



UNIVERSIDADE
Estácio de Sá
CAMPUS NITERÓI

PROJETO FINAL II

“Framework de Segurança”

Professor Orientador: Carlos Alberto Alves Lemos, DSc
Aluno: Phelipe Perboires de Souza

*Niterói
Junho/2010*

SUMÁRIO

1. PROPOSTA DE TRABALHO	9
1.1. INTRODUÇÃO.....	9
1.2. MÉTODO DE TRABALHO	9
1.3. PREVISÃO DE ALOCAÇÃO DE RECURSOS	10
1.4. CRONOGRAMA DO TRABALHO	12
1.5. ORÇAMENTO DO TRABALHO.....	13
2. EXPLORAÇÃO DO SISTEMA PROPOSTO.....	17
2.1. AVALIAÇÃO DE SOLUÇÕES.....	17
2.2. REPRESENTAÇÃO FUNCIONAL.....	22
2.2.1. CARACTERÍSTICAS GERAIS.....	22
2.2.2. MODELO FUNCIONAL	28
2.2.2.1. DIAGRAMAS DE CASOS DE USO	28
2.2.2.1.1. CASOS DE USO DO USUÁRIO.....	28
2.2.2.1.1.1. AUTENTICAÇÃO.....	28
2.2.2.1.1.2. ALTERAÇÃO DE SENHA	28
2.2.2.1.2. CASOS DE USO DO ADMINISTRADOR DE SEGURANÇA.....	29
2.2.2.1.2.1. GERENCIAMENTO DE SISTEMA.....	29
2.2.2.1.2.2. GERENCIAMENTO DE TIPO DE RECURSO.....	29
2.2.2.1.2.3. GERENCIAMENTO DE PAPEL ADMINISTRATIVO	30
2.2.2.1.2.4. GERENCIAMENTO DE USUÁRIO	30
2.2.2.1.2.5. ATRIBUIÇÃO DE PAPEL DE ADMINISTRADOR DE SEGURANÇA.....	31
2.2.2.1.2.6. GERENCIAMENTO DE INATIVAÇÃO DE USUÁRIOS.....	31
2.2.2.1.3. CASOS DE USO DO ADMINISTRADOR DE SISTEMA.....	32
2.2.2.1.3.1. GERENCIAMENTO DE RECURSO.....	32
2.2.2.1.3.2. GERENCIAMENTO DE OPERAÇÃO	32
2.2.2.1.3.3. GERENCIAMENTO DE PERMISSÃO	33
2.2.2.1.3.4. GERENCIAMENTO DE PAPEL COMUM	33
2.2.2.1.3.5. GERENCIAMENTO DE GRUPO MANUAL.....	34
2.2.2.1.3.6. GERENCIAMENTO DE GRUPO CARACTERIZADO	34
2.2.2.1.3.7. GERENCIAMENTO DE CARACTERÍSTICA	35
2.2.2.1.3.8. GERENCIAMENTO DE VALOR DA CARACTERÍSTICA	35
2.2.2.1.3.9. GERENCIAMENTO DE CONTEXTO	36
2.2.2.1.3.10. GERENCIAMENTO DE VALOR DE CONTEXTO	36
2.2.2.1.3.11. GERENCIAMENTO DE PERMISSÕES CONFLITANTES.....	37
2.2.2.1.3.12. GERENCIAMENTO DE CARACTERÍSTICAS DE GRUPO CARACTERIZADO	37
2.2.2.1.3.13. GERENCIAMENTO DE CARACTERÍSTICAS DE USUÁRIO	38
2.2.2.1.3.14. GERENCIAMENTO DE MEMBROS DE GRUPOS MANUAIS	38
2.2.2.1.3.15. GERENCIAMENTO DE INATIVAÇÃO DE GRUPOS MANUAIS	39
2.2.2.1.3.16. GERENCIAMENTO DE INATIVAÇÃO DE GRUPOS CARACTERIZADOS.....	39
2.2.2.1.3.17. CONCESSÃO DE PERMISSÃO PARA PAPEL COMUM	40
2.2.2.1.3.18. ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO	40
2.2.2.1.3.19. ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA USUÁRIO.....	41
2.2.2.1.3.20. ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO MANUAL.....	41
2.2.2.1.3.21. ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA GRUPO MANUAL	42
2.2.2.1.3.22. CONTEXTUALIZAÇÃO DE ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO	42
2.2.2.1.3.23. CONTEXTUALIZAÇÃO DE PERMISSÃO	43
2.2.2.1.3.24. CONTEXTUALIZAÇÃO DE ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO MANUAL.....	43
2.2.2.1.3.25. CONTEXTUALIZAÇÃO DE ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO CARACTERIZADO..	44
2.2.2.1.4. CASOS DE USO DE SISTEMA CLIENTE	45
2.2.2.1.4.1. VERIFICAÇÃO DE AUTORIZAÇÃO DE USUÁRIO EM PERMISSÃO	45
2.2.2.1.4.2. VERIFICAÇÃO DE AUTORIZAÇÃO DE USUÁRIO EM PERMISSÃO CONTEXTUALIZADA	46
2.2.2.1.4.3. CONEXÃO DE SISTEMA CLIENTE.....	47

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

2.2.2.2.	DESCRICAÇÃO DOS CASOS DE USO	48
2.2.3.	DESCRICAÇÃO DOS ATORES	185
2.2.4.	DESCRICAÇÃO DOS ATRIBUTOS DAS CLASSES	186
2.2.5.	PROJETO DE INTERFACES	191
2.2.6.	DIAGRAMAS DE ESTADO	208
2.2.6.1.	USUÁRIO	208
2.2.6.2.	SISTEMA	208
2.2.6.3.	PAPEL	208
2.2.6.4.	GRUPO	209
2.2.6.5.	PERMISSÃO	209
2.2.6.6.	RECURSO	209
2.2.7.	DIAGRAMA DE CLASSES DO MODELO	210
2.2.8.	DIAGRAMAS DE SEQUÊNCIA	211
2.2.8.1.	CONECTAR SISTEMA CLIENTE AO SERVIÇO DE SEGURANÇA	211
2.2.8.2.	DESCONECTAR SISTEMA CLIENTE DO SERVIÇO DE SEGURANÇA	212
2.2.8.3.	REALIZAR LOGON DO USUÁRIO	213
2.2.8.4.	REALIZAR LOGOFF DE USUÁRIO	214
2.2.8.5.	SOLICITAR NOVA SENHA POR E-MAIL	215
2.2.8.6.	ALTERAR SENHA	216
2.2.8.7.	INCLUIR RECURSO	217
2.2.8.8.	ALTERAR RECURSO	218
2.2.8.9.	EXCLUIR RECURSO	219
2.2.8.10.	CONSULTAR RECURSO	220
2.2.8.11.	INCLUIR OPERAÇÃO	221
2.2.8.12.	ALTERAR OPERAÇÃO	222
2.2.8.13.	EXCLUIR OPERAÇÃO	223
2.2.8.14.	CONSULTAR OPERAÇÃO	224
2.2.8.15.	INCLUIR PERMISSÃO	225
2.2.8.16.	ALTERAR PERMISSÃO	226
2.2.8.17.	EXCLUIR PERMISSÃO	227
2.2.8.18.	CONSULTAR PERMISSÃO	228
2.2.8.19.	INCLUIR PAPEL COMUM	229
2.2.8.20.	ALTERAR PAPEL COMUM	230
2.2.8.21.	EXCLUIR PAPEL COMUM	231
2.2.8.22.	CONSULTAR PAPEL COMUM	232
2.2.8.23.	INCLUIR PAPEL ADMINISTRATIVO	233
2.2.8.24.	ALTERAR PAPEL ADMINISTRATIVO	234
2.2.8.25.	EXCLUIR PAPEL ADMINISTRATIVO	235
2.2.8.26.	CONSULTAR PAPEL ADMINISTRATIVO	236
2.2.8.27.	INCLUIR USUÁRIO	237
2.2.8.28.	ALTERAR USUÁRIO	238
2.2.8.29.	EXCLUIR USUÁRIO	239
2.2.8.30.	CONSULTAR USUÁRIO	240
2.2.8.31.	INCLUIR SISTEMA	241
2.2.8.32.	ALTERAR SISTEMA	242
2.2.8.33.	EXCLUIR SISTEMA	243
2.2.8.34.	CONSULTAR SISTEMA	244
2.2.9.	DIAGRAMAS DE ATIVIDADE	245
2.2.9.1.	CONECTAR SISTEMA CLIENTE AO SERVIÇO DE SEGURANÇA	245
2.2.9.2.	DESCONECTAR SISTEMA CLIENTE DO SERVIÇO DE SEGURANÇA	246
2.2.9.3.	REALIZAR LOGON DO USUÁRIO	247
2.2.9.4.	SOLICITAR NOVA SENHA POR E-MAIL	249
2.2.9.5.	ALTERAR SENHA	250
2.2.9.6.	INCLUIR SISTEMA	251
2.2.9.7.	ALTERAR SISTEMA	252
2.2.9.8.	EXCLUIR SISTEMA	253

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

2.2.9.9.	CONSULTAR SISTEMA	254
2.2.9.10.	INCLUIR USUÁRIO.....	255
2.2.9.11.	ALTERAR USUÁRIO.....	256
2.2.9.12.	EXCLUIR USUÁRIO.....	257
2.2.9.13.	CONSULTAR USUÁRIO	258
2.2.9.14.	INCLUIR TIPO DE RECURSO...	259
2.2.9.15.	ALTERAR TIPO DE RECURSO	260
2.2.9.16.	EXCLUIR TIPO DE RECURSO	261
2.2.9.17.	CONSULTAR TIPO DE RECURSO	262
2.2.9.18.	INCLUIR PAPEL COMUM	263
2.2.9.19.	ALTERAR PAPEL COMUM	264
2.2.9.20.	EXCLUIR PAPEL COMUM	265
2.2.9.21.	CONSULTAR PAPEL COMUM.....	266
2.2.9.22.	INCLUIR OPERAÇÃO.....	267
2.2.9.23.	ALTERAR OPERAÇÃO.....	268
2.2.9.24.	EXCLUIR OPERAÇÃO.....	269
2.2.9.25.	CONSULTAR OPERAÇÃO	270
2.2.9.26.	INCLUIR PERMISSÃO	271
2.2.9.27.	ALTERAR PERMISSÃO	272
2.2.9.28.	EXCLUIR PERMISSÃO	273
2.2.9.29.	CONSULTAR PERMISSÃO.....	274
2.2.10.	PROJETO DE TABELAS/ARQUIVOS.....	275
2.2.11.	DIAGRAMA DE MODELO DE DADOS FÍSICO	312
2.2.12.	DIAGRAMA DE MODELO DE DADOS LÓGICO	313
2.2.13.	CONTROLES.....	314
2.2.13.1.	CONTROLE DE ACESSO	314
	ADMINISTRADOR DE SEGURANÇA	314
	ADMINISTRADOR DE SISTEMA	315
2.2.14.	PLANO DE CONTINGÊNCIA.....	317
3.	PLANO DE IMPLEMENTAÇÃO.....	318
3.1.	ESTRATÉGIA DE TRABALHO	318
3.1.1.	DESENVOLVIMENTO.....	318
3.1.2.	VERSIONAMENTO DOS ARTEFATOS	319
3.1.3.	TESTES	319
3.1.4.	CARGA INICIAL	319
3.1.5.	TREINAMENTO	320
3.1.6.	IMPLANTAÇÃO	320
3.2.	RECURSOS ESTIMADOS	321
3.2.1.	FASE DE DESENVOLVIMENTO	321
3.2.2.	FASE DE TESTES	322
3.2.3.	FASE DE TREINAMENTO.....	323
3.2.4.	FASE DE HOMOLOGAÇÃO	324
3.2.5.	FASE DE IMPLANTAÇÃO	324
3.3.	CRONOGRAMA	325
3.4.	ORÇAMENTO	326
3.5.	PLANO DE TESTES.....	330
4.	CONCLUSÃO	341
5.	TRABALHOS FUTUROS	343
6.	GLOSSÁRIO	344
7.	BIBLIOGRAFIA	345

**UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO**

8. ANEXO I – MANUAL DO USUÁRIO 346

TABELAS

Tabela 1: Previsão de alocação de recursos humanos	10
Tabela 2: Previsão de recursos de hardware.....	10
Tabela 3: Previsão de recursos de software	10
Tabela 4: Previsão de materiais de escritório	11
Tabela 5: Cronograma do trabalho	12
Tabela 6: Depreciação dos recursos materiais por mês.....	13
Tabela 7: Utilização dos recursos humanos ao longo da primeira fase do projeto	15
Tabela 8: Utilização dos recursos humanos ao longo da segunda fase do projeto	15
Tabela 9: Despesas com recursos humanos durante a segunda fase do projeto	15
Tabela 10: Despesas com recursos materiais durante a segunda fase do projeto	16
Tabela 11: Cálculo do orçamento final para a segunda fase	16
Tabela 12: Previsão de alocação de recursos humanos na fase de desenvolvimento.....	321
Tabela 13: Previsão de recursos de hardware na fase de desenvolvimento.....	321
Tabela 14: Previsão de recursos de software na fase de desenvolvimento	321
Tabela 15: Previsão de alocação de recursos humanos na fase de testes.....	322
Tabela 16: Previsão de recursos de hardware na fase de testes	322
Tabela 17: Previsão de recursos de software na fase de testes.....	322
Tabela 18: Previsão de alocação de recursos humanos na fase de desenvolvimento.....	323
Tabela 19: Previsão de recursos de hardware na fase de desenvolvimento.....	323
Tabela 20: Previsão de recursos de software na fase de desenvolvimento	323
Tabela 21: Previsão de materiais de escritório na fase de desenvolvimento	323
Tabela 22: Previsão de alocação de recursos humanos na fase de homologação	324
Tabela 23: Previsão de recursos de hardware na fase de homologação	324
Tabela 24: Previsão de alocação de recursos humanos na fase de homologação	324
Tabela 25: Previsão de recursos de hardware na fase de homologação	324
Tabela 26: Cronograma do plano de implementação.....	325
Tabela 27: Depreciação dos recursos materiais por mês.....	326
Tabela 28: Utilização dos recursos humanos ao longo da fase de implementação	328
Tabela 29: Valor por hora dos recursos humanos no projeto	328
Tabela 30: Despesas com recursos humanos durante a fase de implementação	328
Tabela 31: Despesas com recursos materiais durante a fase de implementação	329
Tabela 32: Cálculo do orçamento final para a fase de implementação	329

