que dão suporte à operação e manutenção do sistema.

Figura 44: Arquitetura de Implantação



Fonte: Elaboração Própria

7.1.2 Configuração dos servidores

A configuração dos servidores do sistema Camaleão foi planejada para garantir estabilidade, segurança e desempenho durante o processamento das informações. O ambiente de hospedagem contempla os componentes necessários para a execução dos serviços de backend, armazenamento de dados e comunicação entre as plataformas web e mobile, assegurando a integridade e a disponibilidade contínua da aplicação.

Tabela 52: : Configuração do Servidor

Componente	Especificação Recomendada para o Sistema Camaleão
Processador	4 vCPUs (Intel Xeon ou AMD EPYC) a 3,0 GHz
Memória RAM	8 GB DDR4
Disco Rígido (SSD)	80 GB (armazenamento de dados, logs e mídia)
Sistema Operacional	Ubuntu Server 24.04 LTS (64 bits) ou Windows Server 2022 Standard (64 bits)
Servidor Web	Nginx + Gunicorn (Ubuntu) / IIS 10 + Waitress (Windows)
Banco de Dados	PostgreSQL 16.x
Certificado SSL	Let’s Encrypt (HTTPS habilitado)
Gerenciador de Processos	systemd (Ubuntu) / NSSM (Windows)

Fonte: Elaboração Própria

Tabela 53: Limitações do Plano de Hospedagem

Recurso	Descrição / Limite Configurado
Armazenamento	100 GB SSD
Transferência	Ilimitada
Domínios	1 domínio principal (ex: camaleao.app.br)
Backup	Automático diário (dump PostgreSQL + mídia)
Subdomínios	Ilimitados (ex: api.camaleao.app.br, admin.camaleao.app.br)
Contas FTP	1 (usada apenas para deploy de build estático do React)
Banco de Dados	1 banco PostgreSQL principal + 1 banco de testes
SSH / Acesso remoto	Ubuntu: acesso root via SSH | Windows: acesso RDP com credenciais seguras
Contas de e-mail	3 contas administrativas (ex: suporte@, admin@, no-reply@)
Certificado HTTPS	Incluído gratuitamente (Let’s Encrypt, renovação automática)

Fonte: Elaboração Própria

7.1.3 Configuração dos clientes

Para acessar o sistema Camaleão, o cliente deverá utilizar um computador, tablet ou smartphone compatível com os requisitos mínimos apresentados a seguir. A plataforma foi projetada para operar tanto em ambiente web quanto mobile, exigindo apenas conexão estável com a internet e navegadores atualizados que garantam a correta renderização das interfaces e a segurança das operações realizadas.

Tabela 54: Configuração dos Clientes

Software / Plataforma	Versão Recomendada
Navegador Web (Google Chrome)	Versão 127.0.6533.89 ou superior
Navegador Web (Mozilla Firefox)	Versão 129 ou superior
Navegador Web (Opera)	Versão 112.0.5197.39 ou superior
Navegador Web (Microsoft Edge)	Versão 127.0.2651.86 ou superior
Aplicativo Mobile (Expo Go – Android/iOS)	Versão 50.0.0 ou superior
Sistema Operacional (Android)	Versão 8.0 (Oreo) ou superior
Sistema Operacional (Windows)	Versão 10 ou superior
Conexão à Internet	Mínimo 10 Mbps de velocidade recomendada

Fonte: Elaboração Própria

7.1.4 Infraestrutura necessária

Para o correto funcionamento do sistema Camaleão, tanto em sua versão web quanto mobile, é necessário dispor de uma infraestrutura mínima que assegure o desempenho, a disponibilidade e a segurança das informações. A seguir, são apresentadas as especificações recomendadas para os ambientes do cliente e do servidor, contemplando os recursos tecnológicos essenciais à operação e manutenção da plataforma.

Para o cliente:

- Computador, tablet ou smartphone (Android ou iOS);
- Navegador Web atualizado (Google Chrome, Mozilla Firefox, Opera ou Microsoft Edge);
- Aplicativo Camaleão (versão mobile desenvolvida em React Native com Expo);
- Acesso à Internet estável.

Para o sistema:

- Servidor de aplicação configurado com Django Framework (Python 3.13);
- Banco de dados SQLite em ambiente de desenvolvimento e PostgreSQL em produção;
- Servidor web com suporte a Gunicorn e Nginx;
- Domínio registrado e certificado SSL (HTTPS) ativo;
- Repositório de código e versionamento via GitHub;
- Hospedagem na plataforma cloud (ex.: Render, Railway ou AWS EC2);
- Integração com Expo para distribuição mobile e publicação na Google Play Store;
- Sistema de backup automático do banco de dados e dos arquivos armazenados (documentos e avatares);
- Conectividade com serviço de e-mail SMTP para envio automático de notificações e redefinição de senha.

7.2 CRONOGRAMA DE TREINAMENTOS

Para garantir que as organizações utilizem o sistema Camaleão de forma eficiente e segura, tanto na versão web quanto na versão mobile, foi elaborada uma abordagem estruturada de capacitação dos usuários. Inicialmente, serão disponibilizados tutoriais em vídeo e guias interativos, acessíveis online, contemplando desde o cadastro inicial de usuários e perfis (Administrador, DPO e Gerente) até o uso avançado de módulos como Inventário de Dados, Matriz de Riscos, Checklist de Conformidade e Gestão de Documentos.

Além disso, o projeto prevê um serviço de suporte técnico ativo, disponível de segunda a sexta-feira, para esclarecimento de dúvidas e acompanhamento das empresas no processo de adequação à LGPD. Esse atendimento poderá ser realizado por chat, e-mail ou videoconferência, garantindo respostas rápidas e eficazes, bem como o pleno aproveitamento das funcionalidades oferecidas pela plataforma Camaleão.

8 CONCLUSÃO

A realização deste trabalho permitiu uma compreensão aprofundada sobre a relevância da proteção de dados pessoais na sociedade digital e possibilitou a aplicação prática desses conhecimentos no desenvolvimento de um sistema voltado ao apoio da conformidade com a LGPD. Partindo de uma fundamentação teórica que abordou a evolução histórica da privacidade, os princípios centrais da legislação e seus impactos no ambiente organizacional, o projeto avançou para a construção do sistema Camaleão, uma ferramenta planejada para auxiliar instituições acadêmicas e organizacionais na gestão adequada de informações pessoais.

O sistema desenvolvido demonstrou resultados significativos ao integrar funcionalidades como inventário de dados, matriz de riscos, checklist de conformidade, geração de relatórios e módulo de notificações. Esses recursos fortalecem a governança de dados, promovem transparência e contribuem para o cumprimento das exigências legais, evidenciando a aplicabilidade prática do sistema e seu potencial de adaptação a diferentes realidades institucionais.

Ao longo da implementação, desafios importantes surgiram, como a definição precisa dos requisitos, a integração entre os módulos, a seleção das tecnologias mais adequadas e a necessidade de ajustes contínuos. O uso de ferramentas como o GitHub para controle de versões, aliado a práticas sistemáticas de testes, foi essencial para garantir qualidade, rastreabilidade e evolução consistente do projeto. Esse processo também proporcionou o desenvolvimento de capacidades técnicas e organizacionais importantes, enriquecendo a formação acadêmica e profissional envolvida.

Considerando a constante evolução das demandas relacionadas à privacidade e proteção de dados, o sistema Camaleão representa um ponto de partida promissor. Como perspectivas futuras, destaca-se o aprimoramento dos módulos existentes — especialmente os de relatórios e notificações — buscando torná-los mais completos, inteligentes e alinhados às necessidades reais das organizações. Além disso, prevê-se a inclusão de novas funcionalidades, como dashboards interativos, integração com sistemas corporativos (ERP e CRM) e automação de auditorias com base em critérios de conformidade.

Outro avanço relevante envolve a adoção de inteligência artificial e aprendizado de máquina, visando apoiar a análise de riscos, identificar padrões e sugerir medidas

preventivas. A expansão do aplicativo mobile, com melhorias como notificações push e autenticação multifatorial, reforça ainda mais o compromisso com segurança e acessibilidade. Também se considera a possibilidade de transformar o sistema em uma solução SaaS (Software as a Service), aumentando seu alcance e facilitando o uso por organizações de diversos portes.

No âmbito acadêmico, o projeto abre portas para novas pesquisas multidisciplinares nas áreas de Segurança da Informação, Direito Digital, Engenharia de Software e Governança de Dados, podendo servir como base para estudos futuros e aprimoramentos contínuos.

Assim, o sistema Camaleão reafirma seu compromisso com a ética, a transparência e a segurança no tratamento de dados pessoais, contribuindo para a formação de profissionais preparados para os desafios da era digital e oferecendo caminhos concretos para o fortalecimento da conformidade com a LGPD.

8.1 IMPLEMETAÇÕES FUTURAS

Entre as próximas evoluções do sistema Camaleão estão os módulos de Relatórios e Notificações, que tornarão a plataforma ainda mais completa. O módulo de Relatórios permitirá gerar documentos consolidados sobre riscos, inventário, incidentes e ações, oferecendo análises claras para auditorias e decisões estratégicas. Já o módulo de Notificações trará alertas automáticos sobre prazos, vencimentos e eventos importantes, garantindo que o usuário não perca nenhuma informação relevante. Com essas implementações, o sistema se tornará mais proativo, organizado e eficiente no apoio à gestão da conformidade.

REFERÊNCIAS

ALMEIDA, Fábio. **Proteção de Dados Pessoais:** A LGPD e o Novo Cenário da Privacidade no Brasil. São Paulo: Editora Revista dos Tribunais, 2019.

ANPD – Autoridade Nacional de Proteção de Dados. **Dos poderes da ANPD e das sanções administrativas.** 2022. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 07 abr. 2025.

ANPD – Autoridade Nacional de Proteção de Dados. **Encarregado pelo Tratamento de Dados Pessoais (DPO)**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 07 abr. 2025.

ANPD – Autoridade Nacional de Proteção de Dados. **Guia de boas práticas para a aplicação da LGPD.** 2023. Disponível em: https://www.gov.br/anpd. Acesso em: 02 abr. 2025.

ANPD – Autoridade Nacional de Proteção de Dados. **Guia de boas práticas:** segurança da informação. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 07 abr. 2025.

ANPD – Autoridade Nacional de Proteção de Dados. **Segurança da informação e medidas técnicas e administrativas.** 2022. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 07 abr. 2025.

ANPD – Autoridade Nacional de Proteção de Dados. **Site oficial**. 2020. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 18 mar. 2025.

ARGENTINA. Ley de Protección de los Datos Personales, **Ley nº 25.326**, de 4 de outubro de 2000. Disponível em: http://www.argentina.gob.ar/normativa. Acesso em: 18 mar. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 1, de 28 de outubro de 2021**. Dispõe sobre a aplicação da LGPD para pequenas e médias empresas. Brasília, DF, 2021. Disponível em: https://www.gov.br/anpd/. Acesso em: 02 abr. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1-6, 15 ago. 2018.

CALIFÓRNIA. **California Consumer Privacy Act** (CCPA), 2018. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 18 mar. 2025.

CAVALCANTI, A. L. **Privacidade e segurança de dados:** uma análise da LGPD. Rio de Janeiro: Editora Jurídica, 2020.

CERT.br – Centro de Estudos, **Resposta e Tratamento de Incidentes de Segurança no Brasil.** Guia de gestão de incidentes de segurança. São Paulo: NIC.br, 2021. Disponível em: https://www.cert.br. Acesso em: 07 abr. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2. ed. Rio de Janeiro: Forense, 2021.

GONÇALVES, Ricardo. **LGPD na Prática:** Guia para Empresas e Profissionais de Privacidade. São Paulo: Editora Atlas, 2020.

MENEZES, M. A. **A privacidade no Brasil:** desafios e avanços. Revista Brasileira de Direito Digital, 2020. Disponível em: https://www.revistadireitodigital.com.br/. Acesso em: 18 mar. 2025.

PEREIRA, Eduardo. **Privacidade e Proteção de Dados Pessoais:** Fundamentos e Implicações da LGPD. Porto Alegre: Editora Verbo Jurídico, 2020.

SENAC. **Privacidade e proteção de dados:** guia introdutório sobre a LGPD. São Paulo: SENAC, 2021.

SILVA, A. F. **Implementação da LGPD no Brasil:** desafios e perspectivas. Jornal de Tecnologia e Direito, 2020. Disponível em: https://www.jornaltecnologiadireito.com.br/. Acesso em: 18 mar. 2025.

SOUZA, R. C. **A evolução da legislação sobre dados pessoais no Brasil**. Revista de Direito da Informação, 2019. Disponível em: https://www.revistadireitoinformacao.com.br/. Acesso em: 18 mar. 2025.

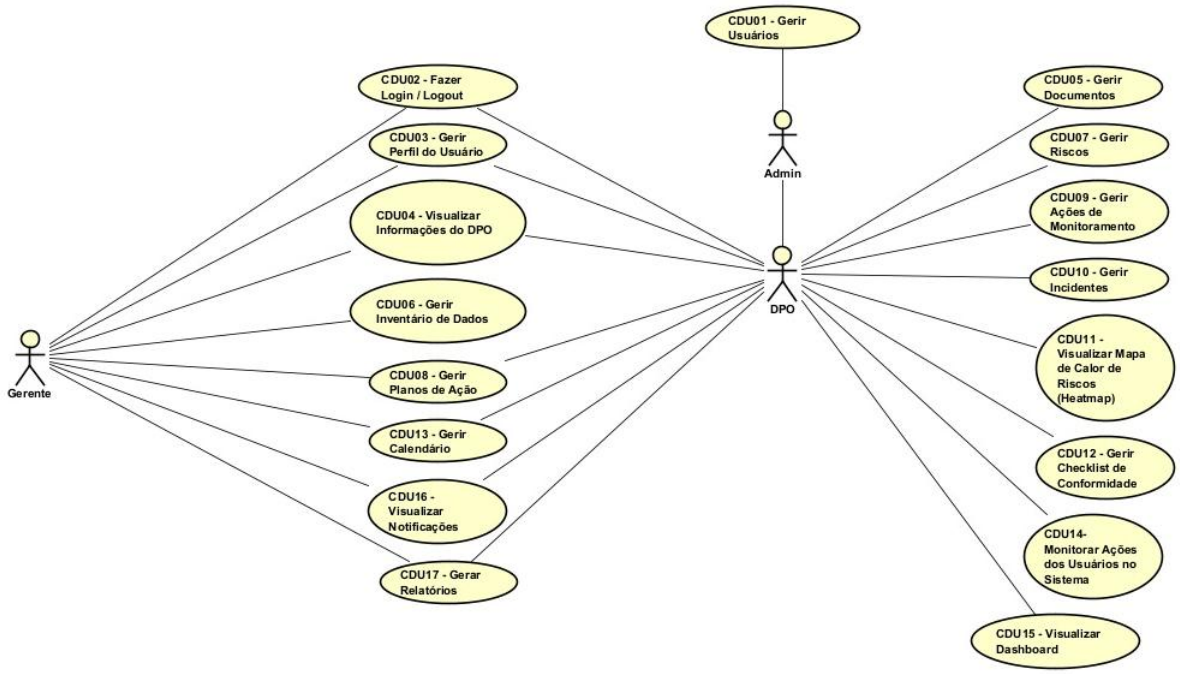
UNIÃO EUROPEIA**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: https://gdpr-info.eu. Acesso em: 18 mar. 2025.

VIOLA, M.; LEAL, **A. LGPD Comentada:** Impactos e Aplicações Práticas da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

APÊNDICE A: DIAGRAMA DE CASOS DE USO

Figura 45: Diagrama de Casos de Uso

Fonte: Elaboração Própria



APÊNDICE B: DESCRIÇÕES DE CASOS DE USO

CDU01 – Gerir Usuários

Sumário: Por meio deste caso de uso, o Administrador poderá cadastrar, editar, desativar e gerenciar os usuários do sistema Camaleão, definindo seus papéis e permissões de acesso (Administrador, DPO ou Gerente). O objetivo é garantir o controle centralizado de contas, perfis e papéis, assegurando a integridade e rastreabilidade do ambiente de conformidade.

Pré-condição: O ator deve estar autenticado como Administrador.

Ator Principal: Administrador.

Ator Secundário: Nenhum.

Fluxo Principal:

1. O Administrador acessa o módulo “Usuários”.
2. O sistema exibe a lista de usuários cadastrados, com informações resumidas (nome, e-mail e papel).
3. O Administrador seleciona uma das opções disponíveis:
   a) “Cadastrar Usuário”;
   b) “Editar Usuário”;
   c) “Desativar Usuário”;
   d) “Reenviar Boas-Vindas”.

O sistema executa a ação correspondente e atualiza a listagem.

Fluxo Secundário: Cadastrar Usuário

1. O sistema exibe o formulário de cadastro de novo usuário.
2. O Administrador informa os campos obrigatórios: nome, sobrenome, e-mail e papel.
3. O sistema valida as regras RN01, RN02 e RN04.
4. Se válido, o sistema cria o usuário com status ativo e envia automaticamente o e-mail de boas-vindas com link para definição de senha.
5. O sistema registra o log de criação e retorna à lista de usuários.

Fluxo Secundário: Editar Usuário

1. O Administrador seleciona um usuário existente.
2. O sistema exibe o formulário de edição com os dados atuais.
3. O Administrador altera as informações desejadas e confirma.
4. O sistema valida RN01 e RN04 (verifica unicidade de DPO).

5. O sistema atualiza as informações e registra o log da operação.

Fluxo Secundário: Desativar Usuário

1. O Administrador seleciona “Desativar Usuário”.
2. O sistema exibe mensagem de confirmação.
3. O Administrador confirma a ação.
4. O sistema altera o status do usuário para “Inativo” e registra o log da desativação.

Fluxo Secundário (3): Reenviar Boas-Vindas

1. O Administrador seleciona “Desativar Usuário”.
2. O sistema exibe mensagem de confirmação.
3. O Administrador confirma a ação.
4. O sistema altera o status do usuário para “Inativo” e registra o log da desativação.

Fluxos de Exceção:

- Violação da RN01 → o sistema informa que há campos obrigatórios não preenchidos.
- Violação da RN02 → o sistema informa que o e-mail informado já está em uso.
- Violação da RN03 → o sistema bloqueia tentativa de alteração de papel sem permissão adequada.
- Violação da RN04 → o sistema impede o cadastro de mais de um usuário com papel de DPO ativo.
- Violação da RN05 → erro de envio do e-mail de boas-vindas.

Regras de Negócio:

- RN01: Todos os campos obrigatórios (nome, sobrenome, e-mail e papel) devem estar preenchidos.
- RN02: O e-mail deve ser único no sistema.
- RN03: Somente o Administrador pode cadastrar, desativar ou alterar o papel de um usuário.
- RN04: O sistema só permite um perfil de DPO ativo por vez.
- RN05: O e-mail de boas-vindas deve conter link seguro e expirar após 24 horas.
- RN06: Todas as operações (criação, edição, desativação, reenvio) devem ser registradas no log de auditoria (CDU14).

Pós-condição: Um novo usuário foi criado, atualizado, desativado ou teve o convite reenviado. O sistema manteve a unicidade do perfil de DPO, garantiu a integridade dos papéis e registrou todas as operações para fins de auditoria e conformidade com a LGPD.

CDU02 – Fazer Login / Logout

Sumário: Por meio deste caso de uso, os usuários do sistema Camaleão (Administrador, DPO ou Gerente) poderão autenticar-se para acessar suas funcionalidades conforme suas permissões e, posteriormente, realizar logout de forma segura. O caso de uso assegura controle de acesso, rastreabilidade das sessões e conformidade com as boas práticas de segurança da informação previstas na LGPD.

Pré-condição: O usuário deve possuir uma conta ativa e válida no sistema.

Atores Principais: Administrador, DPO e Gerente.

Ator Secundário: Sistema (responsável pelo processamento de autenticação, registro de log e encerramento da sessão).

Fluxo Principal (Login):

1. O usuário acessa a tela inicial e seleciona a opção “Entrar”.
2. O sistema exibe o formulário de autenticação com os campos E-mail e Senha.
3. O usuário informa suas credenciais e clica em “Acessar”.
4. O sistema valida as credenciais conforme as regras de negócio RN01 e RN02.
5. Em caso de sucesso, o sistema autentica o usuário e redireciona-o para página inicial (Home)
6. O sistema registra o evento de login na tabela de auditoria (CDU14 – Registrar e Consultar Atividade de Login).
7. O caso de uso é encerrado com o usuário autenticado no sistema.

Fluxo Secundário (Login com Falha):

1. O sistema informa que as credenciais são inválidas.
2. O sistema incrementa o contador de tentativas malsucedidas.
3. Caso o limite de três tentativas consecutivas seja atingido, aplica-se RN04.
4. O usuário pode tentar novamente após o desbloqueio automático.

Fluxo Secundário (Logout):

1. O usuário clica na opção “Sair” no menu principal.
2. O sistema encerra imediatamente a sessão ativa e invalida o token de autenticação.

3. O sistema registra a data e hora do logout na tabela de auditoria (CDU14).
4. O usuário é automaticamente redirecionado para a tela de login.
5. O caso de uso é encerrado.

Fluxos de Exceção:

- Violação da RN01: Campos obrigatórios não preenchidos.
- Violação da RN02: Credenciais inválidas.
- Violação da RN03: Conta do usuário desativada ou bloqueada.
- Violação da RN04: Excesso de tentativas de login (bloqueio temporário).
- Violação da RN05: Falha de comunicação com o servidor de autenticação.

Regras de Negócio:

- RN01: Todos os campos do formulário de login devem ser preenchidos.
- RN02: O e-mail e a senha informados devem corresponder a uma conta existente.
- RN03: O sistema deve impedir o login de contas inativas, bloqueadas ou sem papel atribuído.
- RN04: Após três tentativas de login malsucedidas consecutivas, o sistema deve bloquear temporariamente o acesso do usuário por 15 minutos.
- O evento deve ser registrado nos logs de auditoria (CDU14).
- O DPO deve ser notificado automaticamente via sistema e e-mail institucional.
- RN05: Todo login e logout devem gerar registros na tabela de auditoria (CDU14).
- RN06: O token de sessão expira automaticamente após 15 minutos de inatividade.
- RN07: O logout invalida imediatamente tokens e sessões abertas.
- RN08: Todas as ações de autenticação (sucesso, falha, bloqueio, logout) devem ser registradas com data, hora, IP e ID do usuário.

Pós-condição: O usuário foi autenticado e teve sua sessão registrada com sucesso, ou realizou logout com encerramento seguro. Em caso de bloqueio por tentativas inválidas, o evento foi registrado e comunicado ao DPO. O sistema manteve o histórico completo das operações para auditoria e conformidade com a LGPD.

CDU03 – Gerir Perfil do Usuário

Sumário: Por meio deste caso de uso, o usuário autenticado poderá visualizar e editar informações do seu perfil no sistema Camaleão, podendo alterar sua foto/avatar e/ou senha de acesso. O objetivo é permitir que cada usuário mantenha seus dados pessoais atualizados e seguros, de acordo com as boas práticas de autenticação e segurança previstas pela LGPD.

Pré-condição: O usuário deve estar autenticado no sistema.

Ator Principal: Usuário Autenticado (Administrador, DPO ou Gerente).

Ator Secundário: Sistema (responsável por validar, processar e registrar as alterações).

Fluxo Principal: O usuário acessa o menu “Meu Perfil”.

1. O sistema exibe a página de perfil com as informações do usuário (e-mail, foto/avatar e função).
2. O usuário clica na opção “Editar”.
3. O sistema exibe a janela de edição do perfil, com as opções:
    a. Escolher arquivo ou remover foto/avatar;
    b. Alterar senha preenchendo os campos (requer senha atual).
    c. O usuário realiza as alterações e clica em “Salvar”.
    d. O sistema valida as informações conforme as regras de negócio (RN01 a RN04).
4. O sistema registra o log da operação no módulo de auditoria (CDU14 – Registrar e Consultar Atividades de Login e Operações do Usuário).

Fluxos de Exceção:

- Violação da RN01: Senha atual incorreta ao tentar alterar a senha.
- Violação da RN02: Nova senha não atende aos critérios mínimos de segurança.
- Violação da RN03: Formato de imagem inválido ou tamanho superior ao permitido.
- Violação da RN04: Falha ao salvar as alterações no servidor.

Regras de Negócio:

- RN01: Para alterar a senha, o usuário deve informar corretamente a senha atual.

- RN02: A nova senha deve conter no mínimo 8 caracteres, incluindo letra maiúscula, número e símbolo especial.
- RN03: O formato permitido para foto/avatar é JPEG, JPG, PNG ou WEBP, com tamanho máximo de 5 MB.
- RN04: O usuário pode optar por remover a foto atual, substituí-la por uma nova ou mantê-la inalterada.
- RN05: Apenas o próprio usuário pode editar seu perfil.
- RN06: O sistema deve exibir mensagens claras de sucesso ou erro, conforme o resultado da validação.
- RN07: Todas as alterações (foto, senha ou ambas) devem ser registradas no log de auditoria (CDU14).
- RN08: Caso a sessão expire durante a edição (15 minutos de inatividade), o sistema encerra o processo e solicita novo login.

Pós-condição: O usuário atualizou com sucesso sua senha e/ou foto/avatar, e o sistema registrou a operação para fins de auditoria e conformidade.
Em caso de erro, as alterações não foram aplicadas e o sistema manteve os dados originais, exibindo mensagem explicativa ao usuário.

CDU04 – Visualizar Informações do DPO

Sumário: Por meio deste caso de uso, todos os usuários autenticados poderão visualizar as informações oficiais do DPO, conforme determina a LGPD. O objetivo é garantir a transparência e o acesso facilitado aos dados de contato do DPO, permitindo que qualquer usuário saiba quem é o responsável pela privacidade e pela proteção de dados dentro da organização.

Pré-condição: Deve existir um DPO cadastrado e ativo no sistema, com informações de contato válidas.

Ator Principal: Usuário Autenticado (Administrador, DPO ou Gerente).

Ator Secundário: Nenhum.

Fluxo Principal:

1. O usuário acessa o menu “Informações do DPO”.
2. O sistema consulta o cadastro do DPO ativo.
3. O sistema exibe na tela as informações oficiais do DPO, incluindo:

a. Nome completo;
b. E-mail institucional;
c. Telefone ou celular de contato;
d. Data da nomeação;
e. Data da validade da nomeação.

4. O sistema também exibe um título informativo:
   a. “Encarregado de Proteção de Dados (DPO)”
5. O usuário pode visualizar os dados, mas não pode editá-los.
6. O usuário pode clicar no link do e-mail para enviar um e-mail.
7. O contato telefônico também é um link que direciona o usuário para usar um aplicativo de mensagens ou ligação.
8. Se o acesso for por aplicativo móvel poderá clicar no telefone para ligar para o DPO se assim desejar.
9. O sistema mantém registro de que o módulo foi acessado (para fins de auditoria).

Fluxos de Exceção:

- Violação da RN01 → o sistema informa que não há DPO ativo cadastrado.
- Violação da RN02 → falha na consulta das informações do DPO (problema de conexão).

Regras de Negócio:

- RN01: Deve existir apenas um DPO ativo cadastrado no sistema (ver CDU01 – Gerir Usuários).
- RN02: As informações do DPO devem estar visíveis e acessíveis a todos os usuários autenticados.
- RN03: O módulo “Encarregado” deve estar disponível no menu principal.
- RN04: Nenhum usuário pode alterar ou ocultar as informações exibidas.
- RN05: O sistema deve registrar logs de acesso a esta tela para fins de auditoria.

Pós-condição: O usuário visualizou as informações oficiais do DPO. O sistema garantiu a transparência das informações e registrou o acesso ao módulo para controle de auditoria, em conformidade com os princípios da LGPD.

CDU05 – Gerir Documentos LGPD

Sumário: Por meio deste caso de uso, o usuário poderá cadastrar, revisar e acompanhar os documentos e evidências relacionados à conformidade com a LGPD, como políticas, consentimentos, contratos e relatórios. O sistema permite anexar arquivos, definir dimensões de conformidade e controlar revisões periódicas.

Pré-condição: O ator deve estar autenticado e possuir acesso ao módulo “Documentos LGPD”.

Ator Principal: Administrador ou DPO.

Ator Secundário: Gerente (com permissão de leitura e acompanhamento).

Fluxo Principal:

1. O ator acessa o módulo “Documentos LGPD”.
2. O sistema exibe a lista de documentos cadastrados, com filtros por dimensão, criticidade e status.
3. O ator seleciona uma das opções: “Novo Documento”, “Editar”, “Excluir”, “Upload” ou “Download”.
4. O sistema executa a ação e atualiza a tabela principal.

Fluxo Secundário: Novo Documento

1. O sistema exibe o formulário de cadastro.
2. O ator preenche os campos obrigatórios (dimensão, atividade, base legal, evidência e criticidade).
3. O ator define a próxima data de revisão, se aplicável.
4. O sistema valida as regras RN01 e RN02.
5. O sistema grava o documento e o torna disponível para consulta.

Fluxo Secundário: Editar Documento

1. O ator seleciona um documento existente.
2. O sistema exibe os dados para edição.
3. O ator altera os campos e salva.
4. O sistema registra a atualização e mantém o histórico de alterações.

Fluxo Secundário: Anexar Arquivo

1. O ator seleciona “Upload”.
2. O sistema solicita o envio de um arquivo PDF, DOCX ou outro formato permitido.
3. O sistema vincula o arquivo ao documento e confirma o upload.

Fluxo Secundário: Exportar Documentos

1. O ator clica em “Download”.
2. O sistema faz o download do documento conforme o formato salvo.

Fluxos de Exceção:

- Violação da RN01 → sistema informa que há campos obrigatórios não preenchidos.
- Violação da RN02 → sistema informa formato de arquivo inválido.
- Violação da RN03 → sistema informa falha de conexão ao salvar ou exportar.

Regras de Negócio:

- RN01: Todos os campos obrigatórios devem estar preenchidos.
- RN02: Apenas arquivos com extensões permitidas (.pdf, .docx, .xlsx) podem ser anexados.
- RN03: Cada documento deve pertencer a uma dimensão válida (Governança, Segurança da Informação ou Processos).
- RN04: O sistema deve exibir alerta automático quando a data de revisão estiver próxima.
- RN05: Somente Administradores e DPO podem excluir documentos.

Pós-condição: Um novo documento foi cadastrado, atualizado ou excluído. O sistema mantém o registro histórico de revisões e permite consulta e exportação das evidências de conformidade.

CDU06 – Gerir Inventário de Dados

Sumário: Por meio deste caso de uso, o usuário autorizado poderá cadastrar, consultar, atualizar e acompanhar os registros do Inventário de Dados Pessoais, documentando processos, responsáveis e bases legais de tratamento conforme as exigências da LGPD. A funcionalidade permite identificar os fluxos de tratamento de dados pessoais dentro da organização, manter a rastreabilidade das informações e assegurar a conformidade com o princípio da prestação de contas.

Pré-condição: O ator deve estar autenticado e possuir permissão de acesso ao módulo “Inventário de Dados”.

Atores Principais: Administrador, DPO e Gerente.

Ator Secundário: Sistema (responsável por validar, armazenar e auditar as operações).

Fluxo Principal:

1. O ator acessa o menu “Inventário de Dados”.
2. O sistema exibe a lista de registros existentes com filtros de busca (setor, processo, tipo de dado, base legal, responsável e status).
3. O ator seleciona uma das opções disponíveis:
    a. Novo Registro;
    b. Editar Registro;
    c. Excluir Registro (restrito a Admin/DPO);
    d. Solicitar Exclusão (Gerente, apenas de registros próprios);
    e. Exportar Inventário
    f. Filtrar/Buscar.
4. O sistema executa a ação correspondente e atualiza a tela principal.

Fluxo Secundário: Novo Registro

1. O sistema exibe o formulário de cadastro dividido em etapas: Identificação, Tratamento e Retenção.
2. O ator preenche todos os campos obrigatórios (setor, processo, tipo de dado, base legal, responsável, finalidade, forma de armazenamento e período de retenção).
3. O sistema valida as regras RN01 e RN05.
4. Se válidas, o sistema grava o registro no banco de dados e exibe mensagem de sucesso.
5. O novo item é exibido na lista principal com o nome do autor.

Fluxo Secundário: Editar Registro

1. O ator seleciona um registro existente.
2. O sistema exibe o formulário com as informações atuais.
3. O ator altera os campos desejados e clica em “Salvar Alterações”.
4. O sistema valida as alterações conforme RN01 e permissões de edição (RN04).
5. O sistema salva as alterações, exibe mensagem de sucesso e registra o log de atualização.

Fluxo Secundário: Excluir Registro (Administrador/DPO)

1. O Administrador ou DPO seleciona um registro.
2. O sistema exibe a opção “Excluir”.
3. O ator confirma a ação.

4. O sistema remove o registro da lista ativa, mantendo cópia no log de auditoria.
5. O sistema exibe mensagem de confirmação da exclusão.

Fluxo Secundário: Solicitar Exclusão (Gerente)

1. O Gerente seleciona um registro de sua autoria.
2. O sistema exibe a opção “Solicitar Exclusão”.
3. O Gerente confirma a solicitação.
4. O sistema registra o pedido e notifica o DPO.
5. O DPO analisa a solicitação e, se aprovada, realiza a exclusão conforme RN03.
6. O sistema atualiza o status da solicitação e exibe o resultado ao Gerente.

Fluxo Secundário: Exportar Inventário

1. O ator seleciona a opção “Exportar”.
2. O sistema solicita o formato desejado (CSV, Excel ou PDF).
3. O sistema gera o arquivo e inicia o download automaticamente.

Fluxo Secundário: Filtrar/Buscar

1. O ator utiliza o campo de busca ou filtros avançados (setor, processo, base legal, tipo de dado, período).
2. O sistema retorna apenas os registros correspondentes aos filtros aplicados.

Fluxos de Exceção

- Violação da RN01: Campos obrigatórios não preenchidos.
- Violação da RN02: E-mail do responsável inválido.
- Violação da RN03: Tentativa de exclusão não autorizada (Gerente).
- Violação da RN04: Falha ao registrar solicitação de exclusão.
- Violação da RN05: Falha na conexão ao salvar, excluir ou exportar dados.

Regras de Negócio:

- RN01: Todos os campos obrigatórios devem estar preenchidos.
- RN02: O e-mail informado para o responsável deve ter formato válido.
- RN03: Somente Administradores e DPO podem excluir registros diretamente.
- RN04: O Gerente pode editar apenas registros de sua autoria e solicitar exclusão desses registros ao DPO.
- RN05: Cada registro deve conter uma base legal válida conforme a LGPD.
- RN06: Toda ação (criação, edição, solicitação ou exclusão) deve ser registrada no log de auditoria (CDU14)

- RN07: O sistema deve manter o histórico de versões e exclusões para fins de auditoria e conformidade.

Pós-condição: Um registro do inventário foi criado, atualizado, exportado ou teve exclusão aprovada. O sistema garantiu o controle de permissões e registrou todas as ações no log de auditoria, assegurando a rastreabilidade e conformidade com a LGPD.

CDU07 – Gerir Riscos (Matriz de Riscos LGPD)

Sumário: Por meio deste caso de uso, o usuário autorizado poderá cadastrar, consultar, avaliar e monitorar os riscos relacionados ao tratamento de dados pessoais, compondo a Matriz de Riscos da organização. O sistema calcula automaticamente a pontuação e classifica os riscos por criticidade.

Pré-condição: O ator deve estar autenticado e possuir permissão de acesso ao módulo de Riscos.

Ator Principal: Administrador ou DPO.

Ator Secundário: Gerente (com permissões limitadas de visualização).

Fluxo Principal:

1. O ator acessa o módulo “Matriz de Riscos”.
2. O sistema exibe a lista de riscos existentes, com filtros por unidade, setor, processo, probabilidade e impacto.
3. O ator seleciona uma das opções: “Novo Risco”, “Editar”, “Excluir” ou “Visualizar Heatmap”.
4. O sistema executa a ação escolhida e retorna à tela principal.

Fluxo Secundário: Novo Risco

1. O sistema exibe o formulário de cadastro.
2. O ator preenche os campos obrigatórios (processo, fator de risco, probabilidade, impacto e medidas de controle).
3. O sistema calcula automaticamente a pontuação (Probabilidade × Impacto).
4. O sistema determina a faixa de criticidade (baixo, médio, alto, crítico).
5. O registro é salvo e aparece na matriz.

Fluxo Secundário: Editar Risco

1. O ator seleciona um risco existente.
2. O sistema exibe os dados para edição.

3. O ator altera valores e salva.
4. O sistema recalcula a pontuação e atualiza a classificação.

Fluxo Secundário (3): Visualizar Heatmap

1. O ator clica em “Heatmap”.
2. O sistema exibe o gráfico de calor com a distribuição dos riscos conforme pontuação.

Fluxo Secundário: Ranking de Riscos

1. O ator seleciona “Ranking de Riscos”.
2. O sistema exibe a lista com os riscos ordenados por pontuação.

Fluxos de Exceção:

- Violação da RN01 → sistema informa que há campos obrigatórios não preenchidos.
- Violação da RN02 → sistema impede o cálculo se probabilidade ou impacto estiverem ausentes.
- Violação da RN03 → erro de exportação ou falha no servidor.

Regras de Negócio:

- RN01: Probabilidade e impacto são obrigatórios.
- RN02: A pontuação é sempre calculada automaticamente.
- RN03: Apenas Admin e DPO podem excluir riscos.
- RN04: Os riscos são classificados conforme tabela de faixas de pontuação (baixo, médio, alto, crítico).
- RN05: O cálculo do risco residual considera a eficácia dos controles (quando informado).

Pós-condição: Um risco foi cadastrado, atualizado, classificado e armazenado na Matriz de Riscos. A pontuação e o nível de criticidade ficam disponíveis para consulta e exportação.

CDU08 – Gerir Planos de Ação

Sumário: Por meio deste caso de uso, o usuário poderá cadastrar, acompanhar e atualizar planos de ação relacionados aos riscos identificados na Matriz de Riscos.

Cada plano descreve a medida corretiva ou preventiva a ser executada, o responsável, o prazo e o status de execução.

Pré-condição: O ator deve estar autenticado e possuir acesso ao módulo de Planos de Ação, vinculado à Matriz de Riscos.

Ator Principal: Administrador ou DPO.

Ator Secundário: Gerente (para acompanhamento e atualização de planos sob sua responsabilidade).

Fluxo Principal:

1. O ator acessa o módulo “Planos de Ação”.
2. O sistema exibe a lista de planos existentes, com filtros por risco, status e prazo.
3. O ator seleciona uma das opções: “Novo Plano”, “Editar” ou “Excluir”.
4. O sistema executa a ação escolhida e retorna à lista atualizada.

Fluxo Secundário: Novo Plano

1. O sistema exibe o formulário de criação de plano de ação.
2. O ator preenche os campos obrigatórios (descrição da ação, responsável, prazo e status inicial).
3. O sistema valida as regras RN01 e RN02.
4. O sistema salva o plano vinculado ao risco selecionado.
5. O sistema atualiza automaticamente o status se o prazo estiver vencido.

Fluxo Secundário: Editar Plano

1. O ator seleciona um plano existente.
2. O sistema exibe os dados atuais.
3. O ator altera as informações e salva.
4. O sistema valida as regras RN01 e recalcula o status conforme o novo prazo.

Fluxo Secundário: Excluir Plano

1. O ator seleciona o plano e clica em “Excluir”.
2. O sistema solicita confirmação.
3. O ator confirma e o sistema remove o registro.

Fluxos de Exceção:

- Violação da RN01 → o sistema informa que há campos obrigatórios não preenchidos.
- Violação da RN02 → o sistema informa que o prazo definido é anterior à data atual.

- Violação da RN03 → erro de vinculação de risco inexistente.

Regras de Negócio:

- RN01: Todos os campos obrigatórios devem estar preenchidos.
- RN02: O prazo não pode ser anterior à data atual.
- RN03: Cada plano de ação deve estar associado a um risco existente.
- RN04: O status é atualizado automaticamente para “Atrasado” quando o prazo expira.
- RN05: O campo ordem_manual define a sequência das ações dentro de um mesmo risco.

Pós-condição: Um novo plano de ação foi criado, atualizado ou removido. O sistema atualiza as estatísticas e reflete a nova situação do risco na Matriz de Riscos e no Dashboard.

CDU09 – Gerir Monitoramentos

Sumário: Por meio deste caso de uso, o usuário poderá registrar, acompanhar e atualizar as ações de monitoramento de conformidade realizadas para avaliar a efetividade dos controles e medidas adotadas conforme a LGPD. O sistema permite documentar o escopo avaliado, os resultados obtidos, as deficiências identificadas e as medidas corretivas implementadas. Em situações excepcionais, um registro poderá ser excluído mediante justificativa formal, devidamente registrada para fins de auditoria.

Pré-condição: O ator deve estar autenticado e possuir permissão de acesso ao módulo “Monitoramentos”.

Atores Principais: Administrador e DPO.

Ator Secundário: Não há.

Fluxo Principal:

1. O ator acessa o módulo “Monitoramentos”.
2. O sistema exibe a lista de ações de monitoramento existentes, com filtros por data, responsável, setor e status.
3. O ator seleciona uma das opções:
    a. Novo;
    b. Editar;

    c. Excluir (restrito conforme RN03);
4. O sistema executa a ação escolhida e atualiza a lista principal.

Fluxo Secundário: Novo

1. O sistema exibe o formulário de cadastro.
2. O ator preenche os campos obrigatórios (framework/requisito, escopo, data de monitoramento, responsável e critérios de avaliação).
3. O sistema valida as regras RN01 e RN02.
4. Caso o registro seja válido, o sistema grava a ação no banco de dados e exibe mensagem de sucesso.

Fluxo Secundário: Editar

1. O ator seleciona um monitoramento existente.
2. O sistema exibe os dados atuais.
3. O ator altera as informações e clica em “Salvar Alterações”.
4. O sistema valida as alterações e atualiza os registros associados.
5. O sistema registra o log da modificação e exibe mensagem de sucesso.