FIGURAS

Figura 1: Esquema físico do Framework de Segurança.....	23
Figura 2: Casos de uso de autenticação.....	28
Figura 3: Caso de uso de alteração de senha	28
Figura 4: Casos de uso de gerenciamento de sistema.....	29
Figura 5: Casos de uso de gerenciamento de tipo de recurso.....	29
Figura 6: Casos de uso de gerenciamento de papel administrativo.....	30
Figura 7: Casos de uso de gerenciamento de usuário	30
Figura 8: Casos de uso de atribuição de papel de administrador de segurança	31
Figura 9: Casos de uso de gerenciamento de inativação de usuários	31
Figura 10: Casos de uso de gerenciamento de recurso	32
Figura 11: Casos de uso de gerenciamento de operação	32
Figura 12: Casos de uso de gerenciamento de permissão.....	33
Figura 13: Casos de uso de gerenciamento de papel comum.....	33
Figura 14: Casos de uso de gerenciamento de grupo manual	34
Figura 15: Casos de uso de gerenciamento de grupo caracterizado	34
Figura 16: Casos de uso de gerenciamento de característica	35
Figura 17: Casos de uso de gerenciamento de valor da característica.....	35
Figura 18: Casos de uso de gerenciamento de contexto	36
Figura 19: Casos de uso de gerenciamento de valor de contexto	36
Figura 20: Casos de uso de gerenciamento de permissões conflitantes	37
Figura 21: Casos de uso de gerenciamento de característica de grupos caracterizados	37
Figura 22: Casos de uso de gerenciamento de características de usuário	38
Figura 23: Casos de uso de gerenciamento de membros de grupos manuais.....	38
Figura 24: Casos de uso de gerenciamento de inativação de grupos manuais	39
Figura 25: Casos de uso de gerenciamento de inativação de grupos caracterizados	39
Figura 26: Casos de uso de concessão de permissão para papel comum	40
Figura 27: Casos de uso de atribuição de papel comum para usuário	40
Figura 28: Casos de uso de atribuição de papel administrativo para usuário	41
Figura 29: Casos de uso de atribuição de papel comum para grupo manual.....	41
Figura 30: Casos de uso de atribuição de papel administrativo para grupo manual.....	42
Figura 31: Casos de uso de contextualização de atribuição de papel comum para usuário	42
Figura 32: Casos de uso de contextualização de permissão.....	43
Figura 33: Casos de uso de contextualização de atribuição de papel comum para grupo manual ..	43
Figura 34: Casos de uso de contextualização de atribuição de papel comum para grupo caracterizado	44
Figura 35: Caso de uso de verificação de autorização de usuário em permissão.....	45
Figura 36: Caso de uso de verificação de autorização de usuário em permissão contextualizada.	46
Figura 37: Casos de uso de conexão de sistema cliente	47
Figura 38: Diagrama de Classes do Modelo	210
Figura 39: Diagrama de sequência conectar sistema cliente ao serviço de segurança.....	211
Figura 40: Diagrama de sequência desconectar sistema cliente do serviço de segurança	212
Figura 41: Diagrama de sequência realizar logon do usuário.....	213
Figura 42: Diagrama de sequência realizar logoff do usuário.....	214
Figura 43: Diagrama de sequência solicitar nova senha por e-mail.....	215
Figura 44: Diagrama de sequência alterar senha	216
Figura 45: Diagrama de sequência incluir recurso	217
Figura 46: Diagrama de sequência alterar recurso	218
Figura 47: Diagrama de sequência excluir recurso	219
Figura 48: Diagrama de sequência consultar recurso	220
Figura 49: Diagrama de sequência incluir operação	221
Figura 50: Diagrama de sequência alterar operação	222
Figura 51: Diagrama de sequência excluir operação	223
Figura 52: Diagrama de sequência consultar operação	224
Figura 53: Diagrama de sequência incluir permissão.....	225

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Figura 54: Diagrama de sequência alterar permissão	227
Figura 55: Diagrama de sequência excluir permissão.....	227
Figura 56: Diagrama de sequência consultar permissão.....	228
Figura 57: Diagrama de sequência papel comum.....	229
Figura 58: Diagrama de sequência alterar papel comum	230
Figura 59: Diagrama de sequência excluir papel comum.....	231
Figura 60: Diagrama de sequência consultar papel comum.....	232
Figura 61: Diagrama de sequência incluir papel administrativo.....	233
Figura 62: Diagrama de sequência alterar papel administrativo	234
Figura 63: Diagrama de sequência excluir papel administrativo.....	235
Figura 64: Diagrama de sequência consultar papel administrativo.....	236
Figura 65: Diagrama de sequência incluir usuário	237
Figura 66: Diagrama de sequência alterar usuário.....	238
Figura 67: Diagrama de sequência excluir usuário	239
Figura 68: Diagrama de sequência consultar usuário	240
Figura 69: Diagrama de sequência incluir sistema.....	241
Figura 70: Diagrama de sequência alterar sistema	242
Figura 71: Diagrama de sequência excluir sistema.....	243
Figura 72: Diagrama de sequência consultar sistema.....	244
Figura 73: Diagrama de modelo de dados físico.....	312
Figura 74: Diagrama de modelo de dados lógico	313
Figura 75 - Exemplo de relatório de testes gerado pelo Selenium.....	330
Figura 76 - Exemplo de relatório de testes de cobertura gerado pelo Cobertura	331
Figura 77 - Exemplo de relatório de testes unitários e de integração gerado pelo JUnit	332
Figura 78 - Exemplo de relatório de testes de stress gerado pelo JMeter	333

FÓRMULAS

Fórmula 1: Cálculo do salário	13
Fórmula 2: Cálculo do salário.....	326

1. PROPOSTA DE TRABALHO

1.1. INTRODUÇÃO

Dando continuidade ao trabalho realizado, a segunda parte deste projeto visa realizar a implementação do Framework de Segurança, como uma solução proposta mediante o estudo das informações levantadas na sua primeira fase, visando suprir as necessidades apresentadas pela organização.

1.2. MÉTODO DE TRABALHO

Para a execução do projeto proposto, serão realizadas reuniões com funcionários de diversas áreas da companhia: segurança da informação, auditoria interna, arquitetura de sistemas, infraestrutura, desenvolvimento e com usuários finais do sistema, a exemplo da primeira fase, buscando sempre validar as abstrações realizadas para a implementação do novo sistema. As informações obtidas durante a primeira fase serão cuidadosamente avaliadas, fornecendo subsídios para a criação de soluções de software que atendam as necessidades da companhia.

Todas as propostas de soluções serão apresentadas aos consultores e usuários finais do sistema nessas reuniões, possibilitando a eles opinar a respeito e acrescentar informações, eventualmente corrigindo possíveis erros de interpretação. Ao fim de cada reunião, será confeccionada uma especificação funcional (documento que detalha o escopo e necessidades do produto a ser desenvolvido) com diagramas e especificações de casos de uso, sendo fonte para consulta e direcionamento para o desenvolvimento do sistema, e servindo para constatação de todos os envolvidos no projeto sobre os itens acordados para o produto nas reuniões.

Como ferramenta de apoio a análise e desenvolvimento, além de referência para confecção de diagramas, serão utilizadas as técnicas de construção de modelos UML (Unified Modeling Language), por permitirem a interação com os problemas apresentados e, consequentemente, seu inteiro conhecimento devido ao grau de abstração que os modelos apresentam, representando de forma simplificada uma situação real.

1.3. PREVISÃO DE ALOCAÇÃO DE RECURSOS

A proposta para desenvolvimento do sistema nesta segunda fase conta com os seguintes recursos humanos e materiais:

- Recursos humanos

Quantidade	Recurso
1	Patrocinador do produto
1	Consultor do setor de segurança da informação da companhia
1	Consultor do setor de auditoria da empresa
1	Gerente de projeto
1	Consultor do setor de infraestrutura de TI da companhia
1	Consultor do setor de arquitetura de sistemas da companhia
1	Analista de sistemas
1	Desenvolvedor

Tabela 1: Previsão de alocação de recursos humanos

- Recursos materiais

Hardware	
Quantidade	Recurso
1	Notebook MacBook Intel Core 2 Dual, 2GHz, 2GB de memória.
1	Impressora colorida jato de tinta EPSON TX210

Tabela 2: Previsão de recursos de hardware

Software	
Quantidade	Recurso
1	Microsoft Windows XP Professional
1	Microsoft Visio 2007 Professional
1	Microsoft Project 2007 Professional
1	Microsoft Office 2007 Professional
1	Jude Community 5.2.2
1	Eclipse IDE
1	PostgreSQL 8.4
1	pgAdmin III
1	JBoss Application Server
1	Hudson Continuous Integration Server
1	Spring Roo
1	TortoiseSVN
1	Navegador Mozilla Firefox 3.6

Tabela 3: Previsão de recursos de software

Material de Escritório	
Quantidade	Recurso
1500	Folha de papel A4
50	Folha de papel A3
6	Cartucho de tinta para impressora
2	Caneta preta
2	Caneta azul
3	Lápis
1	Apontador de lápis
2	Borracha
1	Grampeador
1	Caixa de grampos

Tabela 4: Previsão de materiais de escritório

1.4. CRONOGRAMA DO TRABALHO

Esta segunda fase do projeto terá inicio em 01 de fevereiro de 2010, segunda-feira e tem prazo estimado para término em 05 de junho de 2010, sábado.

Serão consideradas 2 (duas) horas por dia dedicadas ao trabalho no mesmo conforme cronograma apresentado a seguir:

#	Nome da tarefa	Duração (dias)	Início	Término
1	Proposta de trabalho	10	01/02/2010	10/02/2010
1.1	Elaborar proposta de trabalho	3	01/02/2010	03/02/2010
1.2	Fazer previsão de alocação de recursos	1	04/02/2010	04/02/2010
1.3	Elaborar cronograma do trabalho	2	05/02/2010	06/02/2010
1.4	Fazer orçamento do trabalho	4	07/02/2010	10/02/2010
2	Exploração do sistema proposto	56	11/02/2010	07/05/2010
2.1	Avaliação das soluções	4	11/02/2010	14/02/2010
2.2	Representação funcional	38	15/02/2010	24/04/2010
2.2.1	Caracterizações gerais	1	15/02/2010	15/02/2010
2.2.2	Modelo funcional	5	16/02/2010	20/02/2010
2.2.3	Modelo de dados	3	21/02/2010	23/02/2010
2.2.4	Diagrama de estado	4	24/02/2010	27/02/2010
2.2.5	Descrição dos atores	3	28/03/2010	02/04/2010
2.2.6	Descrição dos atributos de classe	4	03/04/2010	06/04/2010
2.2.7	Projeto de interface	6	07/04/2010	12/04/2010
2.2.8	Especificações de caso de uso	4	13/04/2010	16/04/2010
2.2.9	Diagrama de sequencia	5	17/04/2010	21/04/2010
2.2.10	Diagrama de atividade	3	22/04/2010	24/04/2010
2.3	Representação Física	14	25/04/2010	07/05/2010
2.3.1	Classe de projeto	4	25/04/2010	28/04/2010
2.3.2	Projeto de tabelas e arquivos	4	29/04/2010	01/05/2010
2.3.3	Controles	3	02/05/2010	04/05/2010
2.3.4	Plano de contingência	3	05/05/2010	07/05/2010
3	Plano de Implementação	17	08/05/2010	28/05/2010
3.1	Estratégia de trabalho	8	08/05/2010	15/05/2010
3.2	Cronograma	3	16/05/2010	18/05/2010
3.3	Recursos estimados	3	19/05/2010	21/05/2010
3.4	Orçamento	3	27/05/2010	28/05/2010
4	Conclusão	5	28/05/2010	30/05/2010
5	Manual do Usuário	5	30/05/2010	02/06/2010
6	Glossário	2	02/06/2010	03/06/2010
7	Bibliografia	1	03/06/2010	05/06/2010

Tabela 5: Cronograma do trabalho

1.5. ORÇAMENTO DO TRABALHO

Todos os valores a seguir serão expressos em reais (R\$).

- Cálculo de salário

Para o cálculo de salário dos integrantes do projeto por hora será utilizada a fórmula a seguir:

$$(\text{SBM} / \text{CHM}) \text{ EM}$$

Fórmula 1: Cálculo do salário

Onde:

- **SBM** corresponde ao salário bruto mensal.
- **CHM** corresponde à carga horária mensal. Será definido o valor 240 para esta variável.
- **EM** corresponde ao valor dos encargos mensais. Será definido o valor 2,54 para esta variável.

Os valores levam em consideração os custos indiretos do salário, tais como FGTS, impostos, férias etc.

- Cálculo de depreciação

Bens e equipamentos depreciam por lei em 5 anos, Com a base de cálculo sendo de 20% por ano. Para isto, foi elaborada a seguinte tabela para calcular a depreciação de cada equipamento em cada mês:

Recurso material	Valor	Depreciação por mês
Notebook	3.000,00	50,00
Impressora colorida	300,00	5,00
MS Windows XP Professional	550,00	9,17
MS Project 2007 Professional	1.700,00	28,34
MS Office 2007 Professional	1.500,00	25,00

Tabela 6: Depreciação dos recursos materiais por mês

- Cálculo de despesas diversas

Calcula-se que as despesas diversas de um projeto giram em torno de 10% (dez por cento) do total de todas as despesas. O cálculo é feito somando todas as demais despesas e dividindo o total desta soma por 9 (nove).

- Cálculo do custo do dinheiro

Sobre um bem ou equipamento quando de sua aquisição, é gerado de imediato, uma despesa referindo-se ao dinheiro. Quando aplicado este dinheiro no mercado financeiro é estimado que renda cerca de 1% ao mês.

- Cálculo do orçamento final

Representa todo o somatório de investimentos e despesas

- Totalização dos cursos

Custo total do projeto, somatório de todos os meses.

- Consolidação dos cálculos.

Abaixo serão apresentadas diversas tabelas que foram usadas para calcular o custo do projeto.

Recurso humano	Fevereiro	Março	Abril	Maio	Junho
Patrocinador do produto	10h	10h	10h	10h	20h
Consultor de segurança	10h	-	-	10h	20h
Consultor de auditoria	10h	-	-	10h	20h
Analista de sistemas	30h	30h	30h	30h	30h
Gerente de projeto	10h	10h	10h	10h	20h
Consultor de infraestrutura	10h	10h	10h	10	10h
Consultor de arquitetura	10h	10h	10h	10h	10h
Desenvolvedor	80h	80h	140h	140h	140h

Tabela 7: Utilização dos recursos humanos ao longo da primeira fase do projeto

A tabela a seguir representa os valores e o cálculo usado para obtenção do valor por hora de cada recurso humano que participará do projeto. O cálculo do valor por hora utiliza a fórmula explicada no item “Cálculo do salário”.

Recurso humano	Salário Bruto Mensal	Valor por hora no projeto
Patrocinador do produto	12.000,00	127,00
Consultor de segurança	8.000,00	84,67
Consultor de auditoria	8.000,00	84,67
Analista de sistemas	6.000,00	63,50
Gerente de projetos	9.000,00	95,25
Consultor de infraestrutura	8.000,00	84,67
Consultor de arquitetura	8.000,00	84,67
Desenvolvedor	5.000,00	52,91

Tabela 8: Utilização dos recursos humanos ao longo da segunda fase do projeto

Multiplicando as horas de cada recurso humano em cada mês pelo seu custo por hora no projeto, obteve-se a tabela a seguir:

Recurso humano	Fevereiro	Março	Abril	Maio	Junho
Patrocinador do produto	1270,00	1270,00	1270,00	1270,00	2540,00
Consultor de segurança	846,70	-	-	846,70	1693,40
Consultor de auditoria	846,70	-	-	846,70	1693,40
Analista de sistemas	1905,00	1905,00	1905,00	1905,00	1905,00
Gerente de projeto	952,50	952,50	952,50	952,50	1905,00
Consultor de infraestrutura	846,70	846,70	846,70	846,70	846,70
Consultor de arquitetura	846,70	846,70	846,70	846,70	846,70
Desenvolvedor	4232,80	4232,80	7407,40	7407,40	7407,40
Total	11.747,10	10.053,70	13.228,30	14.921,70	18.837,60

Tabela 9: Despesas com recursos humanos durante a segunda fase do projeto

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Usando os valores obtidos no cálculo da depreciação e levando em consideração que os recursos materiais a seguir já foram obtidos durante a primeira fase, temos os seguintes gastos com recurso material na segunda fase:

Recurso material	Fevereiro	Março	Abril	<th>Junho</th>	Junho
Notebook	50,00	50,00	50,00	50,00	50,00
Impressora colorida	5,00	5,00	5,00	5,00	5,00
MS Windows XP Pro	9,17	9,17	9,17	9,17	9,17
MS Project 2007 Pro	28,34	28,34	28,34	28,34	28,34
MS Office 2007 Pro	25,00	25,00	25,00	25,00	25,00
Total	117,51	117,51	117,51	117,51	117,51

Tabela 10: Despesas com recursos materiais durante a segunda fase do projeto

Despesa	Fevereiro	Março	Abril	Maio	Junho
Despesas recursos humanos	11.747,10	10.053,70	13.228,30	14.921,70	18.837,60
Despesas recursos materiais	117,51	117,51	117,51	117,51	117,51
Despesas diversas	1.318,29	1.318,29	1.318,29	1.318,29	1.318,29
Custo do dinheiro	131,83	248,04	397,16	564,71	773,09
Total	13.314,73	11.737,54	15.061,26	16.922,21	21.046,49
Totalização dos custos: R\$ 78.082,23					

Tabela 11: Cálculo do orçamento final para a segunda fase

2. EXPLORAÇÃO DO SISTEMA PROPOSTO

2.1. AVALIAÇÃO DE SOLUÇÕES

A seguir serão listadas as alternativas de soluções para os problemas levantados a partir do estudo do sistema atual com suas vantagens e desvantagens, além da justificativa da alternativa escolhida. É importante ressaltar que o problema está atrelado à forma como o desenvolvimento do módulo de segurança dos sistemas é feito. E com isto, tanto o problema, quando as possíveis soluções estarão fortemente relacionadas com conceitos tecnológicos.

- Descrição dos problemas

Todo o módulo de segurança dos sistemas desenvolvidos na empresa é criado do zero. Não existe reuso de componentes já criados anteriormente. Na maioria das vezes, a reutilização destes módulos ocorre na forma de “copia-e-cola”, o que afeta a qualidade do software e consequentemente gera problemas durante a fase de manutenção.

Vale ressaltar que este processo arcaico de desenvolvimento de sistemas gera custos que poderiam ser evitados.

Em geral, os sistemas desenvolvidos possuem apenas conceitos de papéis e recursos, e com isto, o modelo baseado em papéis (RBAC) se encaixa bem. Porém, alguns sistemas possuem granularidade de controle de acesso muito pequenas, a ponto de dois usuários com o mesmo papel não poderem realizar as mesmas operações, pois passam a depender de um contexto.

Outro ponto crítico na empresa é que em muitos sistemas, as permissões estão relacionadas ao cargo do funcionário ou ao local de trabalho (lotação), e este último sofre mudanças com muita frequência.

Quando um funcionário é suspeito de fraude ou algo do gênero, é necessário retirar todas as suas permissões em todos os sistemas e algumas vezes é preciso analisar as operações que este usuário realizou nos sistemas, como solicitação ou aprovação de uma compra, por exemplo.

Alguns sistemas possuem a característica de funcionarem em ambiente offshore, dentro de plataformas ou navios, onde a qualidade da conexão com a rede interna é lenta e muitas vezes inviável.

- **Alternativa A**

É proposto o desenvolvimento de um sistema computacional para gestão da segurança dos sistemas desenvolvidos na companhia.

Este sistema será disponibilizado através de um serviço denominado Serviço de Segurança capaz de se integrar com qualquer sistema da companhia, seja ele desenvolvido internamente ou adquirido de terceiros, pois utilizará tecnologia aberta e de fácil desenvolvimento. Além disto, serão desenvolvidas bibliotecas nas principais linguagens utilizadas pela companhia para consumir o serviço de segurança e com isto, deixará a implementação mais transparente para o desenvolvedor.

Para os sistemas que necessitam apenas do modelo baseado em papéis para tratar seus controles de acesso, existirá um módulo básico capaz de atender este requisito.

Para os sistemas que possuam um controle de acesso mais complexo, será fornecido um módulo que permite contextualizar as permissões concedidas para os usuários.

Para tratar o problema das permissões relacionadas aos cargos e lotações, será criada uma funcionalidade que permite caracterizar os usuários do sistema e atrelar estas características a papéis que possuam concessão em permissões do sistema. Dessa forma, quando a característica de um usuário mudar (essa mudança de lotação, cargo ou qualquer outra coisa que venha a ser criada), automaticamente ele perderá ou ganhará acesso a algum recurso do sistema.

Para a questão de fraudes e negação de todos os acessos de um funcionário, será criada uma funcionalidade que possibilite inativá-lo em todos os sistemas da companhia ou em um específico. Para a auditoria, todas as operações realizadas no sistema serão armazenadas e será criado um módulo para consumir tais informações.

Vantagens:

- Escopo mais abrangente, solucionando todos os problemas identificados na primeira análise da empresa;
- Gerenciamento centralizado dos controles de segurança de todos os sistemas;
- Apenas uma interface gráfica para tratar os controles de segurança em todos os sistemas, dessa forma, o usuário final precisa entender o funcionamento apenas de uma ferramenta de segurança;
- Implementação interna do Serviço de Segurança independente dos artefatos (bibliotecas) usados pelos sistemas clientes;
- Fácil evolução.

Desvantagens:

- Custo elevado para desenvolver o sistema;
- Custo elevado para implantação;
- Custo elevado para treinamento;
- Muitos conceitos novos e complexos que alguns sistemas nunca precisarão usar.

• **Alternativa B**

Desenvolvimento de uma biblioteca de funções capaz de realizar as operações básicas de segurança que o modelo baseado em papéis descreve.

A biblioteca de funções acessará um banco de dados local e os desenvolvedores precisarão modelar o banco de dados de acordo com as especificações contidas nesta biblioteca.

Para os sistemas que necessitam apenas do modelo baseado em papéis para tratar seus controles de acesso, existirá um módulo básico capaz de atender este requisito.

Para os sistemas que possuam um controle de acesso mais complexo, será fornecido um módulo que permite contextualizar as permissões concedidas para os usuários.

Vantagens:

- Alta performance, pois a base de dados ficará localmente;
- Sistema continuaria independente;
- Fácil implementação;
- Baixo custo de desenvolvimento da biblioteca de funções.

Desvantagens:

- Desenvolvedor terá um trabalho extra para modelar um banco baseado na especificação, com o risco de modelar de forma inadequada;
- Não existe um local centralizado para controlar a segurança de todos os sistemas;
- Manutenção complicada, pois diferentes versões da biblioteca de funções estarão em uso pelos desenvolvedores;
- Resolve apenas os problemas básicos de segurança previstos pelo modelo baseado em papéis;
- Não resolve completamente os problemas dos sistemas offshore.

- Alternativa C

Modelagem de uma base de dados corporativa com o objetivo de armazenar as informações de segurança que os sistemas necessitam.

Esta base de dados possuirá funções (functions) e procedimentos (procedures) armazenados que serão chamados pelo sistema cliente.

Para os sistemas que necessitam apenas do modelo baseado em papéis para tratar seus controles de acesso, existirá um módulo básico capaz de atender este requisito.

Para os sistemas que possuam um controle de acesso mais complexo, será fornecido um módulo que permite contextualizar as permissões concedidas para os usuários.

Para tratar o problema das permissões relacionadas aos cargos e lotações, será criada uma funcionalidade que permite caracterizar os usuários do sistema e atrelar estas características a papéis que possuam concessão em permissões do sistema. Dessa forma, quando a característica de um usuário mudar (essa mudança de lotação, cargo ou qualquer outra coisa que venha a ser criada), automaticamente ele perderá ou ganhará acesso a algum recurso do sistema.

Para a questão de fraudes e negação de todos os acessos de um funcionário, será criada uma funcionalidade que possibilite inativá-lo em todos os sistemas da companhia ou em um específico. Para a auditoria, todas as operações realizadas no sistema serão armazenadas e será criado um módulo para consumir tais informações.

Vantagens:

- Escopo mais abrangente, solucionando todos os problemas identificados na primeira análise da empresa;
- Alta performance;
- Fácil implementação;
- Baixo custo no desenvolvimento.

Desvantagens:

- Alta dependência com a base de dados;
- Modelo da base de dados não poderá sofrer alterações, pois afetará os sistemas clientes diretamente.

- Alternativa D

Desenvolvimento de sistemas de segurança independente para cada linguagem/plataforma utilizada pela companhia.

Estes sistemas compartilhariam a mesma base de dados.

Vantagens:

- A utilização do sistema de segurança pelos desenvolvedores será transparente, pois toda a solução será na linguagem/plataforma nativa que está sendo utilizada por ele para desenvolver o sistema cliente;
- Permite tirar proveito das melhores características de cada linguagem/plataforma e fazer uma solução mais específica para cada tecnologia.

Desvantagens:

- Alto custo de desenvolvimento;
- Alto custo de manutenção;
- Alta dependência com a base de dados.

- Justificativa da alternativa escolhida

Todas as alternativas são capazes de oferecer melhoria na qualidade, aumento da produtividade dos desenvolvedores, reforço na segurança, diminuição dos prazos, escopo e custos no desenvolvimento dos sistemas. Porém, a alternativa “A” é capaz de atender a maioria das necessidades da empresa e se mostra uma solução mais flexível e extensível.

2.2. REPRESENTAÇÃO FUNCIONAL

2.2.1. CARACTERÍSTICAS GERAIS

O Framework de Segurança possui três módulos lógicos principais: autenticação, autorização e administração. Estes módulos permitem aos sistemas clientes implementar as funcionalidades de segurança mais requisitadas de forma rápida e fácil.

Fisicamente, o Framework de Segurança possui cinco componentes principais que se relacionam entre si. A seguir a descrição de cada item:

1. Lógica de Segurança

Possui as regras de segurança utilizadas pelo framework.

2. Console Administrativo

É a interface gráfica do Framework de Segurança. Nela é possível realizar as operações de administração dos sistemas clientes, como cadastro de papéis, recursos, operações, permissões, usuários, grupos etc. Bem como atribuição de permissões, papéis etc.

3. Serviço de Segurança

É uma interface consumida pelos clientes e por sistemas desenvolvidos em outras tecnologias diferentes de Java e .NET. Esta interface é capaz de disponibilizar serviços de autenticação, autorização e administração.

4. Cliente Java

É uma API orientada a objetos que facilita o uso do Framework de Segurança em sistemas de desenvolvidos na linguagem Java. Esta API consome o Serviço de Segurança.

5. Cliente .NET

Semelhante ao Cliente Java, é uma API orientada a objetos utilizada por sistemas desenvolvidos na linguagem .NET. Esta API também consome o Serviço de Segurança.

A seguir um esquema da estrutura física do Framework de Segurança e seus principais itens:

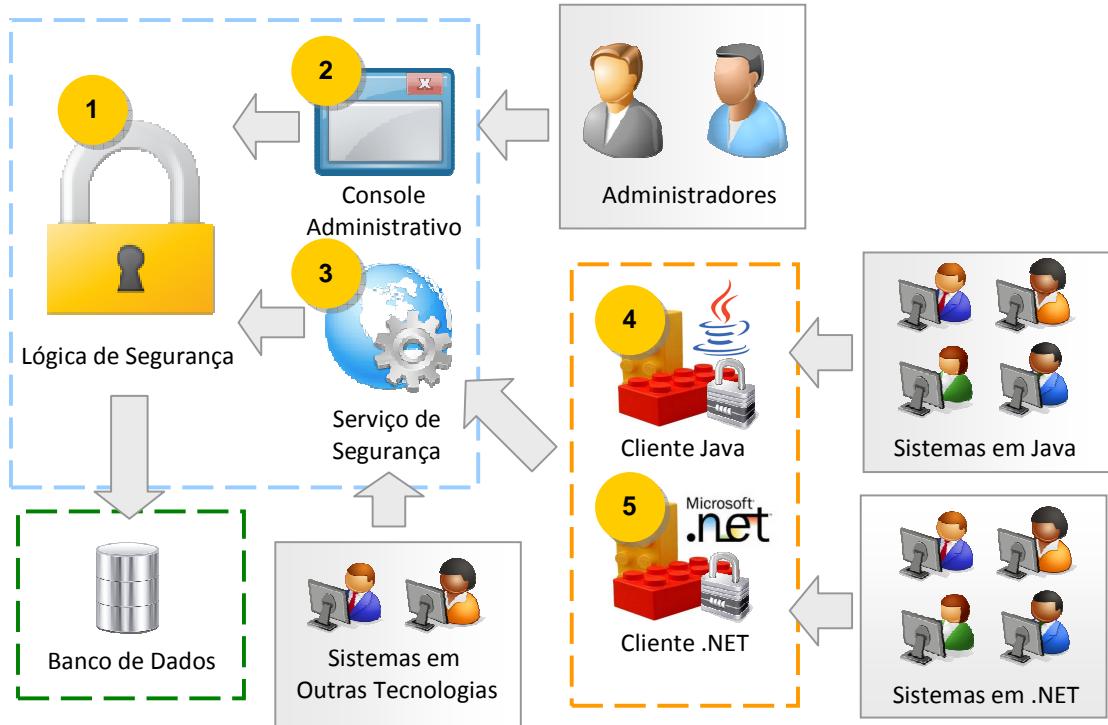


Figura 1: Esquema físico do Framework de Segurança

O sistema funcionará da seguinte forma:

Toda vez que um novo sistema precisar ser desenvolvido na companhia, o analista responsável pelo levantamento dos requisitos deste sistema verificará se o mesmo necessita de algum tipo de segurança, como autenticação, autorização ou auditoria. Caso algum desses requisitos seja necessário, solicitará formalmente, através de um documento interno da empresa, ao administrador de segurança o cadastrado do sistema no Framework de Segurança.

O administrador de segurança entrará no console administrativo através de seu login e senha e realizará o cadastro do sistema informando o código do sistema, nome, descrição, senha e se o mesmo estará habilitado ou não.

Após o cadastro do sistema, prosseguirá com o cadastro de um papel administrativo para este sistema e irá atribuir este papel ao analista que realizou a solicitação e enviará um e-mail ao analista informando a senha que foi informada durante o cadastro do sistema. Após este passo, o analista terá acesso ao console administrativo para gerenciar o sistema em questão.

De posse deste papel, o analista entrará no console administrativo e de acordo com as necessidades de segurança levantadas para o seu sistema, irá modelar as regras de segurança.

O processo de modelagem de segurança consiste no cadastro de diversas entidades no framework. Como papéis, grupos, recursos, operações, permissões, contextos e características. Cada entidade será descrita a seguir:

- **Papel**

Um papel é um conjunto de operações que um usuário pode executar em um sistema. O cadastro de papéis consiste na informação de código de identificação, nome, descrição e se está ativado ou não.

- **Grupo**

Um grupo é definido como um agrupamento de usuários que possuem alguma característica comum. No framework, existem dois tipos de grupos, os manuais e os caracterizados. No caso, os grupos manuais são cadastrados informando o código de identificação, nome, descrição e se está ativado ou não. Além disto, os usuários de grupos manuais devem ser incluídos pelo administrador de sistema.

Já o grupo caracterizado funciona um pouco diferente, o grupo é cadastrado informando todos os mesmos dados de um grupo manual, porém ao invés de incluir usuários, o administrador de sistema irá informar quais as características os usuários devem possuir para fazer parte deste grupo. Essas características podem ser qualquer coisa, desde o cargo que o usuário possui até características físicas, por exemplo. Caso o usuário tenha as características que descrevem o grupo, automaticamente ele é considerado membro do grupo. Caso deixe de possuir determinada característica, o sistema identificará que o mesmo não é mais membro.