Fluxo Secundário: Excluir Monitoramento (Exclusão Justificada)

1. O ator (Administrador ou DPO) seleciona o monitoramento que deseja excluir.
2. O sistema exibe a opção “Excluir” e solicita uma justificativa obrigatória para a exclusão.
3. O ator preenche o campo de justificativa e confirma a ação.
4. O sistema registra nos logs de auditoria:
    a. o usuário responsável pela exclusão,
    b. a data e hora da operação,
    c. o motivo informado.
5. O sistema remove o registro da lista ativa, mantendo uma cópia do histórico no banco de auditoria.
6. O sistema exibe mensagem de confirmação da exclusão.

Fluxos de Exceção:

- Violação da RN01: Campos obrigatórios não preenchidos.
- Violação da RN02: Data de monitoramento inválida (posterior à data atual).
- Violação da RN03: Tentativa de exclusão sem justificativa informada.
- Violação da RN04: Falha de conexão ou erro de gravação nos logs de auditoria.
- Violação da RN05: Falta de permissão para exclusão (perfil Gerente).

Regras de Negócio:

- RN01: Todos os campos obrigatórios devem ser preenchidos.
- RN02: A data de monitoramento não pode ser futura.
- RN03: Apenas Administradores e DPO podem excluir monitoramentos, e somente com justificativa registrada.
- RN04: O sistema deve registrar todas as exclusões com data, hora, ator e justificativa no log de auditoria (CDU14).
- RN05: Cada monitoramento deve estar vinculado a um requisito, framework ou política de conformidade válida.
- RN06: O sistema deve preservar o histórico de todos os monitoramentos, mesmo os excluídos, para fins de auditoria e rastreabilidade.

Pós-condição: Uma nova ação de monitoramento foi criada, atualizada ou, em casos excepcionais, excluída mediante justificativa formal.

Todas as operações foram registradas no log de auditoria, assegurando a rastreabilidade, integridade e conformidade com os princípios da LGPD.

CDU10 – Gerir Incidentes

Sumário: Por meio deste caso de uso, o usuário poderá registrar, acompanhar e atualizar incidentes relacionados à segurança da informação ou à privacidade de dados pessoais, conforme os requisitos da LGPD. O sistema permite documentar a origem, impacto, medidas corretivas e decisões tomadas, além de registrar a rastreabilidade de todo o ciclo de vida do incidente. Em casos estritamente necessários, um incidente poderá ser excluído mediante justificativa formal, que será registrada em log para fins de auditoria e conformidade.

Pré-condição: O ator deve estar autenticado e possuir permissão de acesso ao módulo “Incidentes”.

Atores Principais: Administrador e DPO.

Ator Secundário: Não há.

Fluxo Principal:

1. O ator acessa o módulo “Incidentes”.
2. O sistema exibe a lista de incidentes com filtros por data, status, setor e responsável.

3. O ator seleciona uma das opções:
    a. Novo;
    b. Editar;
    c. Excluir (restrito a Admin/DPO, mediante justificativa);
4. O sistema executa a ação escolhida e atualiza a listagem principal.

Fluxo Secundário: Novo

1. O sistema exibe o formulário de registro de incidente.
2. O ator preenche os campos obrigatórios (descrição, fonte, data de registro, responsável pela análise, impacto e ações recomendadas).
3. O sistema valida as regras RN01 e RN02.
4. Caso os dados sejam válidos, o sistema grava o registro e exibe o novo incidente na lista de incidentes.

Fluxo Secundário: Editar

1. O ator seleciona um incidente existente.
2. O sistema exibe os dados atuais para edição.
3. O ator altera as informações desejadas e clica em “Salvar”.
4. O sistema valida as alterações conforme RN01 e RN02, grava as mudanças e mantém o histórico de versões.
5. O sistema exibe mensagem de sucesso e atualiza a data de modificação.

Fluxo Secundário: Excluir (Exclusão Justificada)

1. O ator (Administrador ou DPO) seleciona o incidente a ser excluído.
2. O sistema exibe a opção “Excluir Incidente” e solicita uma justificativa obrigatória para a exclusão.
3. O ator informa o motivo e confirma a ação.
4. O sistema registra no log de auditoria (CDU14):
    a. o usuário responsável pela exclusão;
    b. a data e hora da operação;
    c. o número do incidente;
    d. a justificativa informada.
5. O sistema remove o incidente da lista, mantendo seu registro no histórico de auditoria.
6. O sistema exibe mensagem de confirmação da exclusão.

Fluxos de Exceção:

- Violação da RN01: Sistema informa que há campos obrigatórios não preenchidos.
- Violação da RN02: Sistema informa que a data de registro é inválida (futura).
- Violação da RN03: Tentativa de exclusão sem justificativa informada.
- Violação da RN04: Falha na gravação do log de auditoria.
- Violação da RN05: Falta de permissão para exclusão (perfil Gerente).

Regras de Negócio:

- RN01: Todos os campos obrigatórios devem ser preenchidos.
- RN02: As datas de registro e atualização devem seguir ordem cronológica.
- RN03: Apenas Administradores e DPO podem excluir incidentes, e somente mediante justificativa formal registrada.
- RN04: Toda exclusão deve ser registrada em log contendo o usuário, data, hora, ID do incidente e motivo informado.
- RN05: O sistema deve permitir o upload de relatórios complementares e evidências relacionadas ao incidente.
- RN06: O histórico de todos os incidentes, incluindo os excluídos, deve ser mantido para auditoria.
- RN07: O DPO deve ser notificado por e-mail sempre que uma exclusão for realizada.

Pós-condição: Um incidente foi registrado, atualizado ou, em casos excepcionais, excluído mediante justificativa formal.

O sistema registrou todos os eventos nos logs de auditoria, assegurando a rastreabilidade e transparência das ações de conformidade e segurança da informação.

CDU11 – Visualizar Mapa de Calor de Riscos

Sumário: Por meio deste caso de uso, o Administrador e o DPO poderão visualizar o Mapa de Calor (Heatmap) dos riscos, gerado automaticamente pelo sistema com base nas classificações de probabilidade × impacto registradas na Matriz de Riscos (CDU07). O objetivo é permitir o acompanhamento visual da distribuição e criticidade dos riscos da organização, facilitando a análise e priorização das ações de mitigação.

Pré-condição: O sistema deve possuir riscos cadastrados e classificados com valores válidos de probabilidade e impacto.

Ator Principal: Administrador ou DPO.

Ator Secundário: Sistema (para geração automática e atualização contínua do Heatmap).

Fluxo Principal:

1. O ator acessa o módulo “Riscos”.
2. O sistema exibe automaticamente o Mapa de Calor (Heatmap) atualizado, gerado com base nos dados da Matriz de Riscos (CDU07).
3. O mapa apresenta os eixos:
    a. Eixo X: Probabilidade (Baixa, Média, Alta, Muito Alta);
    b. Eixo Y: Impacto (Baixo, Médio, Alto, Crítico);
    c. Células coloridas conforme o nível de criticidade.
4. O sistema aplica a escala de cores:
    a. Verde: Baixo risco;
    b. Amarelo: Risco moderado;
    c. Laranja: Risco alto;
    d. Vermelho: Risco crítico.
5. O ator pode ver detalhes dos riscos ao posicionar o mouse sobre um determinado ponto no mapa.
6. O sistema atualiza a visualização do mapa conforme os riscos cadastrados.

Fluxos de Exceção:

1. Violação da RN01 → falha no carregamento ou renderização do gráfico.

Regras de Negócio:

- RN01: O mapa de calor deve ser gerado e atualizado automaticamente pelo sistema sempre que houver alterações na Matriz de Riscos (CDU07).
- RN02: Somente Administrador e DPO podem visualizar o mapa completo.
- RN03: A escala de cores e pontuação segue o padrão:
    a. 1–5: Baixo (verde);
    b. 6–10: Moderado (amarelo);
    c. 11–15:Alto(laranja);
    d. 16–25: Crítico (vermelho).
- RN04: O mapa deve estar integrado ao Dashboard de Conformidade (CDU15) e ser atualizado automaticamente.

- RN05: Caso um novo risco seja adicionado, editado ou removido, o sistema deve recalcular o Heatmap em tempo real.

Pós-condição: O Administrador ou o DPO visualizou o Mapa de Calor atualizado, refletindo a concentração e gravidade dos riscos da organização.

CDU12 – Gerir Checklist de Conformidade LGPD

Sumário: Por meio deste caso de uso, o usuário poderá visualizar, editar e acompanhar o Checklist de Conformidade LGPD, que consolida as ações e controles implementados pela organização. Esse módulo permite mensurar o grau de maturidade e conformidade da empresa, servindo como base para auditorias e planejamento de melhorias contínuas. Somente Administradores e DPO podem atualizar ou excluir registros — sendo a exclusão permitida apenas em casos excepcionais, mediante justificativa formal registrada em log.

Pré-condição: O ator deve estar autenticado e possuir permissão de acesso ao módulo “Checklist LGPD”.

Atores Principais: Administrador e DPO.

Ator Secundário: Gerente (com permissão apenas para visualizar o checklist e acompanhar o progresso).

Fluxo Principal: O ator acessa o módulo “Checklist LGPD”.

1. O sistema exibe a lista de requisitos e ações de conformidade, com colunas de descrição, dimensão, status (☑ Concluído / ☐ Não concluído) e Ações.
2. O ator seleciona uma das opções disponíveis:
    a. Marcar ou Desmarcar item (alterar status);
    b. Editar Requisito;
    c. Excluir Requisito (com justificativa);
    d. Filtrar/Buscar.
3. O sistema executa a ação selecionada conforme as permissões do ator e atualiza o painel principal.

Fluxo Secundário: Atualizar Status (Check/Uncheck)

1. O ator acessa a página do checklist.
2. O sistema exibe o campo de status representado por uma caixa de seleção (☑/☐) em cada registro.

3. O ator marca a caixa para “Concluído” ou desmarca para “Não concluído”.
4. O sistema recalcula automaticamente o índice de maturidade global e o percentual de conformidade por dimensão.
5. O sistema registra a alteração no log de auditoria (CDU14).

Fluxo Secundário: Editar Item do Checklist

1. O ator (Administrador ou DPO) seleciona um item existente.
2. O sistema exibe o formulário de edição com os campos atuais (descrição e dimensão).
3. O ator realiza as alterações necessárias e clica em “Salvar Alterações”.
4. O sistema valida as regras RN01 e RN04, grava as mudanças e atualiza o histórico.

Fluxo Secundário: Excluir Item (Exclusão Justificada)

1. O ator (Administrador ou DPO) seleciona o item que deseja excluir.
2. O sistema exibe a opção “Excluir Item” e solicita uma justificativa obrigatória.
3. O ator informa o motivo da exclusão e confirma.
4. O sistema registra a exclusão no log de auditoria, incluindo:
    a. nome do ator,
    b. data e hora,
    c. item excluído,
    d. justificativa.
5. O sistema remove o item da lista e recalcula automaticamente o índice de maturidade.
6. O sistema exibe mensagem de confirmação e atualiza o painel.

Fluxos de Exceção:

- Violação da RN01: Sistema informa erro ao calcular o índice de maturidade.
- Violação da RN02: Tentativa de alteração ou exclusão sem permissão.
- Violação da RN03: Exclusão sem justificativa informada.
- Violação da RN04: Falha na gravação dos logs de auditoria
- Violação da RN05: Erro na geração do relatório de exportação.

Regras de Negócio:

- RN01: O índice de maturidade é recalculado automaticamente a cada alteração de status.

- RN02: Apenas Administradores e DPO podem editar, marcar/desmarcar ou excluir registros.
- RN03: Toda exclusão requer justificativa formal e registro no log de auditoria (CDU11).
- RN04: O Gerente possui acesso apenas de visualização, sem permissão para alterar status, editar ou excluir.
- RN05: O sistema deve armazenar o histórico completo de atualizações, exclusões e justificativas.

Pós-condição: O status dos requisitos foi atualizado, o índice de maturidade recalculado e o log de auditoria atualizado. O sistema mantém o histórico completo das alterações e exclusões justificadas, assegurando a transparência, rastreabilidade e conformidade com a LGPD.

CDU13 – Gerir Calendário

Sumário: Por meio deste caso de uso, o usuário poderá registrar, consultar, editar e excluir eventos pessoais do calendário (ex.: prazos de ações, revisões de documentos, reuniões de acompanhamento), a fim de organizar atividades relacionadas à conformidade LGPD.

Pré-condição: O ator deve estar autenticado no sistema.

Ator Principal: Administrador, DPO e Gerente Autenticado.

Ator Secundário: Nenhum.

Fluxo Principal:

1. O ator acessa o módulo “Calendário”.
2. O sistema exibe o calendário anual, mensal ou semanal conforme a escolha do usuário.
3. No calendário mensal e semanal o usuário visualiza os eventos do próprio usuário, ordenados por data e hora.
4. O ator seleciona uma das opções: “Novo Evento”, “Editar”, “Excluir” ou “Ver detalhes”.
5. O sistema executa a ação escolhida e atualiza a visualização do calendário.

Fluxo Secundário: Novo Evento

1. O sistema exibe o formulário de criação (hora, descrição e detalhes).

2. O ator preenche os campos obrigatórios e confirma.
3. O sistema valida RN01.
4. O sistema grava o evento associado ao usuário autenticado e retorna ao passo do fluxo principal.

Fluxo Secundário: Editar Evento

1. O ator seleciona um evento existente de sua autoria.
2. O sistema exibe o formulário com os dados atuais.
3. O ator altera as informações e salva.
4. O sistema valida RN01 e atualiza o registro.

Fluxo Secundário: Excluir Evento

1. O ator seleciona um evento existente de sua autoria.
2. O sistema solicita confirmação de exclusão.
3. O ator confirma e o sistema remove o evento.

Fluxos de Exceção:

- Violação da RN01 → sistema informa campos obrigatórios ausentes (hora, descrição, detalhes).
- Violação da RN02 → sistema impede a edição/remoção de evento que não pertence ao usuário autenticado.
- Violação da RN03 → sistema informa erro ao salvar/excluir (falha de conexão ou validação).

Regras de Negócio:

- RN01: Hora, descrição e detalhes são obrigatórios.
- RN02: O usuário só pode ver, criar, editar e excluir os próprios eventos.
- RN03: Eventos passados não podem ser excluídos, só podem ser visualizados.
- RN04: Os eventos devem ser exibidos em ordem cronológica (hora), se mais de um evento para a mesma data.

Pós-condição: Um evento foi criado, atualizado, excluído ou filtrado. A agenda pessoal do usuário permanece organizada para apoiar os prazos e atividades de conformidade.

CDU14 – Registrar e Consultar Atividade de Login e Operações do Usuário

Sumário: Por meio deste caso de uso, o sistema registrará automaticamente cada acesso de usuário, bem como as ações relevantes realizadas dentro do sistema

Camaleão, armazenando usuário(e-mail), data, hora, endereço IP, módulo acessado e tipo de operação. Esses registros poderão ser consultados por usuários com privilégios administrativos para fins de auditoria, rastreabilidade e conformidade com a LGPD.

Pré-condição: O usuário deve possuir uma conta ativa e autenticar-se com sucesso no sistema.

Ator Principal: Sistema (responsável pela geração e armazenamento automático dos registros de log).

Ator Secundário: Administrador e DPO (para consultas, auditorias e exportações dos registros).

Fluxo Principal:

1. O usuário realiza login no sistema (ver CDU02).
2. O sistema valida as credenciais e autêntica o usuário.
3. Após o login, o sistema registra automaticamente os seguintes dados:
    a. Usuário (e-mail);
    b. Data e hora do acesso;
    c. Endereço IP;
4. O sistema armazena essas informações na tabela de auditoria “LoginActivity”.
5. O registro fica disponível para consulta no módulo “Monitoramento”.
6. Durante a sessão, o sistema também monitora e registra as operações executadas nos módulos do sistema.

Fluxo Secundário: Registrar Atividades do Usuário (Operações Internas)

1. O usuário realiza uma ação relevante dentro do sistema (ex.: criar, editar, excluir ou exportar dados).
2. O sistema identifica a operação e gera um registro automático na tabela “UserActivityLog”.
3. O registro inclui as informações:
    a. Usuário responsável;
    b. Módulo e tela acessada;
    c. Tipo de operação (criação, atualização, exclusão, exportação, consulta);
    d. Identificador do registro afetado (ex.: ID do risco, ID do documento, ID do plano de ação);
    e. Data, hora e IP da operação;
4. Resultado da operação (sucesso, erro ou tentativa inválida).

5. O sistema armazena os registros e os vincula ao respectivo módulo e usuário.
6. O DPO ou Administrador poderá futuramente visualizar essas informações no painel “Logs de Atividades”.

Fluxo Secundário: Consultar Atividades de Login e Operações

1. O Administrador ou DPO acessa o módulo “Logs de Atividades”.
2. O sistema exibe duas abas: “Logins” e “Ações Executadas”.
3. O ator seleciona uma aba e visualiza os registros correspondentes, ordenados por data e usuário.
4. O ator aplica filtros opcionais (usuário, módulo, tipo de operação, período, endereço IP, resultado).
5. O sistema atualiza a lista conforme os filtros.
6. O ator pode exportar o relatório completo em formato CSV ou PDF.

Fluxo Secundário: Monitorar Acessos e Atividades Suspeitas

1. O DPO acessa o painel de auditoria e filtra registros recentes.
2. O sistema identifica e destaca eventos suspeitos, como:
    a. Múltiplos logins em horários atípicos;
    b. Alterações críticas (exclusões, mudanças de permissão);
    c. Exportações de grandes volumes de dados;
    d. Acessos simultâneos de IPs distintos.
3. O DPO pode registrar um alerta de auditoria ou abrir um incidente (extend CDU10 – Gerir Incidentes).

Fluxos de Exceção:

- Violação da RN01 → falha no registro de log (problema de conexão ou indisponibilidade do banco).
- Violação da RN02 → falha na exportação de relatório de atividades.
- Violação da RN03 → tentativa de consulta por usuário sem permissão.
- Violação da RN04 → erro de sincronização entre módulos de auditoria.

Regras de Negócio:

- RN01: Todo login bem-sucedido deve gerar automaticamente um registro de acesso.
- RN02: Todas as ações relevantes realizadas por usuários devem ser registradas automaticamente.
- RN03: Os registros não podem ser alterados ou excluídos manualmente.

- RN04: Apenas Administradores e DPO podem consultar e exportar os logs de atividades.
- RN05: O sistema deve armazenar as informações de auditoria (logins e atividades) por, no mínimo, 12 meses.
- RN06: O sistema deve permitir o rastreamento de todas as ações críticas, incluindo exclusões, alterações de papéis e exportações.
- RN07: A exportação dos logs deve conter cabeçalho com data, tipo de relatório e responsável pela exportação.

Pós-condição: O sistema registrou automaticamente o login e todas as operações realizadas durante a sessão. Os registros ficaram disponíveis para consulta, exportação e auditoria pelos Administradores e DPO, garantindo transparência e rastreabilidade total das atividades do usuário conforme as exigências da LGPD.

CDU15 – Visualizar Dashboard

Sumário: Por meio deste caso de uso, o usuário poderá visualizar indicadores consolidados de conformidade com a LGPD, permitindo o acompanhamento em tempo real do desempenho da organização em relação aos requisitos de privacidade e segurança. O módulo apresenta gráficos, índices e listagens interativas.

Pré-condição: O ator deve estar autenticado no sistema.

Ator Principal: Administrador ou DPO.

Ator Secundário: Nenhum.

Fluxo Principal:

1. O ator acessa o módulo “Dashboard”.
2. O sistema exibe os indicadores consolidados, tais como:
    a. Percentual de Conformidade;
    b. Nº de Riscos Mapeados;
    c. Ações Atrasadas
    d. Docs Vencendo (30d);
    e. Índice de Maturidade LGPD;
    f. Distribuição de Riscos por Criticidade;
    g. Heatmap;
    h. Riscos por Setor;

i. Os 5 Riscos de maior pontuação;
j. Status dos planos de Ação;
k. Gráfico Planejado X Executado;
l. Percentual de Ações Concluídas;
m. Documentos a vencer;
n. Notificações recentes;
o. Últimos acessos;
p. Usuários mais ativos;

3. O ator aplica filtros visualiza detalhes ao passar o mouse sobre os gráficos.
4. O sistema exibe dinamicamente os detalhes conforme o tipo de gráfico.

Fluxos de Exceção:

- Violação da RN01 → erro de carregamento dos indicadores (falha de rede ou processamento).

Regras de Negócio:

- RN01: Todos os indicadores exibidos devem ser atualizados com base nas fontes oficiais do sistema (Riscos, Ações, Documentos, Checklist e Incidentes).
- RN02: O índice de maturidade é recalculado automaticamente a cada alteração no checklist e planos de ações.
- RN03: O Dashboard deve atualizar os indicadores em tempo real a cada acesso.

Pós-condição: O usuário visualizou os indicadores consolidados de conformidade e obteve uma visão geral da situação atual da organização frente à LGPD.

CDU16 – Visualizar Notificações e Alertas de Prazo e Segurança

Sumário: Por meio deste caso de uso, os usuários poderão visualizar as notificações e alertas gerados automaticamente pelo sistema. Essas notificações incluem avisos de prazos de conformidade (documentos, planos de ação, incidentes e eventos do calendário) e alertas de segurança direcionados ao DPO quando forem detectadas atividades suspeitas, tentativas de acesso não autorizadas ou ações críticas incomuns. O objetivo é permitir o acompanhamento preventivo das obrigações de conformidade e garantir a rastreabilidade e segurança das operações do sistema Camaleão.

Pré-condição: O usuário deve estar autenticado. Devem existir notificações e/ou alertas gerados automaticamente pelo sistema (ver CDU14).

Ator Principal: Usuário Autenticado (Administrador, DPO ou Gerente).

Ator Secundário: Sistema (responsável por gerar, registrar e atualizar as notificações).

Fluxo Principal:

1. O usuário acessa o módulo “Notificações”.
2. O sistema exibe a lista de notificações disponíveis, módulo de origem e status (Pendente, Visualizado, Resolvido).
3. O sistema filtra e exibe apenas as notificações relacionadas ao usuário:
4. Administrador: recebe notificações de prazos gerais e alertas sobre atrasos críticos em qualquer módulo;
5. DPO: recebe todas as notificações e alertas de segurança detectados;
6. Gerente: recebe notificações de prazos e monitoramentos sob sua responsabilidade;
7. O usuário clica em uma notificação para visualizar seus detalhes.
8. O sistema exibe as informações completas (tipo, descrição, data de emissão, prazo e módulo de origem).
9. O usuário pode optar por marcar como resolvida ou acessar o módulo correspondente (ex.: Documentos, Planos de Ação, Incidentes, Calendário).
10. O sistema atualiza o status da notificação e registra o log de visualização.

Fluxo Secundário: Visualizar Alertas de Segurança (DPO)

1. O DPO acessa o painel “Alertas de Segurança”.
2. O sistema exibe a lista de eventos suspeitos detectados (data, hora, módulo, usuário e tipo de ação).
3. O DPO analisa o alerta e decide se deve abrir um incidente (extend CDU10 – Gerir Incidentes).
4. O DPO pode marcar o alerta como “Investigado” ou “Falso Positivo”.
5. O sistema atualiza o status e registra o log de auditoria.

Fluxo Secundário: Marcar como resolvida

1. O usuário seleciona uma notificação.
2. O sistema exibe a opção “Marcar como resolvida”.
3. O usuário confirma a ação.
4. O sistema atualiza o status e registra a data e hora da resolução.

Fluxos de Exceção:

- Violação da RN01 → falha na leitura ou atualização das notificações.
- Violação da RN02 → erro de sincronização ao exibir alertas recentes.
- Violação da RN03 → falha na comunicação ao atualizar status ou logs.

Regras de Negócio:

- RN01: O sistema gera notificações de prazo automaticamente a cada semana, considerando prazos até 30 dias à frente.
- RN02: Alertas de segurança são criados imediatamente após a detecção de eventos suspeitos nos logs (CDU14).
- RN03: Cada notificação ou alerta deve conter: módulo de origem, tipo de evento, descrição, responsável e data de emissão.
- RN04: O sistema exibe apenas notificações correspondentes ao usuário autenticado.
- RN05: O DPO é o único ator autorizado a visualizar alertas de segurança e investigar ocorrências.
- RN06: O sistema deve remover automaticamente notificações de prazo expiradas há mais de 90 dias, preservando os registros de alerta e auditoria.
- RN07: Todos os eventos (criação, envio, leitura e resolução) devem ser registrados em log.
- RN08: O DPO deve receber um aviso imediato por e-mail em caso de alerta de segurança de nível crítico.

Pós-condição: O usuário visualizou suas notificações e, se aplicável, marcou-as como resolvidas. O DPO recebeu e analisou os alertas de segurança, podendo abrir incidentes ou registrar investigação. O sistema manteve o histórico completo de todas as notificações e alertas, garantindo rastreabilidade, transparência e conformidade com a LGPD.

CDU17 – Gerar Relatórios de Conformidade

Sumário: Por meio deste caso de uso, o usuário poderá gerar relatórios detalhados com base nas informações dos módulos do sistema (Inventário, Riscos, Planos de Ação, Documentos, Checklist, Incidentes e Auditorias). Esses relatórios servem como evidência de conformidade e suporte para auditorias internas e externas.

Pré-condição: O ator deve estar autenticado e possuir permissão de exportação de relatórios.

Ator Principal: Administrador, DPO ou Gerente (com permissões limitadas).

Ator Secundário: Nenhum.

Fluxo Principal:

1. O ator acessa o módulo “Relatórios”.
2. O sistema apresenta os tipos de relatórios disponíveis:
    a. Inventário de Dados;
    b. Ranking de Riscos;
    c. Heatmap de Riscos;
    d. Planos de Ação;
    e. Documentos LGPD;
    f. Checklist de Conformidade;
    g. Auditoria de Logins.
3. O ator seleciona o tipo de relatório desejado.
4. O sistema solicita o formato de exportação (CSV, XLSX ou PDF).
5. O ator aplica filtros opcionais (período, setor, criticidade).
6. O sistema processa os dados, gera o arquivo e disponibiliza o download.

Fluxos de Exceção:

- Violação da RN01 → sistema informa que não há dados disponíveis para os filtros selecionados.
- Violação da RN02 → erro de processamento ou falha na geração do arquivo.
- Violação da RN03 → usuário sem permissão para exportar determinado relatório.

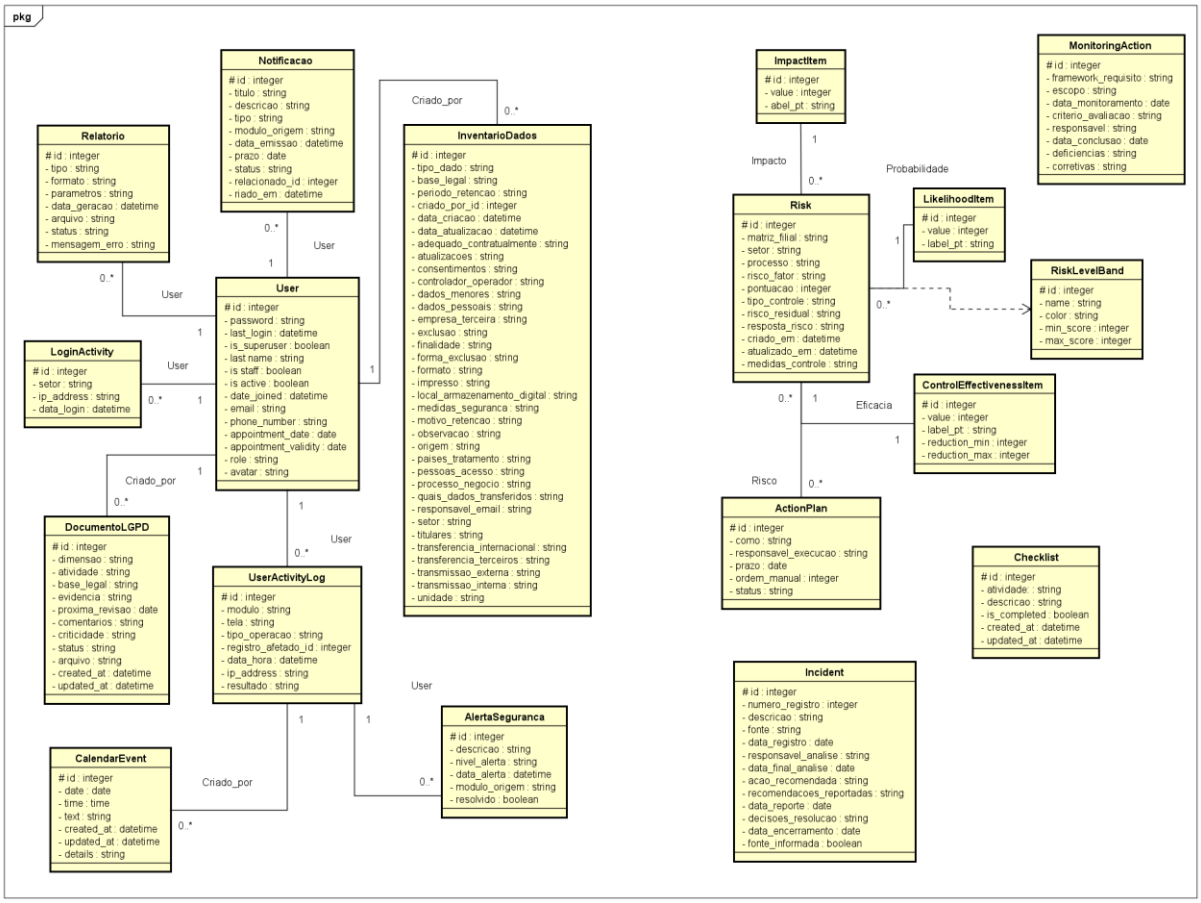
Regras de Negócio:

- RN01: Os relatórios respeitam os filtros aplicados pelo usuário.
- RN02: Formatos suportados: (CSV, XLSX, PDF).
- RN04: O sistema deve registrar logs de todas as exportações realizadas (data, usuário e tipo de relatório).
- RN05: Todos os relatórios devem conter título, data de geração e origem dos dados.

Pós-condição: Um relatório foi gerado e exportado com sucesso. O sistema registrou a operação e disponibilizou o arquivo ao usuário para download e arquivamento.

APÊNDICE C: DIAGRAMA DE CLASSES DE DADOS

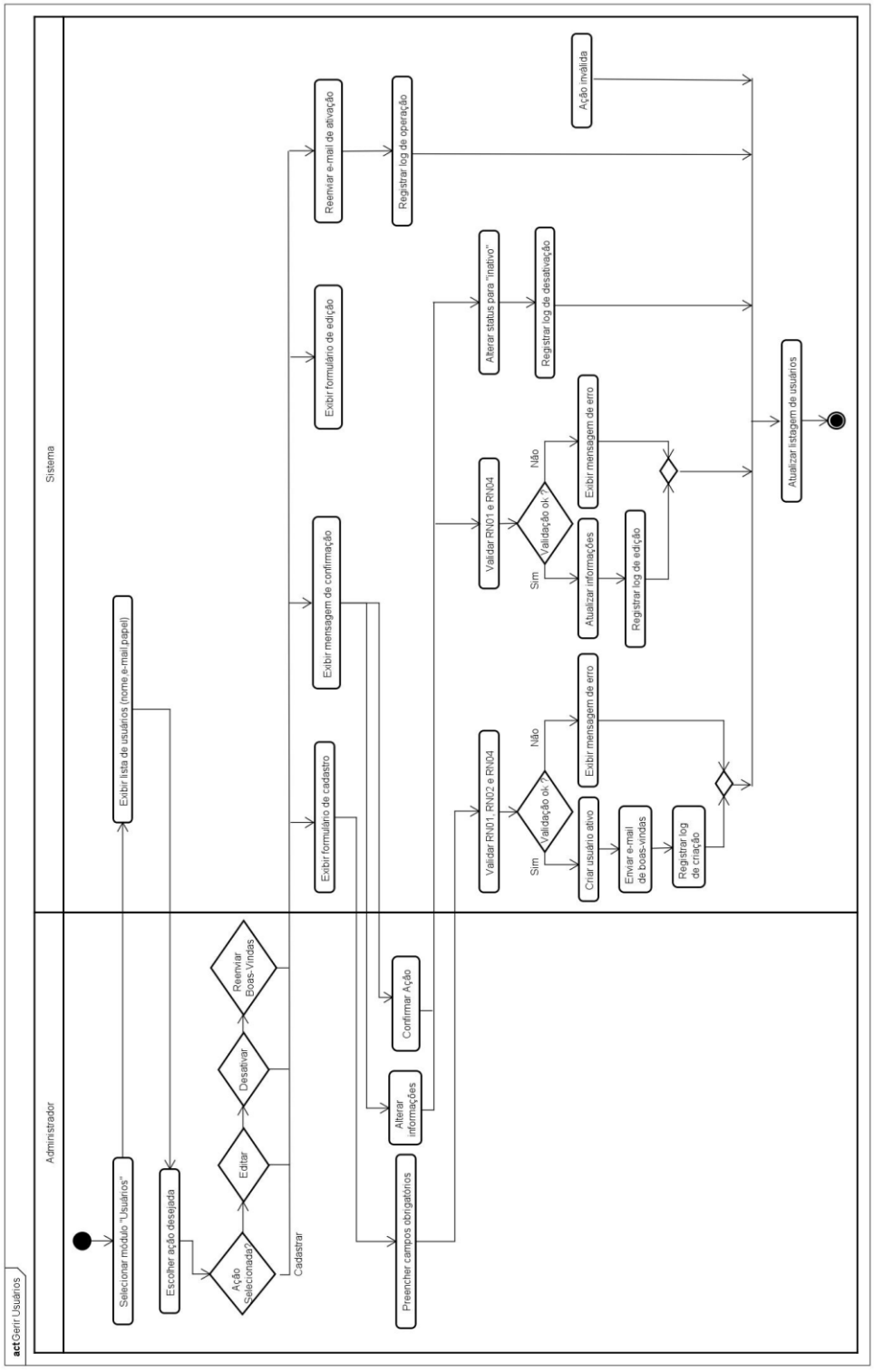
Figura 46: Diagrama de Classes de Dados



Fonte: Elaboração Própria

APÊNDICE D: DIAGRAMA DE ATIVIDADES

Figura 47: Gerir Usuários (Diagrama de Atividades)



Fonte: Elaboração Própria

Figura 48: Fazer Login/Logout (Diagrama de Atividades)

Fonte: Elaboração Própria

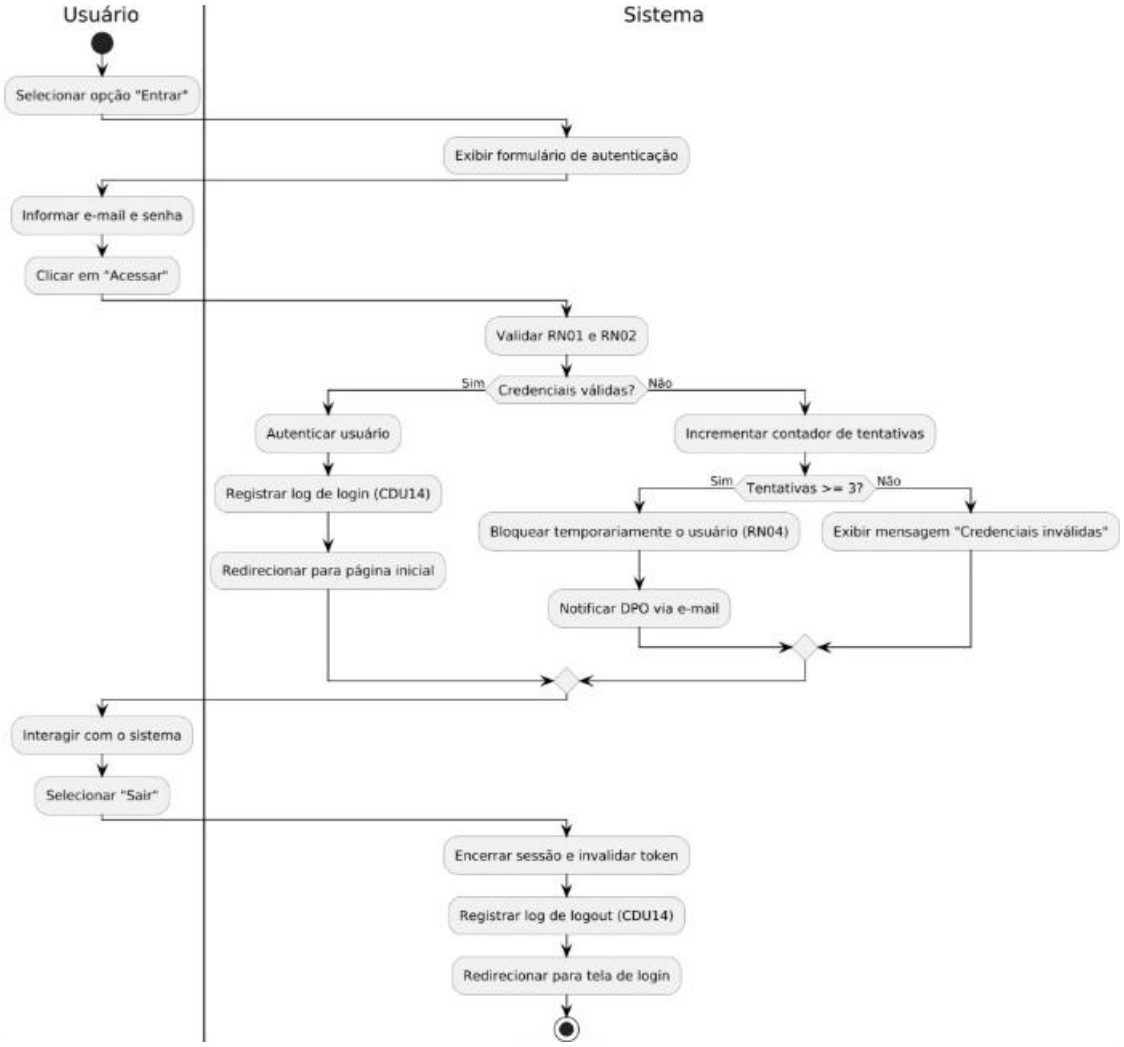
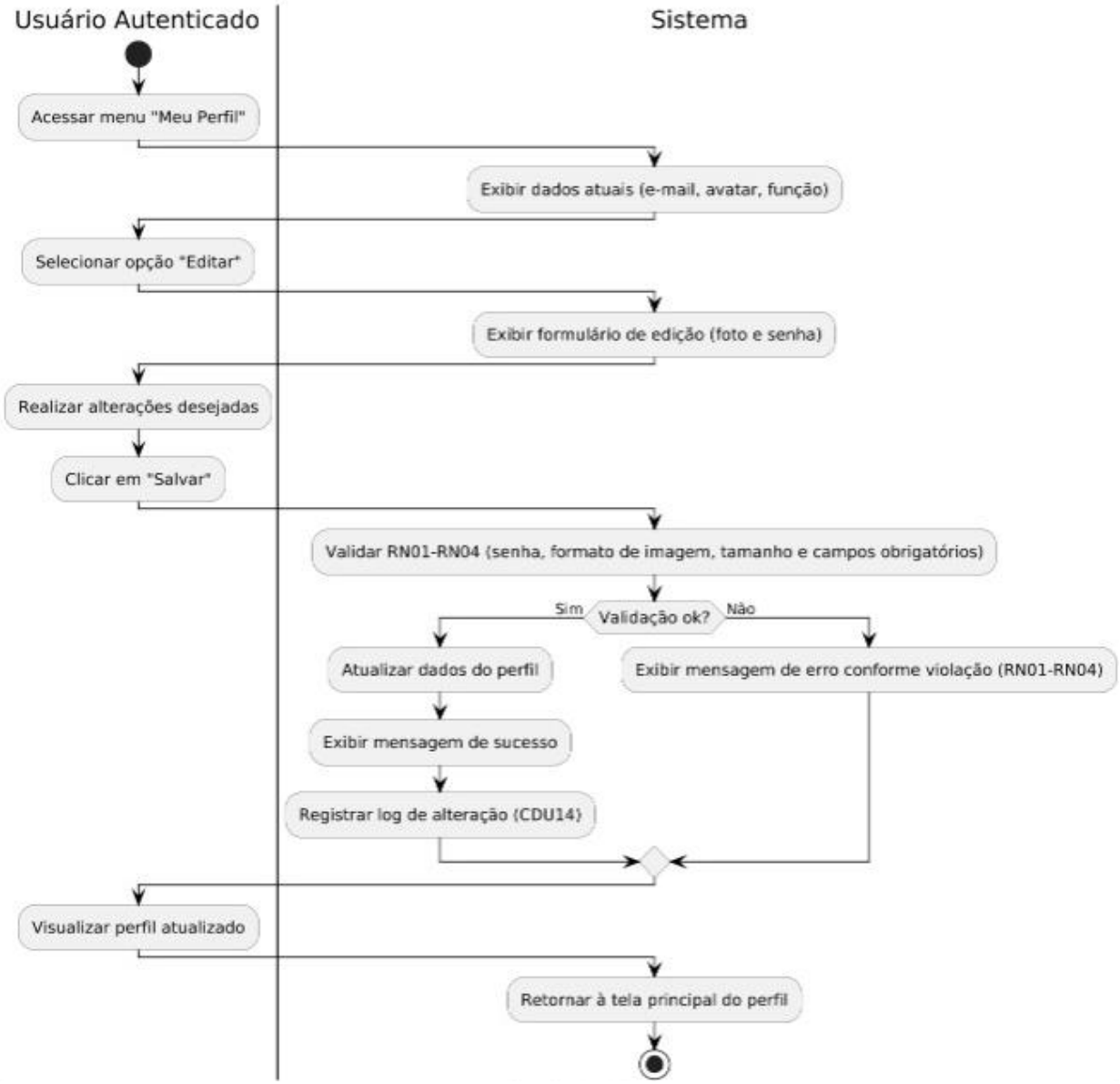
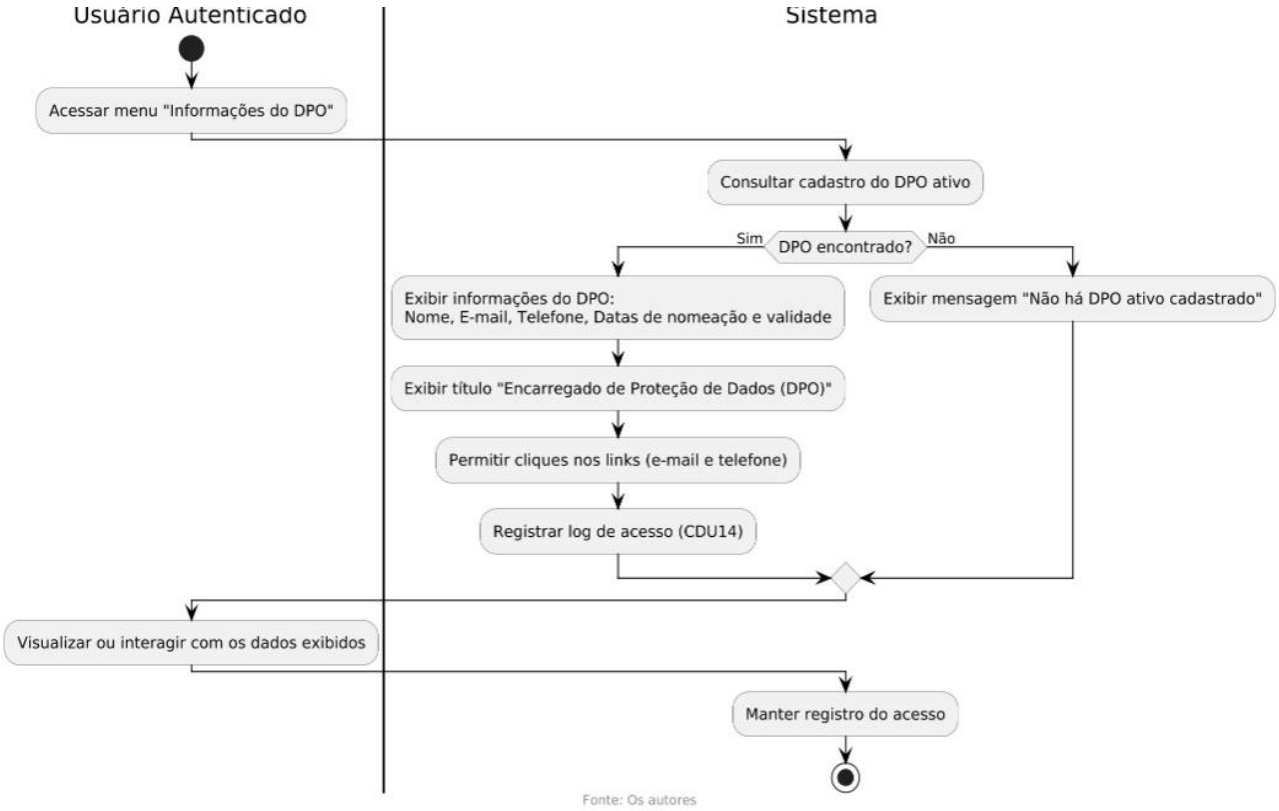