A caracterização dos usuários é feita pelo administrador de segurança ou por uma carga ETL que poderá ser configurada.

- **Recurso**

Um recurso é qualquer coisa que precisa ser assegurado no sistema. Podendo ser botões, links, tabelas, telas, campos, formulários, casos de uso ou até conceitos do negócio do sistema como poços, plataformas, navios etc. No framework, um recurso pode ser hierarquizado, dessa forma, é possível modelar a estrutura hierárquica dos objetos de

uma tela, como por exemplo, cadastrar uma tela e informar os botões e campos que fazem parte desta tela.

Para cadastrá-lo no Framework de Segurança, basta informar o código de identificação, nome, descrição, se está ativado ou não e se possuir hierarquia, informar o recurso pai.

- **Operação**

Uma operação é qualquer ação que pode ser realizada em um recurso. Podendo ser operações simples como clicar, visualizar, editar, excluir, incluir ou operações que estão relacionadas com conceitos do negócio do sistema como perfurar (no caso de um recurso poço). No framework, uma operação é cadastrada informando o código de identificação, nome e descrição.

- **Permissão**

Uma permissão é o relacionamento entre o recurso e a operação. Ela define as ações que podem ser realizadas no sistema, como por exemplo, clicar em um botão, visualizar uma tela, perfurar um poço ou parar uma bomba.

Além disto, é preciso informar se a mesma é auditada, ou seja, se ao ser executada, irá gerar um log para posterior auditoria. É preciso também informar se está ou não ativada e se é contextualizada. A contextualização será descrita posteriormente.

É possível também definir quais permissões são conflitantes no sistema. Esta funcionalidade é importante, pois impede que um mesmo usuário tenha permissões em um sistema que são conflitantes, como por exemplo, uma permissão de realizar uma compra e de autorizá-la. Esta funcionalidade impede que fraudes ocorram no sistema.

Para cadastrar um conflito de permissões, basta informar as duas permissões que são conflitantes, o nome do conflito e uma descrição.

- **Contexto**

Um contexto permite especificar uma permissão que um usuário possui. Em muitas situações, não basta saber que um usuário possui um determinado papel para permitir que o mesmo realize algumas ações no sistema. Pois as ações devem ser realizadas em um contexto específico como, por exemplo, a ação de lançar nota (permissão) que um professor (papel) realiza só pode acontecer para as turmas onde o mesmo leciona. Isto é

claro, pois o sistema não poderia permitir que um professor de uma turma modificasse as notas lançadas pelo professor de outra turma. Nesse cenário, a turma é o contexto da permissão. Ou seja, um professor só pode lançar nota nas turmas onde ele lecionada.

O cadastro de contexto é feito informando o código de identificação, nome e descrição. Além do contexto, é preciso cadastrar os valores que esse contexto pode assumir. Este cadastro também é feito informando o código de identificação, nome e descrição.

A contextualização de uma permissão é feita através da associação entre a permissão e um contexto. Isto informará ao framework que determinada permissão só poderá ser usada sob um contexto.

- **Característica**

Uma característica é alguma informação sobre um usuário, como por exemplo, um cargo, função, características físicas, local de trabalho etc.

O cadastro de características é feito através da informação do código de identificação, nome e descrição. Além de cadastrar a característica, é preciso informar os valores que esta característica pode assumir. Este cadastro também é feito informando o código de identificação, nome e descrição.

Após o cadastro destas entidades básicas de segurança do sistema, é preciso definir as concessões e atribuições:

- **Concessão**

A concessão é uma associação entre uma permissão e um papel. Ela define quais permissões um determinado papel possui. Com isto, os usuários que possuem o papel podem executar as permissões que estão associadas o mesmo.

Para cadastrar uma concessão no framework de segurança, basta informar o papel e a permissão que será concedida.

- **Atribuição**

Uma atribuição é a designação de um papel para um usuário ou grupo.

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Para atribuir um papel, basta informar o papel que será atribuído e o usuário ou grupo que receberá o papel. Também é possível informar o início e término da validade da atribuição.

Além destes cadastros, é possível realizar inativações de usuários e grupos. A inativação de usuários é realizada pelo administrador de segurança e a de grupos é realizada pelo administrador de sistema.

Para cadastrar uma inativação, basta informar o usuário ou grupo e o motivo da inativação. Também é possível informar um período de validade da inativação.

Após modelar a segurança do sistema, será preciso configurar o sistema para acessar o serviço de segurança. Esta configuração se faz necessária, pois o sistema precisa questionar ao serviço se uma determinada permissão pode ser autorizada ou não para um usuário. Além desta funcionalidade, o serviço também permite realizar o processo de autenticação (login e logoff) do usuário.

Este acesso pode ocorrer através dos clientes disponíveis nas tecnologias Java e .NET. E para outras tecnologias, o acesso será feito diretamente ao serviço.

2.2.2. MODELO FUNCIONAL

Neste item, encontra-se o modelo funcional do Framework de Segurança, representado através das ferramentas disponibilizadas pela UML (Unified Modeling Language).