Figura 49: Gerir Perfil do Usuário (Diagrama de Atividades)



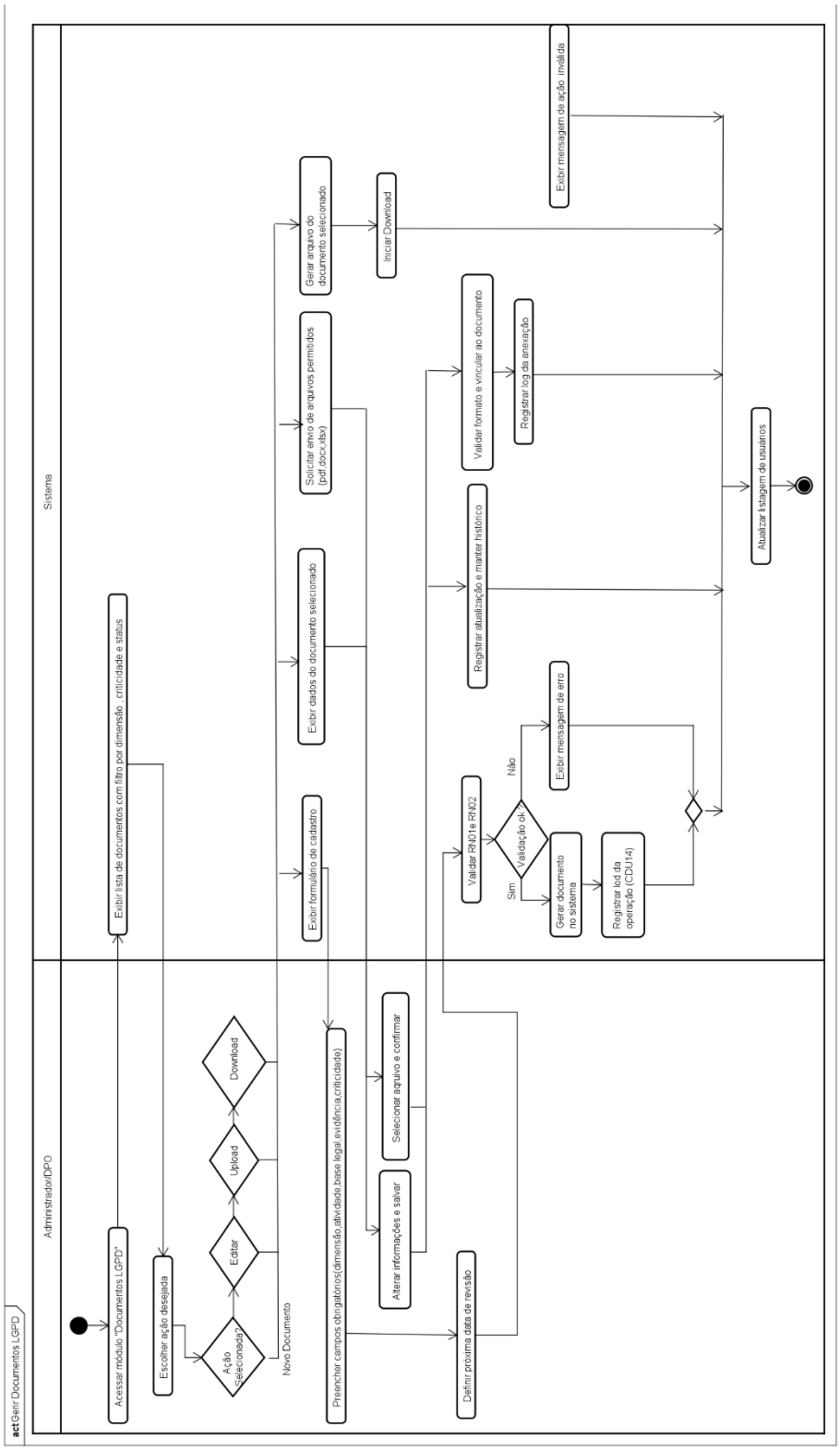
Fonte: Elaboração Própria

Figura 50: Visualizar Informações do DPO (Diagrama de Atividades)



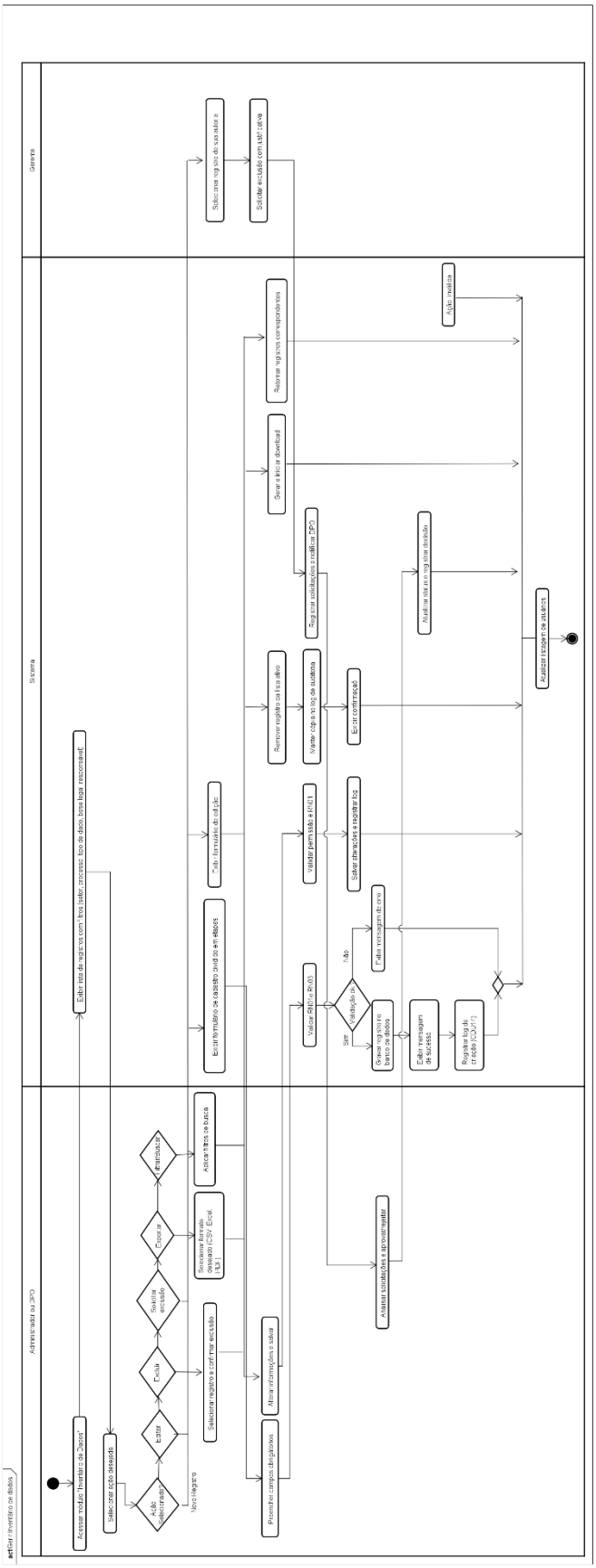
Fonte: Elaboração Própria

Figura 51 Gerir Documentos LGPD (Diagrama de Atividades)



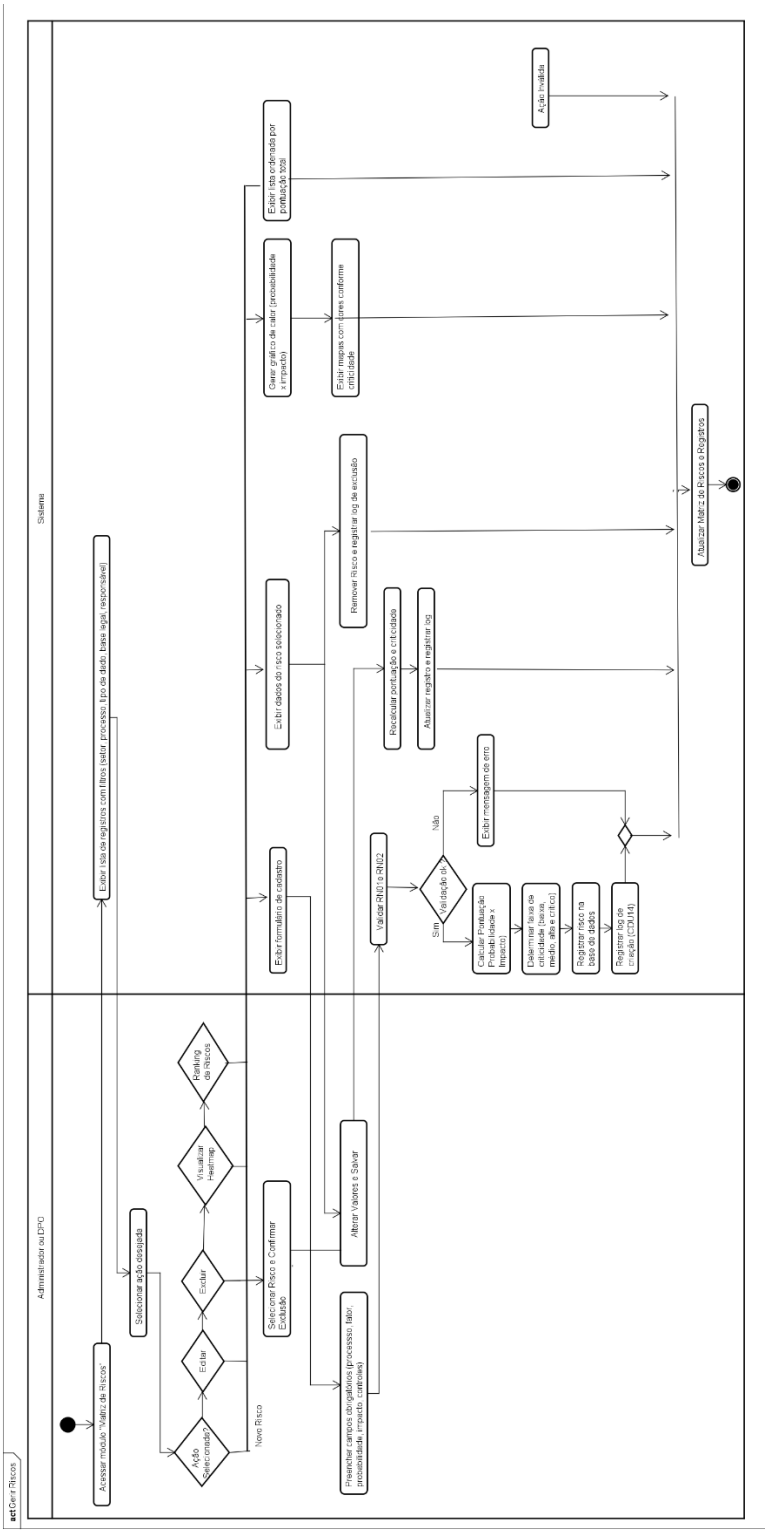
Fonte: Elabração Própria

Figura 52: Gerir Inventário de Dados (Diagrama de Atividade)



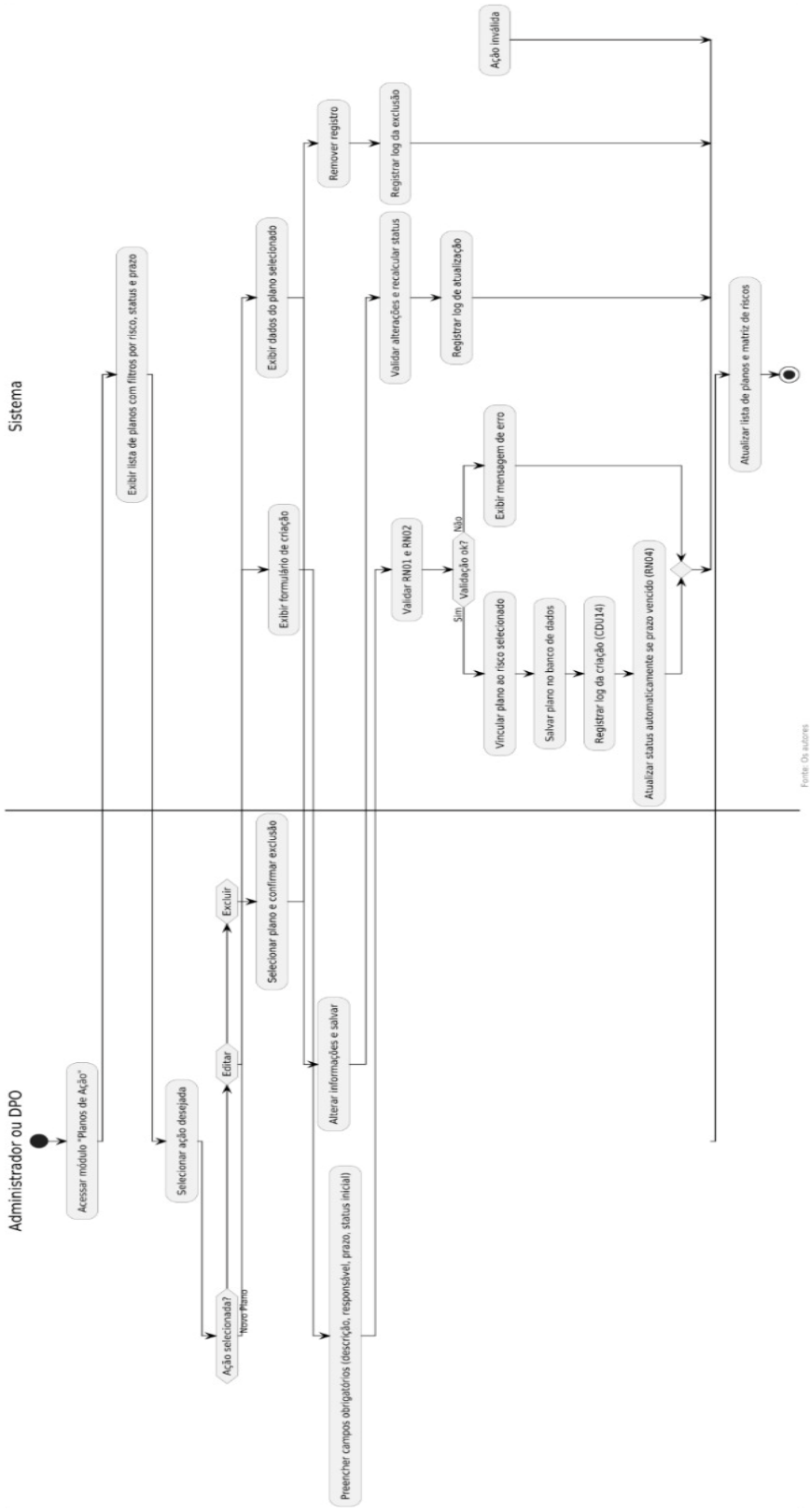
Fonte: Elabração Própria

Figura 53: Gerir Riscos - Matriz de Riscos LGPD (Diagrama de Atividades)



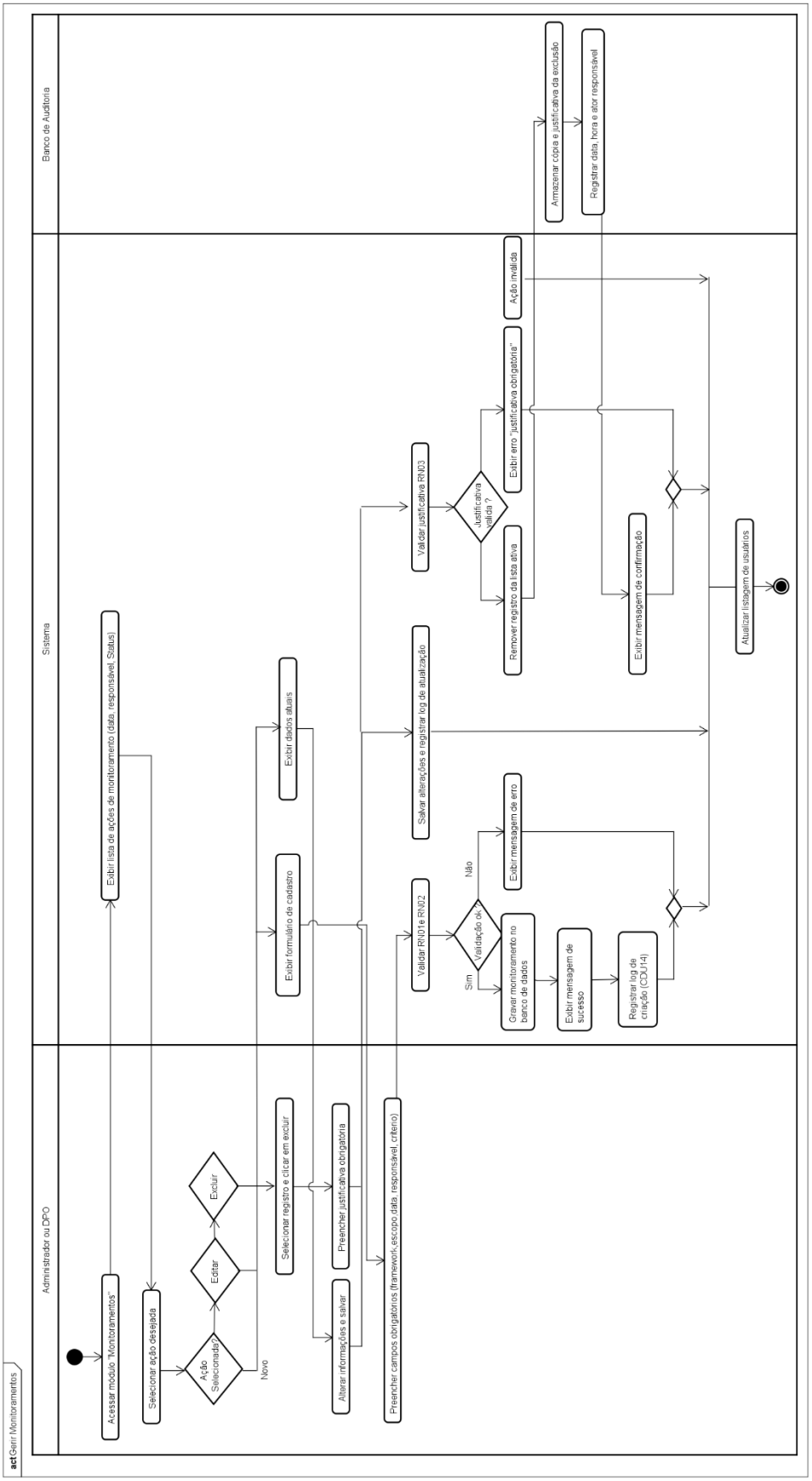
Fonte: Elabração Própria

Figura 54: Gerir Planos de Ação (Diagrama de Atividades)



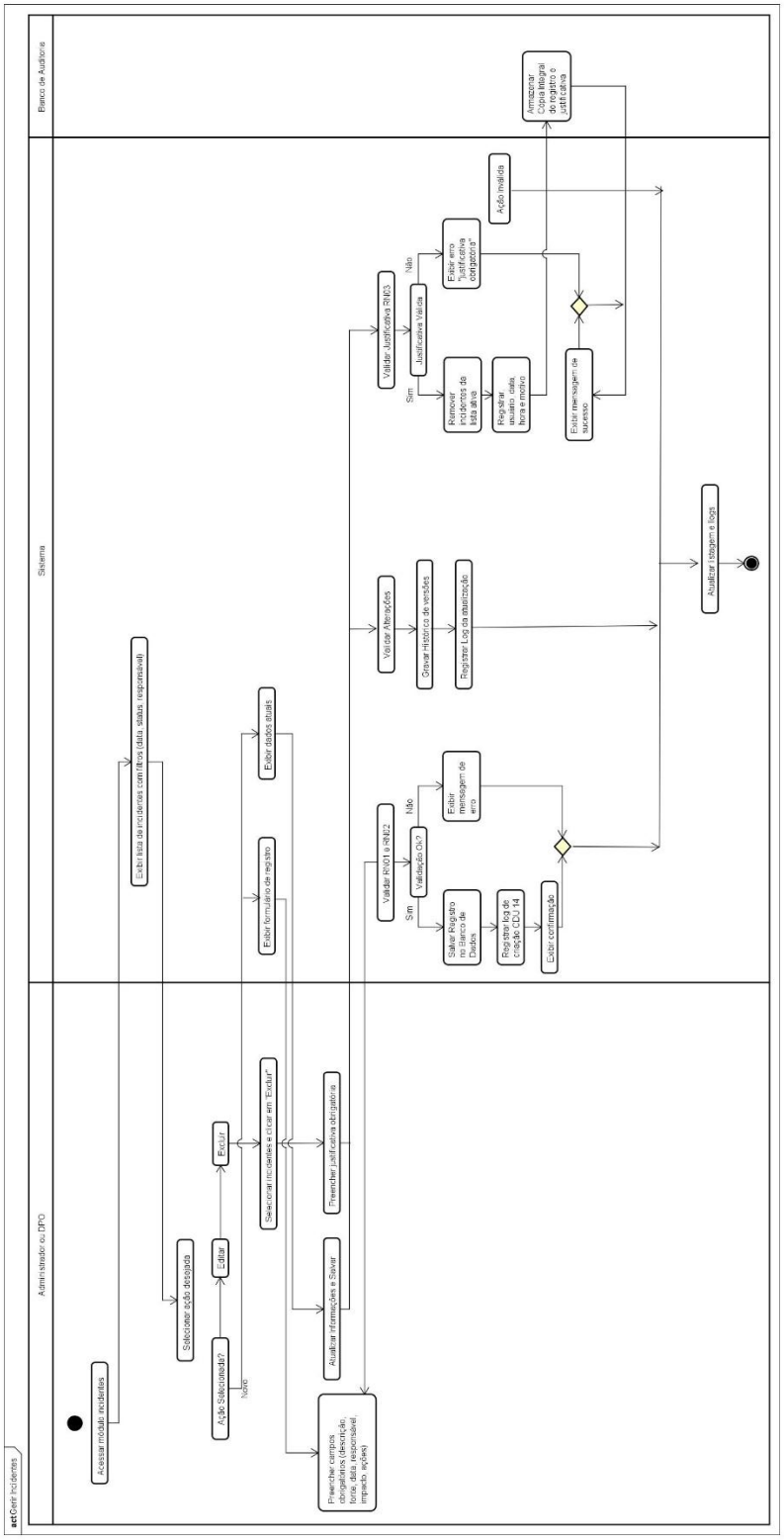
Fonte: Elabração Própria

Figura 55: Gerir Monitoramentos (Diagrama de Atividades)



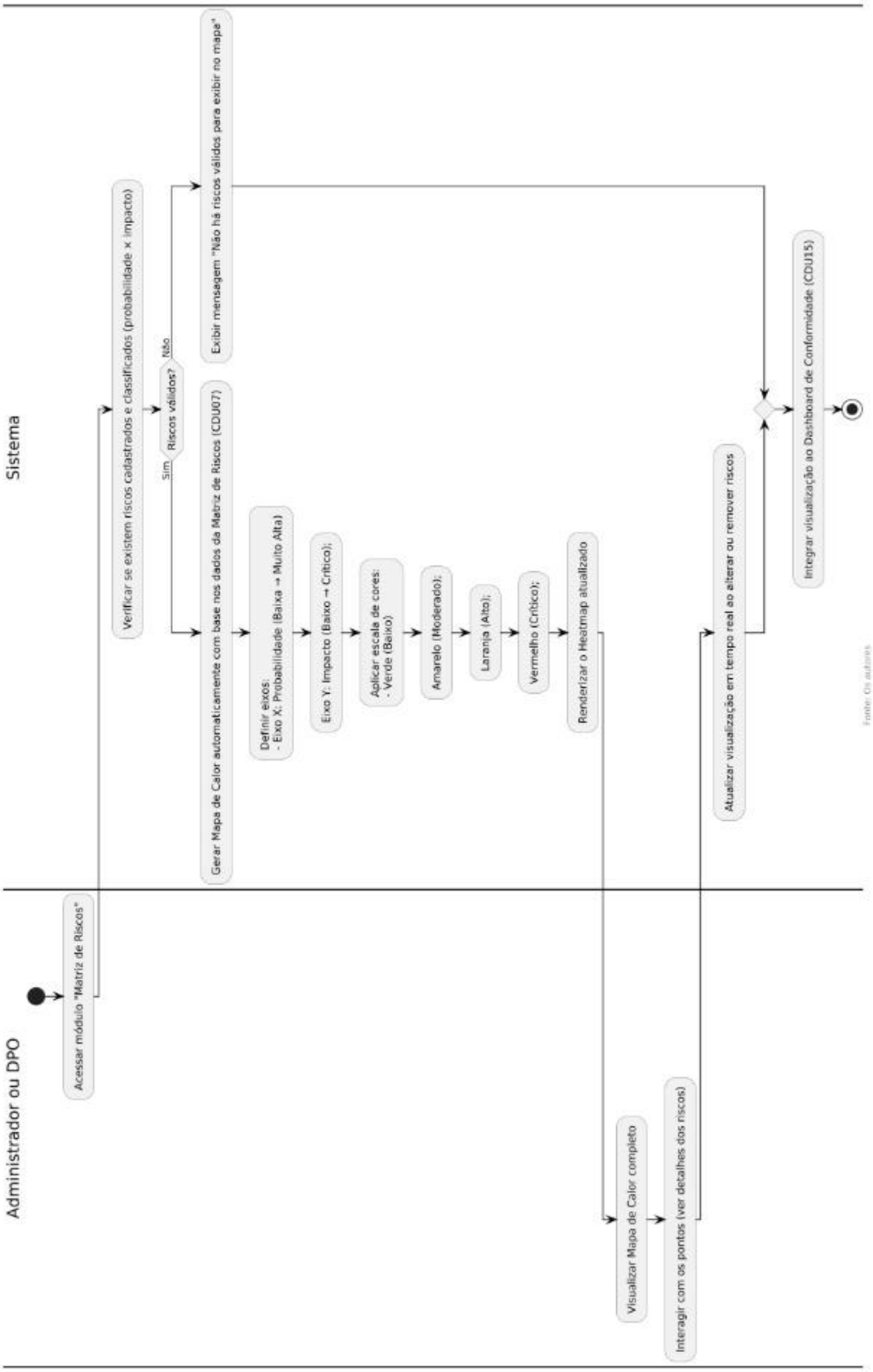
Fonte: Elaboração Própria

Figura 56: Gerir Incidentes(Diagrama de Atividades)



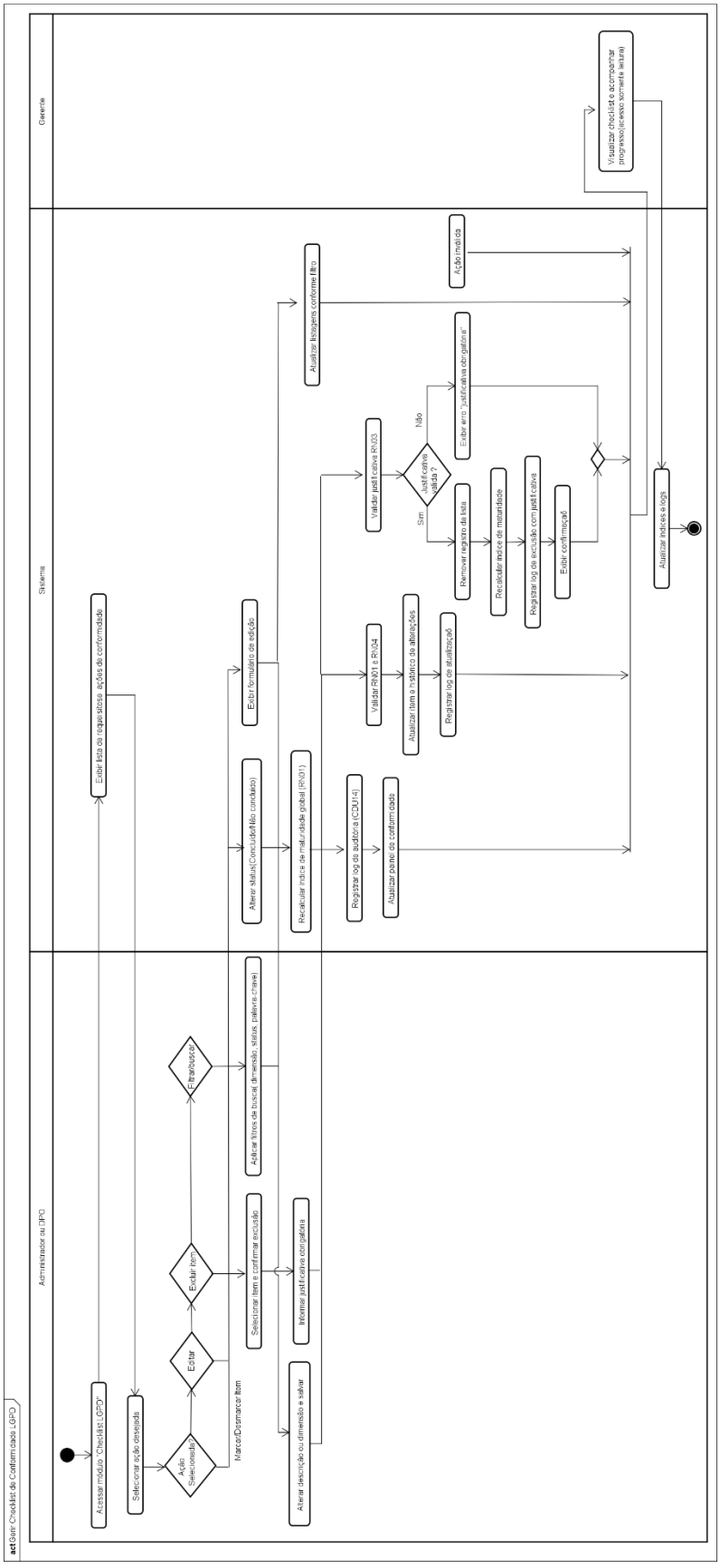
Fonte Elaboração Própria

Figura 57: Visualizar Mapa de Calor de Riscos (Diagrama de Atividades)



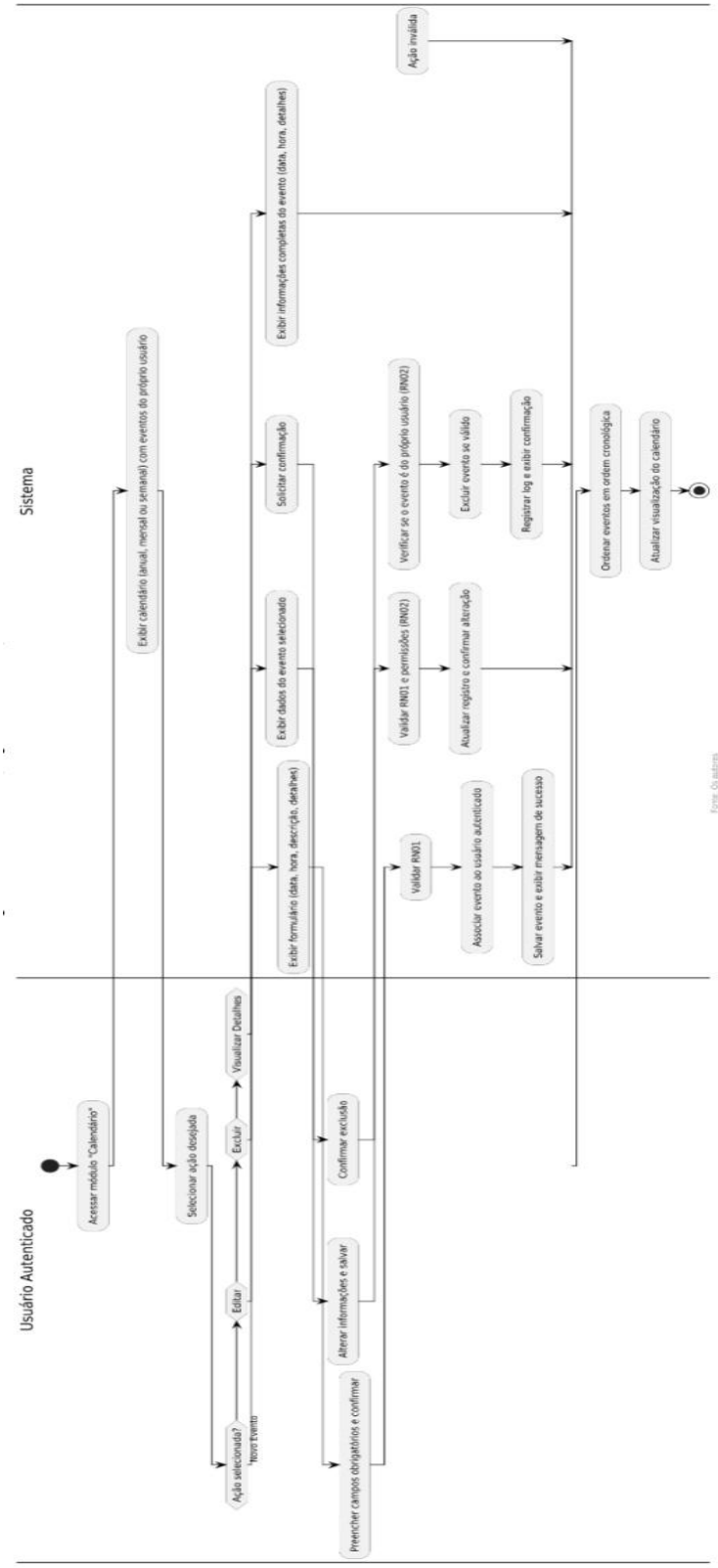
Fonte:Elaboração Própria

Figura 58: Gerir Checklist de Conformidade LGPD (Diagrama de Atividades)



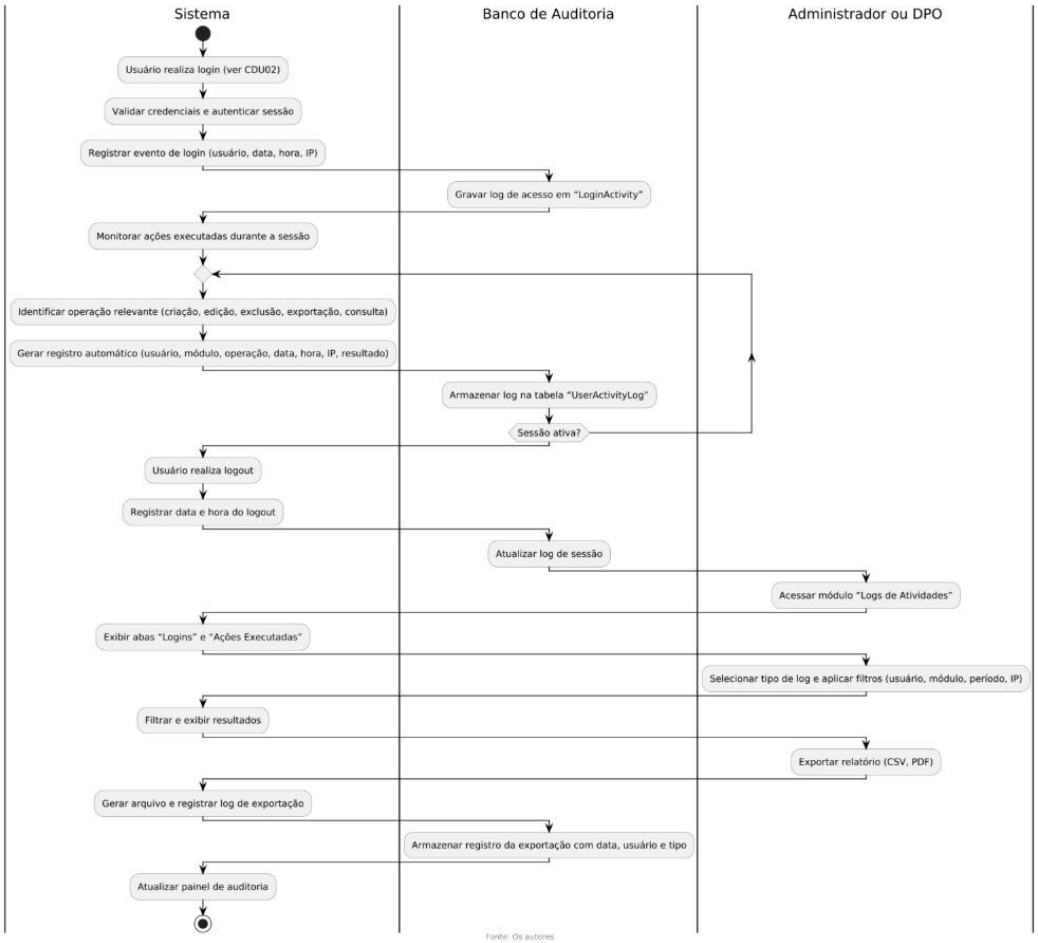
Fonte:Elaboração Própria

Figura 59: Gerir Calendári (Diagrama de Atividades)



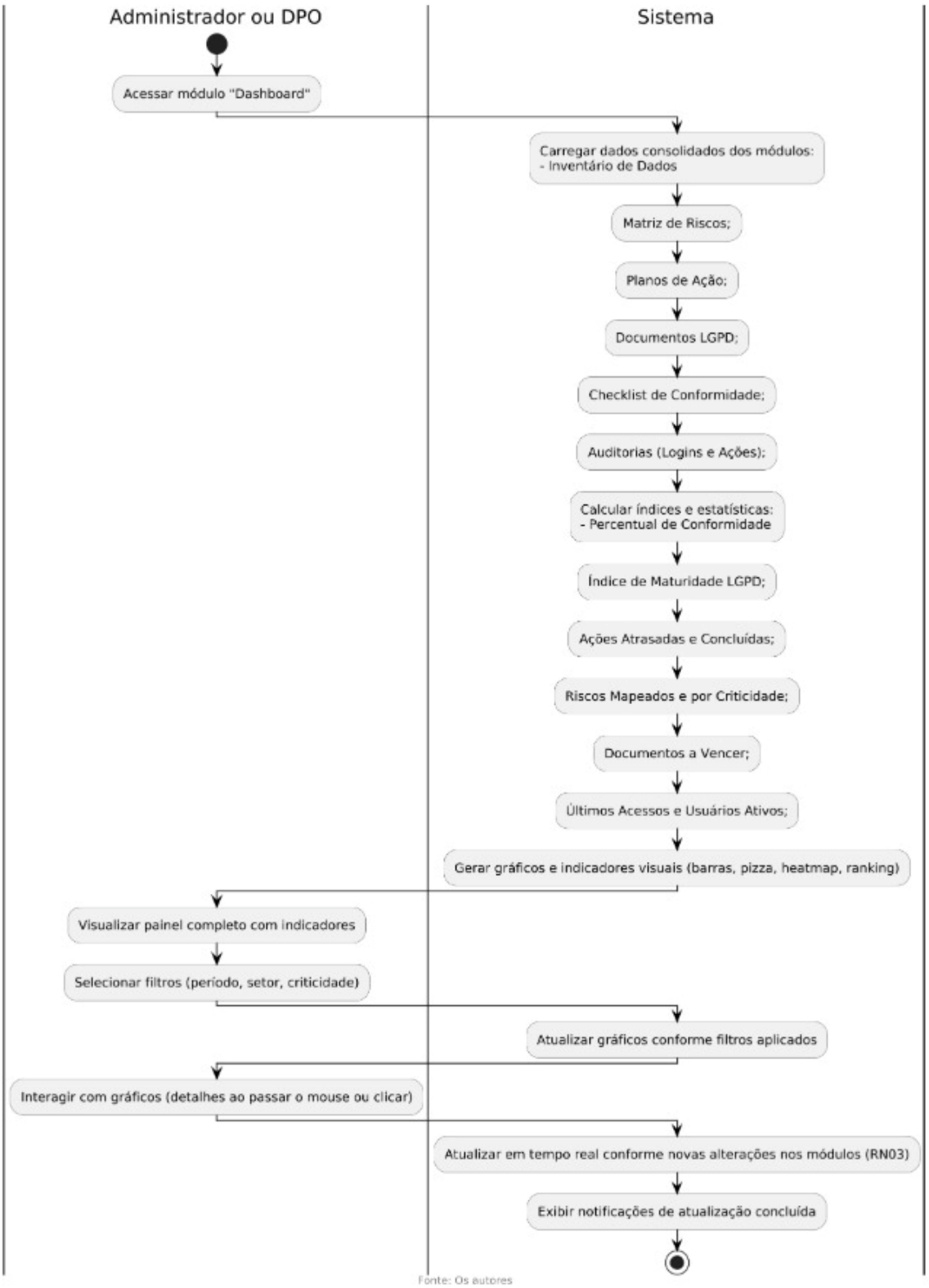
Fonte:Elaboração Própria

Figura 60: Registrar e Consultar Atividade de Login e Operações do Usuário (Diagrama de Atividades)