2.2.2.1. DIAGRAMAS DE CASOS DE USO

2.2.2.1.1. Casos de uso do usuário

2.2.2.1.1.1. Autenticação

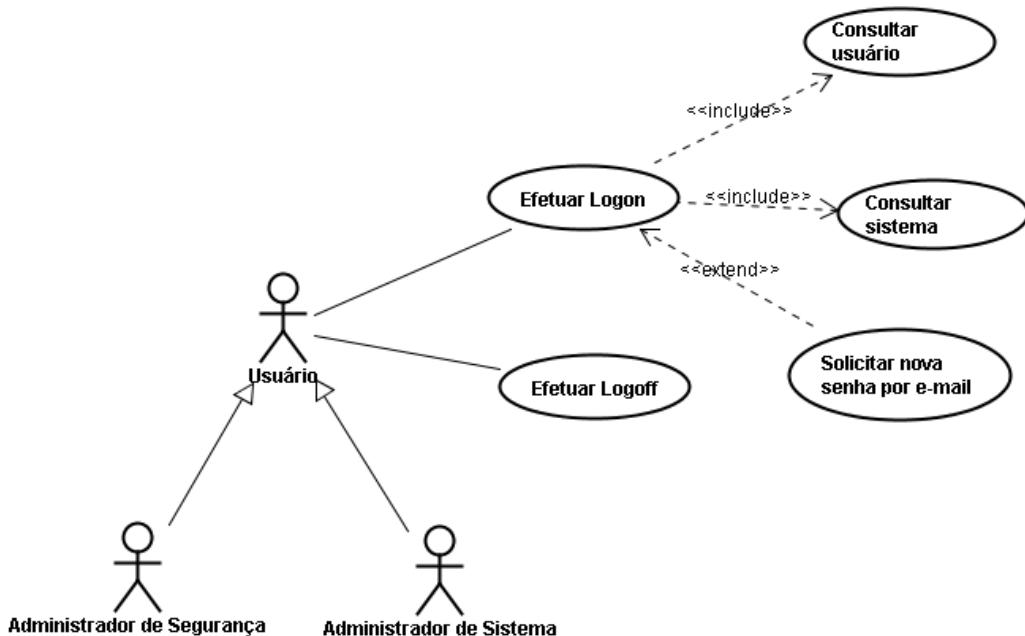


Figura 2: Casos de uso de autenticação

2.2.2.1.1.2. Alteração de Senha

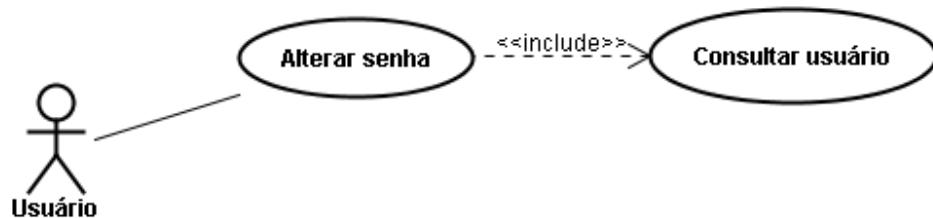


Figura 3: Caso de uso de alteração de senha

2.2.2.1.2. Casos de uso do administrador de segurança

2.2.2.1.2.1. Gerenciamento de sistema

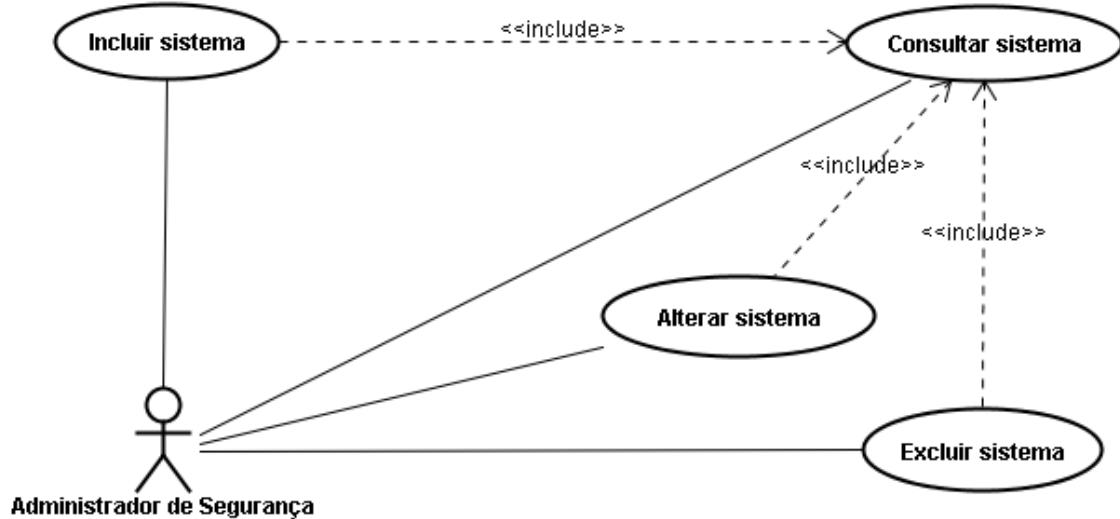


Figura 4: Casos de uso de gerenciamento de sistema

2.2.2.1.2.2. Gerenciamento de tipo de recurso

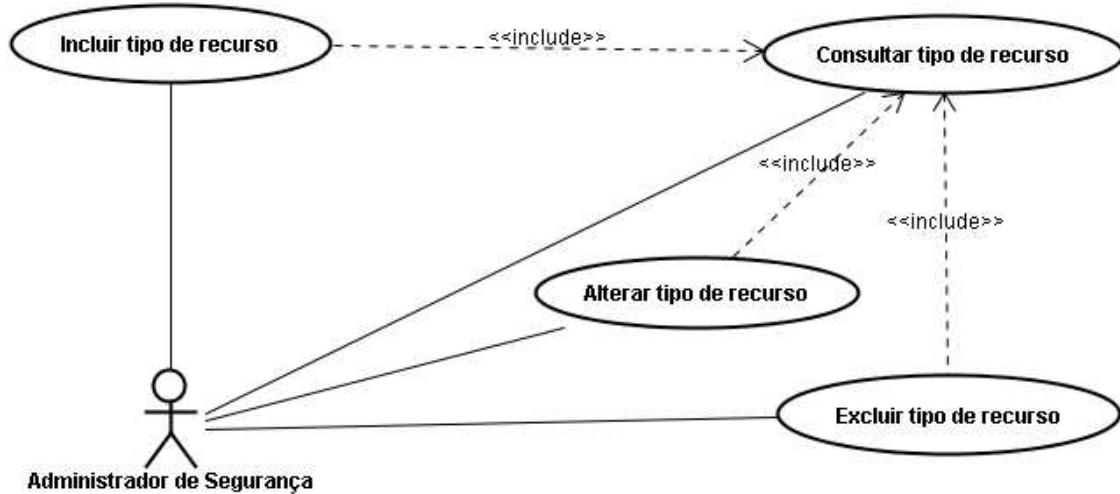


Figura 5: Casos de uso de gerenciamento de tipo de recurso

2.2.2.1.2.3. Gerenciamento de papel administrativo

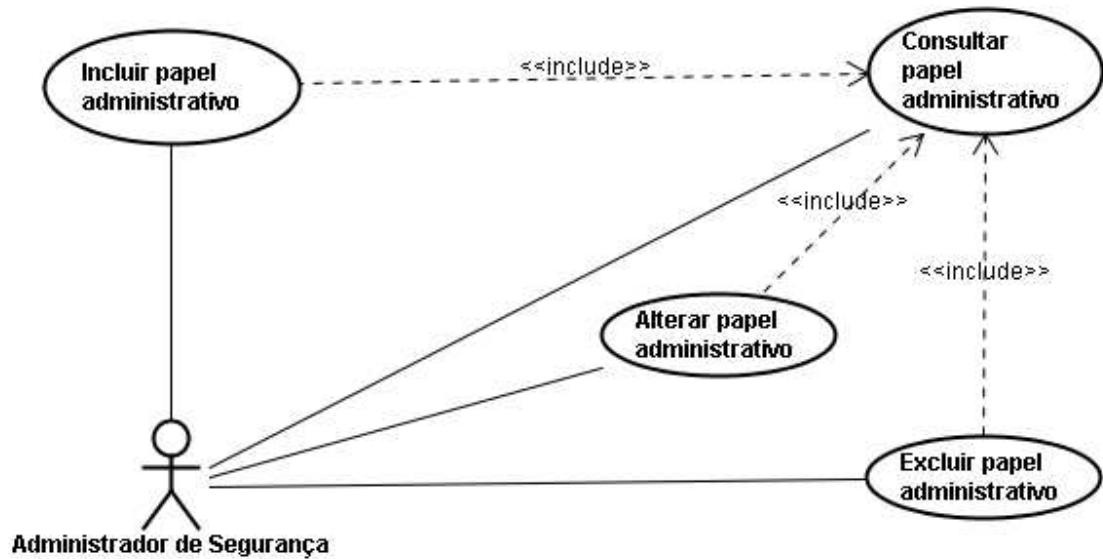


Figura 6: Casos de uso de gerenciamento de papel administrativo

2.2.2.1.2.4. Gerenciamento de usuário

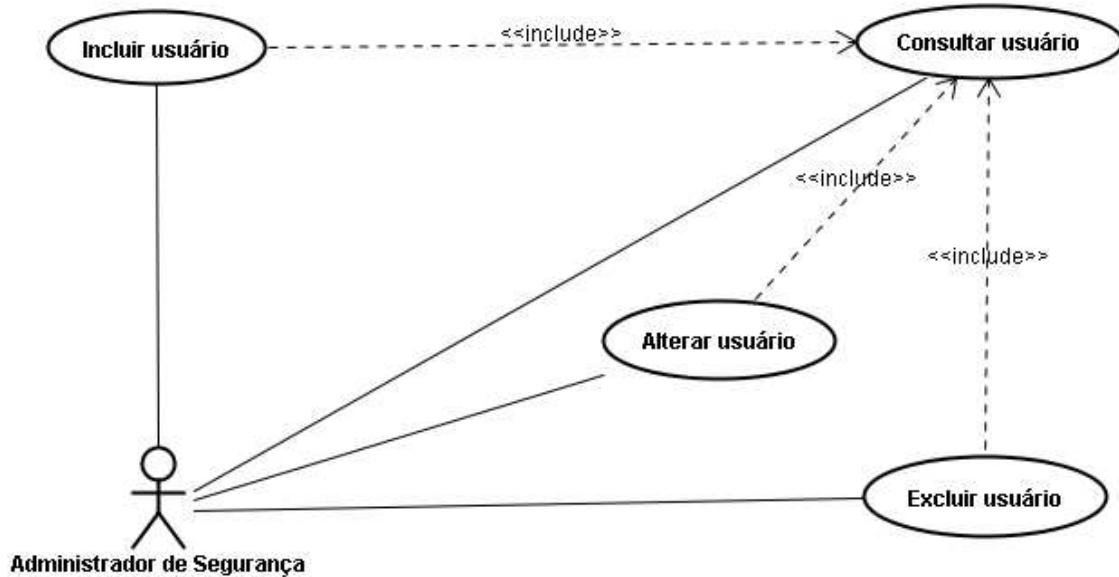


Figura 7: Casos de uso de gerenciamento de usuário

2.2.2.1.2.5. Atribuição de papel de administrador de segurança

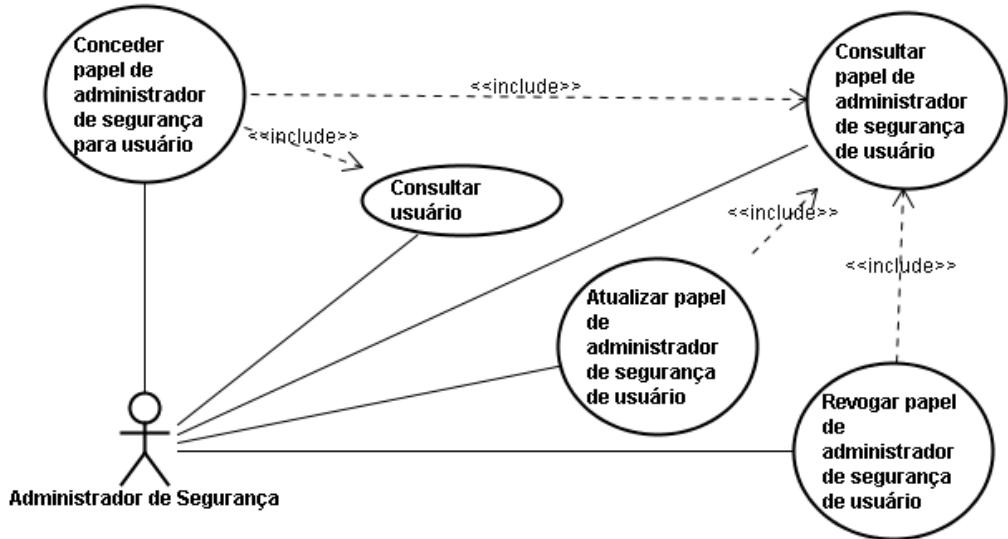


Figura 8: Casos de uso de atribuição de papel de administrador de segurança

2.2.2.1.2.6. Gerenciamento de inativação de usuários

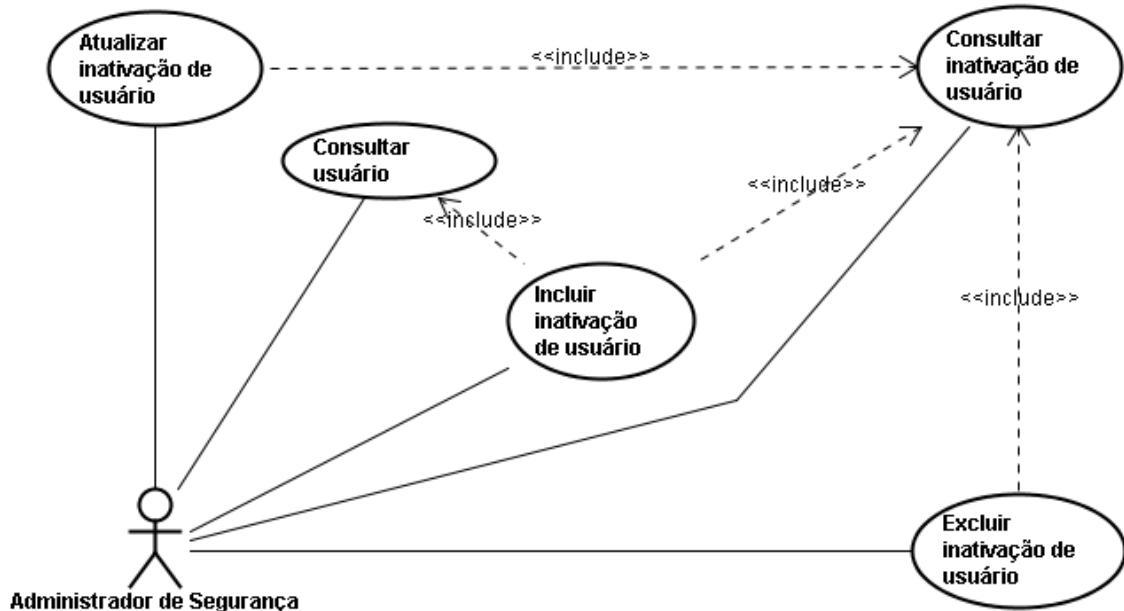


Figura 9: Casos de uso de gerenciamento de inativação de usuários

2.2.2.1.3. Casos de uso do administrador de sistema

2.2.2.1.3.1. Gerenciamento de recurso

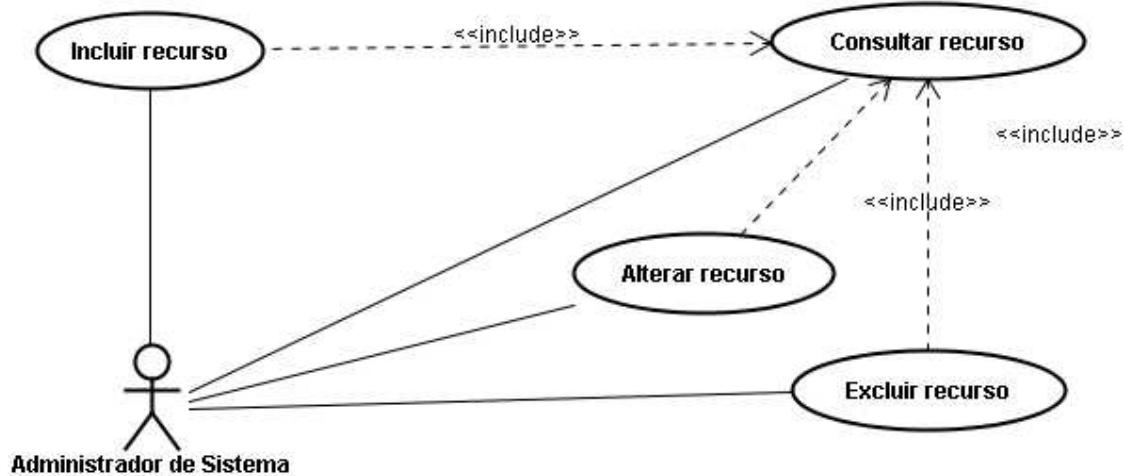


Figura 10: Casos de uso de gerenciamento de recurso

2.2.2.1.3.2. Gerenciamento de operação

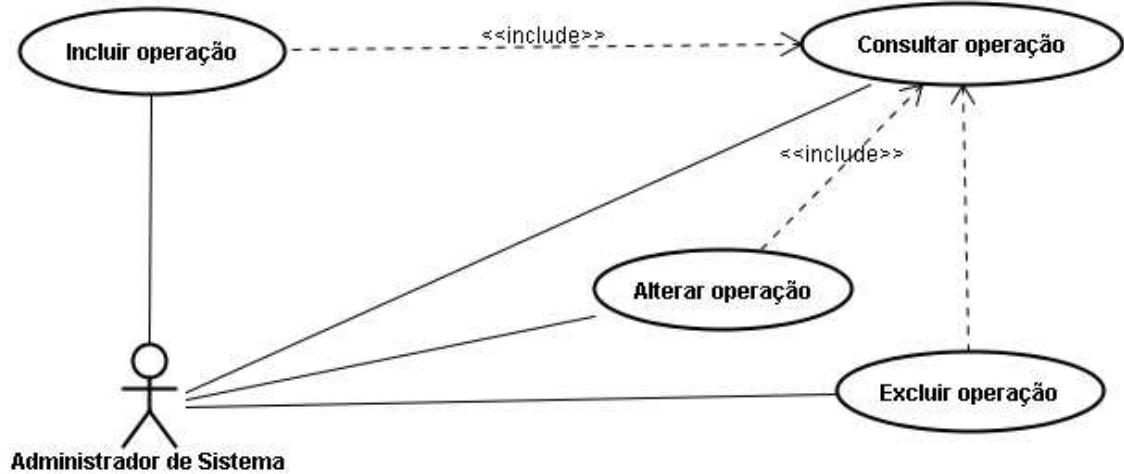


Figura 11: Casos de uso de gerenciamento de operação

2.2.2.1.3.3. Gerenciamento de permissão

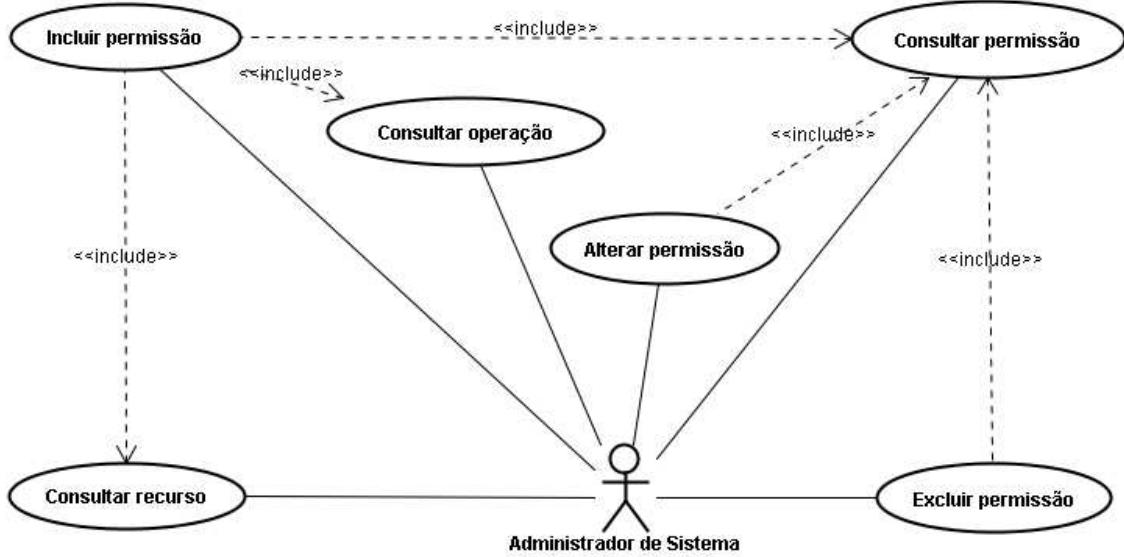


Figura 12: Casos de uso de gerenciamento de permissão

2.2.2.1.3.4. Gerenciamento de papel comum

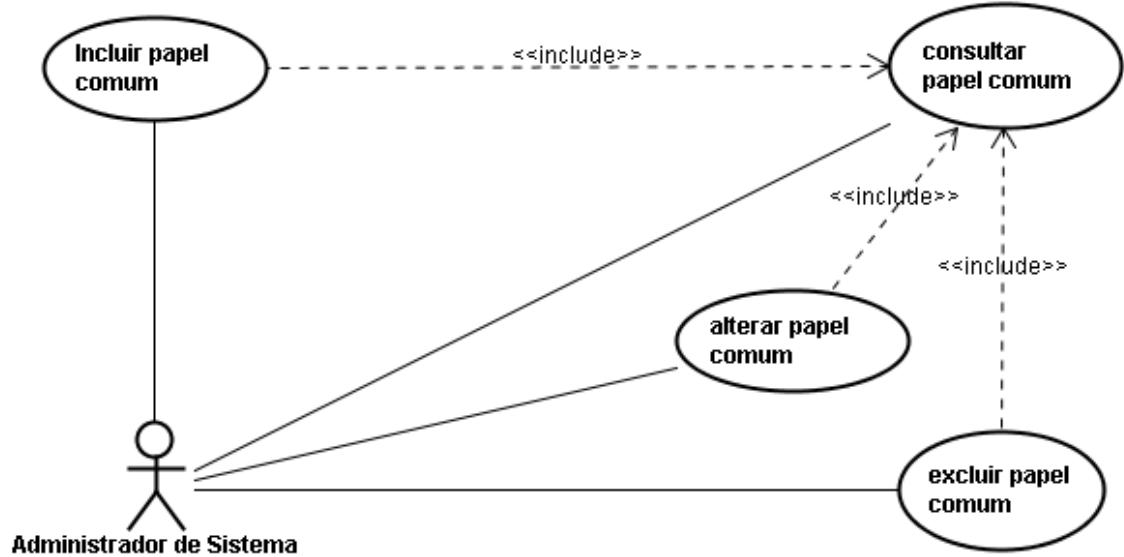


Figura 13: Casos de uso de gerenciamento de papel comum

2.2.2.1.3.5. Gerenciamento de grupo manual

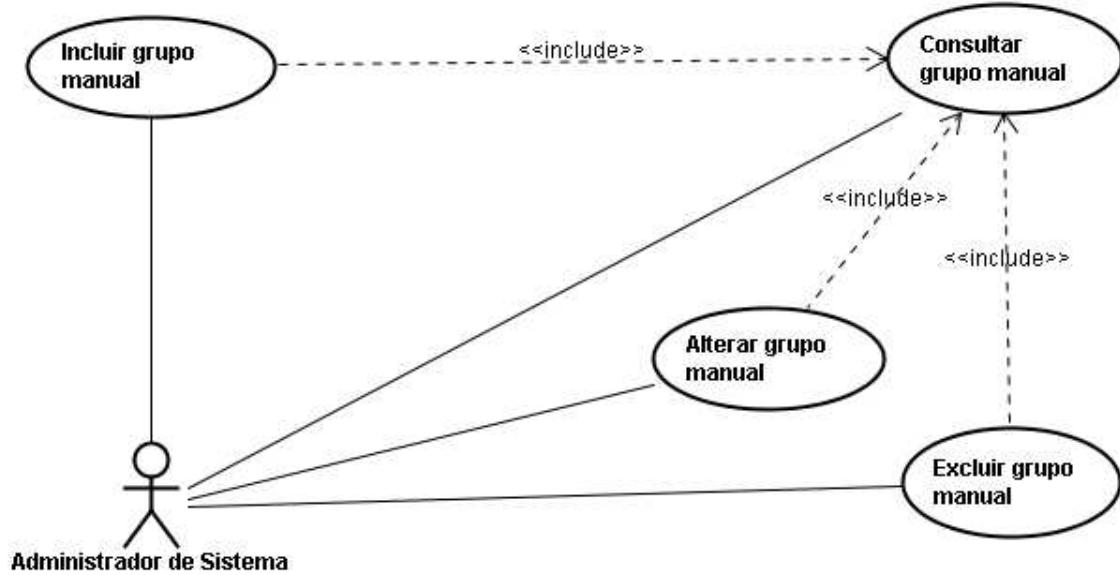


Figura 14: Casos de uso de gerenciamento de grupo manual

2.2.2.1.3.6. Gerenciamento de grupo caracterizado

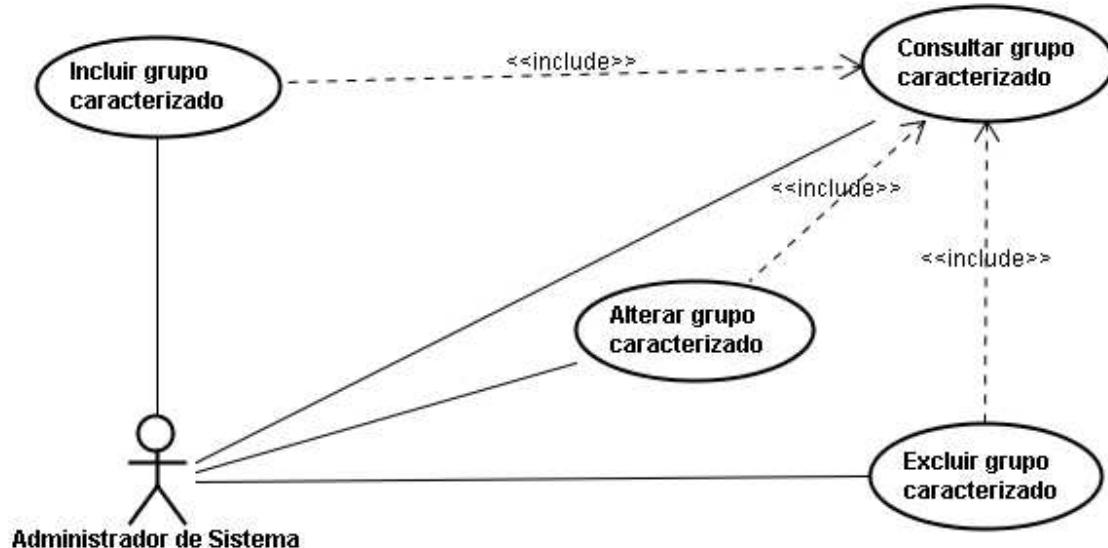


Figura 15: Casos de uso de gerenciamento de grupo caracterizado

2.2.2.1.3.7. Gerenciamento de característica

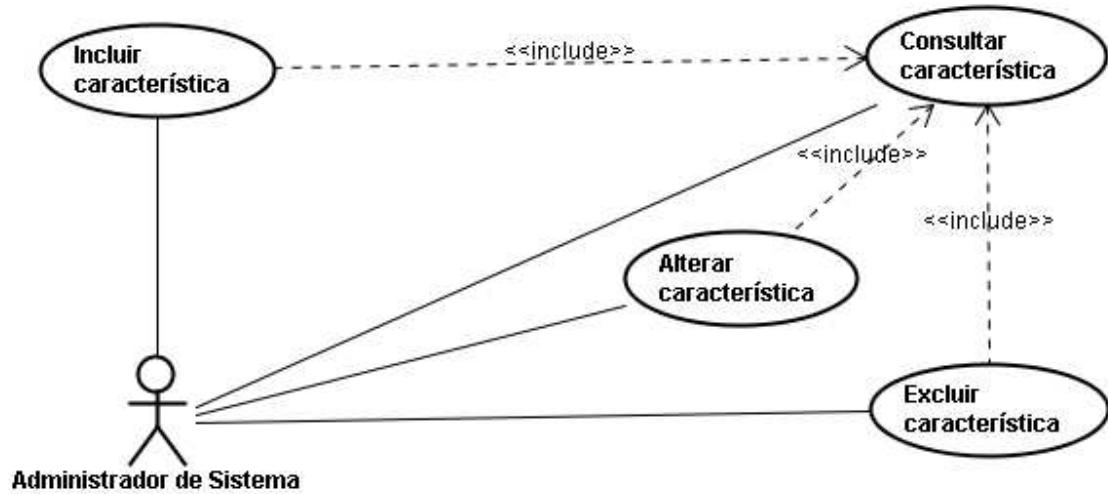


Figura 16: Casos de uso de gerenciamento de característica

2.2.2.1.3.8. Gerenciamento de valor da característica

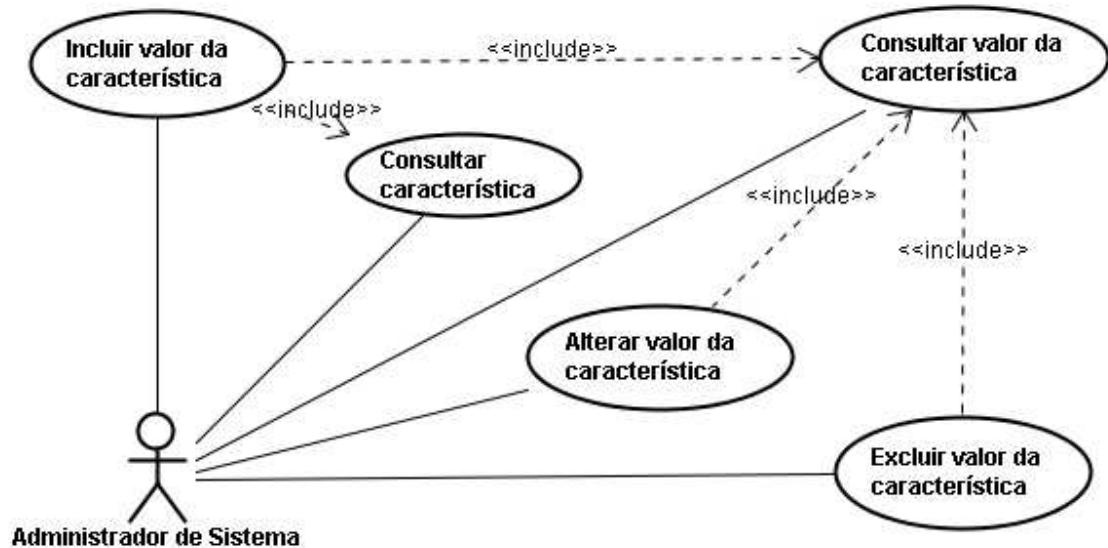


Figura 17: Casos de uso de gerenciamento de valor da característica

2.2.2.1.3.9. Gerenciamento de contexto

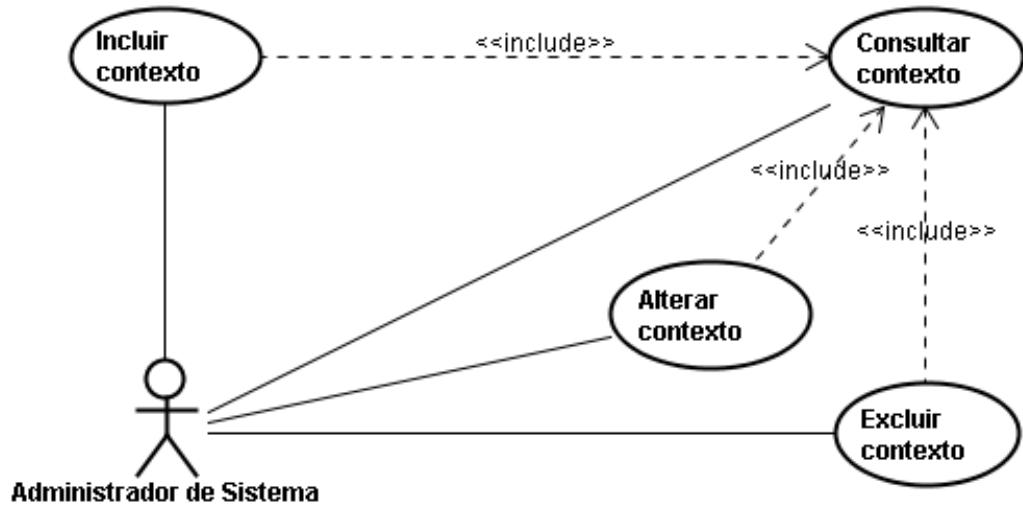


Figura 18: Casos de uso de gerenciamento de contexto

2.2.2.1.3.10. Gerenciamento de valor de contexto

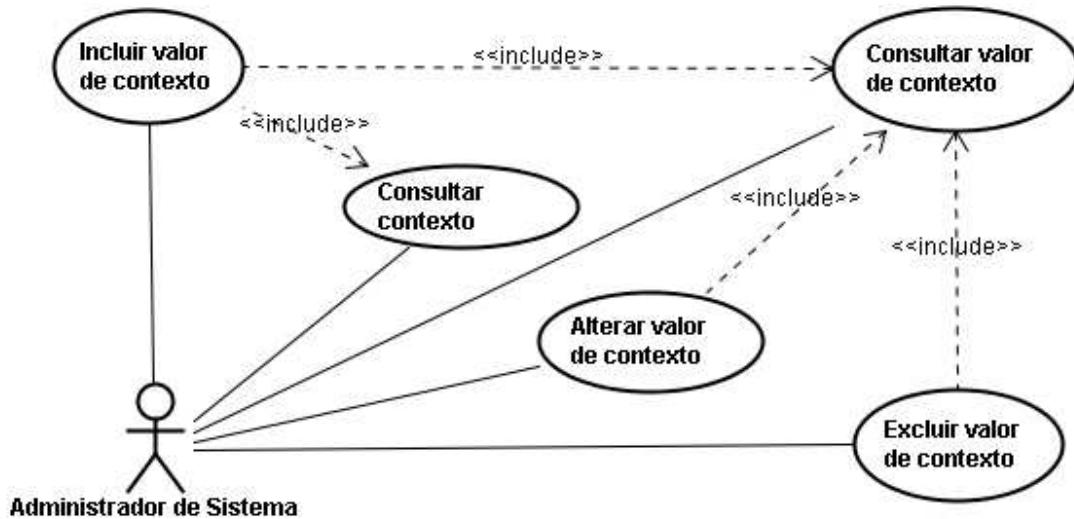


Figura 19: Casos de uso de gerenciamento de valor de contexto

2.2.2.1.3.11. Gerenciamento de permissões conflitantes

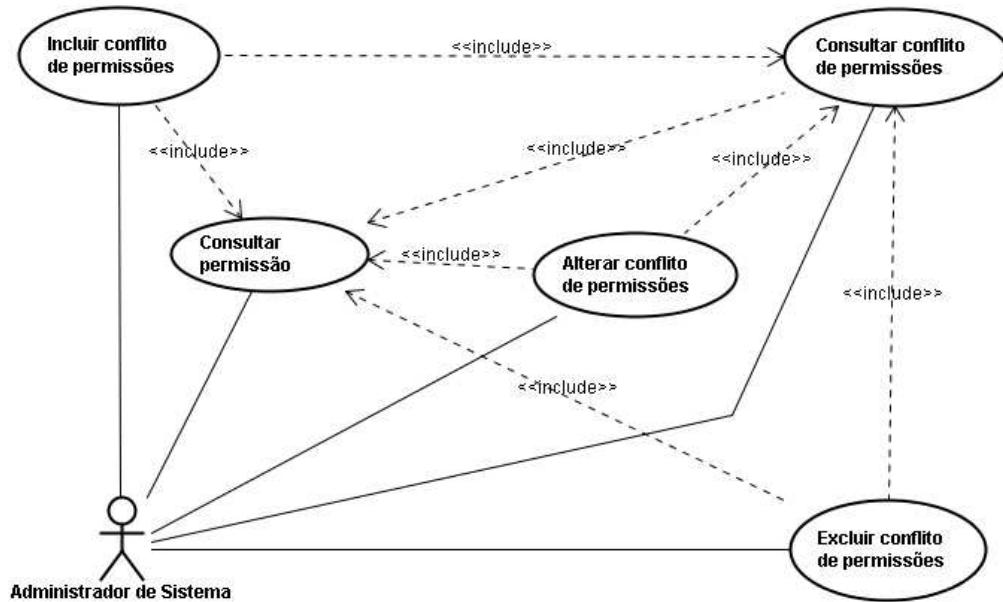


Figura 20: Casos de uso de gerenciamento de permissões conflitantes

2.2.2.1.3.12. Gerenciamento de características de grupo caracterizado

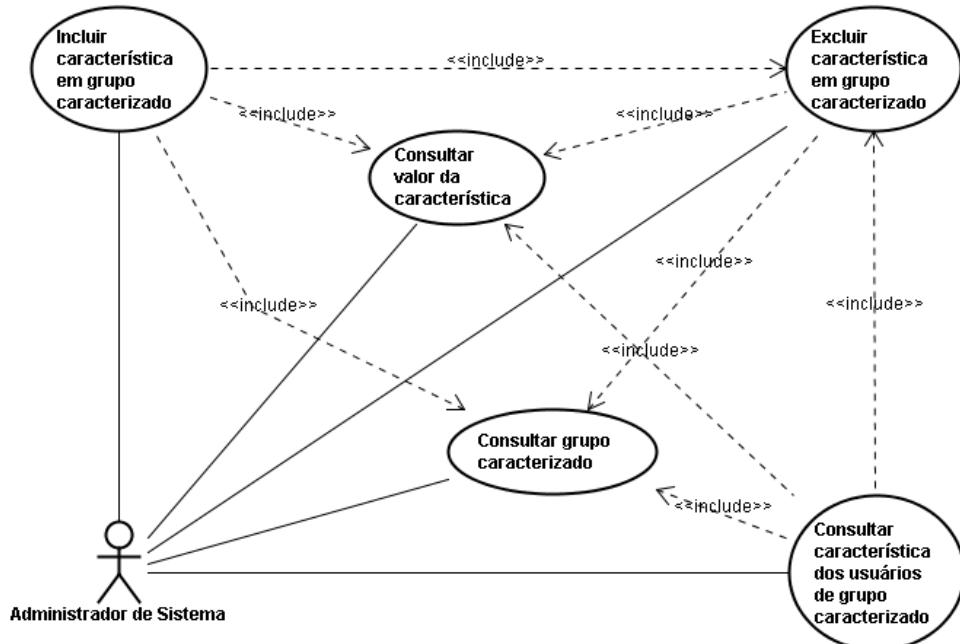


Figura 21: Casos de uso de gerenciamento de característica de grupos caracterizados