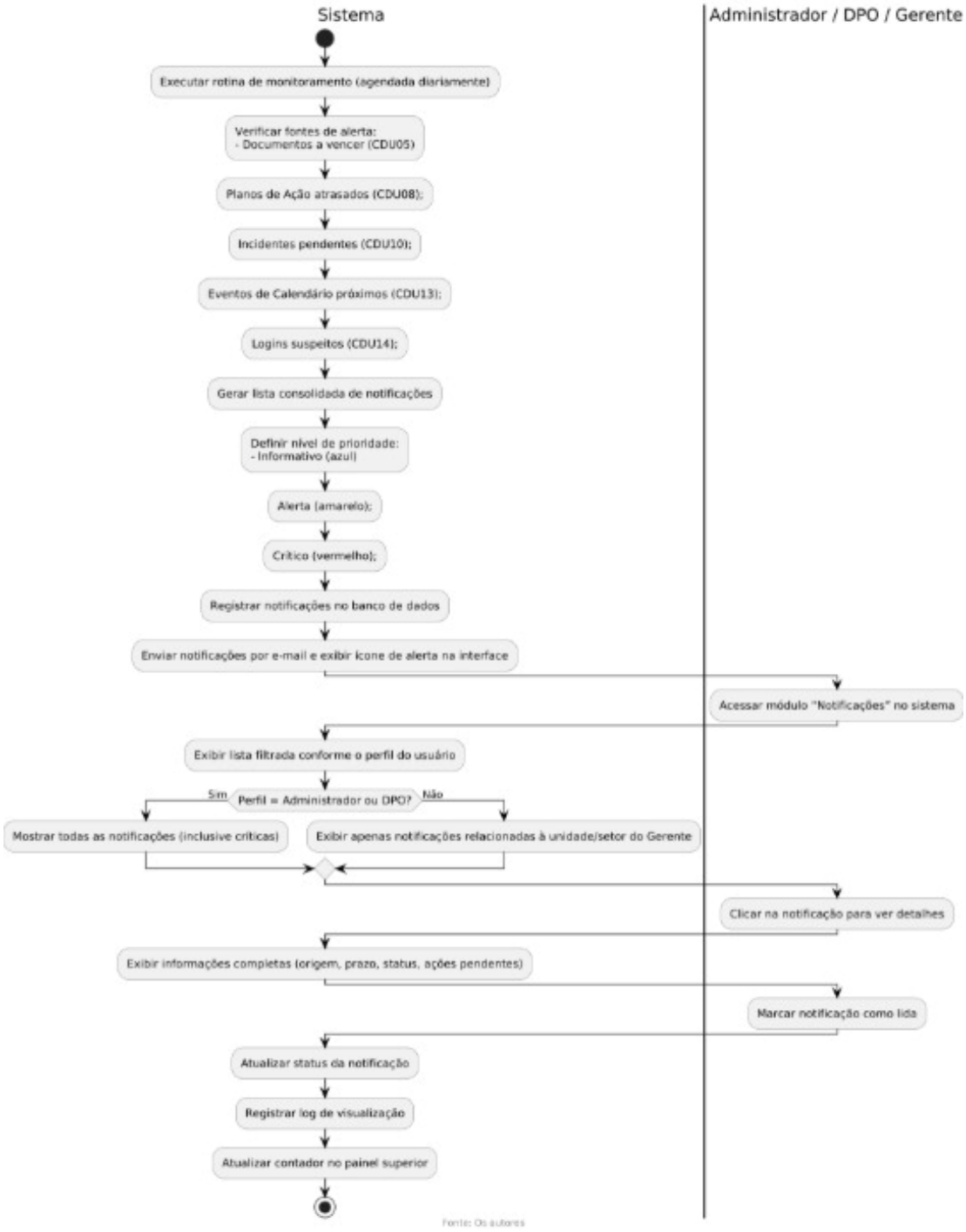
Fonte: Elaboração Própria

Figura 61: Visualizar Dashboard



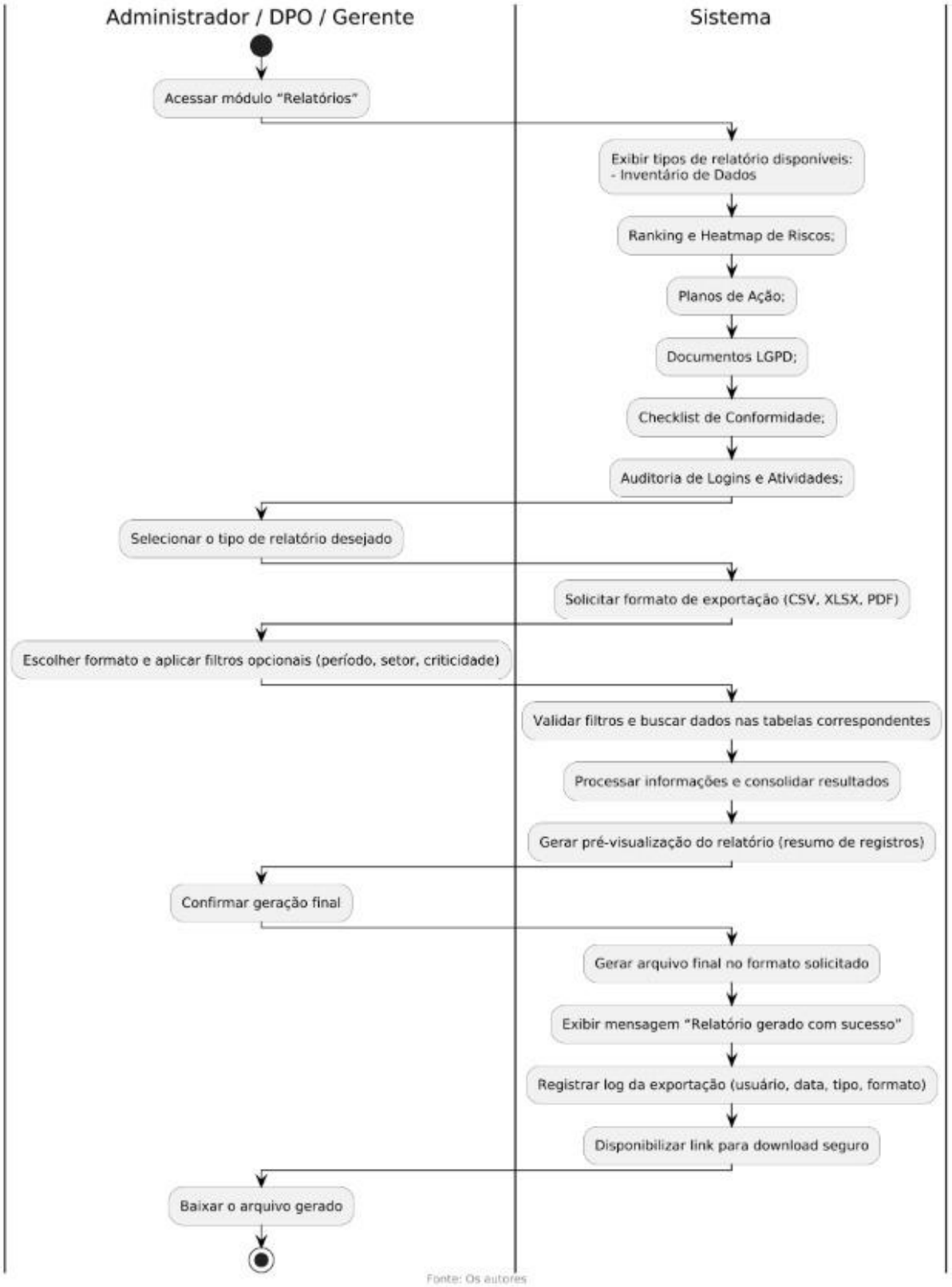
Fonte: Elaboração Própria

Figura 62: Visualizar Notificações e Alertas de Prazo e Segurança(Diagrama de Atividades)



Fonte: Elaboração Própria

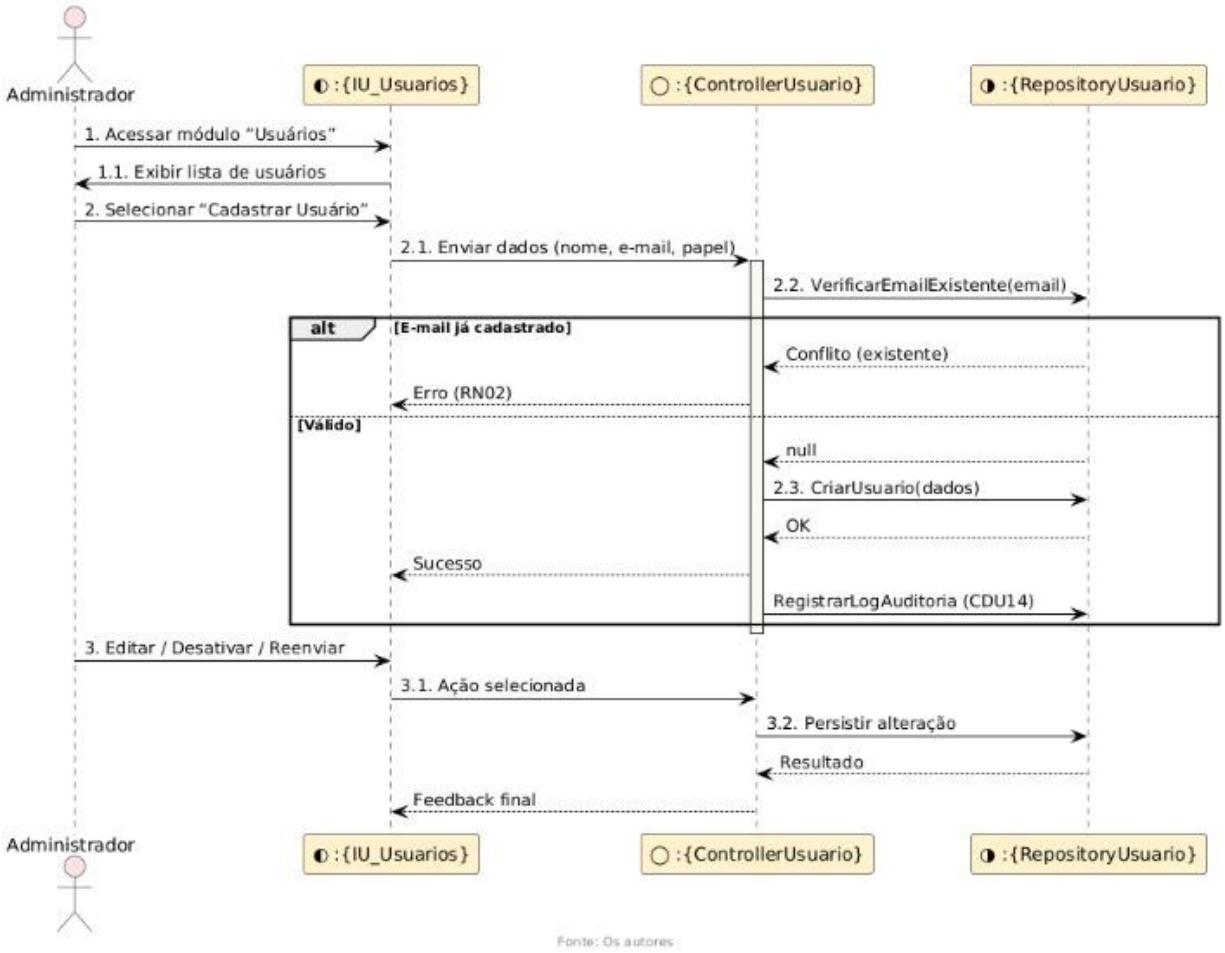
Figura 63: Gerar Relatórios de Conformidade (Diagrama de Atividades)



Fonte: Elaboração Própria

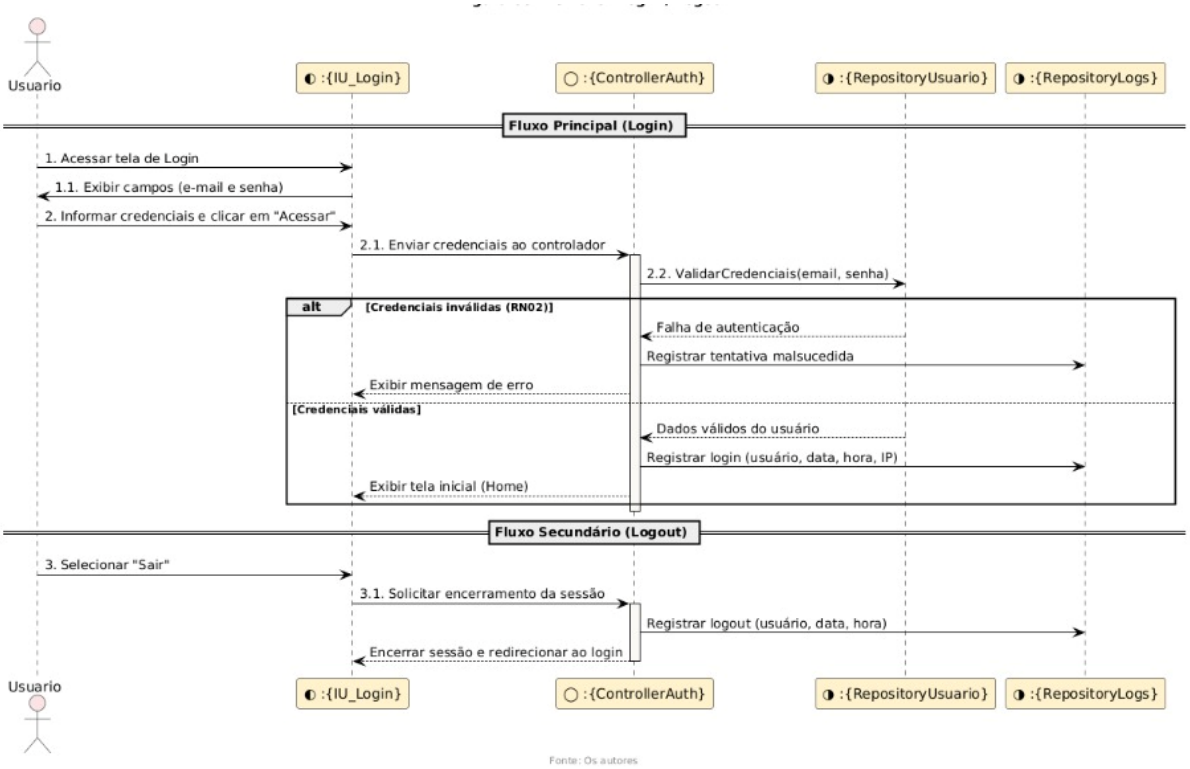
APÊNDICE E: DIAGRAMA DE SEQUÊNCIA

Figura 64: Gerir Usuário



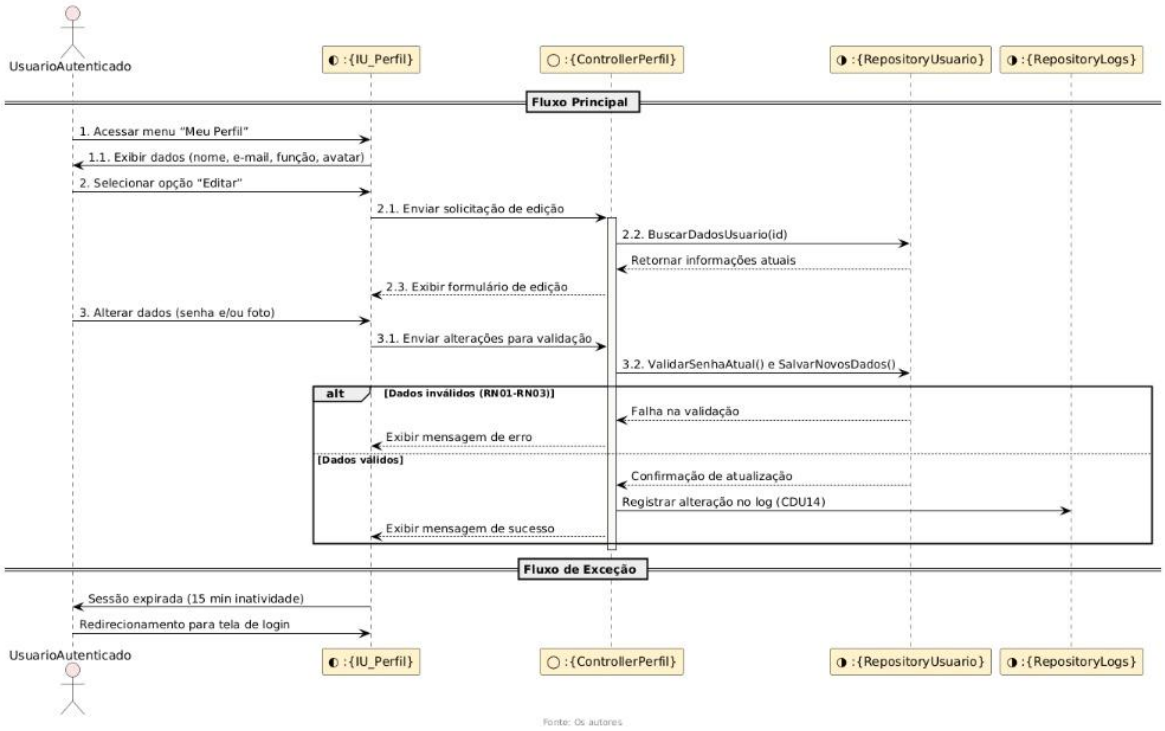
Fonte: Elaboração Própria

Figura 65: Login/Logout



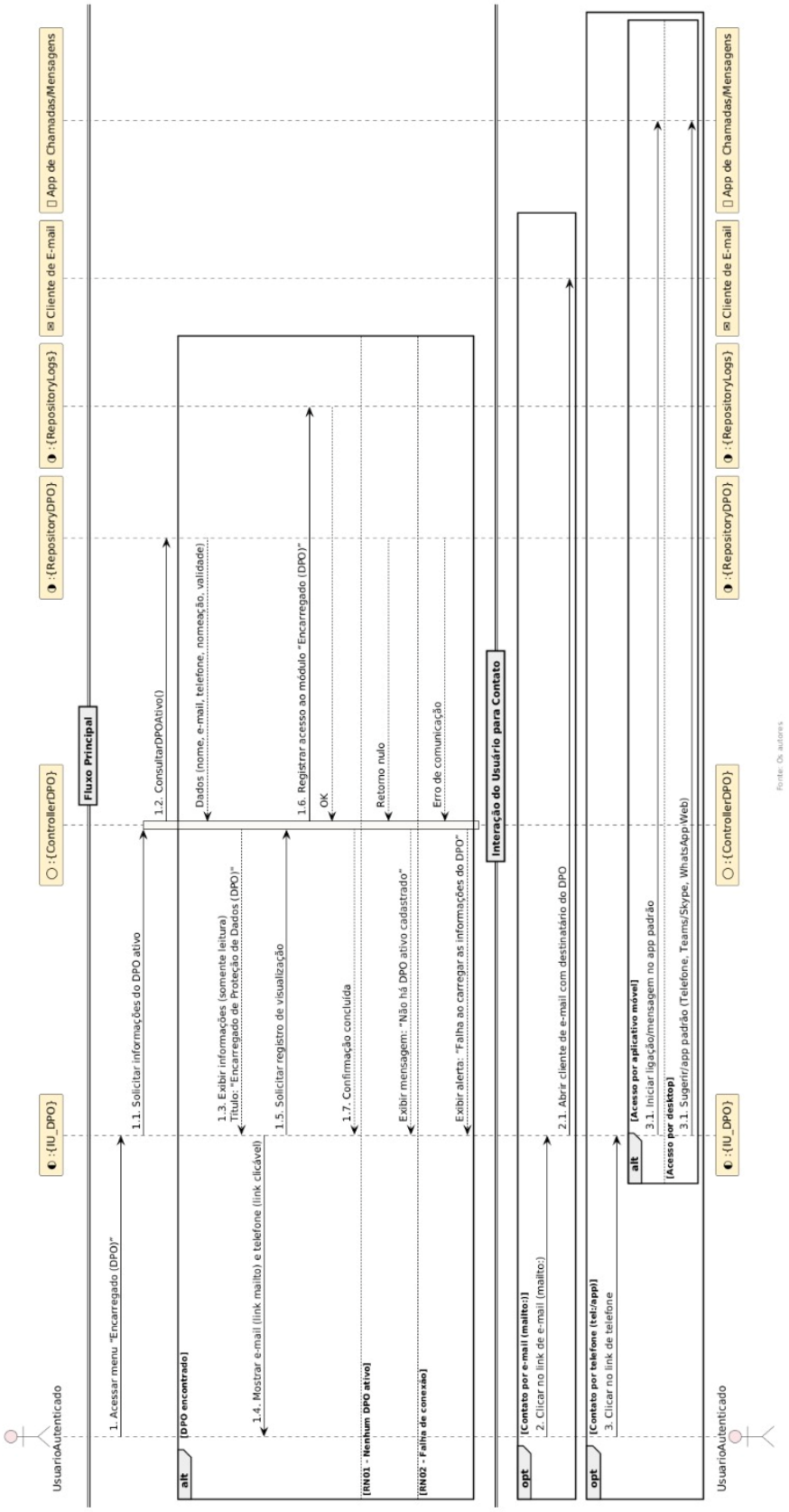
Fonte: Elaboração Própria

Figura 66: Gerir Perfil



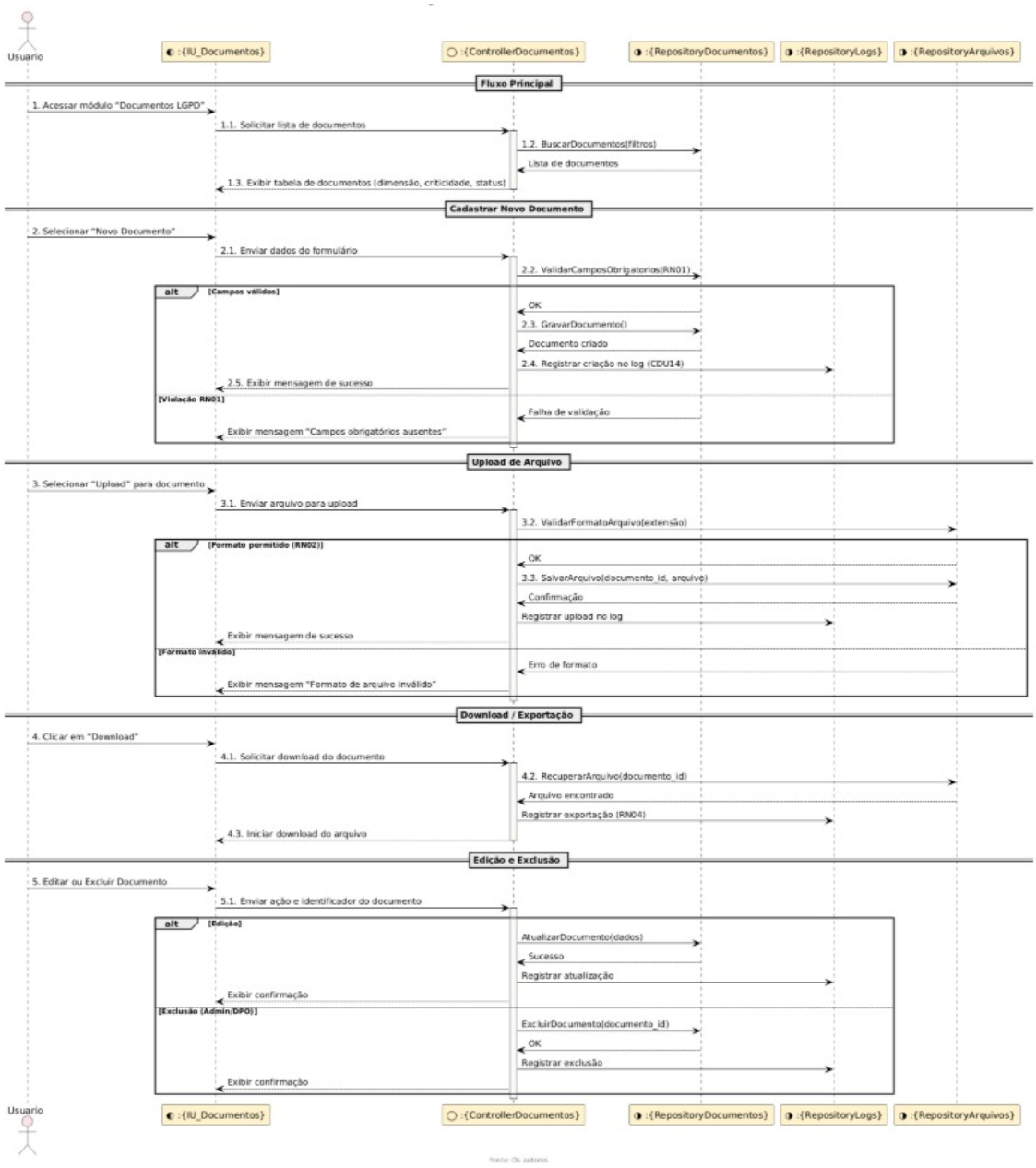
Fonte: Elaboração Própria

Figura 67: Página do Encarregado (DPO)



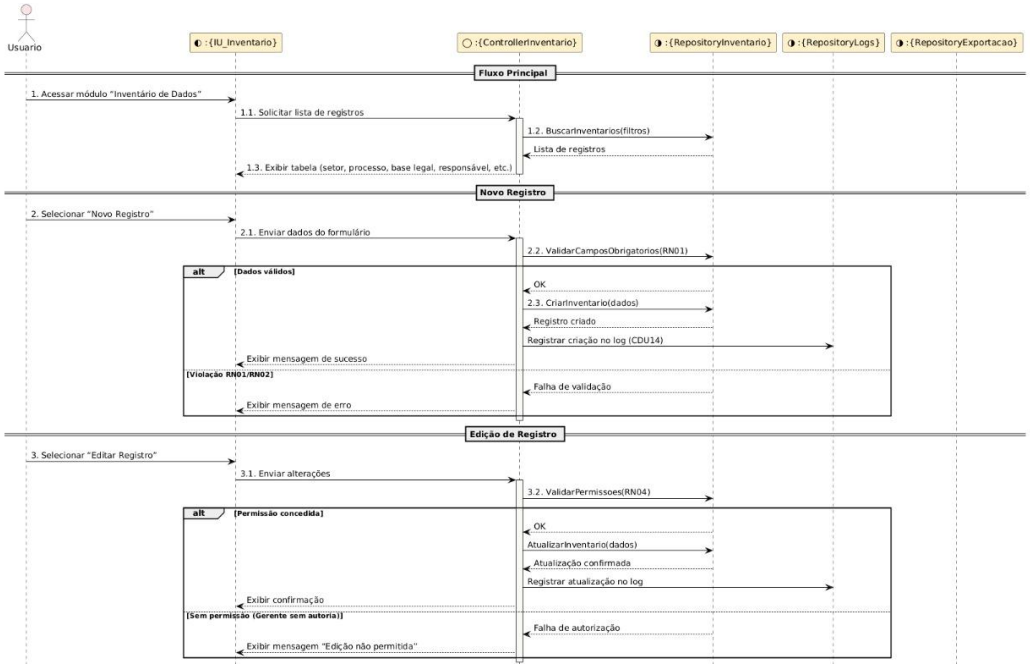
Fonte: Elaboração Própria

Figura 68: Gerir Documentos



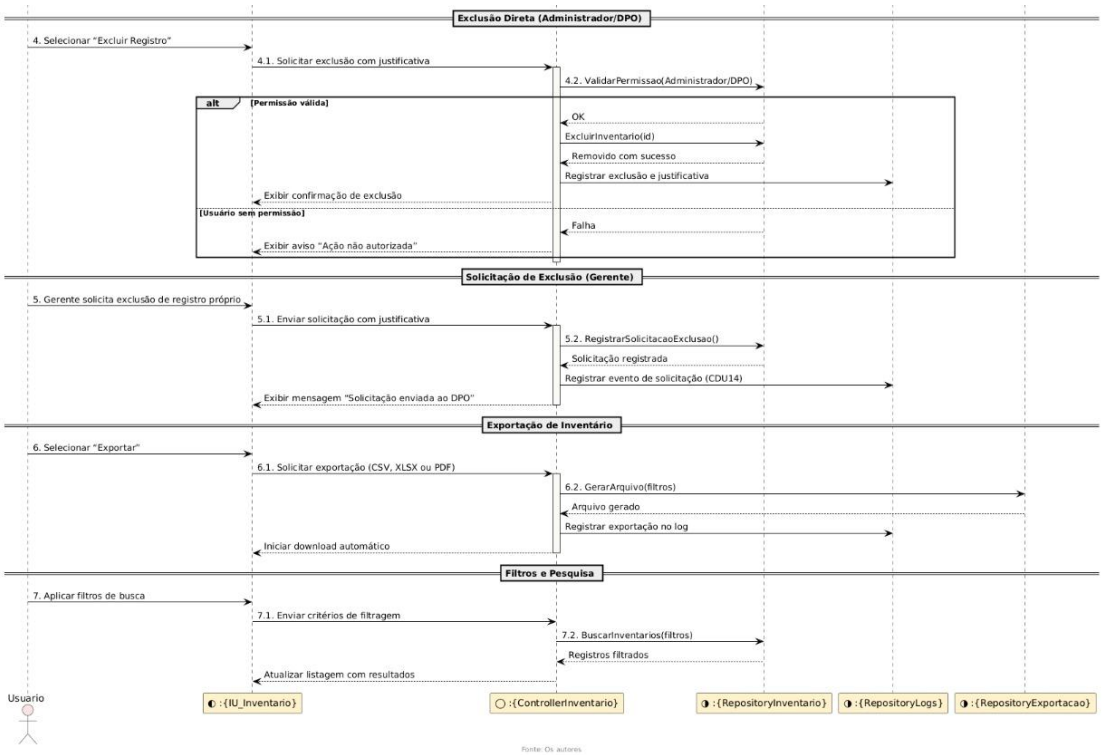
Fonte: Elaboração Própria

Figura 69: Gerir Inventário de Dados (Figura 1)



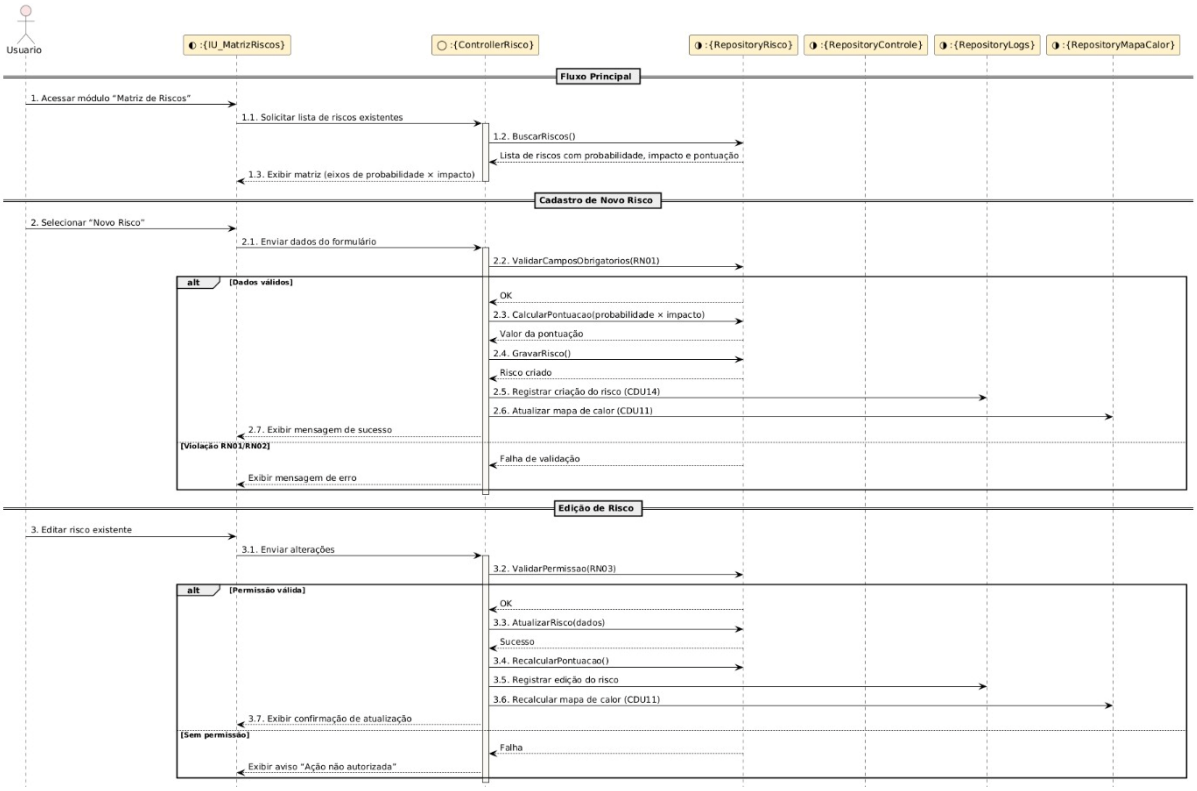
Fonte: Elaboração Própria

Figura 70: Gerir Inventário de Dados (Figura 2)



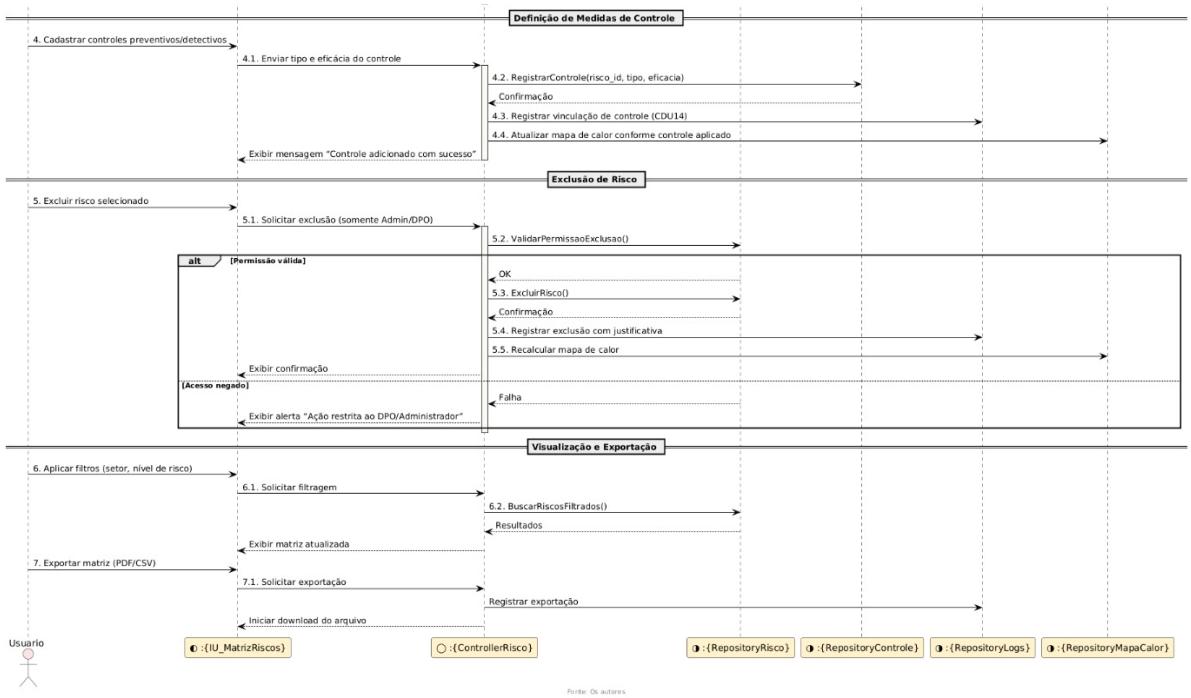
Fonte: Elaboração Própria

Figura 71: Gerir Riscos (Figura 1)



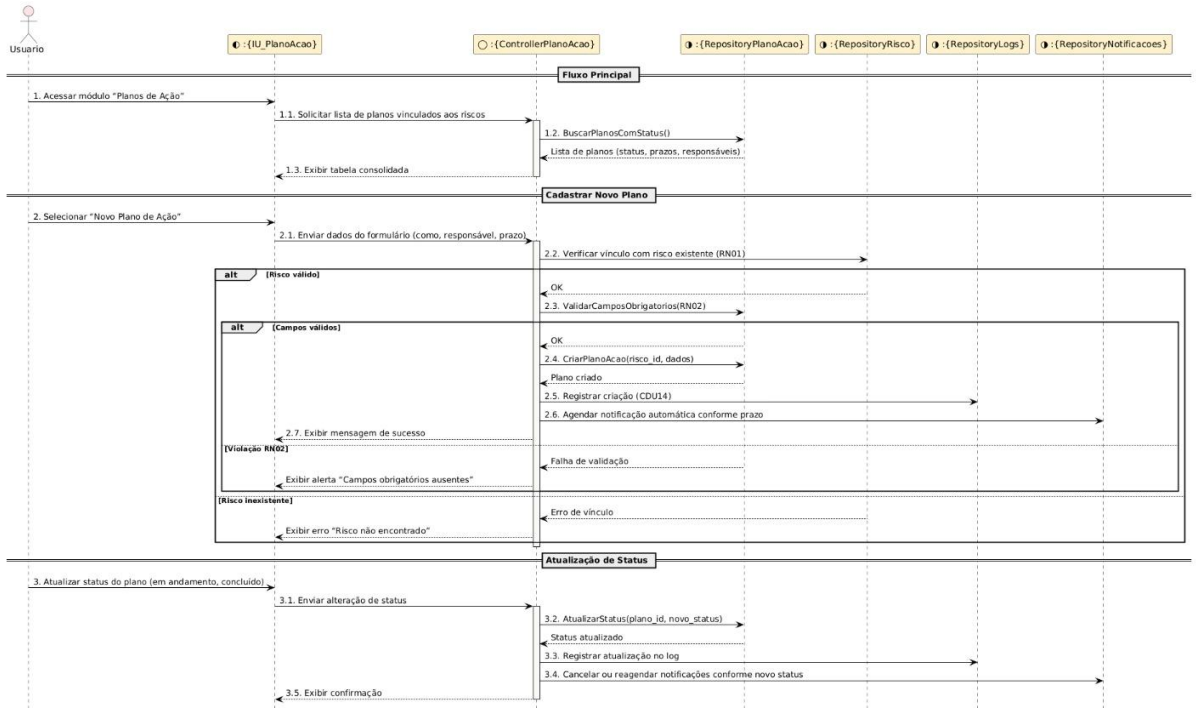
Fonte: Elaboração Própria

Figura 72: Gerir Riscos (Figura 2)



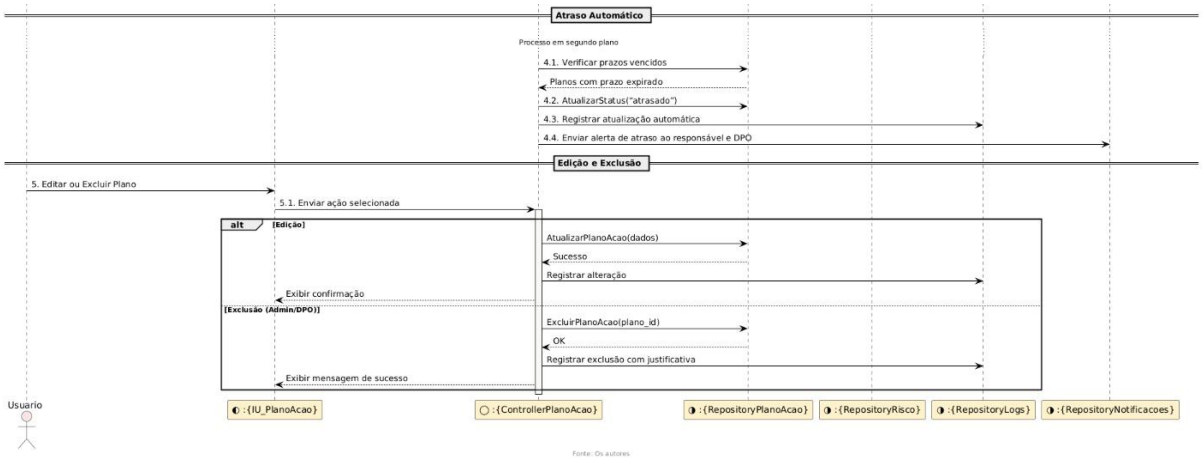
Fonte: Elaboração Própria

Figura 73: Gerir Plano de Ação (Figura 1)



Fonte: Elaboração Própria

Figura 74: Gerir Plano de Ação(Figura 2)