2.2.2.1.3.13. Gerenciamento de características de usuário

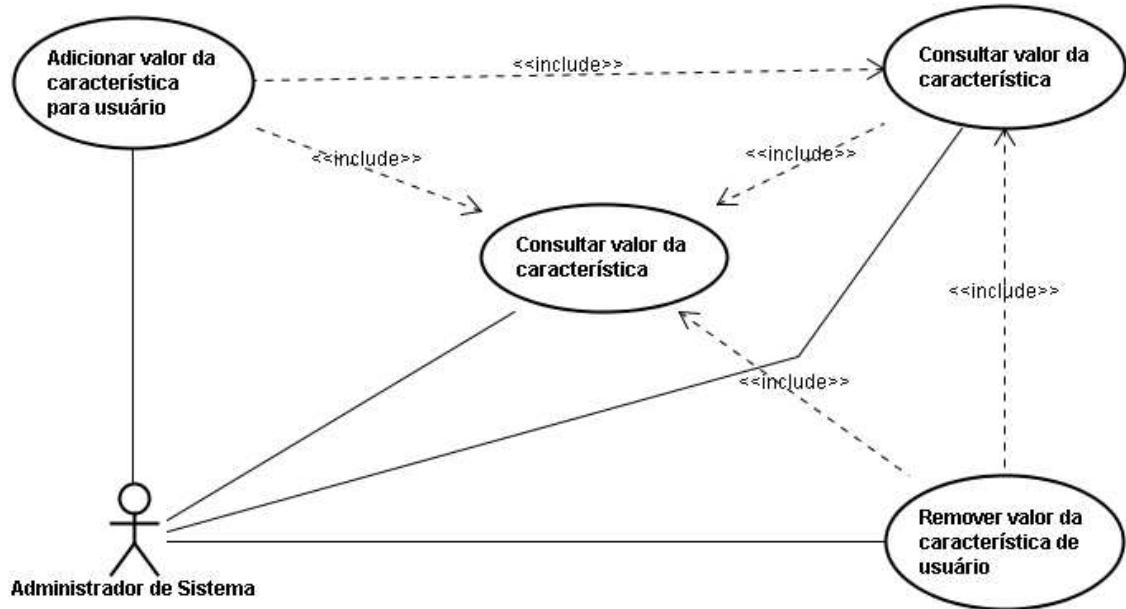


Figura 22: Casos de uso de gerenciamento de características de usuário

2.2.2.1.3.14. Gerenciamento de membros de grupos manuais

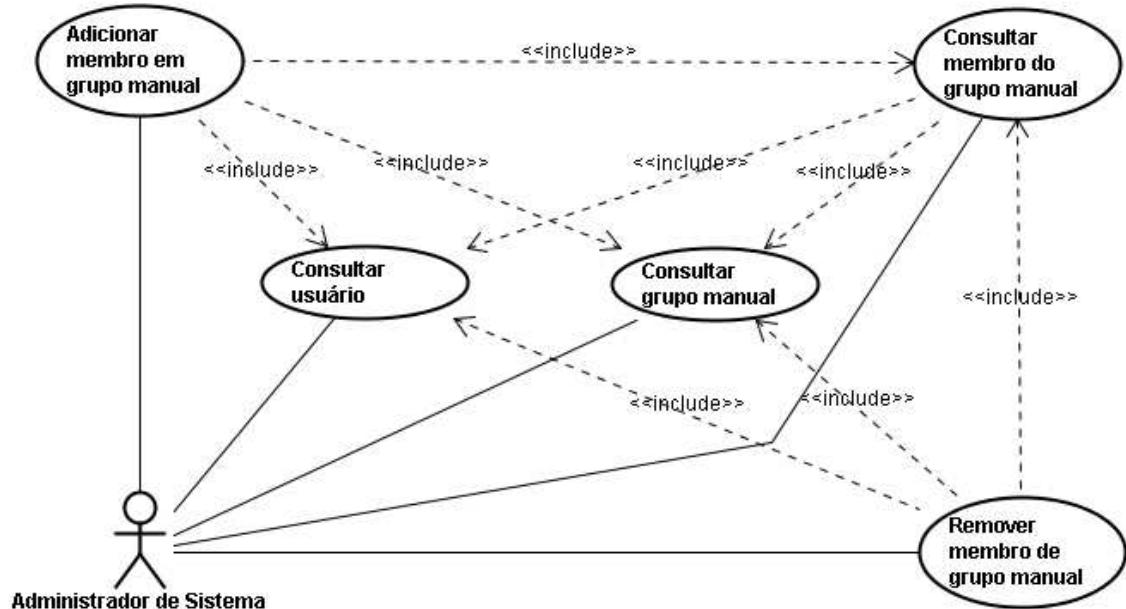


Figura 23: Casos de uso de gerenciamento de membros de grupos manuais

2.2.2.1.3.15. Gerenciamento de inativação de grupos manuais

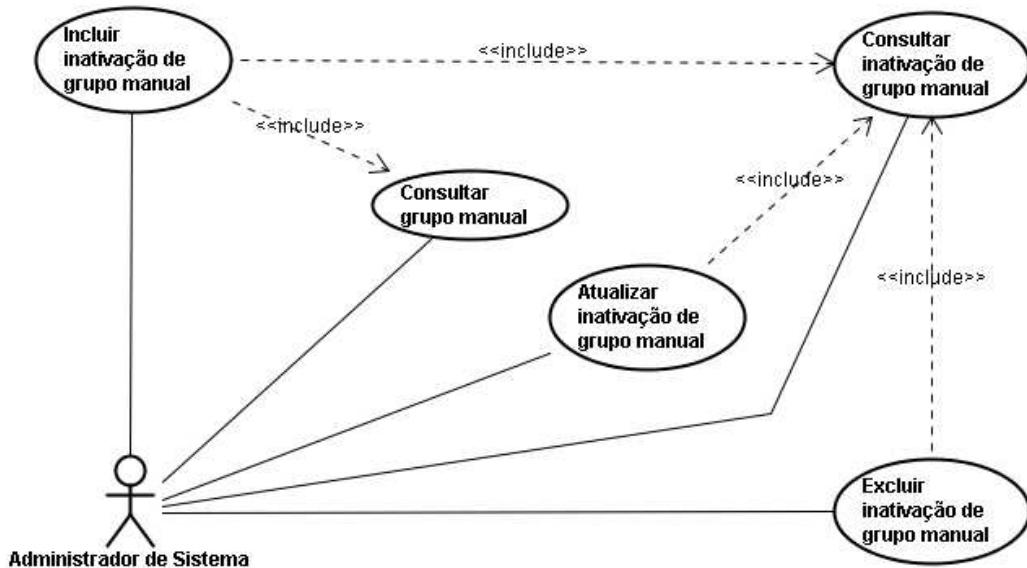


Figura 24: Casos de uso de gerenciamento de inativação de grupos manuais

2.2.2.1.3.16. Gerenciamento de inativação de grupos caracterizados

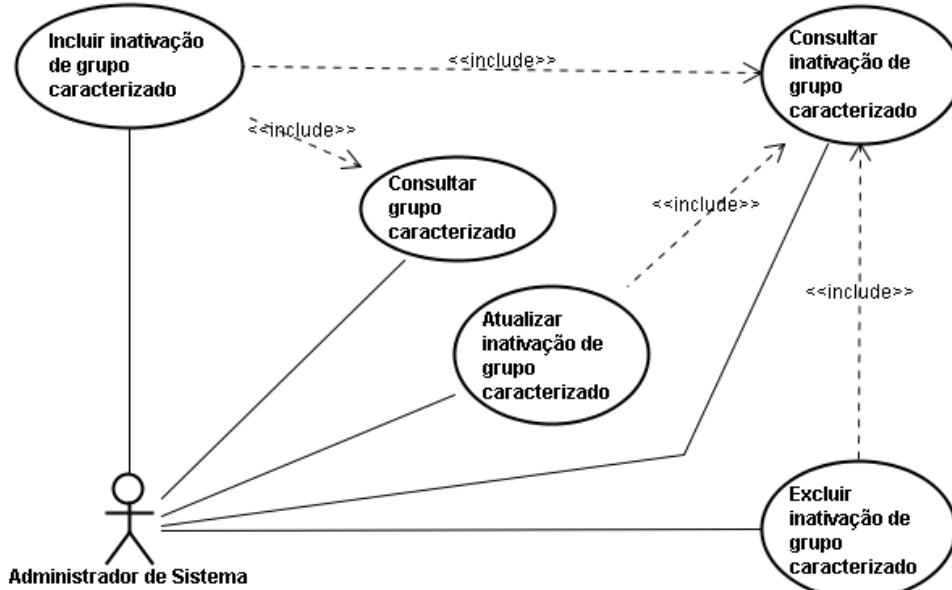


Figura 25: Casos de uso de gerenciamento de inativação de grupos caracterizados

2.2.2.1.3.17. Concessão de permissão para papel comum

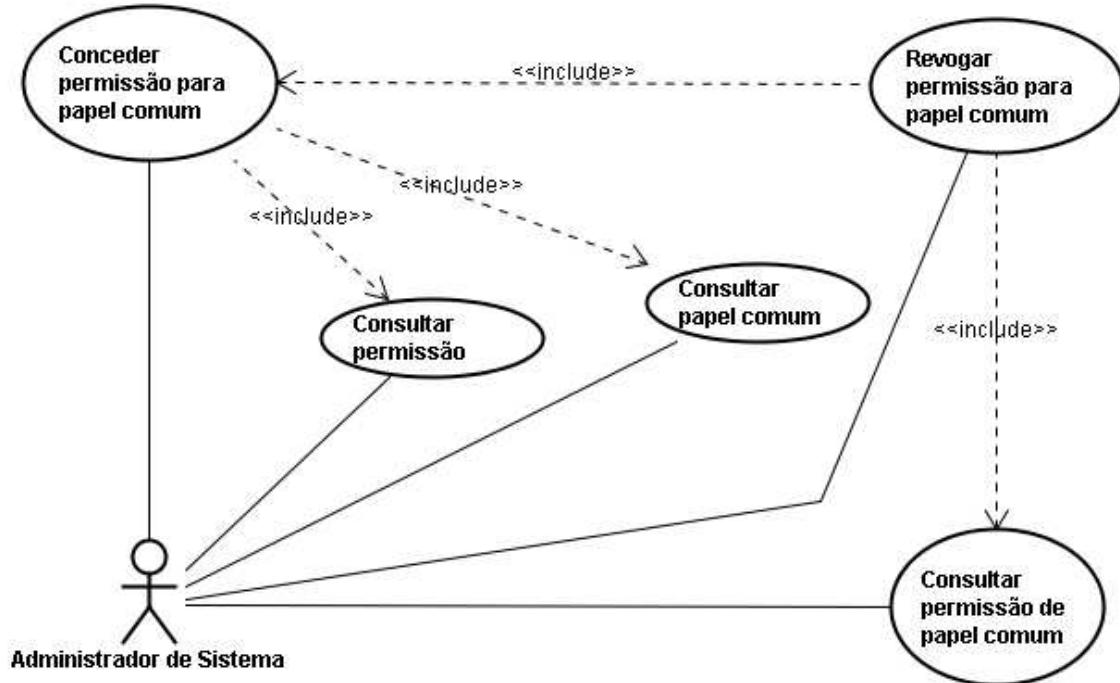


Figura 26: Casos de uso de concessão de permissão para papel comum

2.2.2.1.3.18. Atribuição de papel comum para usuário

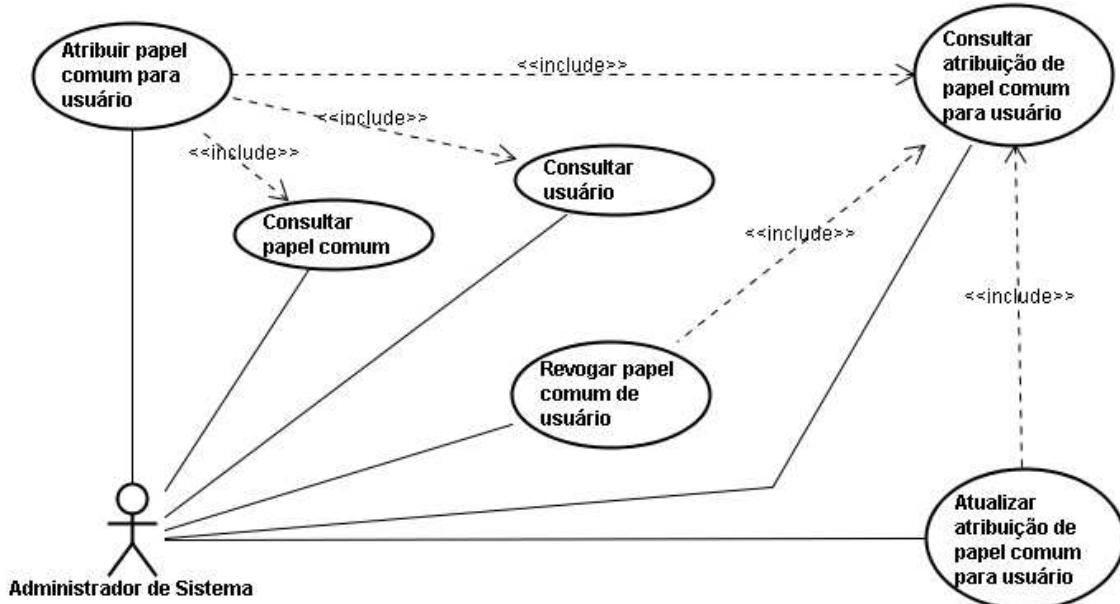


Figura 27: Casos de uso de atribuição de papel comum para usuário

2.2.2.1.3.19. Atribuição de papel administrativo para usuário

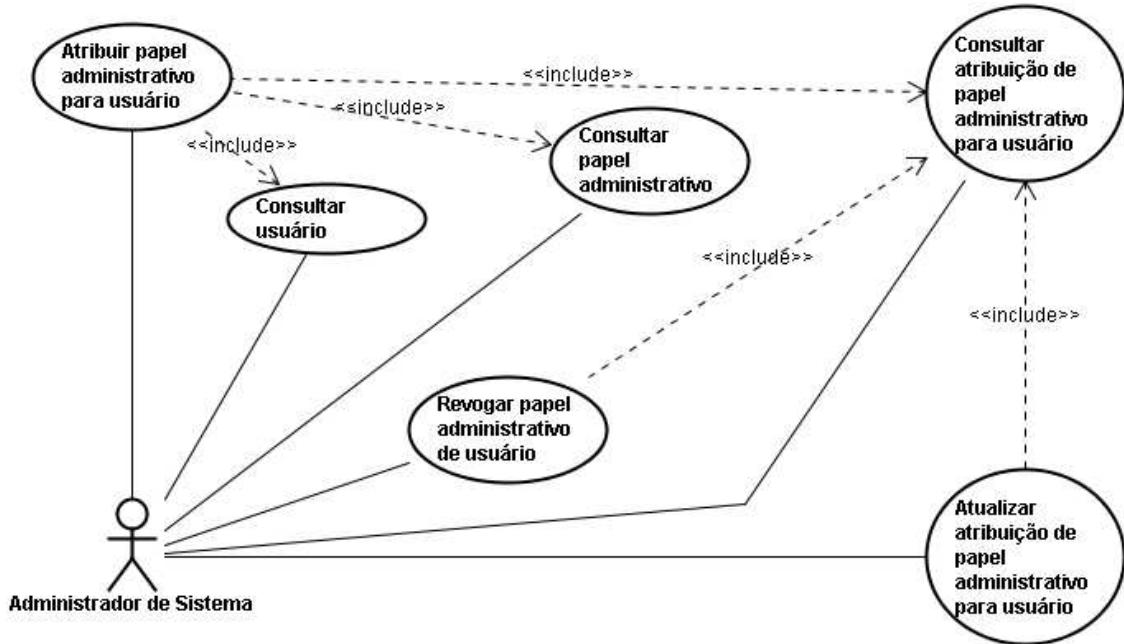


Figura 28: Casos de uso de atribuição de papel administrativo para usuário

2.2.2.1.3.20. Atribuição de papel comum para grupo manual

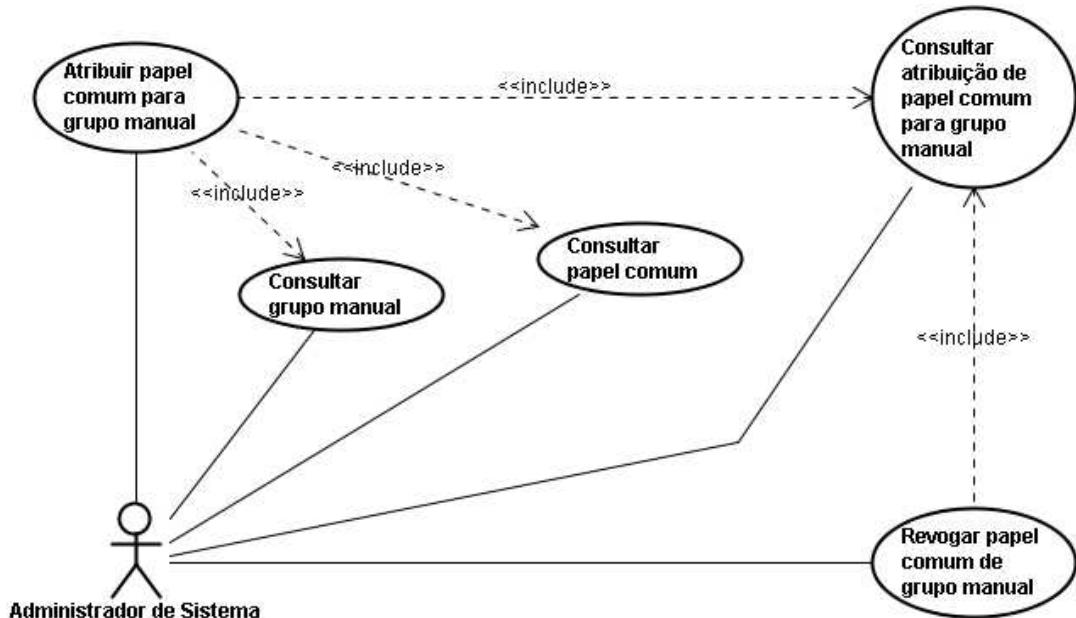