Fonte: Elaboração Própria

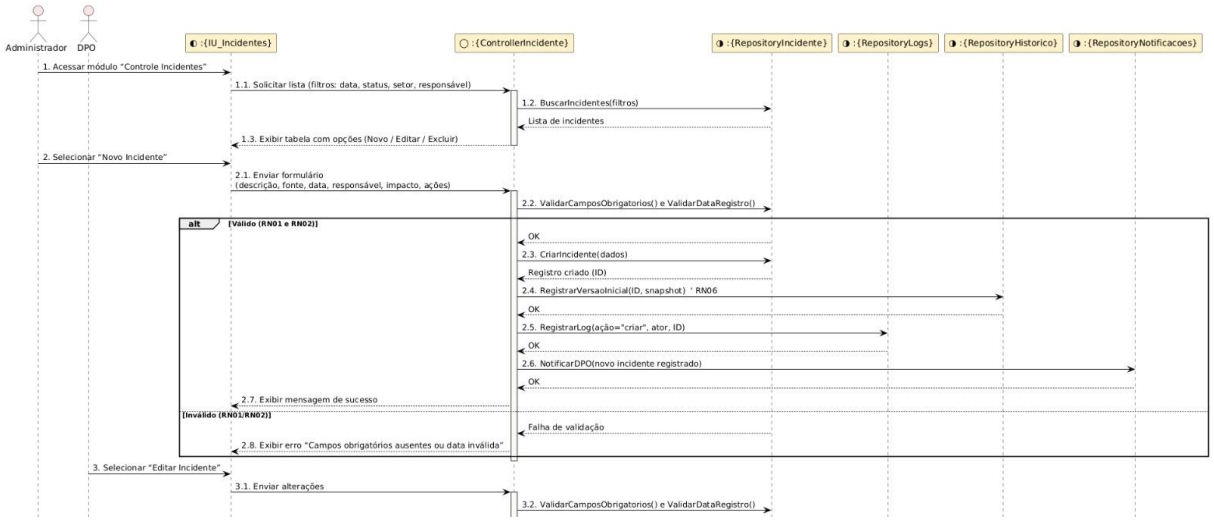
Figura 75: Gerir Monitoramento(Figura 1)

Fonte: Elaboração Própria

Figura 76: Gerir Monitoramento(Figura 2)

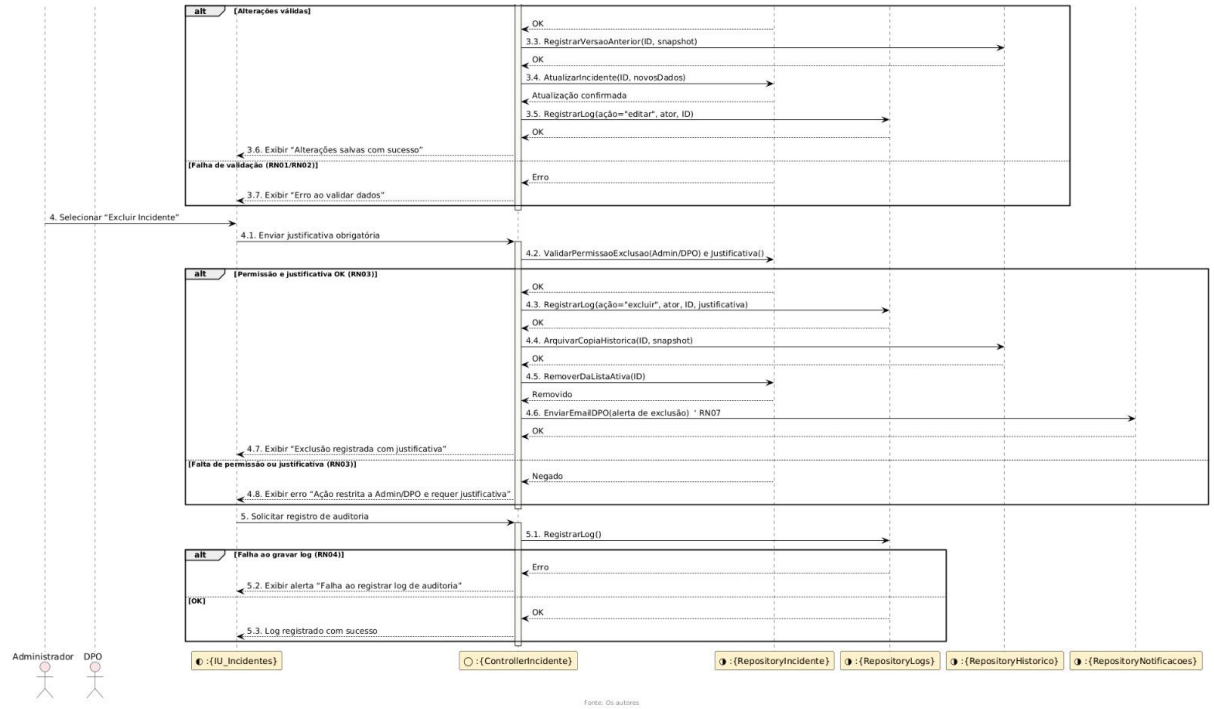
Fonte: Elaboração Própria

Figura 77: Gerir Incidentes (Figura 1)



Fonte: Elaboração Própria

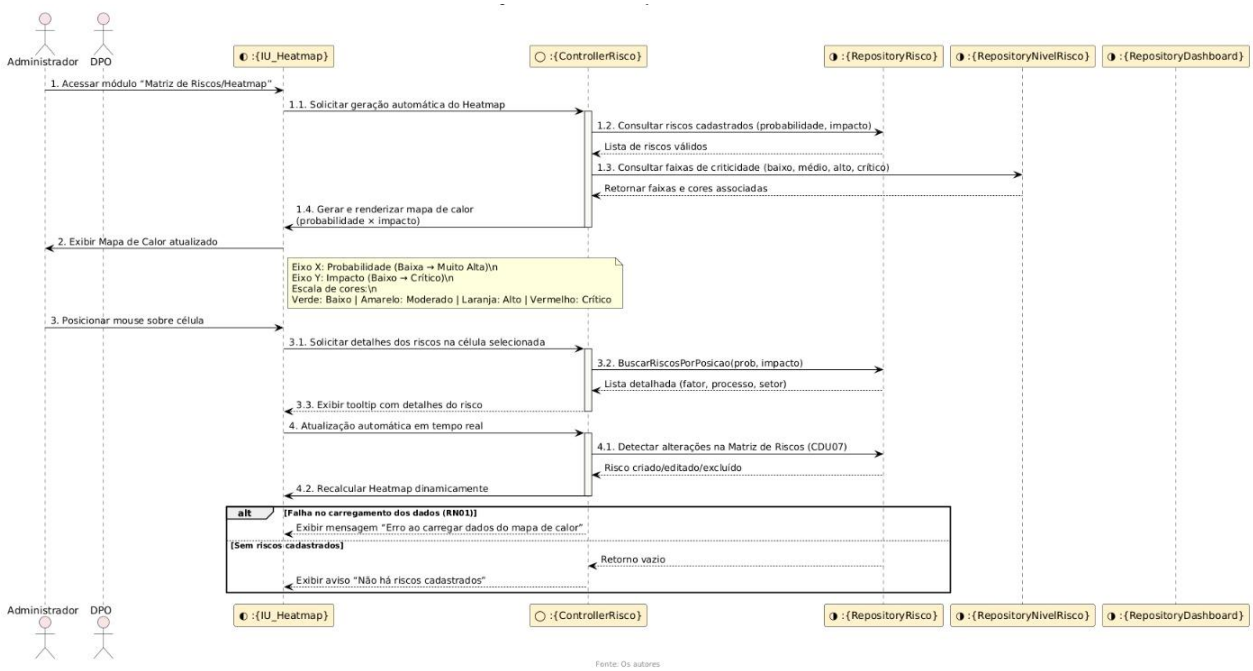
Figura 78: Gerir Incidentes (Figura 2)



Fonte: Os autores

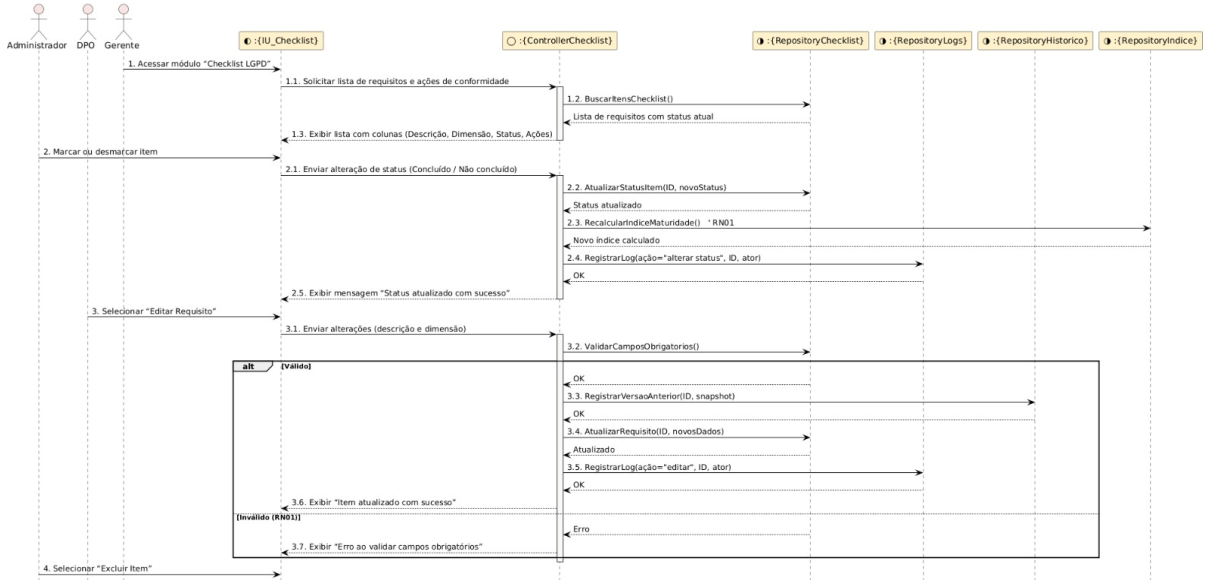
Fonte: Elaboração Própria

Figura 79: Visualizar Heatmap



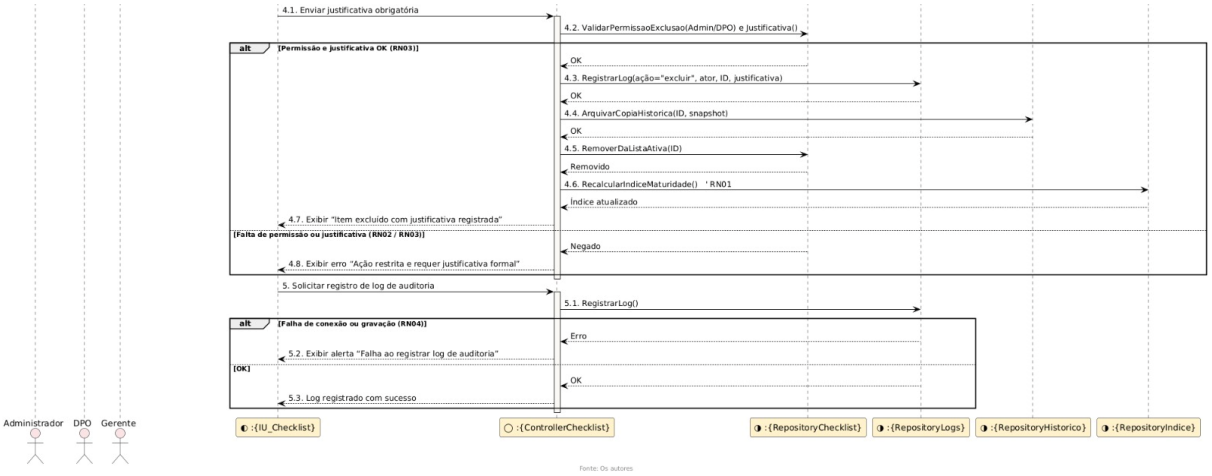
Fonte: Elaboração Própria

Figura 80: Gerir Checklist(Figura 1)



Fonte: Elaboração Própria

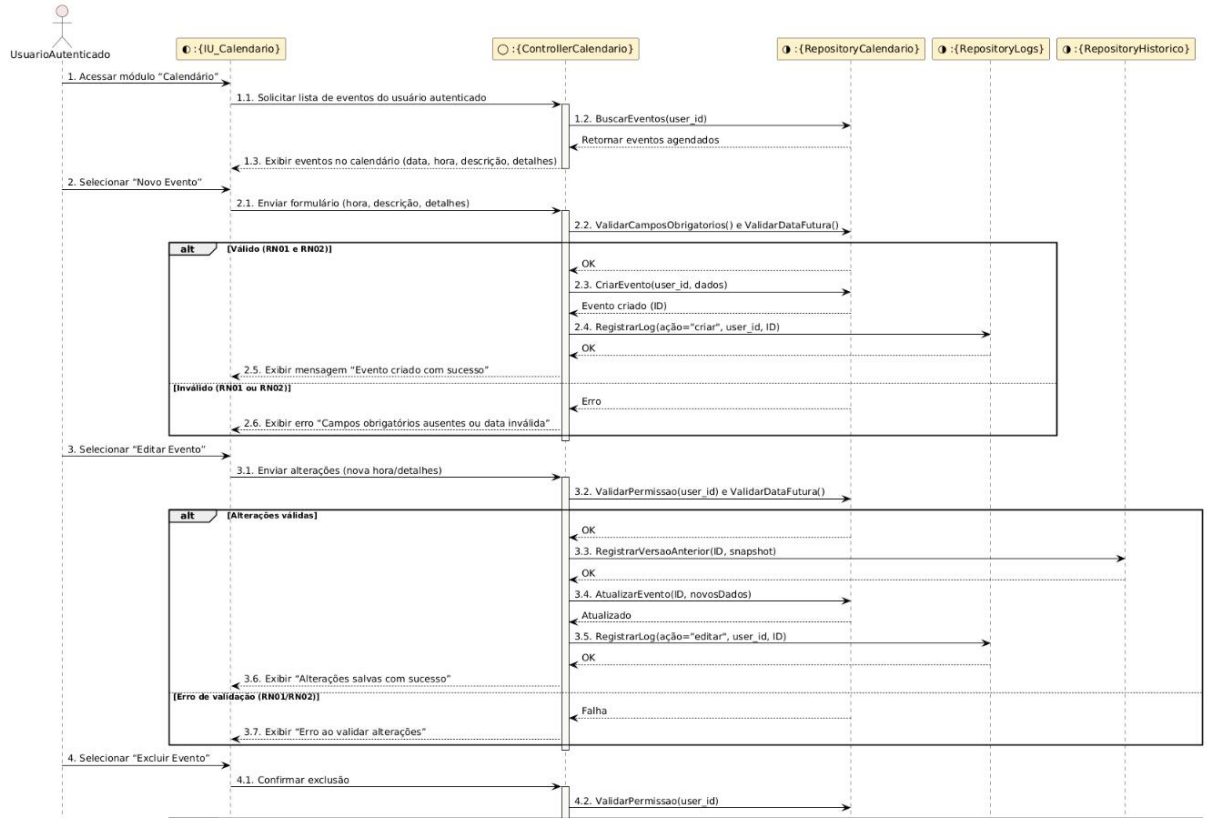
Figura 81: Gerir Checklist(Figura 2)



Fonte: Os autores

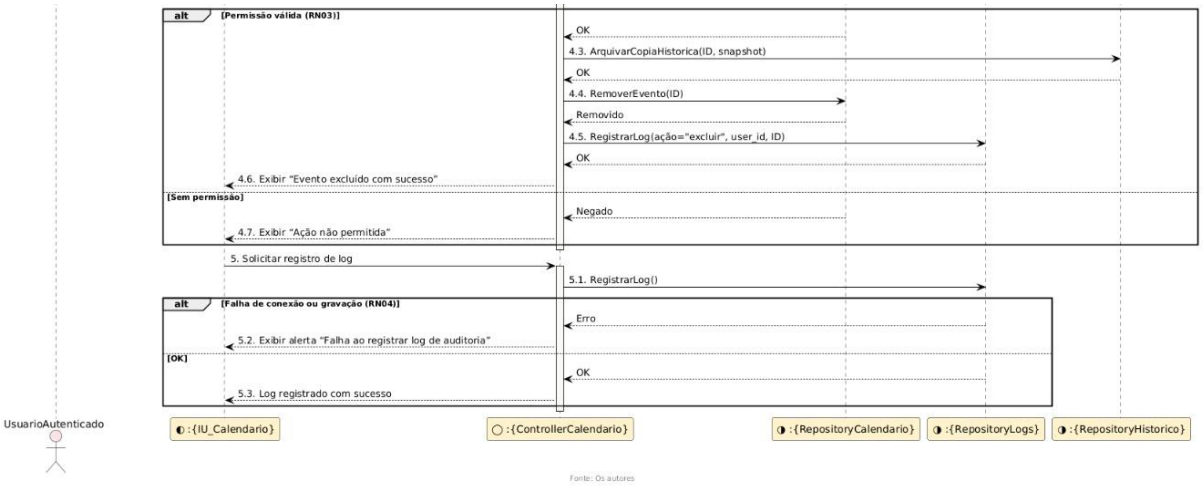
Fonte: Elaboração Própria

Figura 82: Gerir Calendário(Figura 1)



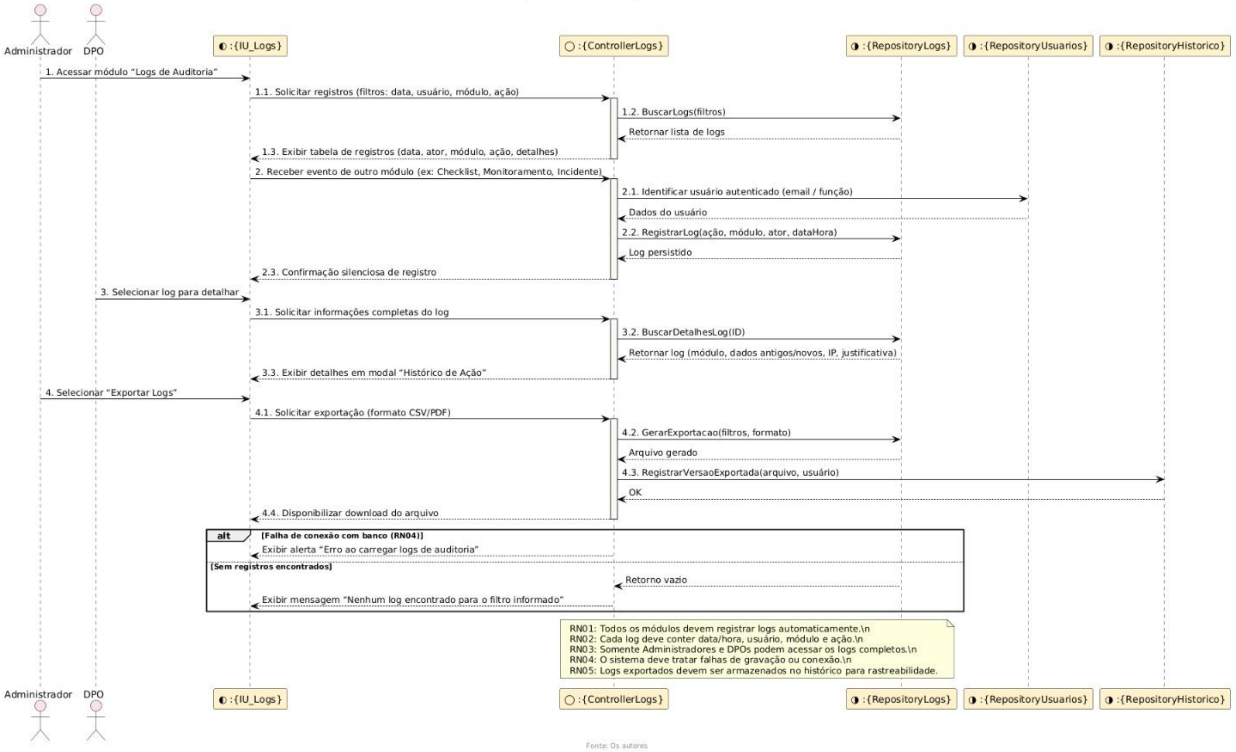
Fonte: Elaboração Própria

Figura 83: Gerir Calendário(Figura 2)



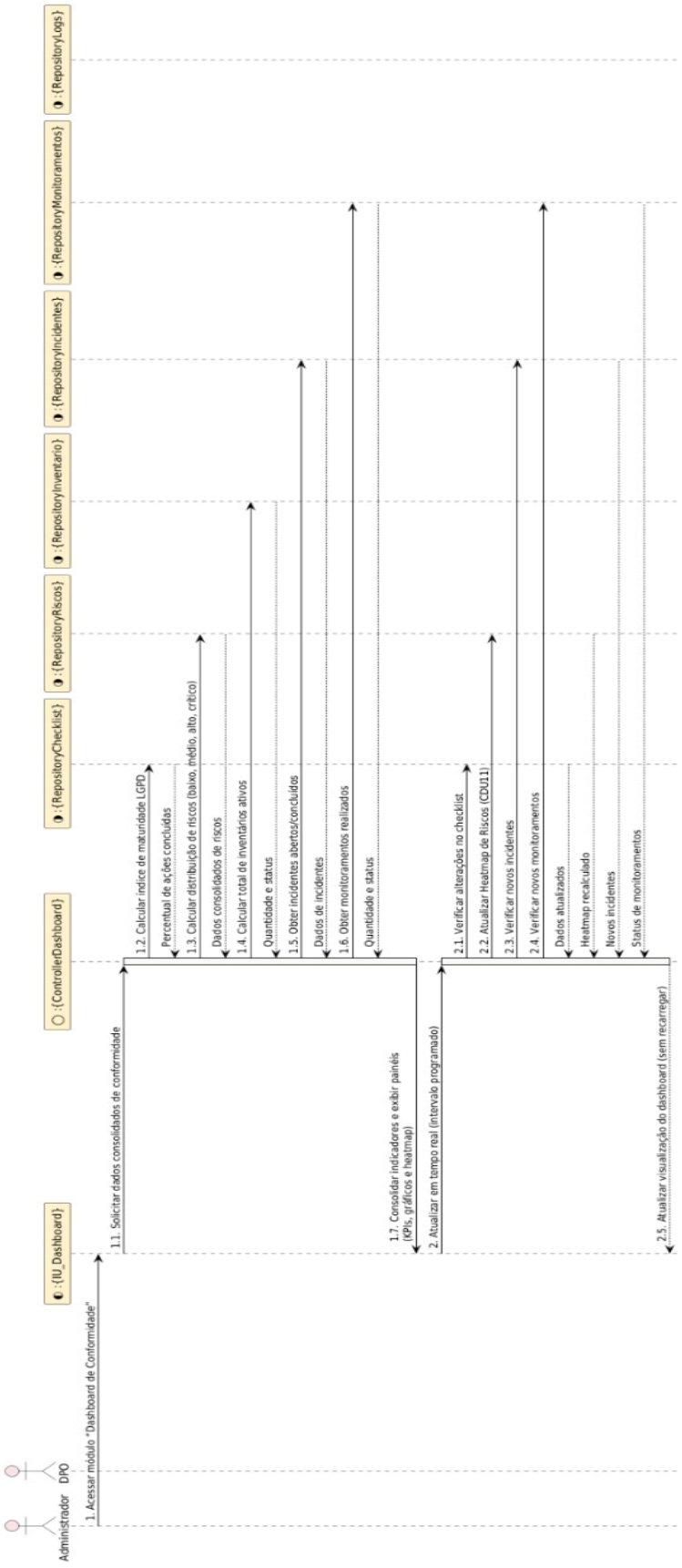
Fonte: Elaboração Própria

Figura 84: Registrar e consultar logs de ações dos usuários



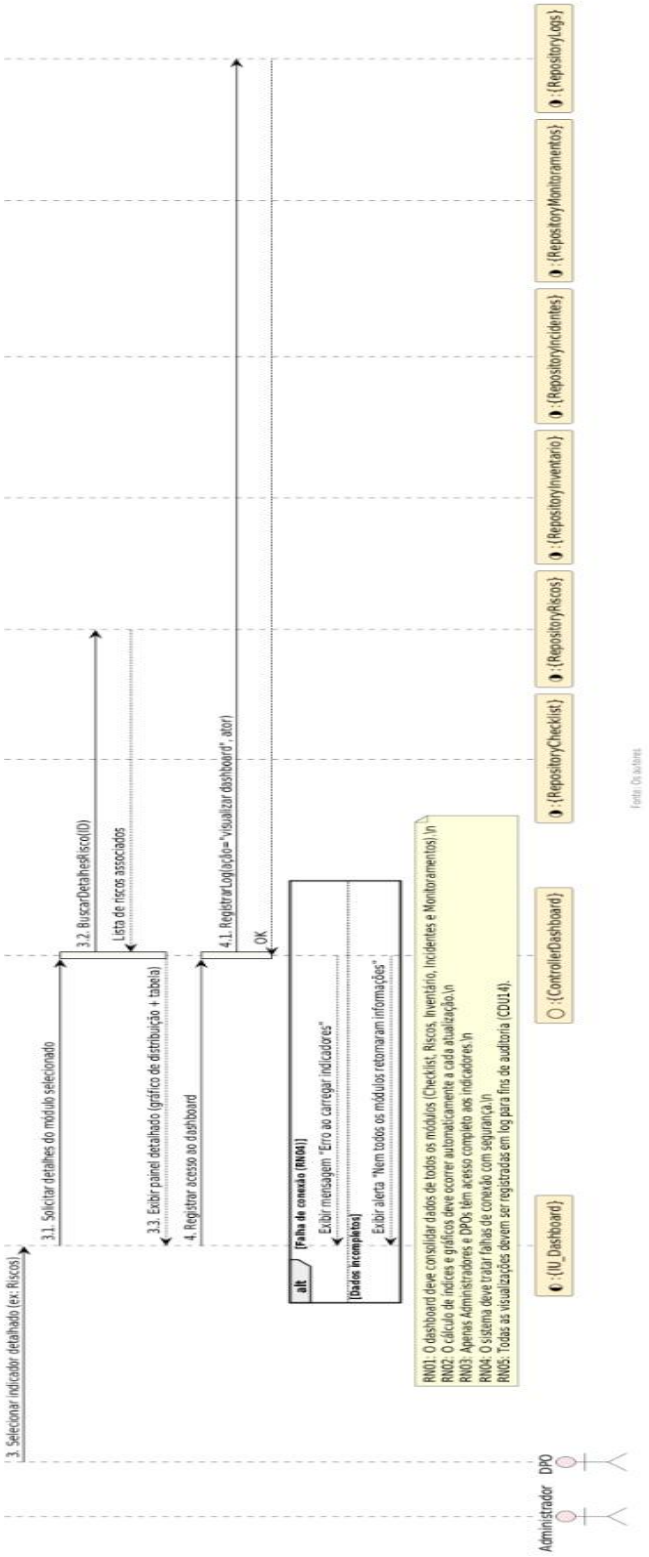
Fonte: Elaboração Própria

Figura 85: Visualizar Dashboard



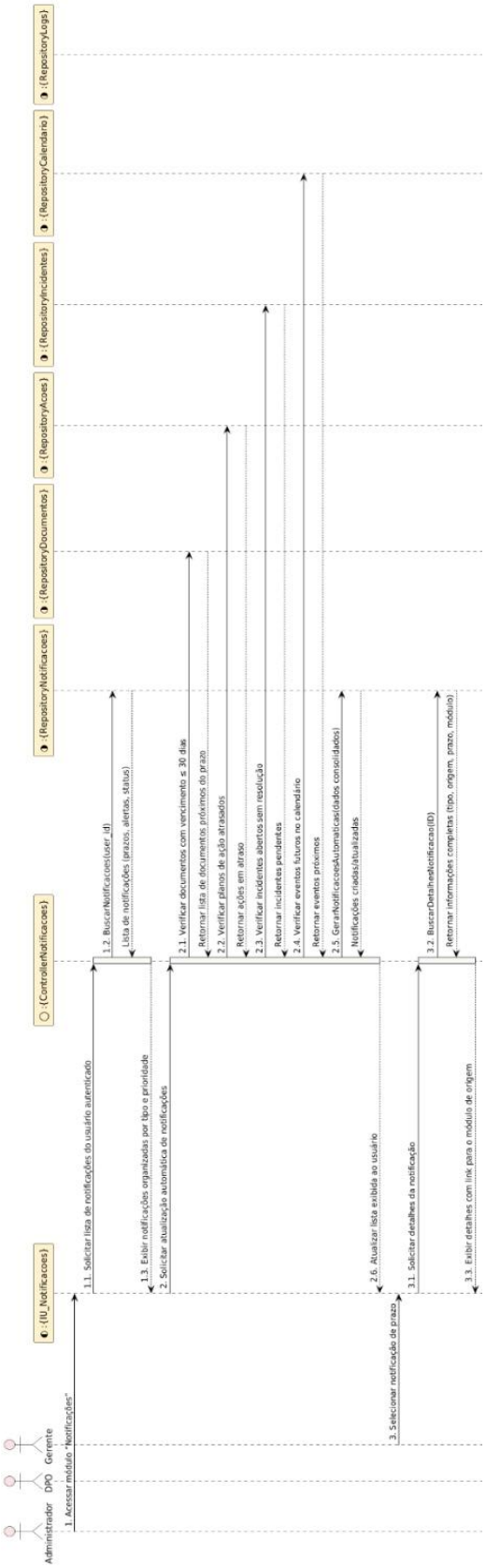
Fonte: Elaboração Própria

Figura 86: Visualizar Dashboard



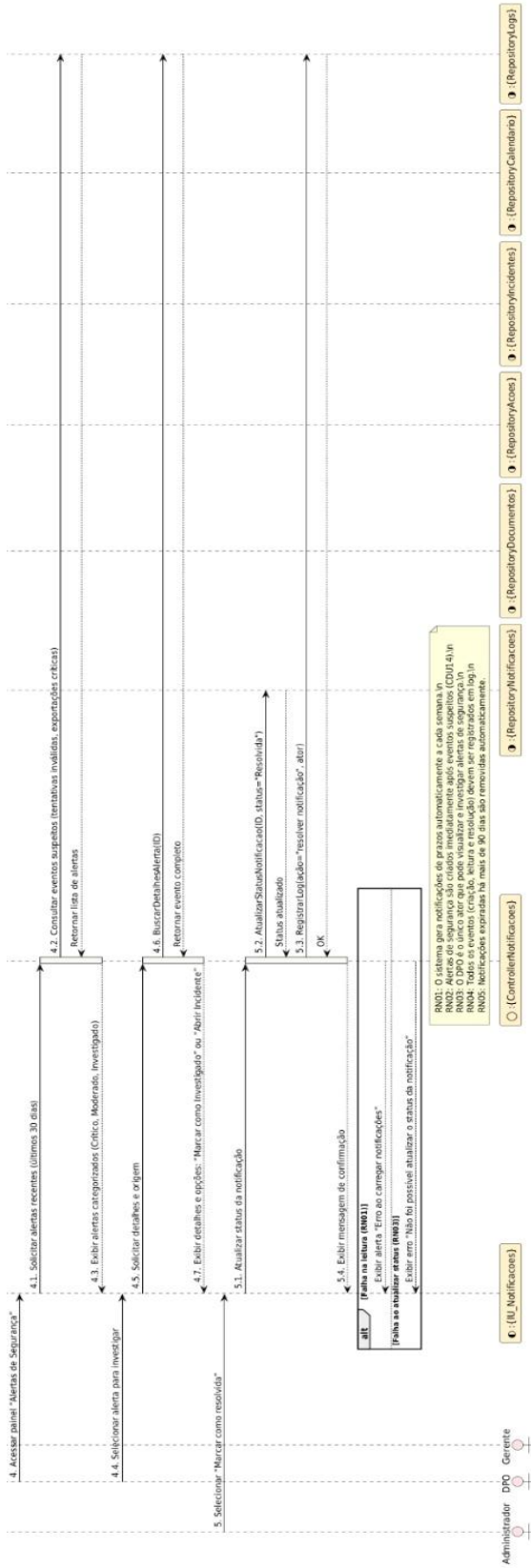
Fonte: Elaboração Própria

Figura 87: Visualizar Notificações



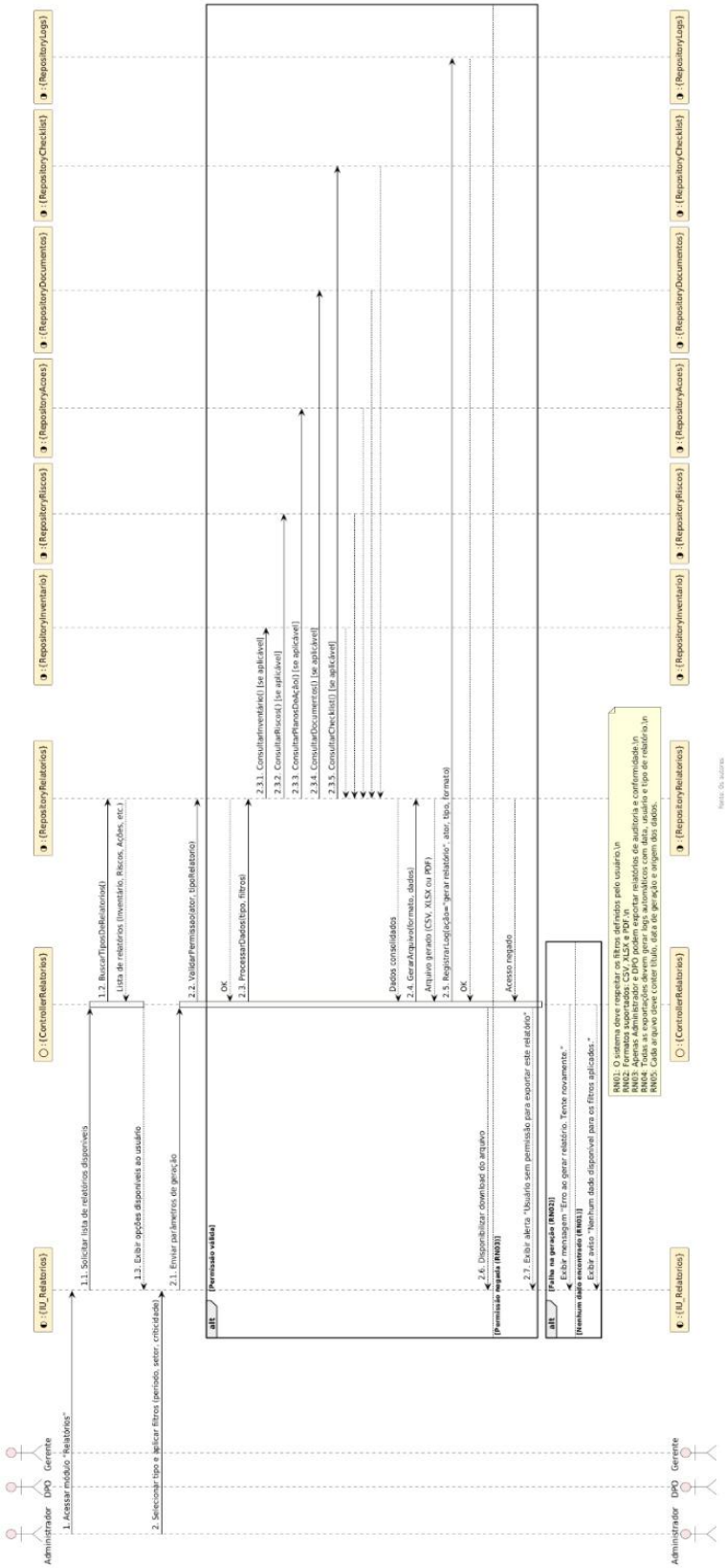
Fonte: Elaboração Própria

Figura 88: Visualizar Notificações



Fonte: Elaboração Própria

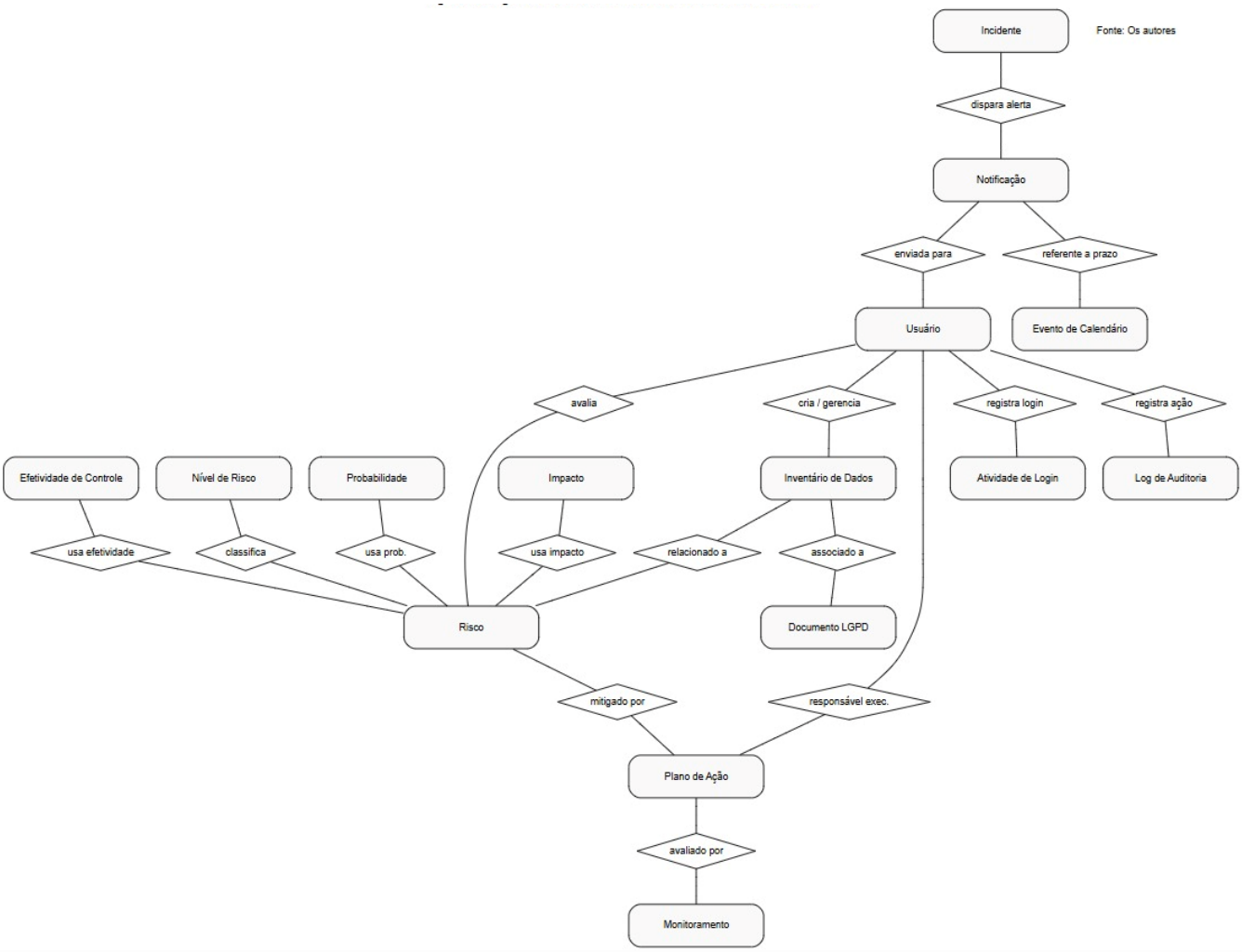
Figura 89: Gerar Relatórios



Fonte: Elaboração Própria

APÊNDICE F: DIAGRAMA DE ENTIDADE E RELACIONAMENTO

Figura 90: Diagrama de Entidade e Relacionamento



Fonte: Elaboração Própria

APÊNDICE G: DICIONÁRIO DE DADOS

Tabela	LoginActivity
Descrição	Registra automaticamente todos os logins realizados pelos usuários do sistema Camaleão, incluindo data, hora, IP e resultado da autenticação.
Observações	Os registros são gerados automaticamente pelo sistema para fins de auditoria e conformidade com a LGPD. Não podem ser alterados ou excluídos manualmente.

Campos

Nome	Descrição	Tipo de Dado	Tamanho	Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)
id	Identificador único do registro de login.	int	—	PK / Identity
usuário	Usuário autenticado (referência ao modelo User).	FK	—	Not Null / FK → User.id / On Delete: CASCADE
email_usuário	Endereço de e-mail do usuário que realizou o login.	varchar	255	Not Null
data_login	Data e hora em que o login foi realizado.	datetime	—	Default=timezone.now / Not Null
ip_address	Endereço IP do dispositivo utilizado no acesso.	ipaddress	—	Nullable
resultado_login	Resultado da tentativa de login ('sucesso', 'falha', 'tentativa').	varchar	20	Default='sucesso' / Not Null / Check ('sucesso','falha','tentativa')
criado_em	Data e hora de criação do registro de log.	datetime	—	Auto Now Add / Not Null

Fonte: Elaboração Própria

Tabela 33: Dicionário de dados (Tabela: Incidentes)

Tabela				
		Incidentes		
Descrição		Registra os incidentes relacionados à segurança e proteção de dados pessoais, incluindo descrição, análise, medidas corretivas e encerramento.		
Observações		Cada registro representa um incidente tratado pela equipe de conformidade, permitindo rastreabilidade e histórico completo das ações e decisões tomadas.		
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do incidente registrado.	int	—	PK / Identity
numero_registro	Número de controle sequencial e único do incidente.	int	—	Unique / Not Null
descricao	Descrição detalhada do incidente de segurança ou privacidade ocorrido.	text	—	Not Null
fonte	Origem da informação ou canal de reporte do incidente.	varchar	120	Not Null
data_registro	Data em que o incidente foi registrado no sistema.	date	—	Not Null
responsavel_analise	Nome do responsável pela análise e tratamento do incidente.	varchar	120	Not Null
data_final_analise	Data de conclusão da análise do incidente.	date	—	Nullable

acao_recomendada	Medidas recomendadas para mitigar o incidente.	text	—	Nullable
recomendacoes_reportadas	Recomendações comunicadas às partes interessadas.	varchar	200	Nullable
data_reporte	Data de reporte do incidente às autoridades competentes, se aplicável.	date	—	Nullable
decisoes_resolucao	Decisões tomadas durante o processo de resolução do incidente.	text	—	Nullable
data_encerramento	Data de encerramento do incidente.	date	—	Nullable
fonte_informada	Indica se a fonte do incidente foi formalmente informada (True/False).	boolean	—	Default=False / Not Null
criado_por	Usuário responsável pelo registro do incidente (referência ao modelo User).	FK	—	Nullable / FK → User.id / On Delete: SET_NULL
justificativa_exclusao	Motivo informado pelo ator responsável ao excluir o registro de incidente.	text	—	Nullable
data_exclusao	Data e hora em que o incidente foi excluído do módulo ativo.	datetime	—	Nullable

Tabela 34: Dicionário de dados (Tabela: Monitoramentos)

Tabela	Monitoramentos
Descrição	Registra as ações de monitoramento realizadas para avaliar a efetividade dos controles e medidas de conformidade da organização com a LGPD.

Observações			Cada registro representa uma ação de monitoramento com seus respectivos resultados, responsáveis, deficiências e medidas corretivas, mantendo histórico e rastreabilidade.	
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único da ação de monitoramento.	int	—	PK / Identity
framework_requisito	Referência ao framework, requisito ou política avaliada no monitoramento.	varchar	200	Not Null
escopo	Descrição do escopo e contexto do monitoramento realizado.	text	—	Not Null
data_monitoramento	Data em que o monitoramento foi realizado.	date	—	Not Null
criterio_avaliacao	Critério ou metodologia utilizada para avaliação da conformidade.	varchar	200	Not Null
responsavel	Nome do responsável pela execução do monitoramento.	varchar	120	Not Null

data_conclusao	Data de conclusão do monitoramento.	date	—	Nullable
deficiencias	Descrição das deficiências ou não conformidades encontradas.	text	—	Nullable
corretivas	Medidas corretivas ou ações recomendadas para solucionar as deficiências encontradas.	text	—	Nullable
criado_por	Usuário responsável pelo registro do monitoramento (referência ao modelo User).	FK	—	Nullable / FK → User.id / On Delete: SET_NULL
justificativa_exclusao	Motivo informado pelo ator responsável ao excluir o registro de monitoramento.	text	—	Nullable
data_exclusao	Data e hora em que o registro foi excluído do módulo ativo.	datetime	—	Nullable

Fonte: Elaboração Própria

Tabela 35: Dicionário de dados (Tabela: ChecklistLGPD)

Tabela	ChecklistLGPD
Descrição	Registra os requisitos e ações de conformidade da organização com a LGPD, permitindo o acompanhamento do progresso de implementação.
Observações	Cada item do checklist representa uma atividade de conformidade que pode ser marcada como concluída ou não concluída.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do item de checklist LGPD.	int	—	PK / Identity
atividade	Nome da atividade de conformidade a ser verificada.	varchar	255	Not Null
descricao	Descrição detalhada da atividade de conformidade LGPD.	text	—	Not Null
is_completed	Indica se o item está concluído (True) ou não (False).	boolean	—	Default=False / Not Null
created_at	Data e hora de criação do registro.	datetime	—	Auto Now Add / Not Null
updated_at	Data e hora da última atualização do registro.	datetime	—	Auto Now / Not Null

Fonte: Elaboração Própria

Tabela 36: Dicionário de dados (Tabela: DocumentosLGPD)

Tabela	**DocumentosLGPD**			
Descrição	Armazena as informações, evidências e documentos relacionados às práticas de conformidade da organização com a LGPD.			
Observações	Cada registro representa um documento ou requisito vinculado a uma dimensão de conformidade, permitindo o acompanhamento de criticidade, status e revisões periódicas.			
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do documento LGPD.	int	—	PK / Identity
dimensao	Dimensão ou área de conformidade à qual o documento pertence (Gestão de Privacidade, Gestão de SI, Processos).	char	3	Not Null / Check ('GPV','GSI','PRC')
atividade	Descrição do requisito, atividade ou documento exigido pela conformidade LGPD.	text	—	Not Null
base_legal	Base legal aplicável à atividade documentada.	varchar	255	Nullable
evidencia	Evidência documental que comprova a execução da atividade ou requisito.	varchar	255	Nullable
proxima_revisao	Data prevista para a próxima revisão do documento.	date	—	Nullable
comentarios	Observações ou anotações adicionais relacionadas ao documento.	text	—	Nullable

criticidade	Nível de importância do documento para a conformidade ('NA','BP','BX','MD','AL').	char	2	Not Null / Default='NA' / Check ('NA','BP','BX','MD','AL')
status	Situação atual do documento ('NA','NI','EA','FI').	char	2	Not Null / Default='NI' / Check ('NA','NI','EA','FI')
arquivo	Arquivo anexo relacionado ao documento (PDF, DOCX, XLSX).	FileField (path)	255	Nullable / Upload: 'documentos/%Y/%m/'
created_at	Data e hora de criação do registro.	datetime	—	Auto Now Add / Not Null
updated_at	Data e hora da última atualização do registro.	datetime	—	Auto Now / Not Null
criado_por	Usuário responsável pela criação do registro (referência ao modelo User).	FK	—	Nullable / FK → User.id / On Delete: SET_NULL

Fonte: Elaboração Própria

Tabela 37: Dicionário de dados (Tabela: RiskLevelBand)

Tabela	**RiskLevelBand**			
Descrição	Define as faixas de classificação dos riscos conforme a pontuação calculada (Probabilidade × Impacto), indicando o nível de criticidade e a cor correspondente.			
Observações	Esta tabela é utilizada pelo sistema para gerar o mapa de calor (Heatmap) de riscos, aplicando a escala de cores padrão para cada faixa de pontuação.			
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único da faixa de risco	int	—	PK / Identity
descricao	Descrição textual da faixa de risco	varchar	50	Not Null / Unique

	(Baixo, Moderado, Alto, Crítico)			
limite_inferior	Valor mínimo da pontuação que define o início da faixa	int	—	Not Null / Check (>= 0)
limite_superior	Valor máximo da pontuação que define o fim da faixa	int	—	Not Null / Check (>= limite_inferior)
nivel	Classificação ordinal do nível de risco (1=Baixo, 2=Médio, 3=Alto, 4=Crítico)	int	—	Check (1–4) / Not Null
cor	Cor descritiva associada à faixa de risco	enum	—	Check ('Verde','Amarelo','Laranja','Vermelho') / Not Null

Fonte: Elaboração Própria

Tabela 38: Dicionário de dados (Tabela: Risk)

Tabela			**Risk**	
Descrição			Registra os riscos identificados na organização, incluindo suas classificações de probabilidade, impacto, eficácia dos controles e pontuação total para composição do mapa de calor.	
Observações			Cada risco pode possuir múltiplos planos de ação associados e é classificado automaticamente conforme as faixas definidas na tabela RiskLevelBand.	
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do risco	int	—	PK / Identity

matriz_filial	Identifica se o risco pertence à matriz, filial ou ambas	varchar	120	Not Null
setor	Setor ao qual o risco está associado	varchar	120	Not Null
processo	Nome do processo relacionado ao risco	varchar	200	Not Null
risco_fator	Descrição do risco e seu fator causador	text	—	Not Null
probabilidade_id	Nível de probabilidade associado ao risco	int (FK)	—	FK → LikelihoodItem.id / Not Null / On Delete PROTECT
impacto_id	Nível de impacto associado ao risco	int (FK)	—	FK → ImpactItem.id / Not Null / On Delete PROTECT
pontuacao	Pontuação total calculada (Probabilidade × Impacto)	int	—	Default = 0 / Calculado automaticamente
medidas_controle	Descrição das medidas de controle existentes	text	—	Nullable
tipo_controle	Tipo de controle implementado (C=Preventivo, D=Detectivo)	char	1	Check ('C','D') / Nullable
eficacia_id	Eficácia do controle associado	int (FK)	—	FK → ControlEffectivenessItem.id / Nullable / On Delete SET NULL
risco_residual	Classificação do risco residual	varchar	20	Nullable / Check ('baixo','medio','alto')

	(baixo, médio, alto)			
resposta_risco	Plano de ação ou resposta ao risco	text	—	Nullable
criado_em	Data e hora de criação do registro	datetime	—	Auto Now Add / Not Null
atualizado_em	Data e hora da última atualização do registro	datetime	—	Auto Now / Not Null

Fonte: Elaboração Própria

Tabela 39: Dicionário de dados (Tabela: User)

Tabela	**User**			
Descrição	Armazena as informações dos usuários do sistema Camaleão, incluindo dados de autenticação, contato, função e status de atividade.			
Observações	Cada usuário possui um papel definido (Administrador, DPO, Gerente ou Comum) e pode estar ativo ou inativo no sistema.			
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do usuário	int	—	PK / Identity
email	Endereço de e-mail do usuário (utilizado para login)	varchar	150	Not Null / Unique
phone_number	Telefone de contato do usuário	varchar	20	—
appointment_date	Data de nomeação ou	date	—	—

	designação do usuário (quando aplicável)			
appointment_validity	Data de validade da nomeação do DPO ou responsável	date	—	—
avatar	Imagem associada ao perfil do usuário	image	—	—
role	Tipo de papel do usuário no sistema (Administrador, DPO, Gerente, Comum)	enum	—	Not Null / Check (‘ADMIN’, ‘DPO’, ‘GERENTE’)
is_active	Indica se o usuário está ativo no sistema	boolean	—	Default = True / Not Null

Fonte: Elaboração Própria

Tabela 40: **Dicionário de dados (Tabela: InventarioDados)**

Tabela	**InventarioDados**			
Descrição	Registra os inventários de tratamento de dados pessoais, conforme as etapas definidas pela LGPD, permitindo o controle de origem, finalidade, base legal, armazenamento, retenção e medidas de segurança.			
Observações	O inventário é dividido em três etapas: identificação das atividades, fluxos e controle de dados; análise de armazenamento e transferência; e revisão de adequação e medidas de segurança.			
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do registro do inventário	int	—	PK / Identity

criado_por	Usuário responsável pela criação do inventário	int (FK)	—	FK → User.id / Nullable
data_criacao	Data de criação do registro	datetime	—	Not Null / Default = now()
data_atualizacao	Data da última atualização do registro	datetime	—	Not Null / Auto-update
unidade	Identifica se a unidade é Matriz, Filial ou ambas	varchar	15	Check ('matriz', 'filial', 'matriz_filial')
setor	Setor organizacional responsável pelo tratamento	varchar	120	Nullable
responsavel_email	E-mail do responsável pelo tratamento de dados	varchar	254	Nullable
processo_negocio	Nome do processo de negócio mapeado	varchar	200	Nullable
finalidade	Finalidade do tratamento de dados	text	—	Nullable
dados_pessoais	Descrição dos tipos de dados pessoais tratados	text	—	Nullable
tipo_dado	Tipo de dado tratado (Pessoal, Sensível, Anonimizado)	varchar	12	Check
origem	Origem dos dados coletados	varchar	200	Nullable
formato	Formato dos dados (Digital,	varchar	16	Check

	Físico ou Híbrido)			
impresso	Indica se há versão impressa	varchar	3	Check ('sim','nao')
titulares	Descrição dos titulares dos dados (ex: clientes, colaboradores)	text	—	Nullable
dados_menores	Indica se há tratamento de dados de menores	varchar	3	Check ('sim','nao')
base_legal	Base legal aplicável ao tratamento	text	—	Nullable
pessoas_acesso	Pessoas com acesso aos dados	text	—	Nullable
atualizacoes	Periodicidade de atualização dos dados	text	—	Nullable
transmissao_interna	Fluxo de transmissão interna de dados	text	—	Nullable
transmissao_externa	Fluxo de transmissão externa de dados	text	—	Nullable
local_armazenamento_digital	Local físico ou digital onde os dados são armazenados	varchar	200	Nullable
controlador_operador	Define se a organização atua como Controlador, Operador ou ambos	varchar	12	Check ('controlador','operador','ambos')

motivo_retencao	Justificativa da retenção dos dados	text	—	Nullable
periodo_retencao	Prazo de retenção dos dados	varchar	100	Nullable
exclusao	Forma ou procedimento de exclusão dos dados	text	—	Nullable
forma_exclusao	Método utilizado para exclusão dos dados	text	—	Nullable
transferencia_terceiros	Indica se há transferência de dados a terceiros	varchar	3	Check ('sim','nao')
quais_dados_transferidos	Descrição dos dados transferidos a terceiros	text	—	Nullable
transferencia_internacional	Indica se há transferência internacional	varchar	3	Check ('sim','nao')
empresa_terceira	Nome da empresa terceira envolvida	varchar	200	Nullable
adequado_contratualmente	Indica se há cláusulas contratuais adequadas	varchar	3	Check ('sim','nao')
paises_tratamento	Países onde ocorre o tratamento de dados	varchar	200	Nullable
medidas_seguranca	Medidas de segurança aplicadas ao tratamento de dados	text	—	Nullable

consentimentos	Descrição dos consentimentos obtidos	text	—	Nullable
observacao	Observações gerais sobre o inventário	text	—	Nullable

Fonte: Elaboração Própria

Tabela 41: Dicionário de dados (Tabela: Relatorios)

Tabela	**Relatorios**
Descrição	Armazena os relatórios de conformidade gerados automaticamente ou sob demanda no sistema Camaleão, contendo informações sobre riscos, planos de ação, incidentes e demais módulos de controle.
Observações	Os registros incluem o tipo de relatório, período de referência, formato de exportação e o usuário responsável pela geração. O sistema mantém o histórico para auditoria e rastreabilidade.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do relatório gerado.	int	—	PK / Identity
titulo	Título do relatório gerado.	varchar	255	Not Null
tipo_relatorio	Tipo de relatório (Riscos, Ações, Incidentes, Inventário, etc.).	varchar	100	Not Null
periodo_inicio	Data inicial do período de referência do relatório.	date	—	Nullable

periodo_fim	Data final do período de referência do relatório.	date	—	Nullable
modulo_origem	Nome do módulo do sistema que originou o relatório.	varchar	100	Not Null
formato	Formato do arquivo gerado (PDF, CSV, XLSX).	varchar	10	Default='PDF' / Not Null
caminho_arquivo	Caminho completo ou URL do arquivo armazenado.	varchar	500	Nullable
usuario	Usuário responsável pela geração do relatório.	FK	—	Not Null / FK → User.id / On Delete: SET NULL
data_emissao	Data e hora da geração do relatório.	datetime	—	Auto Now Add / Not Null
status	Status da operação de geração (Sucesso, Erro, Em processamento).	varchar	30	Default='Sucesso' / Not Null
observacoes	Observações adicionais sobre o relatório gerado.	text	—	Nullable

Fonte: Elaboração Própria

Tabela 42: Dicionário de dados (Tabela: CalendarEvent)

Tabela	**CalendarEvent**
Descrição	Registra os eventos de calendário vinculados aos usuários autenticados do sistema

	Camaleão, permitindo o acompanhamento de prazos, reuniões e atividades de conformidade.
Observações	Os eventos são criados e gerenciados pelos usuários com acesso autorizado. Cada evento está associado a um usuário específico e é exibido no painel de calendário do sistema.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do evento de calendário.	int	—	PK / Identity
user	Usuário autenticado responsável pelo evento.	FK	—	Not Null / FK → User.id / On Delete: CASCADE
date	Data agendada para o evento.	date	—	Not Null / Index
time	Horário do evento.	time	—	Not Null
text	Descrição breve do evento (título exibido no calendário).	varchar	255	Not Null
details	Informações complementares sobre o evento.	text	—	Nullable
created_at	Data e hora de criação do evento.	datetime	—	Auto Now Add / Not Null
updated_at	Data e hora da última atualização do evento.	datetime	—	Auto Now / Not Null

Fonte: Elaboração Própria

Tabela 43: Dicionário de dados (Tabela: ControlEffectivenessItem)

Tabela	**ControlEffectivenessItem**
Descrição	Armazena os níveis de efetividade dos controles implementados, utilizados para calcular o risco residual na Matriz de Riscos.

Observações	Cada registro representa um nível de efetividade entre 1 e 5, incluindo a faixa percentual mínima e máxima de redução de risco aplicada.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do nível de efetividade do controle.	int	—	PK / Identity
value	Valor numérico que representa o nível de efetividade (1 a 5).	int	1 a 5	Unique / Not Null / Check (1 ≤ value ≤ 5)
label_pt	Descrição textual do nível de efetividade (por exemplo: Muito efetivo, Parcialmente efetivo, etc.).	varchar	60	Not Null
reduction_min	Percentual mínimo de redução do risco aplicado conforme o nível de efetividade.	int	0 a 100	Not Null / Check (0 ≤ reduction_min ≤ 100)
reduction_max	Percentual máximo de redução do risco aplicado conforme o nível de efetividade.	int	0 a 100	Not Null / Check (0 ≤ reduction_max ≤ 100)

Fonte: Elaboração Própria

Tabela 44: Dicionário de dados (Tabela: ImpactItem)

Tabela	ImpactItem
Descrição	Armazena os níveis de impacto utilizados na Matriz de Riscos para determinar a gravidade dos riscos identificados no sistema.
Observações	Cada registro representa um nível de impacto único (1 a 5), associado à sua descrição textual correspondente.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK,**

				Not Null, Check, Default, Identity)
id	Identificador único do nível de impacto.	int	—	PK / Identity
value	Valor numérico que representa o nível de impacto (1 a 5).	int	1 a 5	Unique / Not Null / Check (1 ≤ value ≤ 5)
label_pt	Descrição textual do nível de impacto (por exemplo: Baixo, Médio, Crítico, etc.).	varchar	60	Not Null

Fonte: Elaboração Própria

Tabela 45: Dicionário de dados (Tabela: LikelihoodItem)

Tabela	**LikelihoodItem**
Descrição	Armazena os níveis de probabilidade utilizados na Matriz de Riscos para calcular a pontuação dos riscos cadastrados no sistema.
Observações	Cada registro representa um nível de probabilidade único (1 a 5), acompanhado de sua descrição textual correspondente.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do nível de probabilidade.	int	—	PK / Identity
value	Valor numérico que representa o nível de probabilidade (1 a 5).	int	1 a 5	Unique / Not Null / Check (1 ≤ value ≤ 5)
label_pt	Descrição textual do nível de probabilidade (por exemplo: Muito Baixa, Alta, etc.).	varchar	60	Not Null

Fonte: Elaboração Própria

Tabela 46: Dicionário de dados (Tabela: Notificacoes)

Tabela	**Notificacoes**
Descrição	Registra automaticamente todas as notificações geradas pelo sistema Camaleão, incluindo prazos de documentos, planos de ação, incidentes, eventos do calendário e alertas de segurança.
Observações	Os registros são criados exclusivamente pelo sistema, não podendo ser inseridos ou modificados manualmente. As notificações são exibidas aos usuários autenticados conforme suas permissões.

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único da notificação.	int	—	PK / Identity
usuario	Usuário destinatário da notificação.	FK	—	Not Null / FK → User.id / On Delete: CASCADE
titulo	Título ou assunto resumido da notificação.	varchar	255	Not Null
descricao	Descrição detalhada do conteúdo da notificação.	text	—	Not Null
tipo	Tipo de notificação (Prazo, Segurança, Incidente, Checklist, etc.).	varchar	100	Not Null
modulo_origem	Módulo do sistema que originou a notificação.	varchar	100	Not Null
data_emissao	Data e hora em que a notificação foi emitida.	datetime	—	Default=timezone.now / Not Null
prazo	Data limite relacionada ao	date	—	Nullable

	evento notificado (se aplicável).			
status	Status atual da notificação (Pendente, Visualizado, Resolvido).	varchar	30	Default='Pendente' / Not Null
relacionado_id	Identificador do registro relacionado à notificação (ex.: ID de documento, ação ou incidente).	int	—	Nullable
criado_em	Data e hora de criação do registro.	datetime	—	Auto Now Add / Not Null

Fonte: Elaboração Própria

Tabela 47: Dicionário de dados (Tabela: AlertasSeguranca)

Tabela	**AlertasSeguranca**
Descrição	Registra automaticamente eventos e tentativas suspeitas de acesso ou operação detectadas pelo sistema Camaleão, incluindo logins não autorizados, atividades anômalas e violações de segurança.
Observações	Os registros são criados exclusivamente pelo sistema e não podem ser alterados ou excluídos. Servem de base para os alertas apresentados ao DPO no módulo de Notificações (CDU16).

Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do alerta de segurança.	int	—	PK / Identity
usuario	Usuário associado ao evento, se aplicável (pode ser nulo em tentativas externas).	FK	—	Nullable / FK → User.id

tipo_alerta	Tipo de alerta gerado (tentativa de acesso não autorizado, login suspeito, exportação anômala, etc.).	varchar	120	Not Null
descricao	Descrição detalhada do evento de segurança detectado.	text	—	Not Null
nivel_criticidade	Nível de gravidade do alerta (Baixo, Médio, Alto, Crítico).	enum	—	Check ('Baixo','Médio','Alto','Crítico') / Default='Médio'
data_alerta	Data e hora em que o alerta foi registrado.	datetime	—	Default=timezone.now / Not Null
ip_origem	Endereço IP de origem do evento suspeito.	ipaddress	—	Nullable
status	Situação atual do alerta (Pendente, Investigado, Falso positivo, Confirmado).	enum	—	Default='Pendente' / Not Null / Check ('Pendente','Investigado','Falso positivo','Confirmado')
registrado_por_sistema	Indica que o registro foi criado automaticamente pelo sistema.	boolean	—	Default=True / Not Null

Fonte: Elaboração Própria

Tabela 48: Dicionário de dados (Tabela: UserActivityLog)

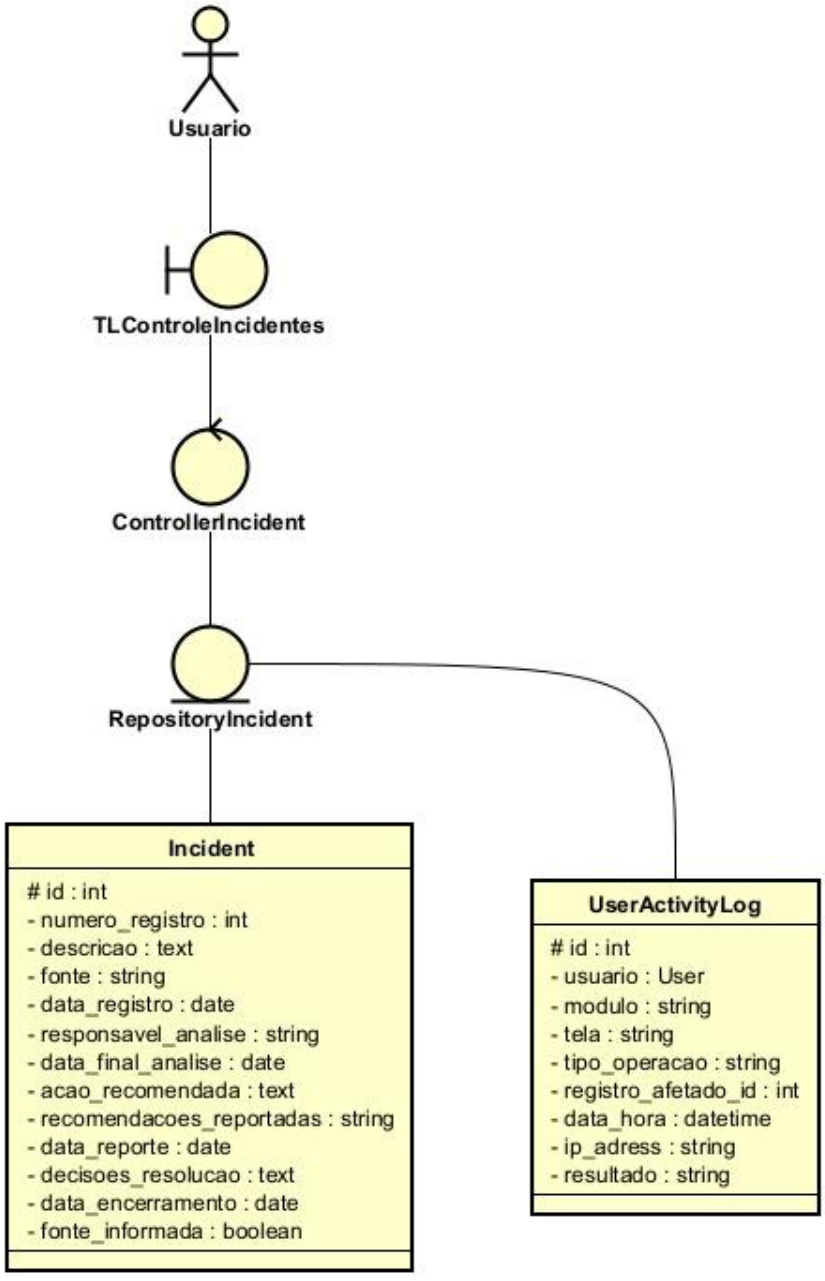
Tabela	UserActivityLog			
Descrição	Registra automaticamente todas as operações executadas pelos usuários dentro do sistema Camaleão, como criação, atualização, exclusão, exportação e consulta de registros.			
Observações	Os registros são criados automaticamente pelo sistema e utilizados para fins de auditoria e rastreabilidade. Não podem ser alterados ou excluídos manualmente.			
Campos				
Nome	**Descrição**	**Tipo de Dado**	**Tamanho**	**Restrições de domínio (PK, FK, Not Null, Check, Default, Identity)**
id	Identificador único do registro de atividade.	int	—	PK / Identity
usuario	Usuário responsável pela	FK	—	Not Null / FK → User.id / On Delete: CASCADE

	operação executada.			
modulo	Nome do módulo ou funcionalidade do sistema em que ocorreu a ação.	varchar	120	Not Null
tipo_operacao	Tipo de operação executada (criação, atualização, exclusão, exportação, consulta).	varchar	50	Not Null / Check ('criação','atualização','exclusão','exportação','consulta')
registro_afetado_id	Identificador do registro afetado pela operação, quando aplicável.	int	—	Nullable
data_operacao	Data e hora em que a operação foi realizada.	datetime	—	Default=timezone.now / Not Null
ip_address	Endereço IP do dispositivo que executou a operação.	ipaddress	—	Nullable
resultado_operacao	Resultado da operação ('sucesso', 'erro', 'tentativa inválida').	varchar	20	Not Null / Default='sucesso' / Check ('sucesso','erro','tentativa inválida')
criado_em	Data e hora de criação do registro de log.	datetime	—	Auto Now Add / Not Null

Fonte: Elaboração Própria

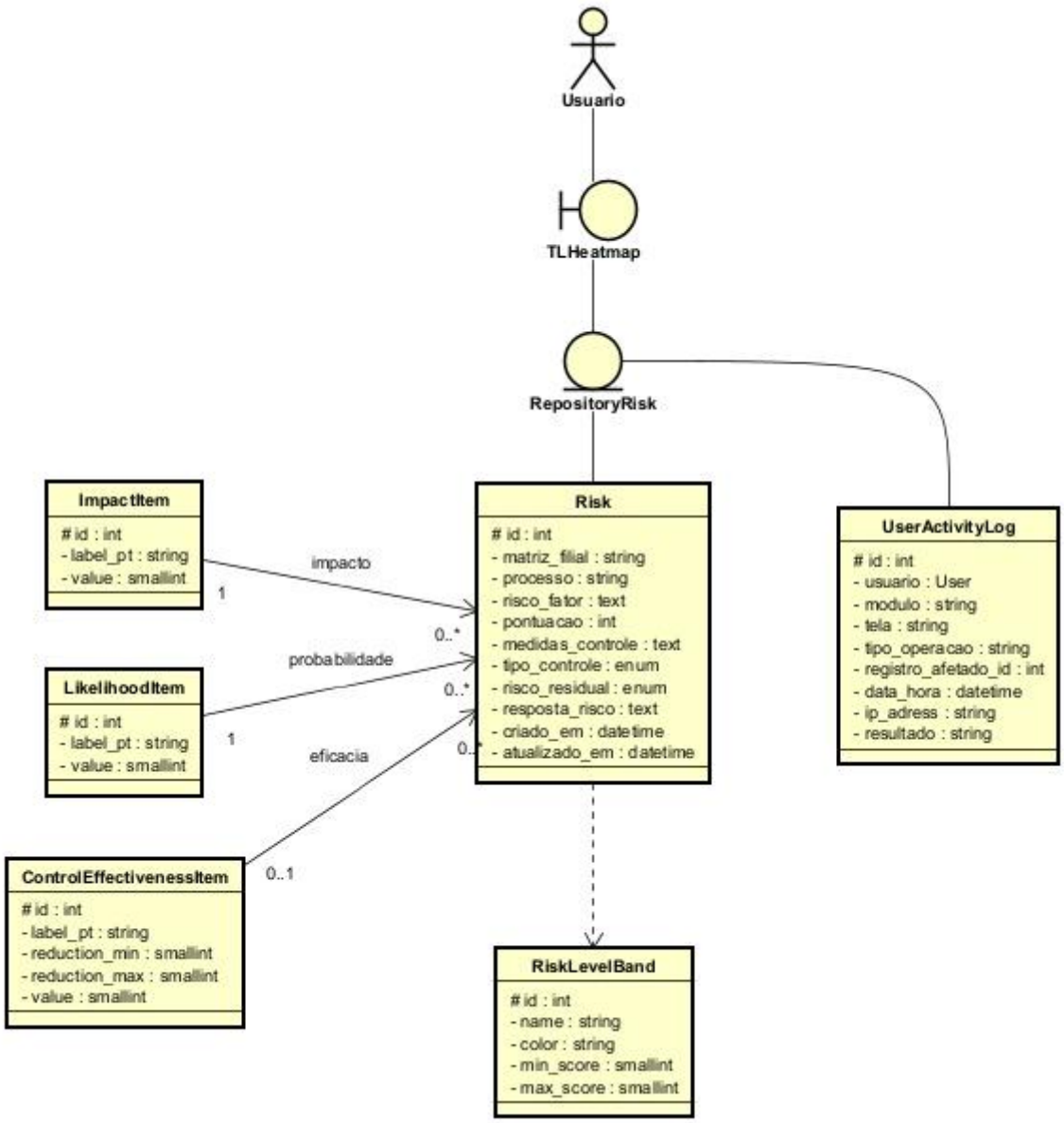
17 APÊNDICE H: DIGRAMAS DE CLASSES PARTICIPANTES

Figura 91: Autenticar Usuário



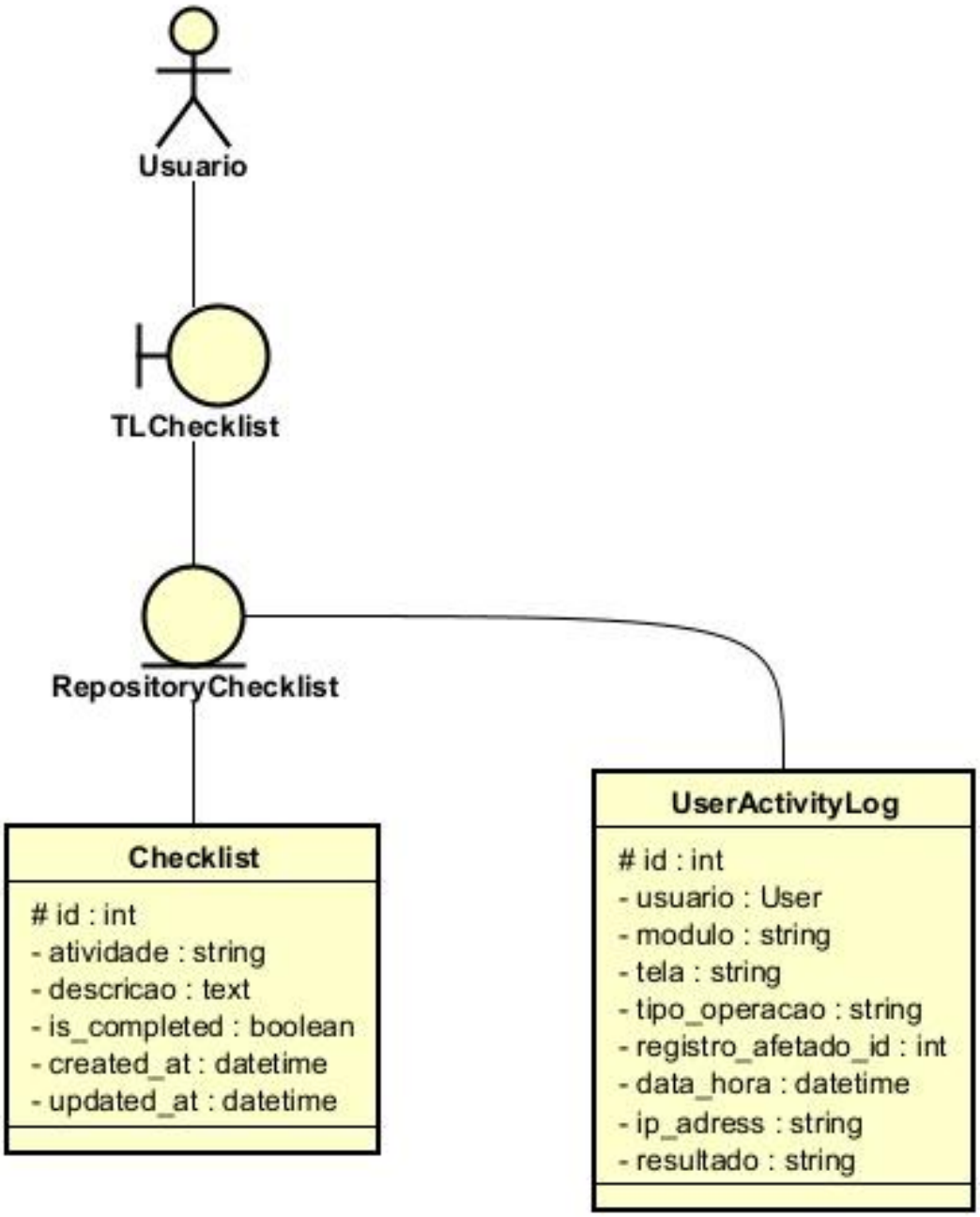
Fonte: Elaboração Própria

Figura 92: Visualizar Heatmap



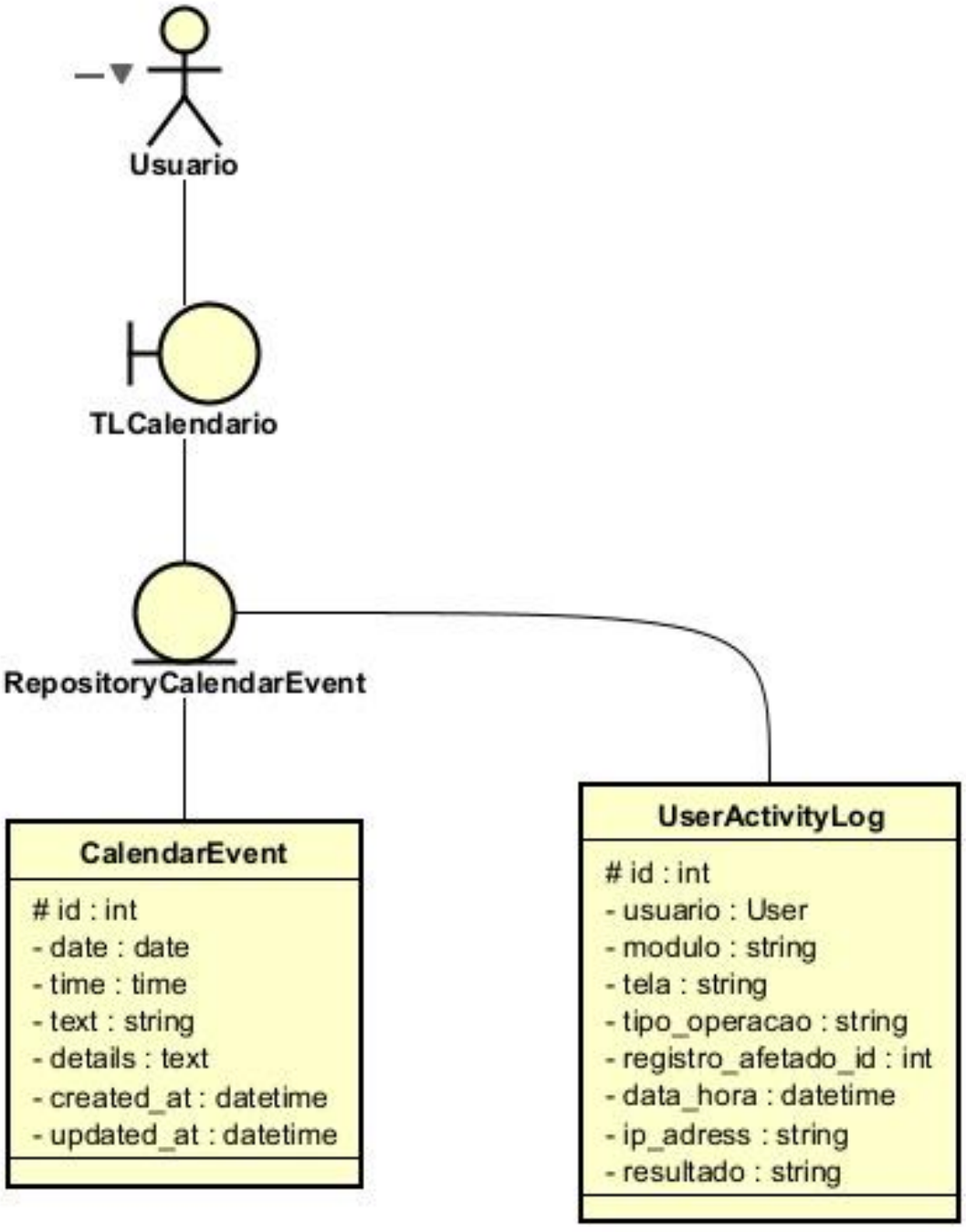
Fonte: Elaboração Própria

Figura 93: Gerir Checklist



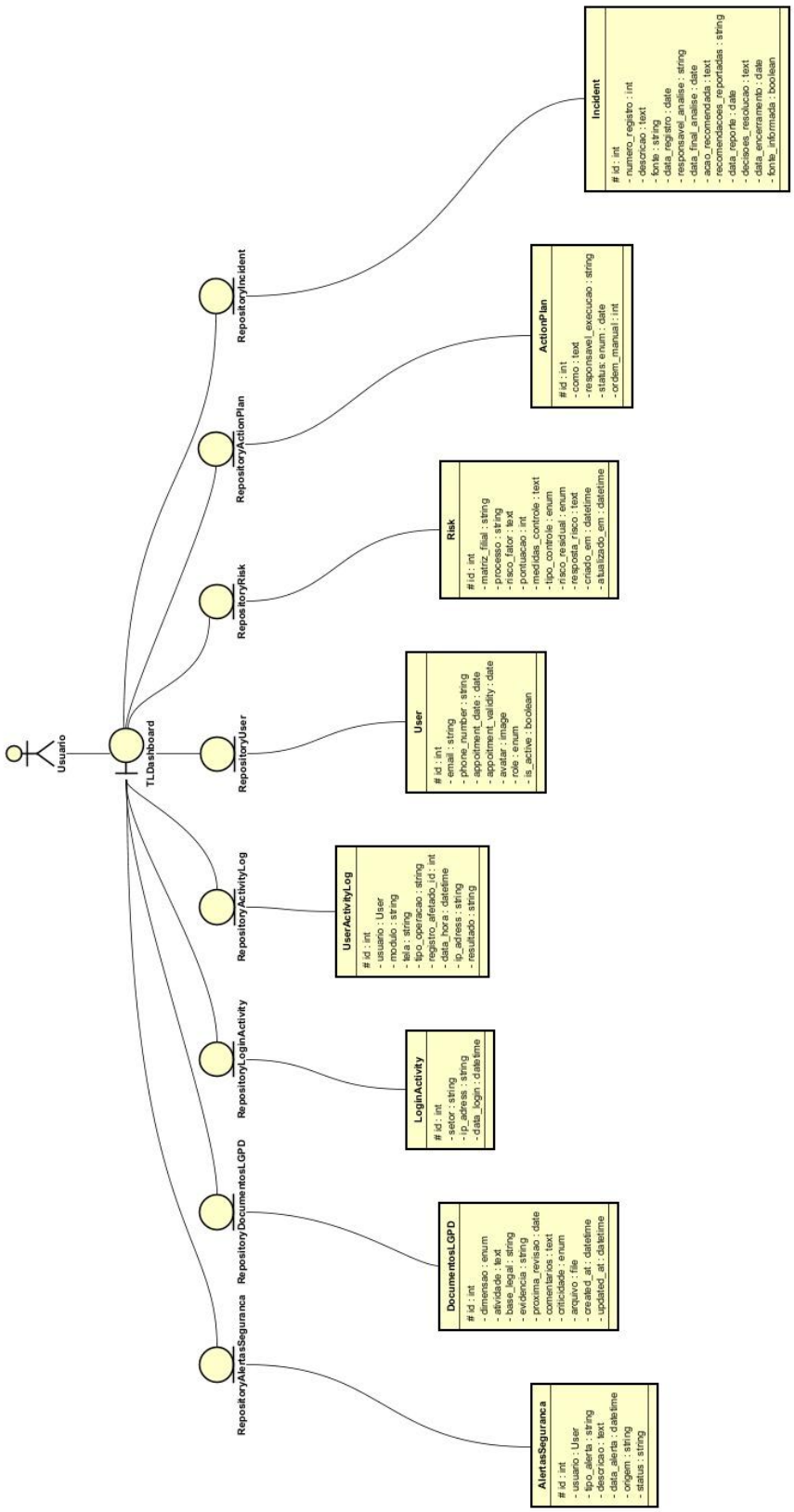
Fonte: Elaboração Própria

Figura 94: Gerir Calendário



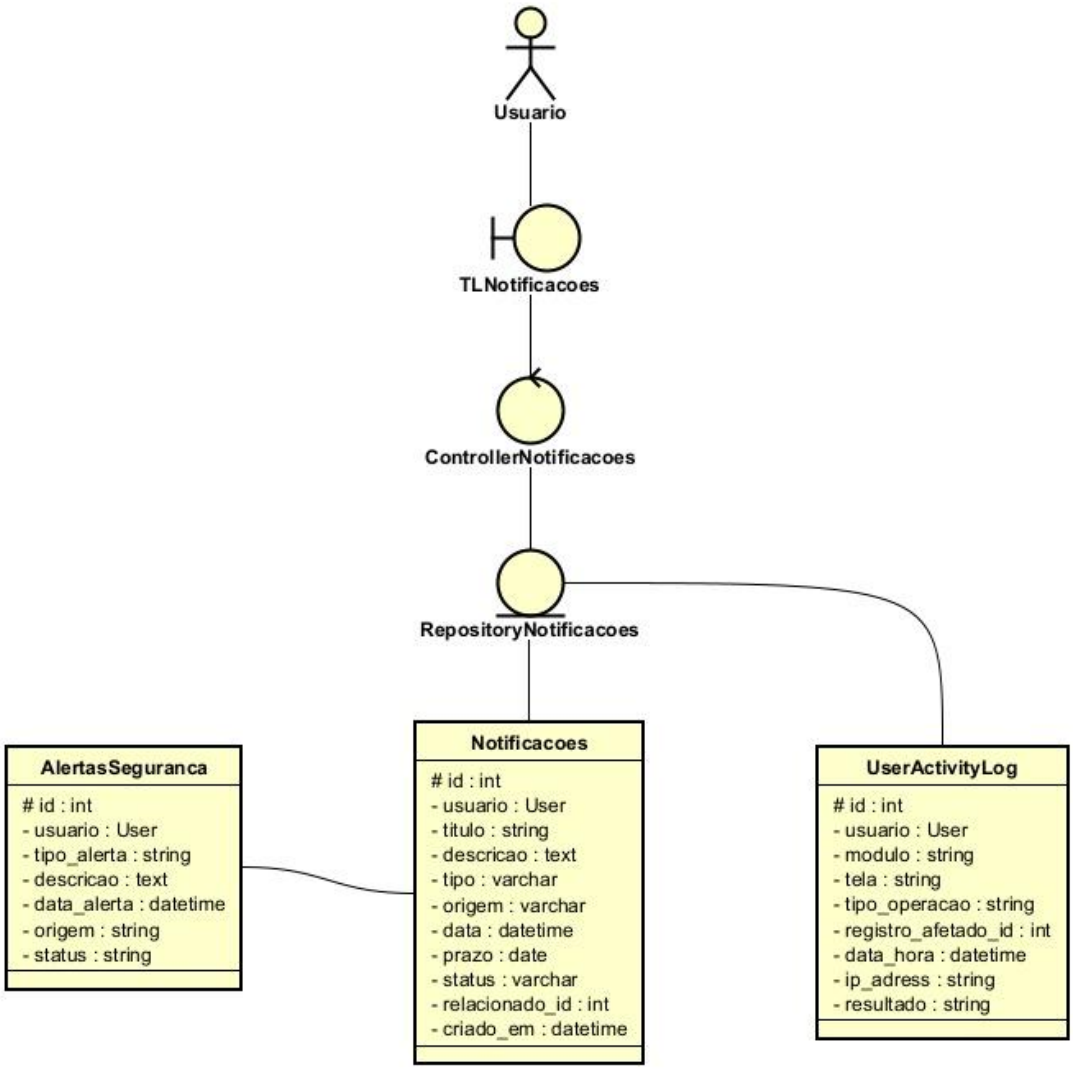
Fonte: Elaboração Própria

Figura 95: Visualizar Dashboard



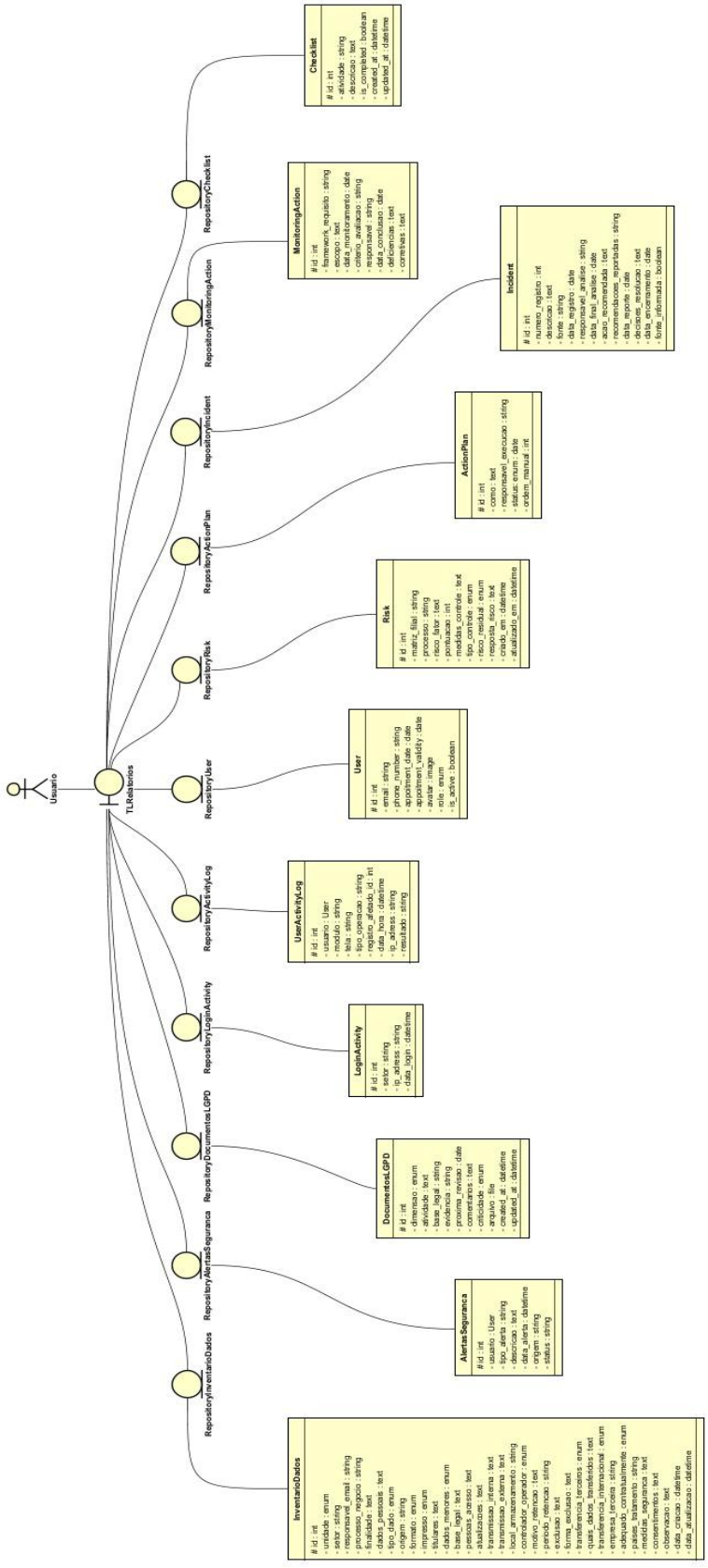
Fonte: Elaboração Própria

Figura 96: Visualizar Notificações



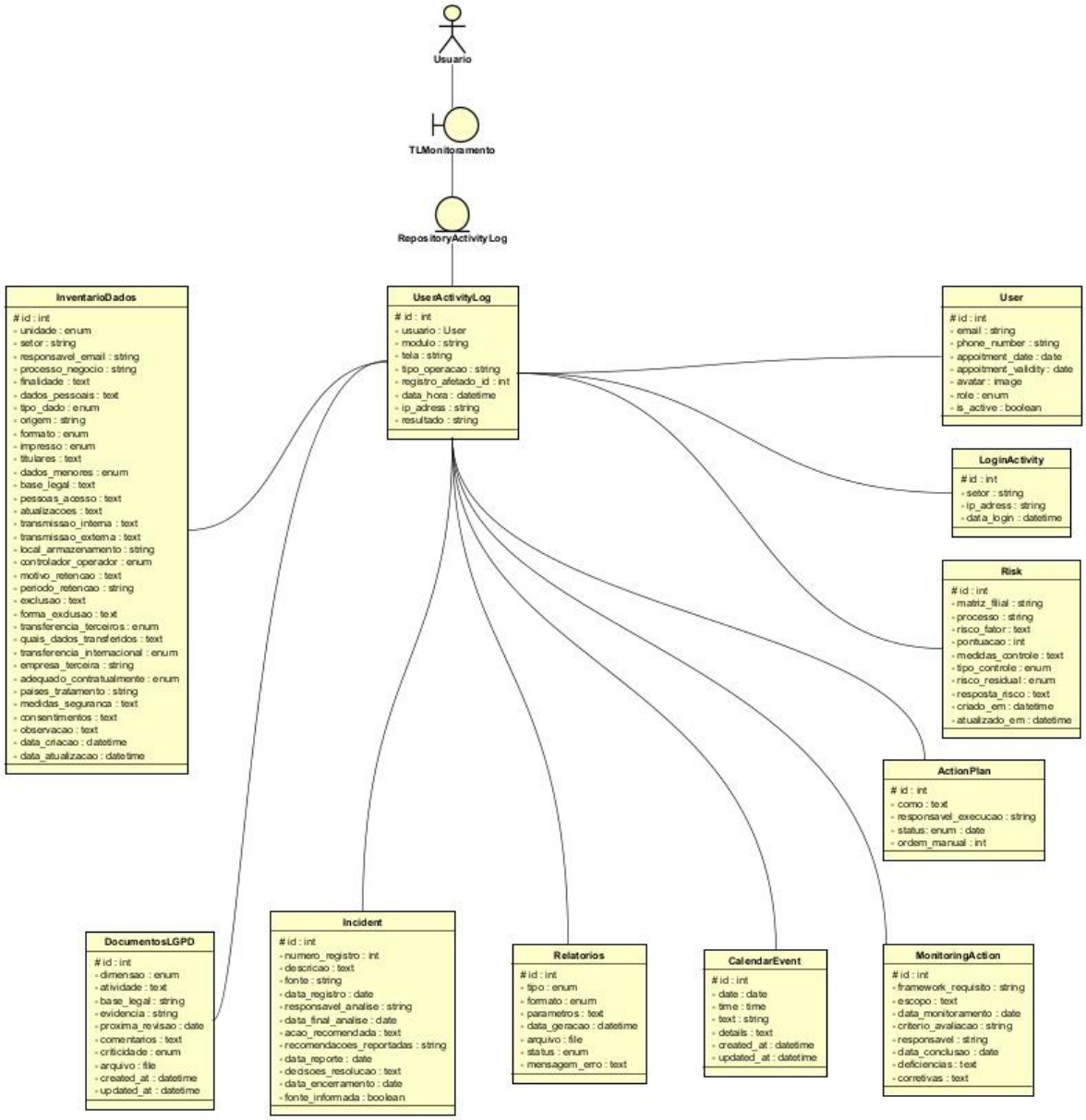
Fonte: Elaboração Própria

Figura 97: Gerar Relatórios



Fonte: Elaboração Própria

Figura 98: Visualizar / Monitorar Ações dos Usuários



Fonte: Elaboração Própria

MANUAL DO USUÁRIO WEB

Este manual tem por objetivo fornecer um guia aos usuários (Gerente, DPO, Admin.) referente ao sistema Camaleão, site e aplicativo, para o suporte a regulamentação da LGPD.

Tela Cadastro Usuário:

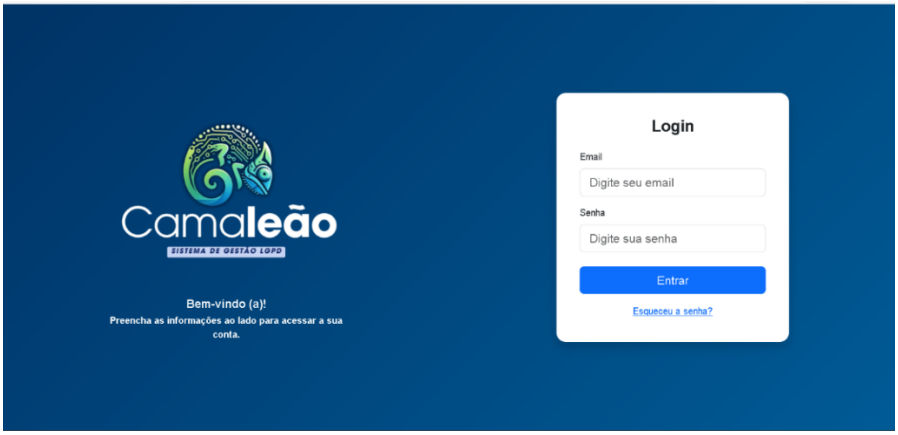
A tela de Cadastro de Usuário permite ao Administrador registrar novos acessos ao sistema. Conforme Figura 99, é possível definir o tipo de usuário (Admin, DPO ou Gerente) e informar e-mail, nome, sobrenome e senha inicial. Após o cadastro, o usuário recebe um e-mail de boas-vindas com link para criar sua própria senha, não sendo mais acessível pelo Administrador. A tela também permite listar, buscar, filtrar, editar, excluir, ativar e desativar usuários. Ao reativar um cadastro, um novo e-mail de boas-vindas é enviado automaticamente. Observação: somente um DPO pode ser cadastrado, conforme exigido pela legislação.

Figura 99: Tela Cadastro de Usuário

Tela de Login:

Tela destinada ao acesso e gerenciamento dos usuários cadastrados no sistema pelo Administrador, conforme apresentado na Figura 100.

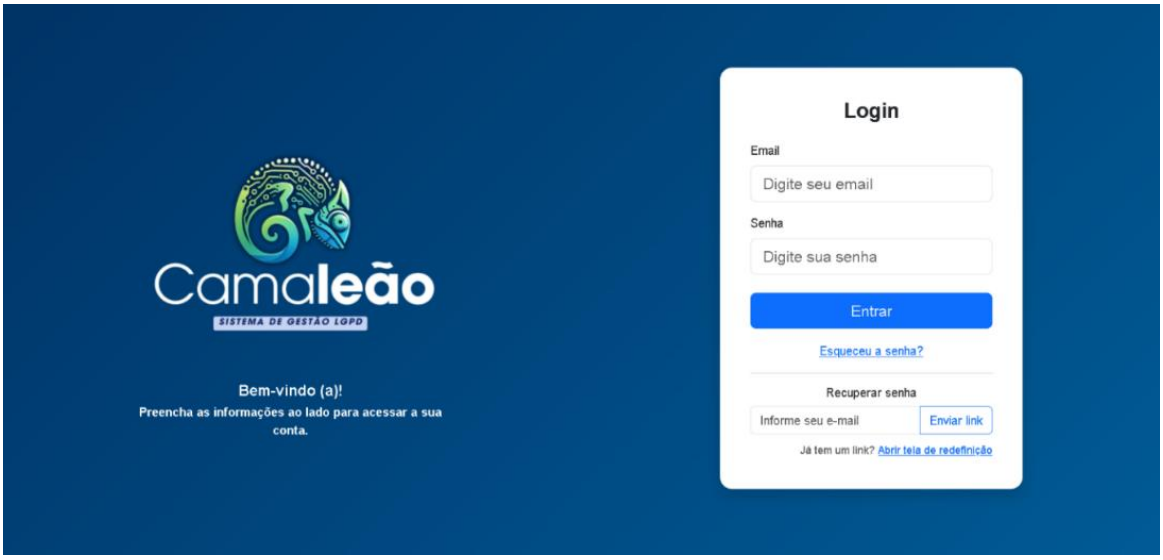
Figura 100: Página de Login



Fonte: Elaboração Página

Em caso de esquecimento da senha, o usuário pode selecionar “Esqueceu a senha?”, permitindo o envio de um link de recuperação para o e-mail informado. O usuário então recebe as instruções para redefinir sua senha, conforme demonstrado na figura abaixo.

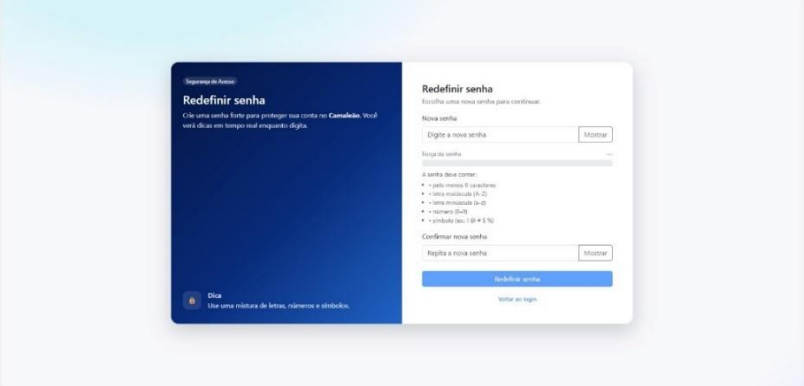
Figura 101: Página Login Esqueceu senha



Fonte: Elaboração Página

Depois de checar o e-mail enviado e clicar no link enviado você será redimensionado para alteração de senha, conforme figura 102, e deverá criar uma senha forte e segura conforme instruções. Feito isto, volte a tela de login e efetue seu login.

Figura 102: Página de Redefinição de Senha

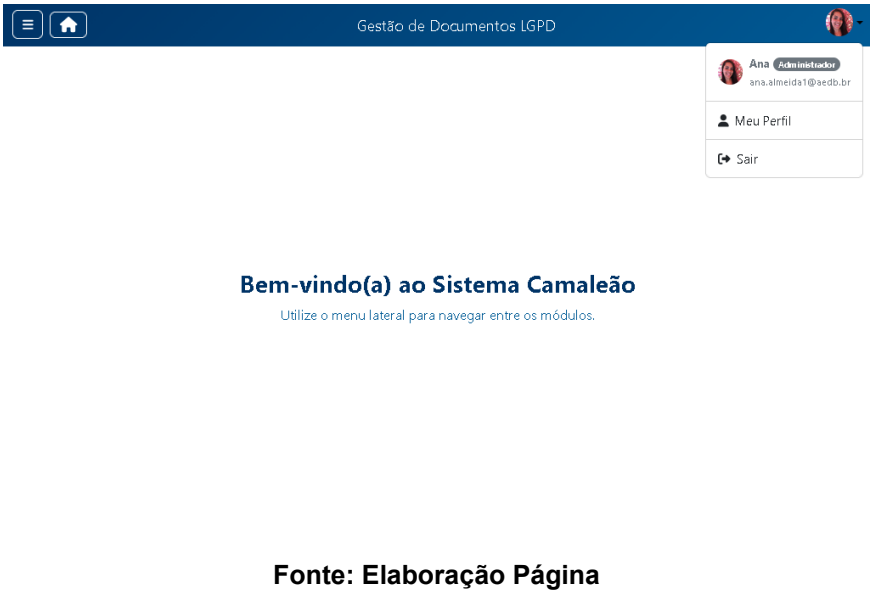


Fonte: Elaboração Página

Tela Principal:

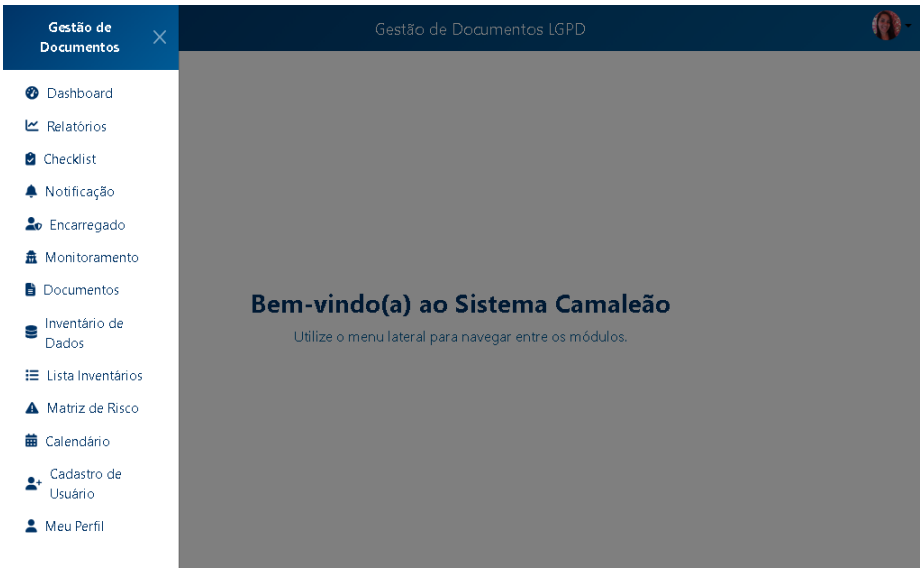
A tela principal possui uma interface simples, com menu lateral e barra superior. No ícone de perfil, o usuário acessa as opções “Meu Perfil”, “Layout” e “Sair” (Figura 102). O menu lateral permite navegar pelas funcionalidades do sistema (Figura 103)

Figura 103: Página Principal



Fonte: Elaboração Página

Figura 104: Tela Menu lateral

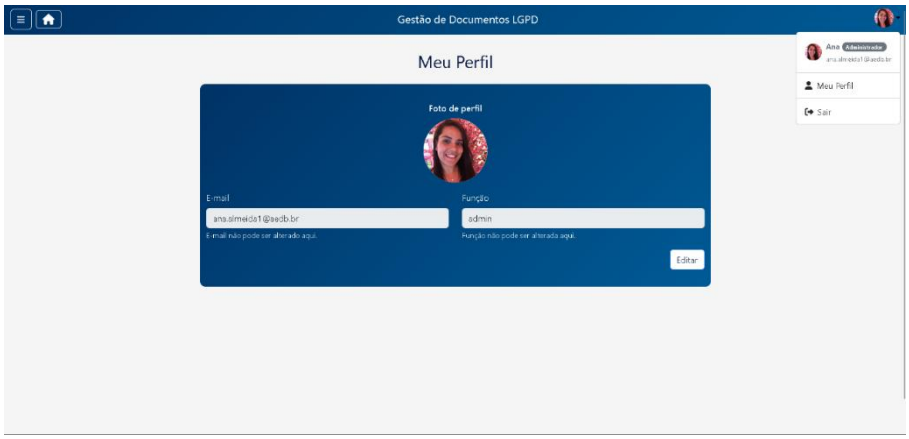


Fonte: Elaboração Página

Tela Perfil Usuário

A tela de perfil do usuário pode ser acessada pela barra de navegação, ao clicar no ícone da foto. Nessa interface, o usuário pode atualizar sua senha, além de fazer upload ou remover a própria foto de perfil, conforme ilustrado nas Figuras 105 e 106.

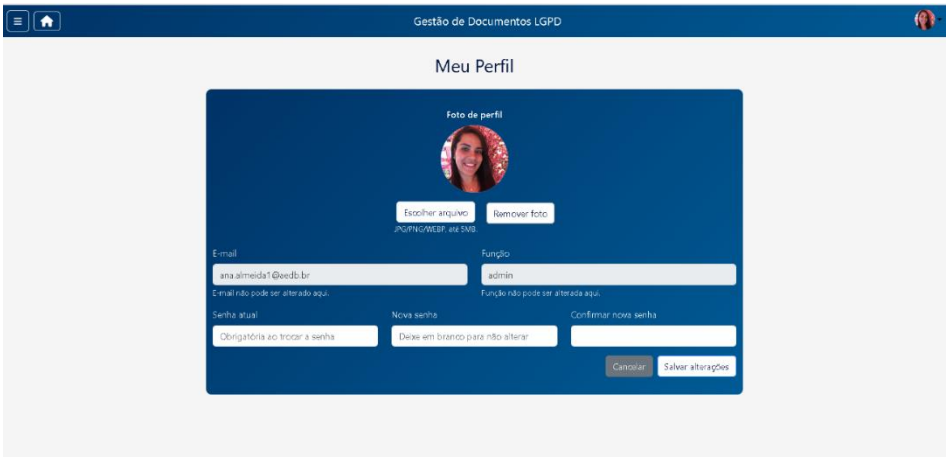
Figura 105: Página de Perfil



Fonte: Elaboração Página

A nova senha deve conter no mínimo 8 caracteres, incluindo uma letra maiúscula, um número e um símbolo especial, garantindo maior segurança no acesso ao sistema.

Figura 106: Página Edição Perfil



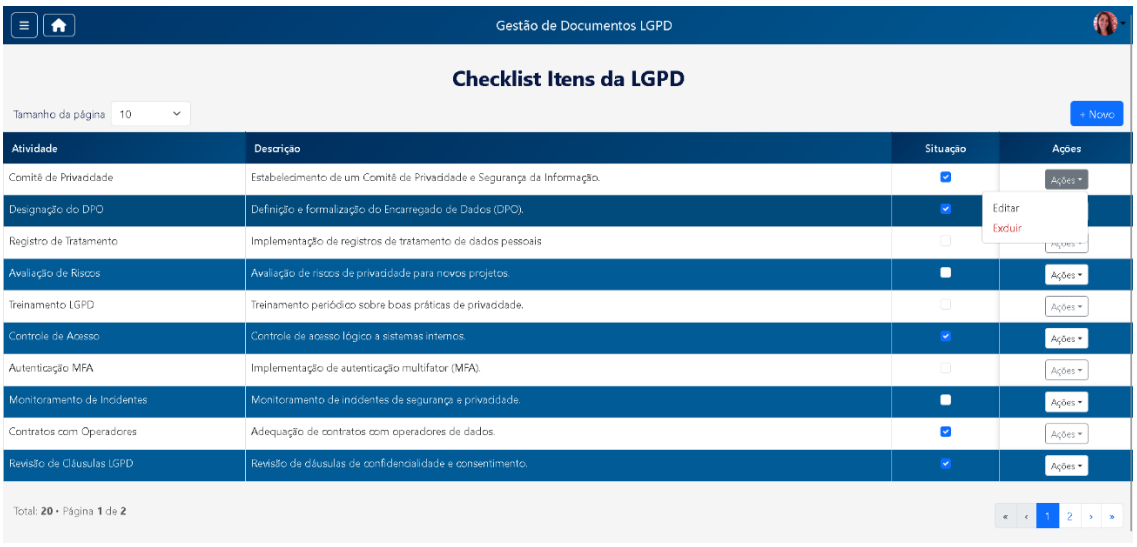
Fonte: Elaboração Página

A edição de E-mail e Função do usuário é permitida na tela de cadastro de usuário, sendo que somente quem tem acesso a alteração é o perfil administrador.

Tela Checklist:

A tela de checklist tem como objetivo estar listando as atividades exigidas pela lei e está realizando um check na coluna “Status” para saber se estão adequados, conforme a figura 107.

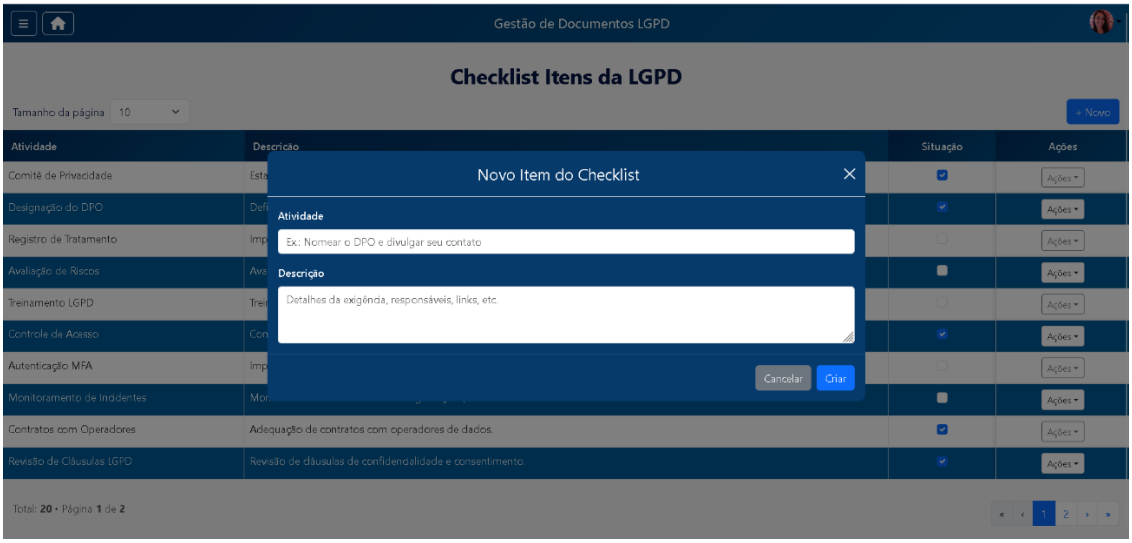
Figura 107: Página Checklist



Fonte: Elaboração Página

Ainda assim, é possível editar ou excluir uma atividade já criada por meio da coluna “Ações”, ou adicionar uma nova atividade clicando no botão “+ Novo”, que abrirá a tela de novo checklist, conforme ilustrado na Figura 108.

Figura 108: Página de Novo item do Checklist



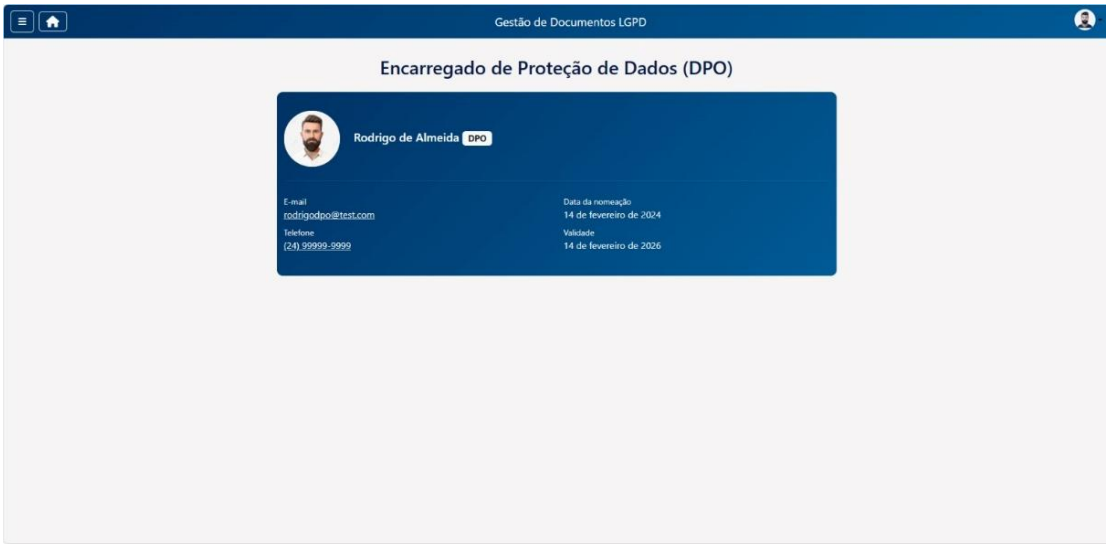
Fonte: Elaboração Página

Obs.: O perfil Gerente possui apenas permissão de visualização da página, sem acesso às ações de edição, inclusão ou exclusão. Já a exclusão de registros, disponível apenas para Administradores e DPO, só pode ser realizada mediante justificativa.

Tela do Encarregado:

A tela do Encarregado exibe o contato do responsável pela proteção de dados (DPO), conforme exigido pelo Art. 41 da LGPD. Suas informações são apresentadas de forma clara e objetiva, conforme Figura 109.

Figura 109: Página do Encarregado (DPO)



Fonte: Elaboração Página

Tela Atividades da LGPD:

O formulário de Atividades registra e acompanha ações de conformidade com a LGPD. Conforme a Figura 110, permite cadastrar atividades ou documentos, informando base legal, evidências, status e data da próxima revisão.

Figura 110: Página Atividades da LGPD

Fonte: Elaboração Página

O sistema também permite editar ou excluir registros, além de realizar o upload de arquivos relacionados. Ao clicar no botão “+Novo”, a tela de criação de uma nova atividade é exibida, conforme apresentado na figura 111.

Figura 111: Página Nova Atividade LGPD

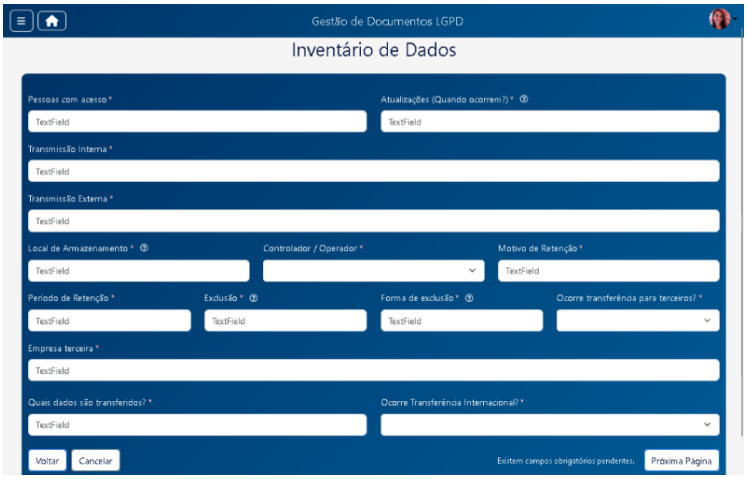
Fonte: Elaboração Página

Obs.: O perfil de Gerente possui acesso exclusivamente para leitura e acompanhamento das informações.

Tela Inventário de Dados:

A tela de Inventário de Dados mapeia cada dado pessoal tratado, registrando origem, finalidade, base legal, responsáveis e armazenamento. Como mostrado na Figura 112, só é possível avançar após preencher todos os campos obrigatórios.

Figura 112: Página Cadastro de Inventário de Dados (Parte 1)



Fonte: Elaboração Própria

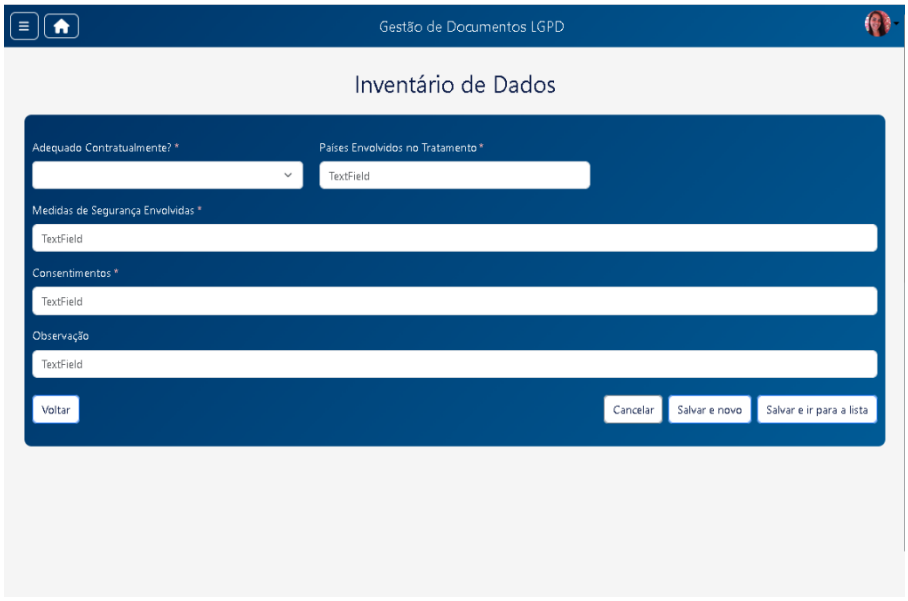
Ao avançar para a página seguinte, são exibidas as informações relacionadas ao armazenamento, ao compartilhamento e ao descarte do dado, conforme apresentado na Figura 113.

Figura 113: Página Cadastro de Inventário de Dados (Parte 2)

Fonte: Elaboração Própria

Ao avançar para a última página, apresentada na Figura 114, são exibidas as informações relacionadas à segurança e à conformidade do dado, incluindo adequação contratual, transferências internacionais, medidas de proteção e registros de consentimento.

Figura 114: Página Cadastro de Inventário de Dados (Parte 3)



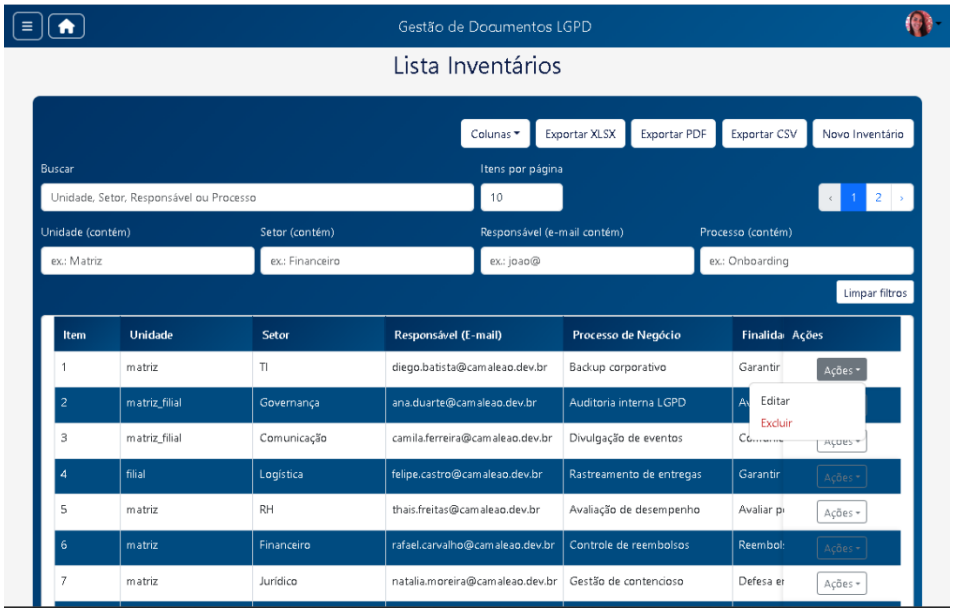
Fonte: Elaboração Própria

Após finalizar o preenchimento das informações, o usuário pode clicar em “Salvar e Novo” para cadastrar outro inventário, ou selecionar “Salvar e ir para a lista”, que o redireciona para a tela de Lista de Inventário de Dados.

Tela Lista de Inventários.

A tela de Lista de Inventário de Dados permite visualizar todos os inventários cadastrados. Na parte superior (Figura 115) estão os filtros, a opção “Colunas” e o recurso de exportação. O botão “Novo Inventário” leva à criação de um novo registro. A tabela inferior exibe todos os inventários, permitindo edição e exclusão conforme permissões. Somente Administradores e DPO podem editar ou excluir inventários.

Figura 115: Página Lista de Inventário



Fonte: Elaboração Própria

Sendo assim, apenas Admin e DPO podem editar ou excluir qualquer inventário. O Gerente pode editar e solicitar exclusão apenas dos registros que ele mesmo criou.

Tela Avaliação de Risco:

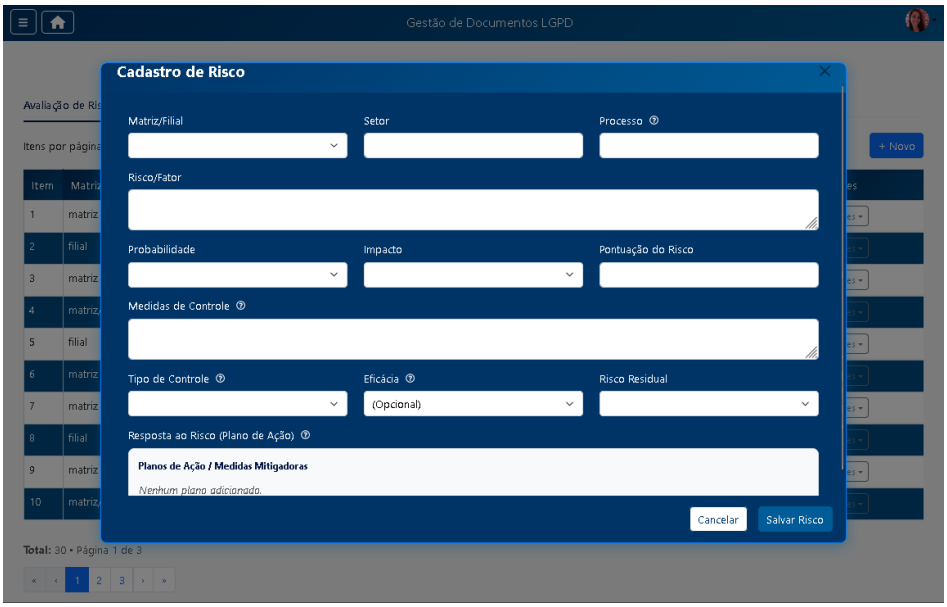
A tela de Avaliação de Risco, conforme apresentado na Figura 115, permite visualizar os registros relacionados aos riscos do tratamento de dados pessoais dentro da organização. Nela, o usuário pode consultar as informações utilizadas para identificar, avaliar e documentar cada risco, facilitando o mapeamento, o acompanhamento, a análise e a tomada de decisão da empresa.

Figura 116: Página Avaliação de Risco

Fonte: Elaboração Própria

Ao clicar em “+Novo”, o sistema abre a tela de criação de risco (Figura 117). Após o cadastro, é possível editar ou excluir registros já existentes. Admin e DPO possuem acesso total, enquanto o Gerente tem permissões apenas de visualização. A exclusão de riscos é permitida somente para Admin e DPO.

Figura 117: Página Cadastro de Risco

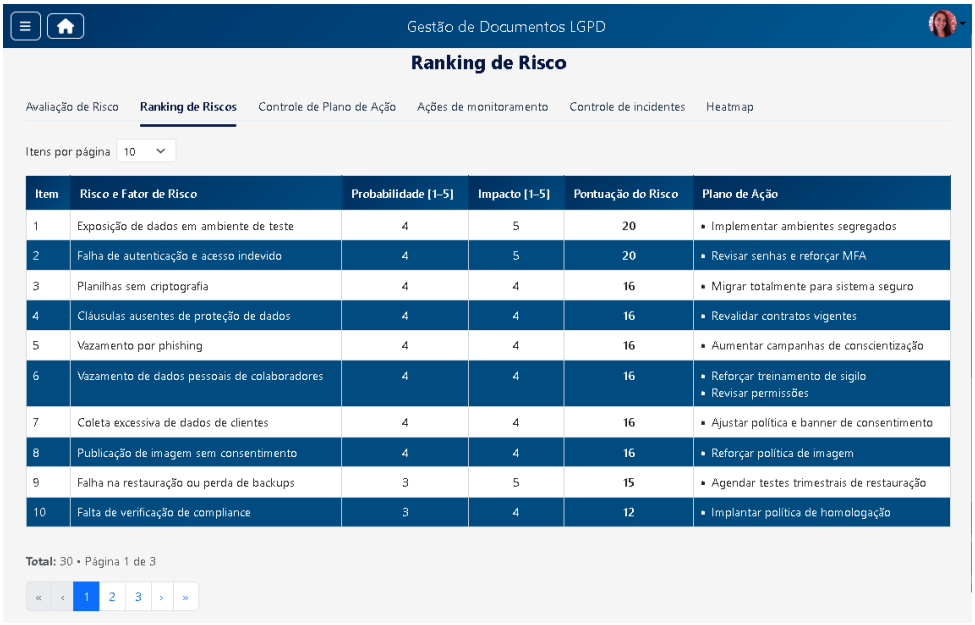


Fonte: Elaboração Própria

Tela Ranking de Risco:

A tela de Ranking, no módulo de Riscos, exibe a classificação dos riscos do maior para o menor, conforme a pontuação definida na Avaliação de Risco. A pontuação combina probabilidade e impacto, destacando os riscos mais críticos (Figura 118).

Figura 118: Página Ranking de Risco

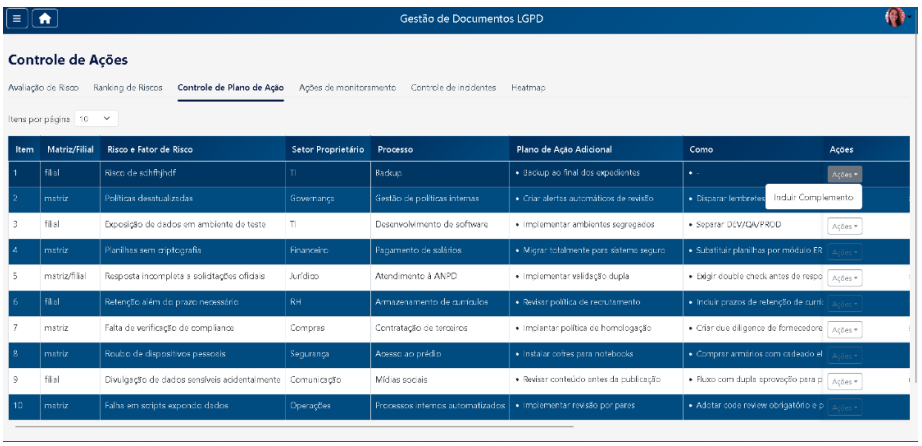


Fonte: Elaboração Própria

Tela Controle de Plano de Ação:

A tela de Controle de Plano de Ação gerencia as ações definidas para cada risco, detalhando execução, responsáveis e prazos (Figura 119). Ao criar um risco, o botão “Incluir Complemento” permite adicionar um plano de ação, podendo registrar múltiplos complementos quando necessário.

Figura 119: Página Controle de Plano de Ação



Fonte: Elaboração Própria

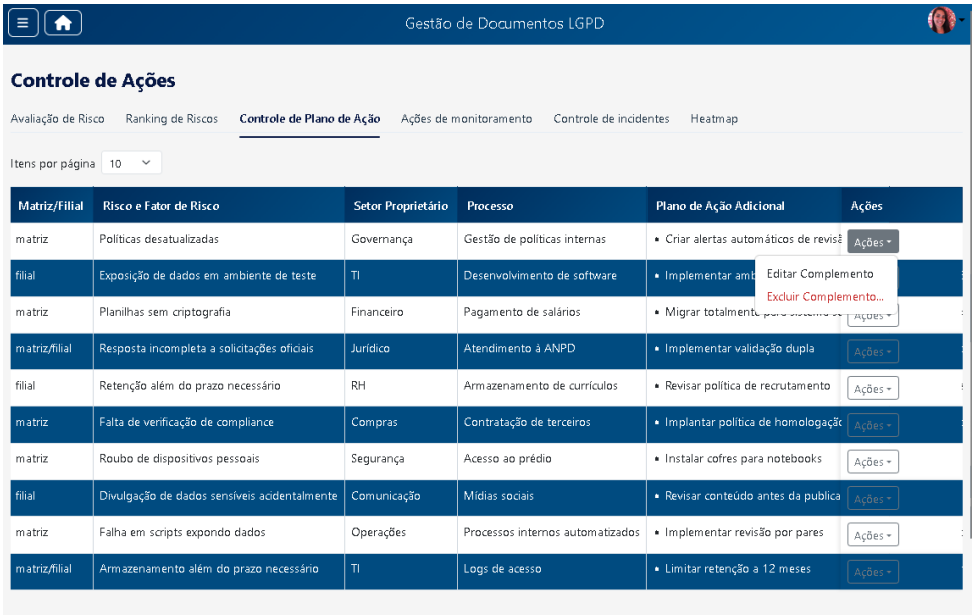
Ao clicar em “Incluir”, será aberta a tela de cadastro do complemento de ação, conforme apresentado na Figura 120.

Figura 120: Página Incluir Complemento da Controle de Ação

Fonte: Elaboração Própria

Após a inclusão, conforme mostrado na Figura 121, serão exibidas as opções de edição e exclusão do registro.

Figura 121: Página Controle de Ações, editar e Excluir



Fonte: Elaboração Própria

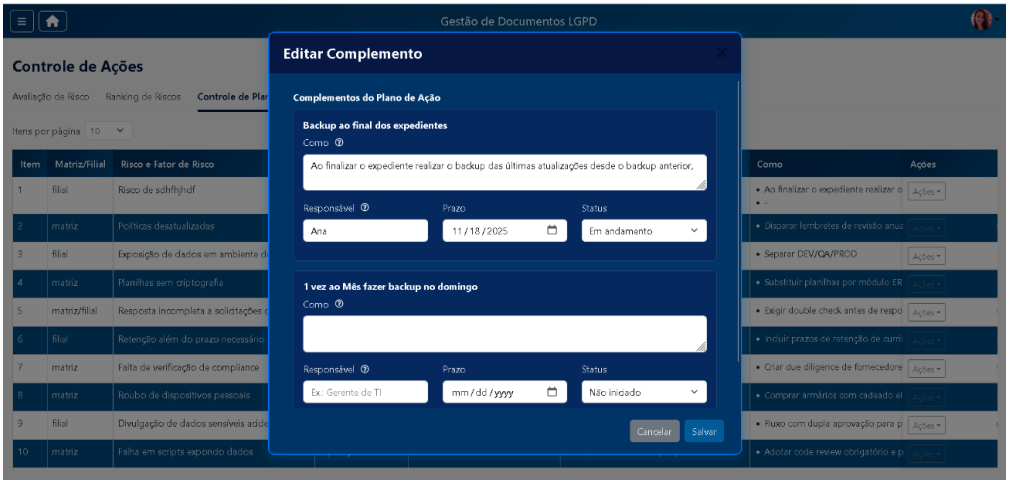
Ao clicar em “Editar”, são exibidos os mesmos campos utilizados no momento da criação do complemento, permitindo ajustar as informações já cadastradas. Já na opção “Excluir”, caso existam vários complementos registrados — dependendo da quantidade de ações vinculadas — o usuário pode remover apenas o complemento desejado, conforme mostrado na Figura 122.

Figura 122: Página Controle Plano Ação, Excluir Complemento

Fonte: Elaboração Própria

Ao excluir um dos complementos de ação, para adicioná-lo novamente basta clicar em “Editar”. Essa opção abrirá a tela com o campo em branco para novo preenchimento, conforme mostrado na Figura 123.

Figura 123: Página Controle Plano de Ação, Adicionando Complemento Pós Exclusão



Fonte: Elaboração Própria

Os perfis de Administrador e DPO possuem acesso total ao módulo. Já o perfil de Gerente tem acesso para acompanhamento e pode atualizar apenas os planos de ação que estiverem sob sua responsabilidade.

Tela Ações de Monitoramento:

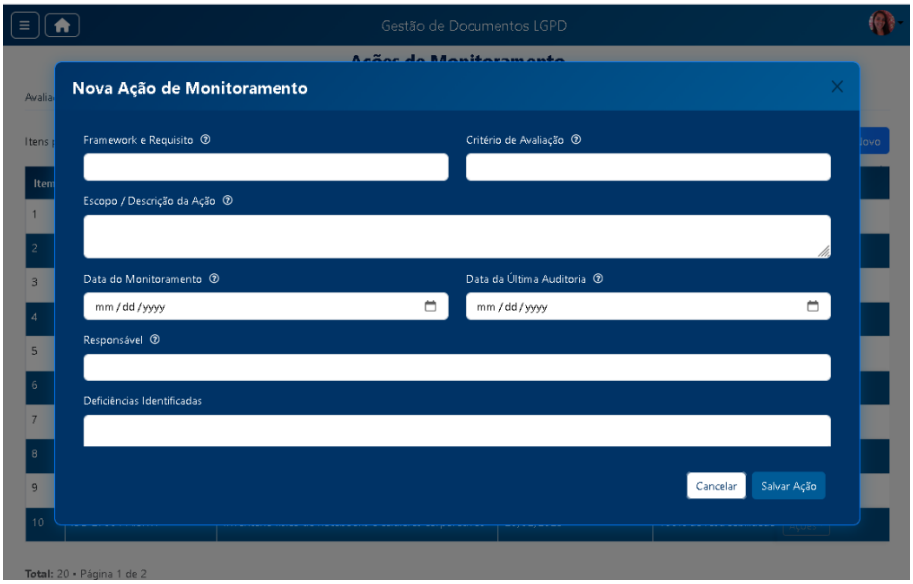
A tela de Ação de Monitoramento permite registrar atividades de verificação e auditoria relacionadas à conformidade. Nela, o usuário informa o requisito avaliado, a descrição da ação, as datas, o responsável e eventuais deficiências identificadas, conforme mostrado na Figura 124. Também é possível editar ou excluir registros já existentes.

Figura 124: Página Ações de Monitoramento

Fonte: Elaboração Própria

Além disso, ao clicar em “+Novo”, uma nova ação de monitoramento pode ser adicionada, conforme mostrado na Figura 125.

Figura 125: Página Adição Nova Ação Monitoramento



Fonte: Elaboração Própria

Somente os perfis de Admin e DPO tem acesso a está parte. A opção de excluir por questões de auditoria, aparecerá quando clicar em excluir um campo para preencher o motivo da exclusão.

Tela Controle de Incidentes:

A tela de Controle de Incidentes registra e acompanha ocorrências relacionadas à proteção de dados, reunindo informações de identificação, análise e

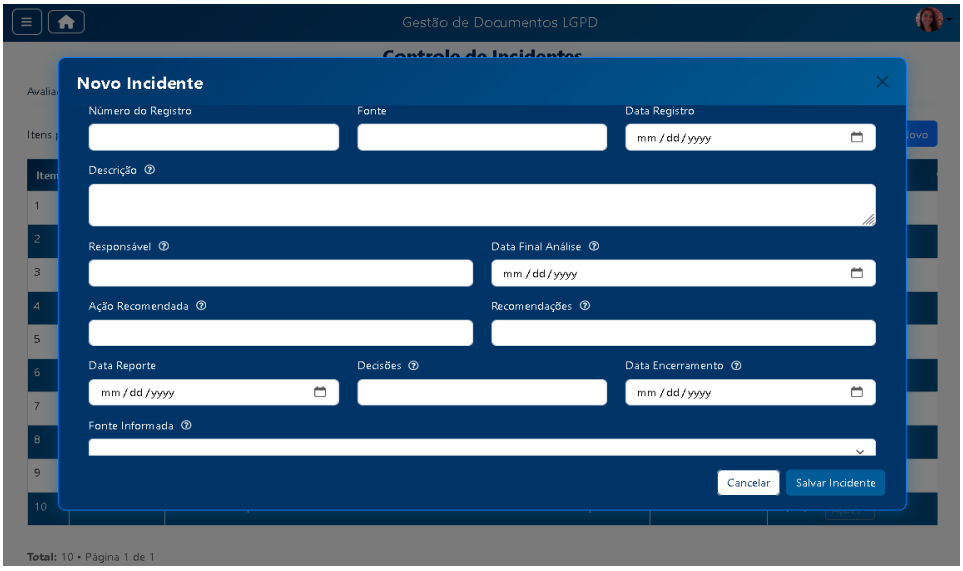
ações tomadas. Após o cadastro (Figura 126), o usuário pode visualizar, editar ou excluir o incidente conforme suas permissões.

Figura 126: Controle de Incidentes

Fonte: Elaboração Própria

Para registrar um novo incidente, basta clicar em “+ Novo”, o que abrirá o formulário de cadastro conforme ilustrado na Figura 127.

Figura 127: Página Novo Incidente



Fonte: Elaboração Própria

Somente os perfis de Admin e DPO tem acesso a está parte. A opção de excluir por questões de auditoria, aparecerá quando clicar em excluir um campo para preencher o motivo da exclusão.

Tela Heatmap:

A tela de Heatmap de Risco, conforme Figura 128, apresenta de forma visual a relação entre probabilidade e impacto dos riscos cadastrados, além dos cards que mostram a quantidade total de riscos e suas classificações (Crítico, Alto, Médio e Baixo).

Em relação à prioridade:

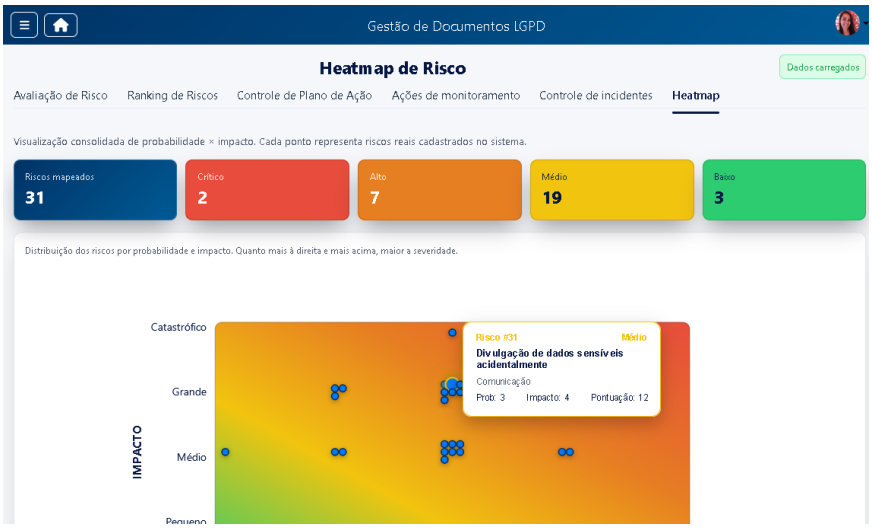
- Crítico (vermelho): exige atenção imediata.
- Alto (laranja): requer ação rápida e monitoramento frequente.
- Médio (amarelo): precisa de acompanhamento regular.
- Baixo (verde): demanda apenas monitoramento básico, sem urgência.

Figura 128: Página Heatmap

Fonte: Elaboração Própria

Ainda assim, ao clicar em qualquer ponto exibido no gráfico, conforme Figura 129, o sistema exibe qual risco está associado àquela classificação de probabilidade e impacto.

Figura 129: Página Heatmap Gráfico



Fonte: Elaboração Própria

Somente o Admin e o DPO têm acesso completo ao Heatmap.

Tela Dashboard:

A tela de Dashboard apresenta uma visão geral dos principais indicadores do sistema. Conforme Figura 129, exibe métricas como conformidade geral, riscos mapeados, ações atrasadas, documentos a vencer e alertas. Logo abaixo, os gráficos de Distribuição de Riscos e o Heatmap permitem visualizar rapidamente a severidade dos riscos e a relação entre probabilidade e impacto.

Figura 130: Dashboard de Conformidade LGPD

Fonte: Elaboração Própria

Conforme Figura 131, a tela exibe dois gráficos adicionais. O gráfico Riscos por Setor mostra a quantidade de riscos identificados em cada área. Já o Top 5 Riscos

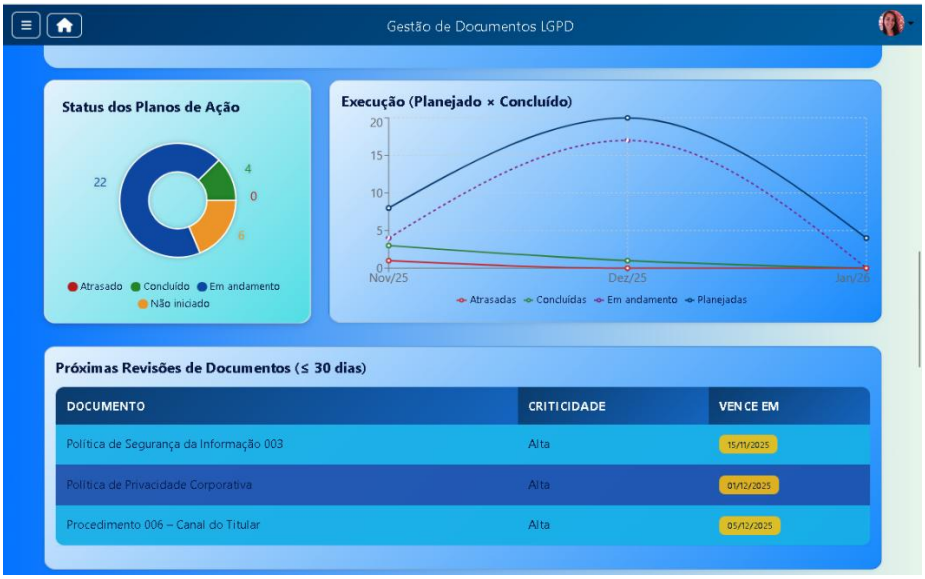
destaca os riscos mais críticos, apresentando sua pontuação, setor e processo de negócio, facilitando a priorização das ações.

Figura 131: Página Dashboards Riscos

Fonte: Elaboração Própria

Conforme Figura 132, a tela apresenta o gráfico Status dos Planos de Ação, que mostra a quantidade de ações concluídas, em andamento, não iniciadas e atrasadas. Ao lado, o gráfico Execução (Planejado × Concluído) permite acompanhar a evolução mensal das atividades. Abaixo, a seção Próximas Revisões de Documentos exibe os documentos que vencem nos próximos 30 dias, destacando sua criticidade e data de revisão.

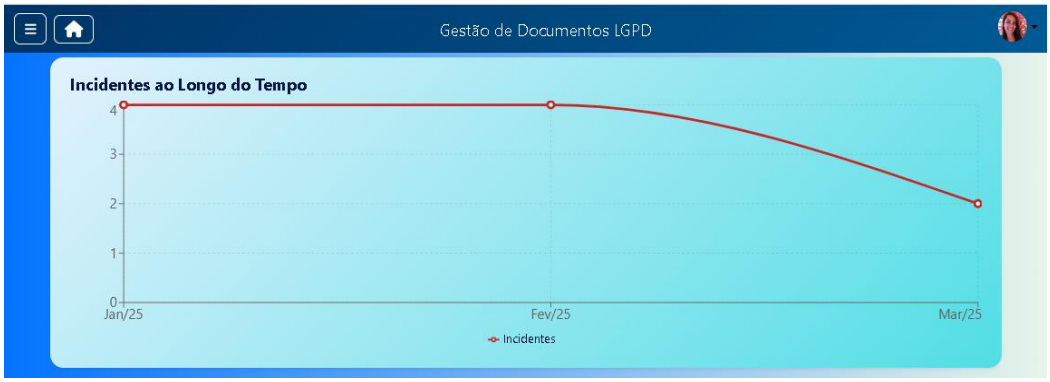
Figura 132: Página Dashboard Ações



Fonte: Elaboração Própria

Conforme Figura 133, a tela apresenta o gráfico Incidentes ao Longo do Tempo, que demonstra a quantidade de incidentes registrados em cada período. Esse acompanhamento permite visualizar tendências e identificar aumento ou redução de ocorrências ao longo dos meses.

Figura 133: Página Dashboards Incidentes



Fonte: Elaboração Própria

Conforme Figura 134, a tela apresenta a seção Últimos Acessos, que mostra os registros mais recentes de login dos usuários, incluindo nome, função e horário do acesso. Ao lado, o gráfico Top 10 Usuários Mais Ativos destaca os usuários que mais interagem com o sistema, permitindo identificar padrões de uso e níveis de atividade.

Figura 134: Página Dashboards Acessos e Usuários

Fonte: Elaboração Própria

Conforme Figura 135, o indicador de Índice de Maturidade LGPD mostra o percentual de ações concluídas, permitindo avaliar rapidamente o avanço da conformidade. Ele evidencia o progresso geral e os pontos que ainda requerem atenção. Ao clicar em “Ir para o topo”, o sistema retorna ao início da página, facilitando a navegação.

Figura 135: Página Dashboards Índice de maturidade

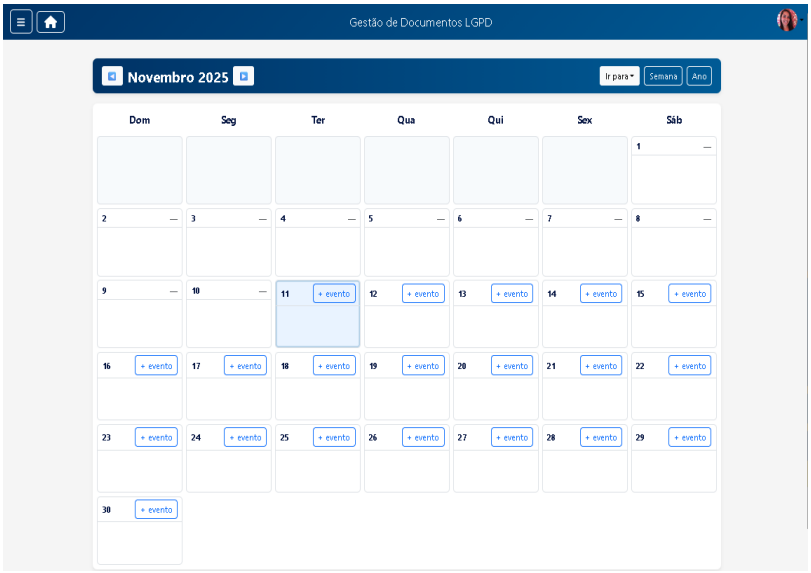
Fonte: Elaboração Própria

Somente Admin e DPO tem acesso a tela de Dashboards.

Tela de Calendário:

O Calendário é utilizado pelo DPO para registrar e acompanhar eventos, prazos e atividades importantes da organização, facilitando o planejamento das rotinas de privacidade. Conforme Figura 136, a visualização mensal permite adicionar eventos em cada dia e navegar entre os meses.

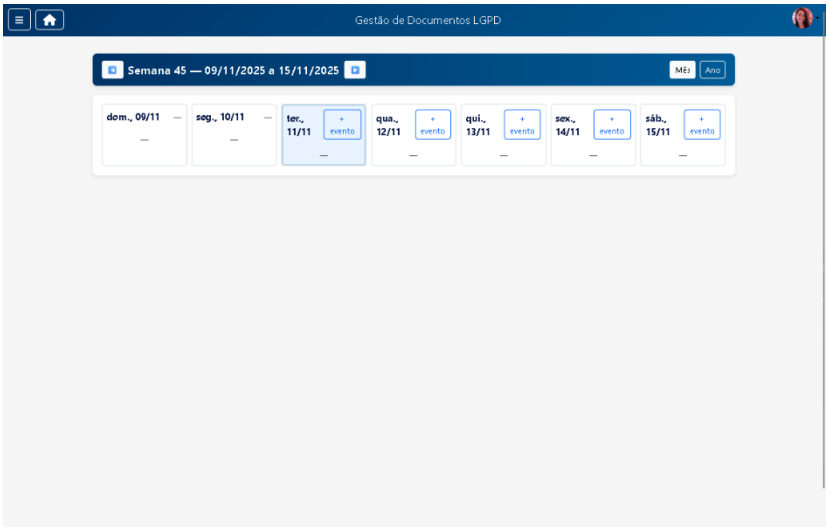
Figura 136: Página Calendário



Fonte: Elaboração Própria

Na Figura 137, o modo semanal mostra os eventos distribuídos ao longo da semana.

Figura 137: Página Calendário Semanal



Fonte: Elaboração Própria

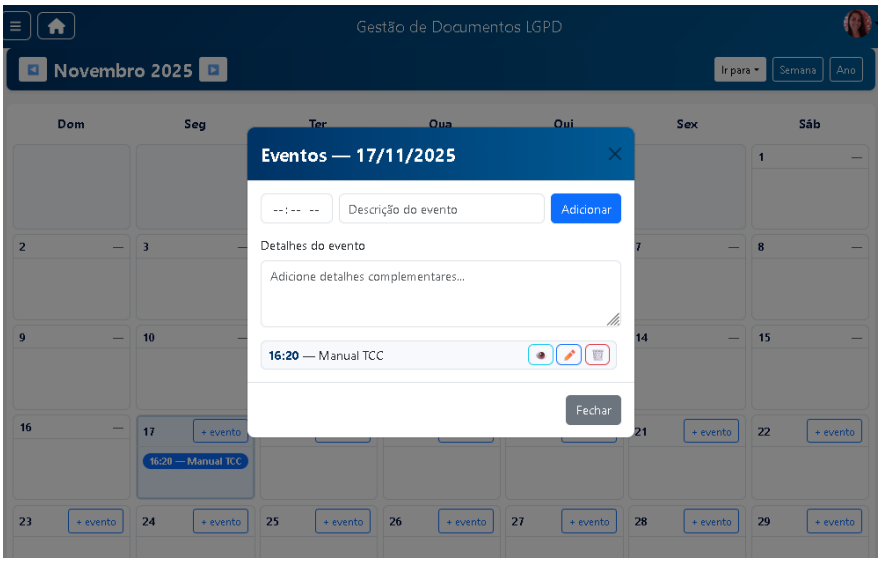
Já a Figura 138 apresenta a visão anual, reunindo todos os meses para facilitar o planejamento de longo prazo.

Figura 138: Página Calendário Anual

Fonte: Elaboração Própria

Ainda conforme figura 139, para realizar o cadastro de um evento o usuário deve clicar em +evento, que abrira o campo para preencher um novo evento, ao adicionar um horário e tema. Depois pode-se visualizar, editar e excluir.

Figura 139: Página de Novo Evento Calendário



Fonte: Elaboração Própria

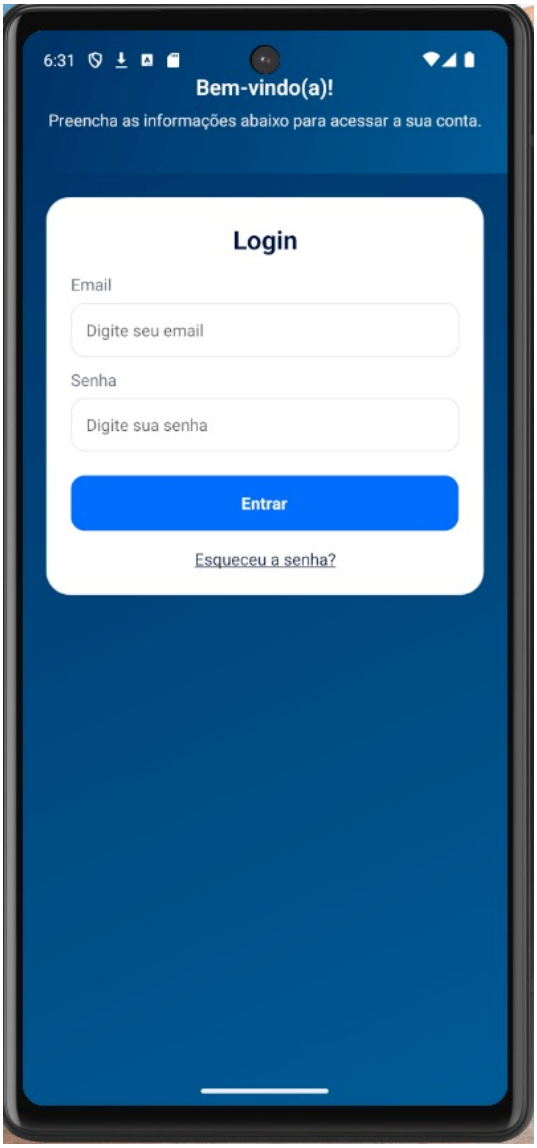
A edição e exclusão dos eventos só podem ser realizadas pelo usuário que criou, os eventos passados não podem ser excluídos apenas visualizado.

MANUAL DO USUÁRIO MOBILE

Tela de Login Mobile:

A versão mobile do sistema Camaleão oferece acesso rápido e seguro às funcionalidades essenciais. Conforme Figura 140, a tela de Login permite entrar no sistema informando e-mail e senha.

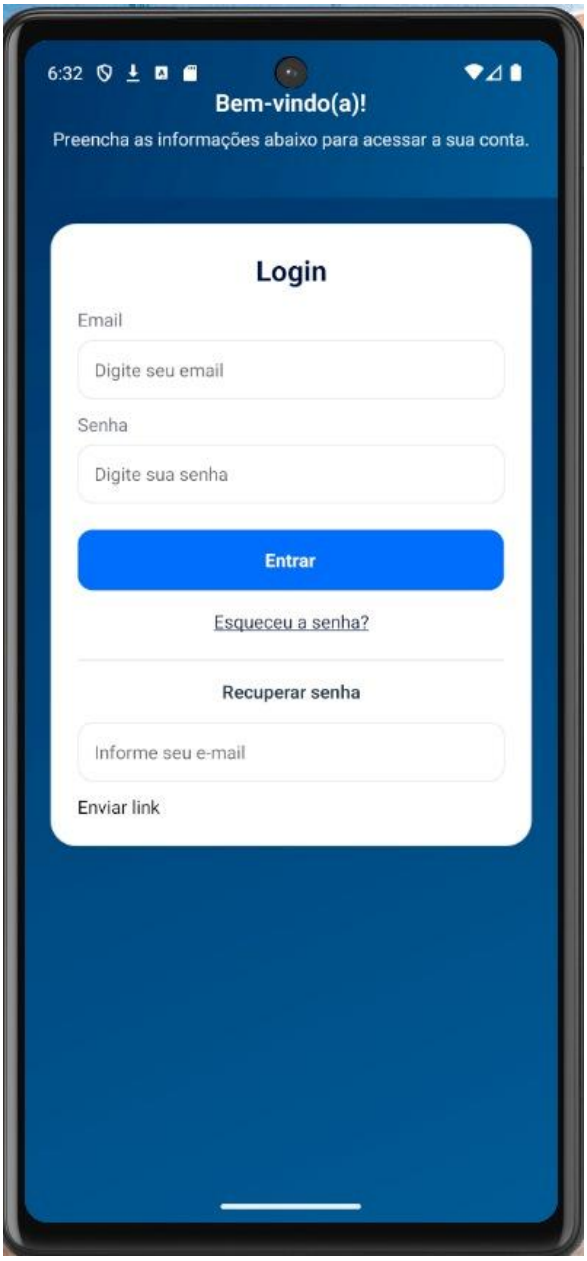
Figura 140: Página Login Mobile



Fonte: Elaboração Própria

Já a Figura 141 apresenta a opção de recuperação de senha, permitindo que o usuário solicite o link de redefinição diretamente pelo aplicativo.

Figura 141: Página Recuperação Senha Login Mobile



Fonte: Elaboração Própria

Tela Home Mobile:

A tela inicial da versão mobile reúne os principais módulos do sistema, oferecendo acesso rápido às funcionalidades essenciais da gestão LGPD. Conforme Figura 142, a Home apresenta atalhos para Encarregado, Monitoramento, Checklist, Documentos, Dashboards, Inventário de Dados, Matriz de Risco e Relatórios.

Figura 142: Página Home Mobile

Fonte: Elaboração Própria

Já a Figura 143 apresenta o menu lateral, onde o usuário encontra todas as opções de navegação do aplicativo, além das informações do seu perfil.

Figura 143: Página Menu Lateral

Fonte: Elaboração Própria

Tela Perfil Usuário Mobile:

A tela de Perfil do Usuário na versão mobile permite que cada usuário visualize suas informações de acesso e mantenha seus dados atualizados de forma simples. Conforme Figura 144, a tela exibe a foto de perfil, o e-mail (que não pode ser alterado) e a função do usuário no sistema. A opção editar permite atualizar dados permitidos, como a foto de perfil ou a senha, garantindo mais autonomia e segurança no uso do aplicativo.

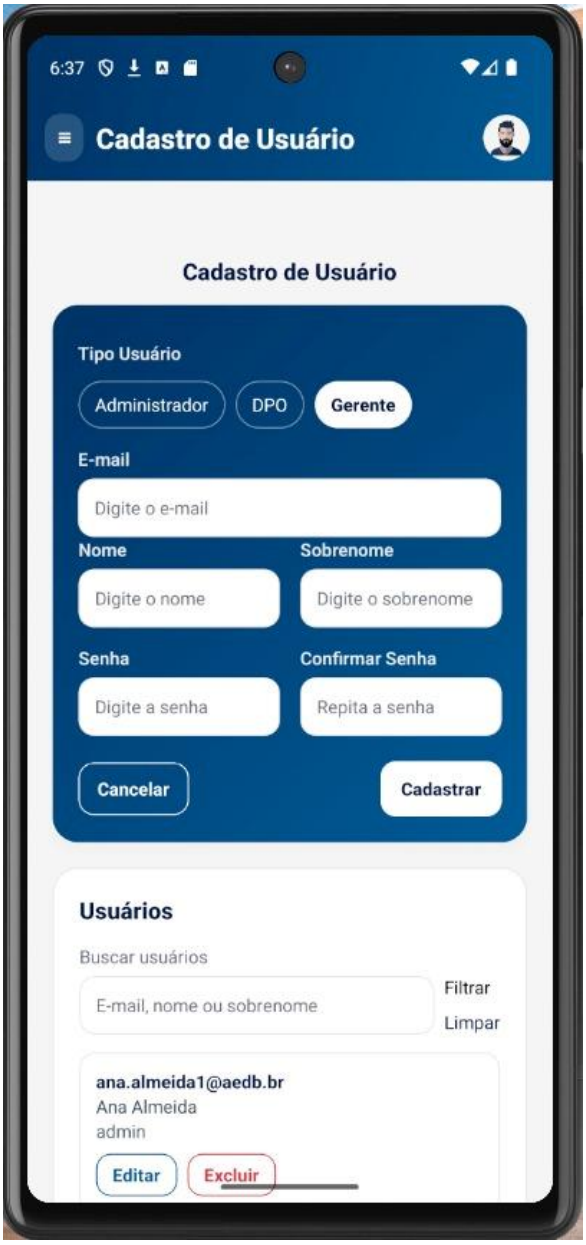
Figura 144: Página Perfil Usuário Mobile

Fonte: Elaboração Própria

Tela Cadastro de Usuário Mobile:

A tela de *Cadastro de Usuário* na versão mobile mantém as funções da versão web, sendo acessada exclusivamente pelo administrador do sistema. Conforme Figura 47, o administrador pode definir o tipo de usuário (Administrador, DPO ou Gerente), inserir e-mail, nome, sobrenome e senha para criar acessos. A tela também permite editar, excluir e buscar usuários já cadastrados, garantindo o controle total de quem pode utilizar o aplicativo.

Figura 145: Página Cadastro de Usuário Mobile



Fonte: Elaboração Própria

Tela Checklist Mobile:

A tela de *Checklist da LGPD* na versão mobile apresenta os itens que compõem a lista de verificação de conformidade da organização. Conforme Figura 48, o usuário pode visualizar cada requisito, sua descrição e o status da situação. Perfis autorizados (Administrador e DPO) podem adicionar novos itens e acessar as ações disponíveis. Obs.: O perfil Gerente possui apenas permissão de visualização, sem acesso às ações de edição ou inclusão.

Figura 146: Página Checklist Mobile

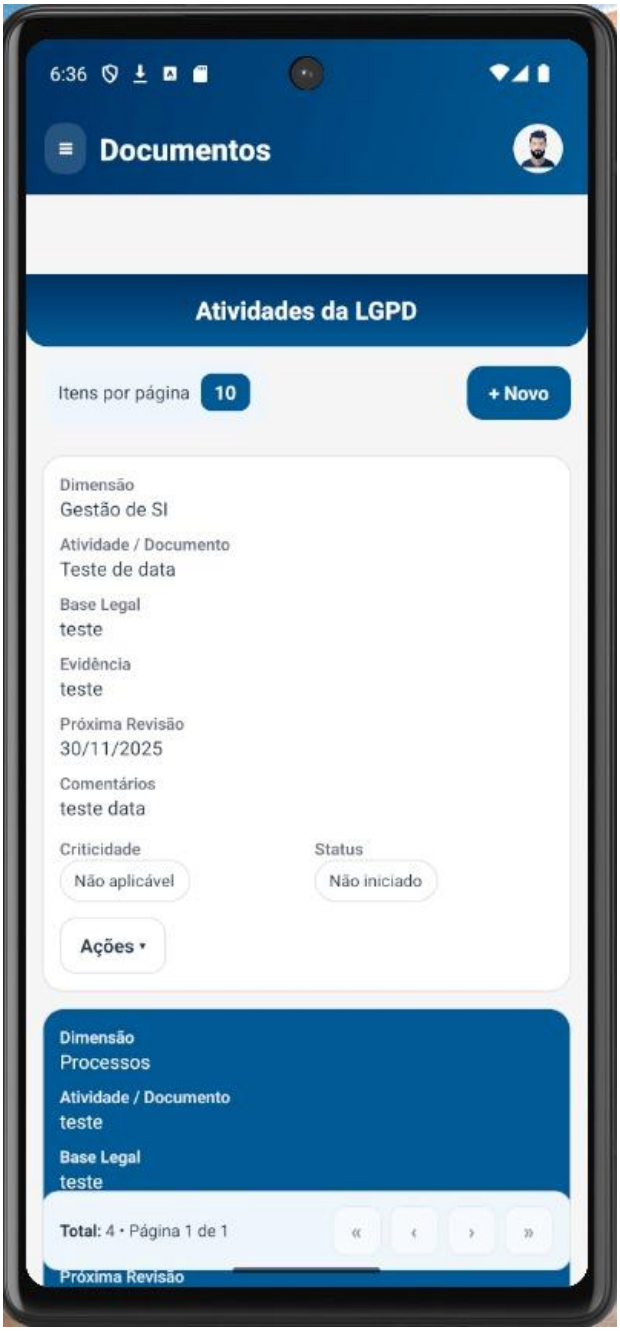
Fonte: Elaboração Própria

Tela Atividades da LGPD Mobile:

A tela de Atividades da LGPD na versão mobile apresenta a lista de atividades registradas, exibindo informações como dimensão, base legal, evidências, próxima

revisão, comentários, criticidade e status. Conforme Figura 49, todos os usuários podem adicionar novas atividades, bem como acessar as ações disponíveis para editar ou excluir registros, garantindo a atualização contínua das informações diretamente pelo aplicativo.

Figura 147: Página Atividades Mobile



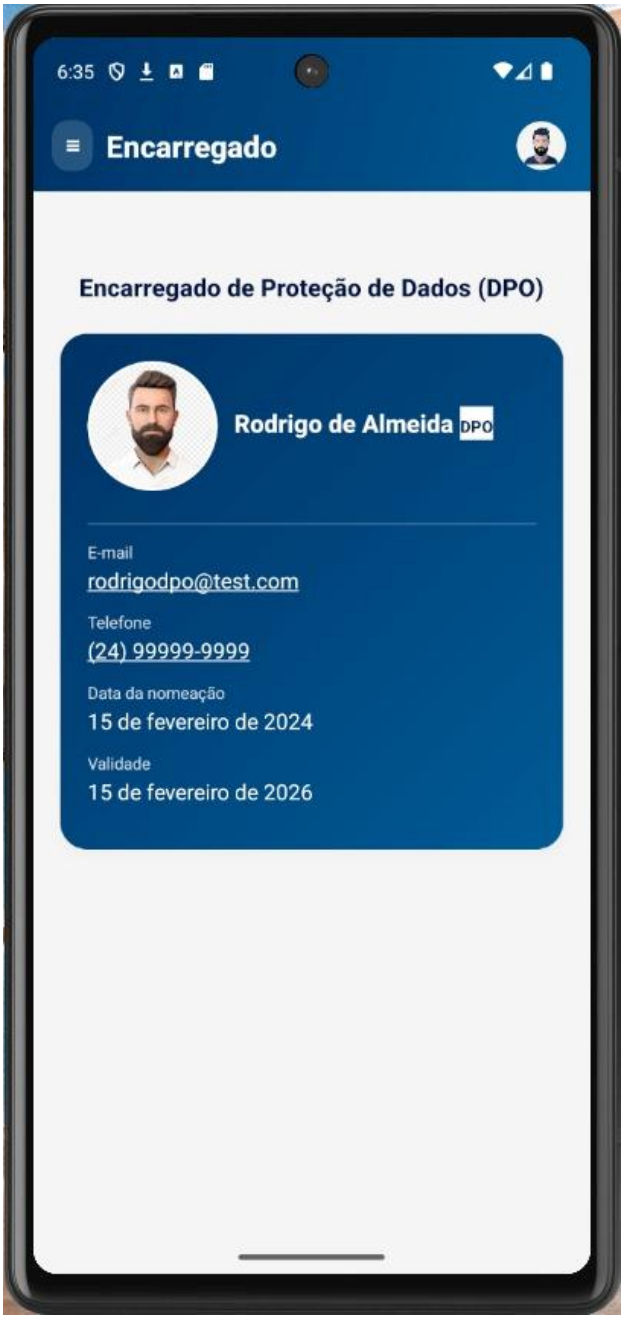
Fonte: Elaboração Própria

Tela Encarregado de Dados (DPO) Mobile:

A tela de Encarregado de Proteção de Dados (DPO) na versão mobile apresenta as informações de contato e nomeação do responsável pelo tratamento de

dados pessoais na organização. Conforme Figura 50, são exibidos dados como nome, e-mail, telefone, data de nomeação e validade do mandato, permitindo rápida consulta às informações oficiais do DPO pelo aplicativo.

Figura 148: Página Encarregado de Dados (DPO) Mobile



Considerações Finais:

Este manual consolidou as principais instruções de uso do Sistema Camaleão, cobrindo a versão web e mobile e apresentando cada recurso disponível ao usuário.

Ao seguir as orientações aqui descritas, a utilização da plataforma torna-se mais intuitiva, contribuindo para a organização, o controle e a conformidade das atividades relacionadas à proteção de dados pessoais.

O Sistema Camaleão foi desenvolvido para oferecer praticidade, segurança e eficiência, e este manual cumpre o papel de apoiar usuários em sua jornada de utilização da ferramenta.