Figura 29: Casos de uso de atribuição de papel comum para grupo manual

2.2.2.1.3.21. Atribuição de papel administrativo para grupo manual

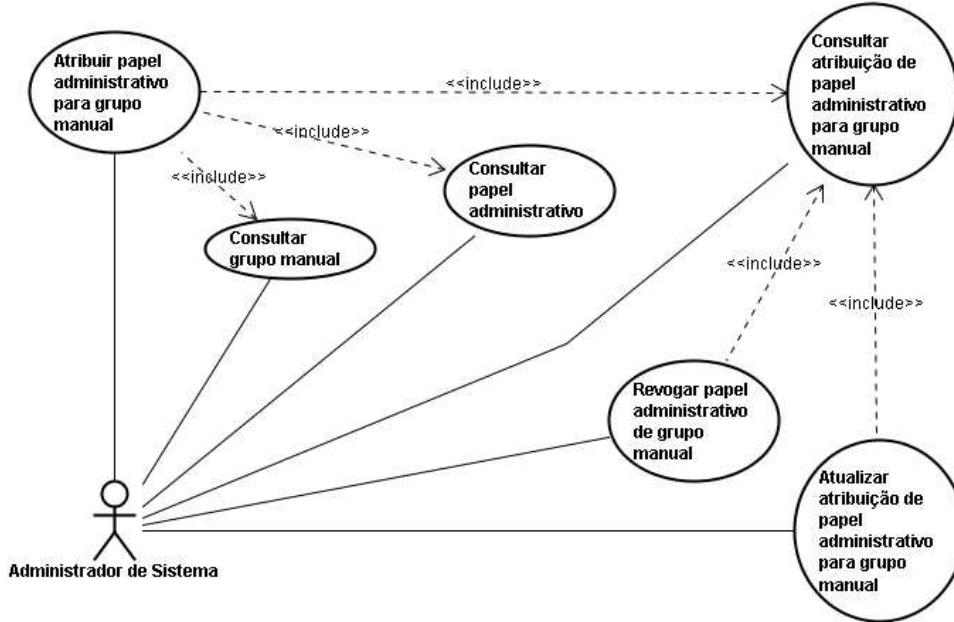


Figura 30: Casos de uso de atribuição de papel administrativo para grupo manual

2.2.2.1.3.22. Contextualização de atribuição de papel comum para usuário

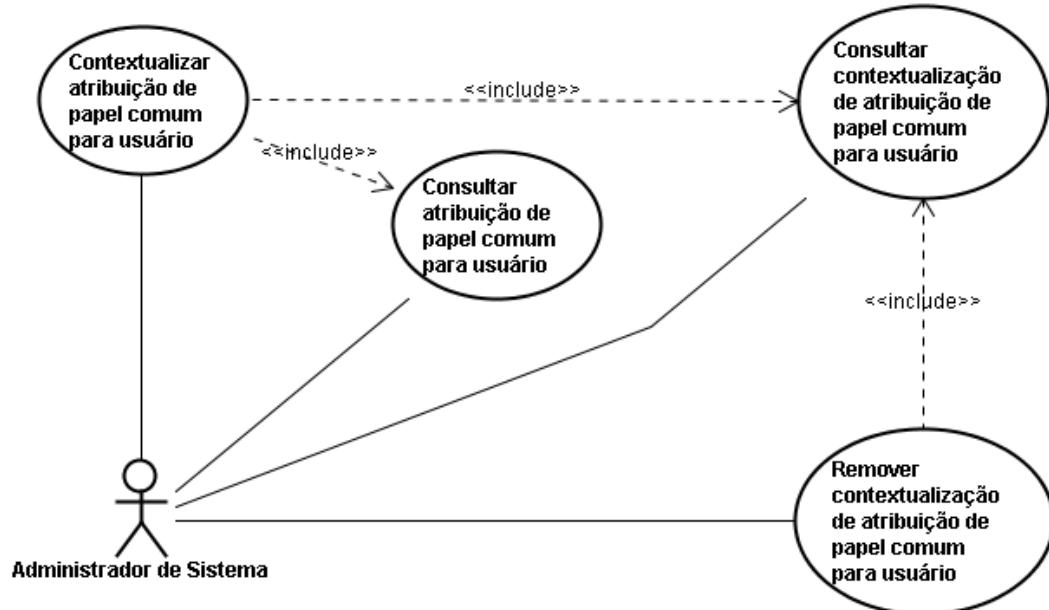


Figura 31: Casos de uso de contextualização de atribuição de papel comum para usuário

2.2.2.1.3.23. Contextualização de permissão

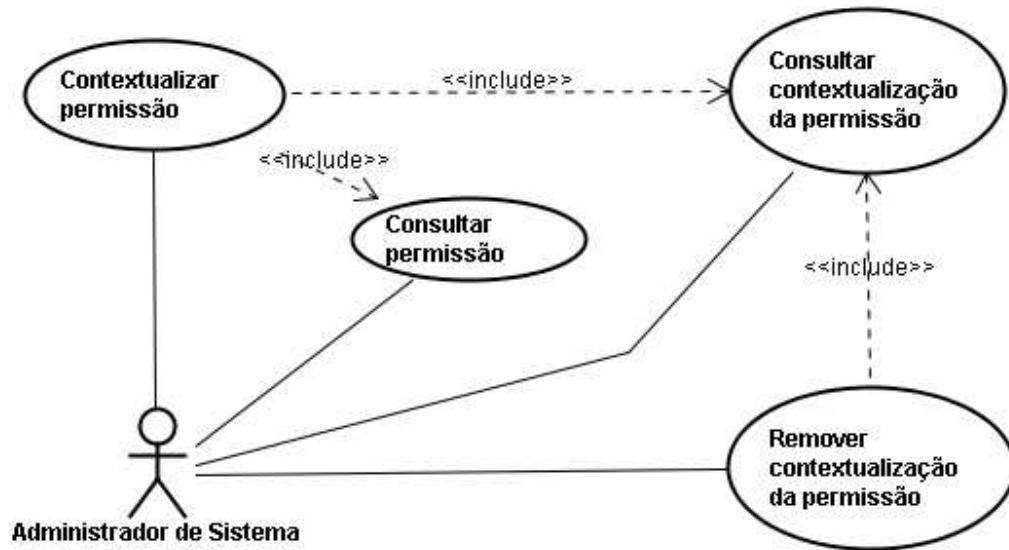


Figura 32: Casos de uso de contextualização de permissão

2.2.2.1.3.24. Contextualização de atribuição de papel comum para grupo manual

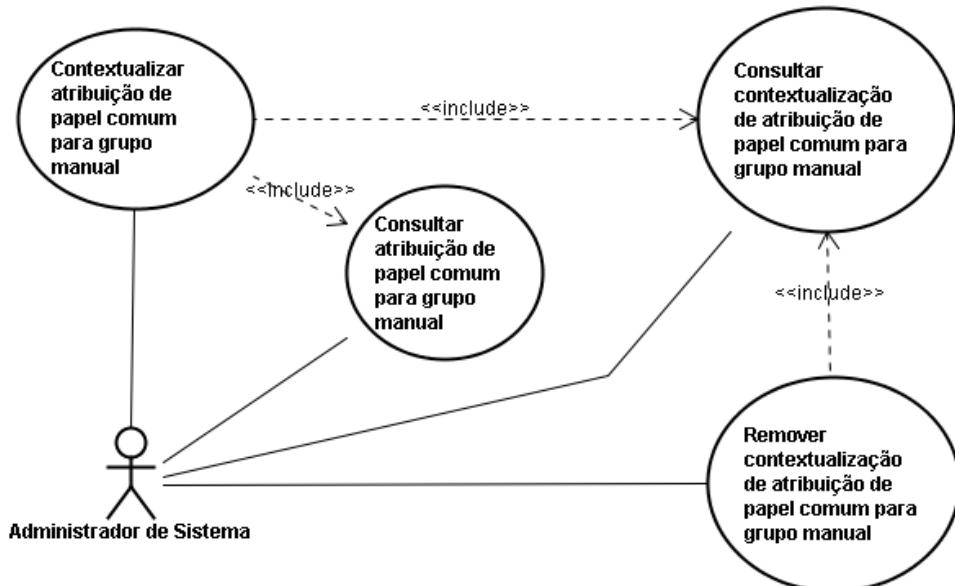


Figura 33: Casos de uso de contextualização de atribuição de papel comum para grupo manual

2.2.2.1.3.25. Contextualização de atribuição de papel comum para grupo caracterizado

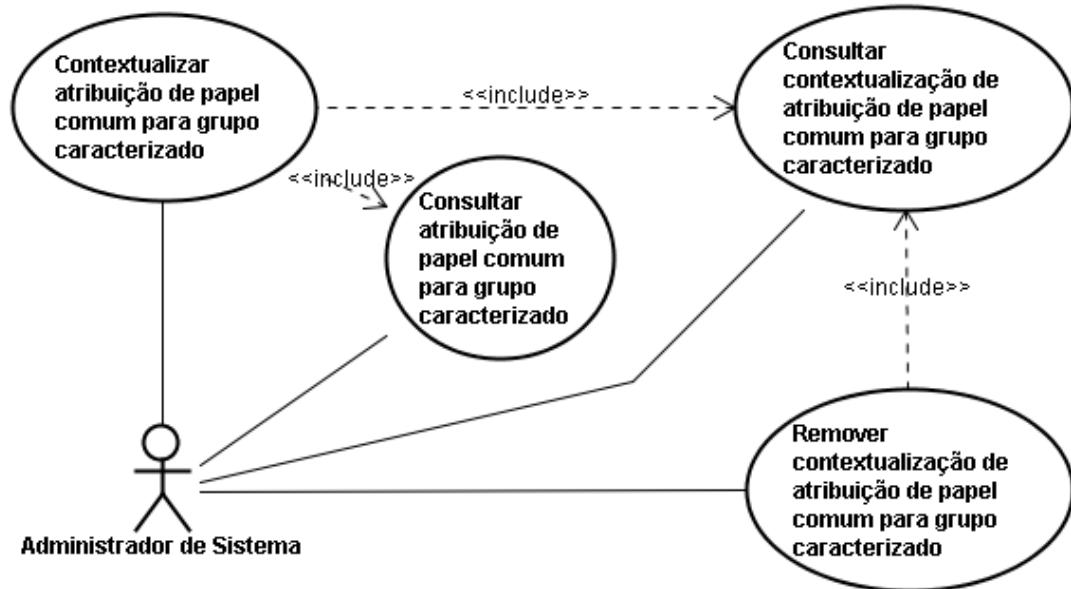


Figura 34: Casos de uso de contextualização de atribuição de papel comum para grupo caracterizado

2.2.2.1.4. Casos de Uso de Sistema Cliente

2.2.2.1.4.1. Verificação de autorização de usuário em permissão

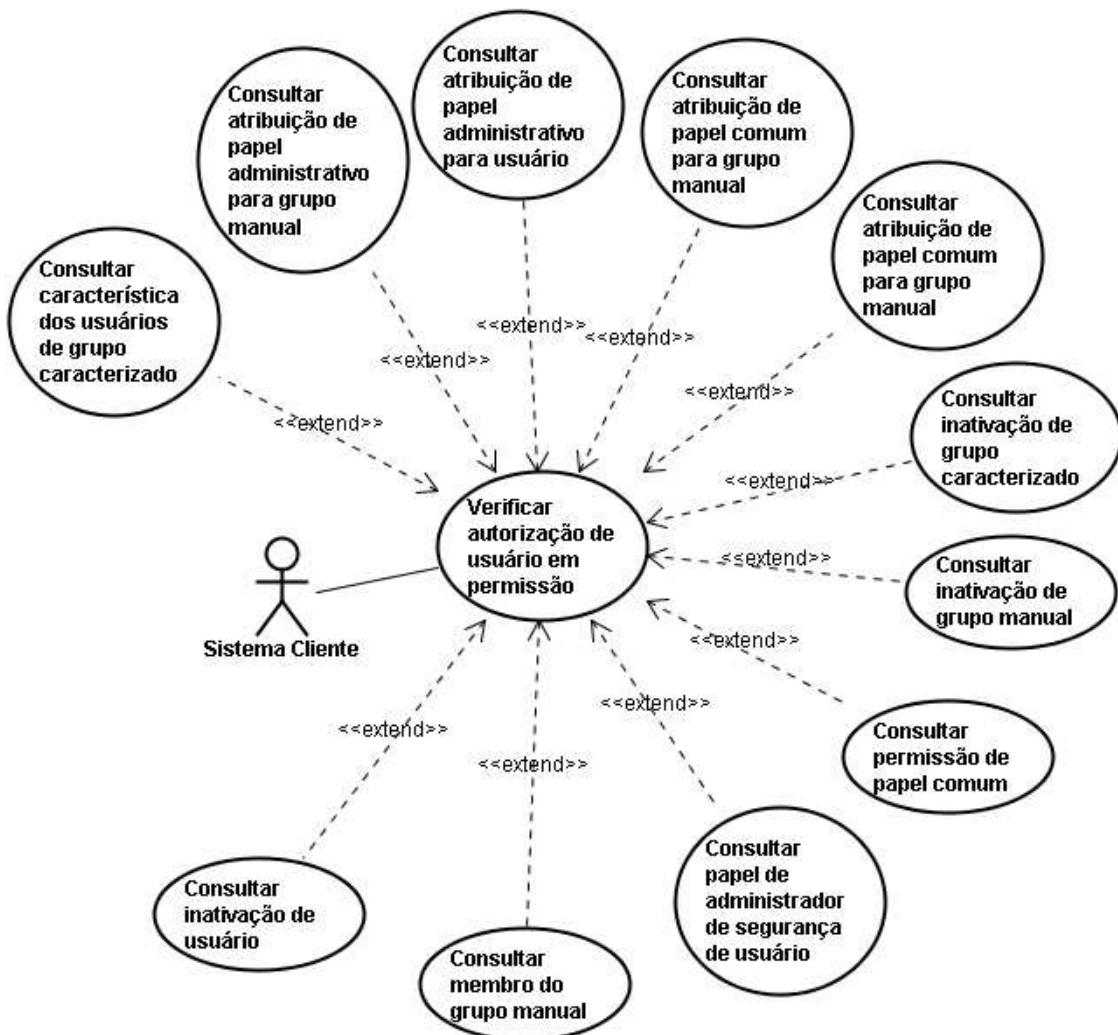


Figura 35: Caso de uso de verificação de autorização de usuário em permissão

2.2.2.1.4.2. Verificação de autorização de usuário em permissão contextualizada

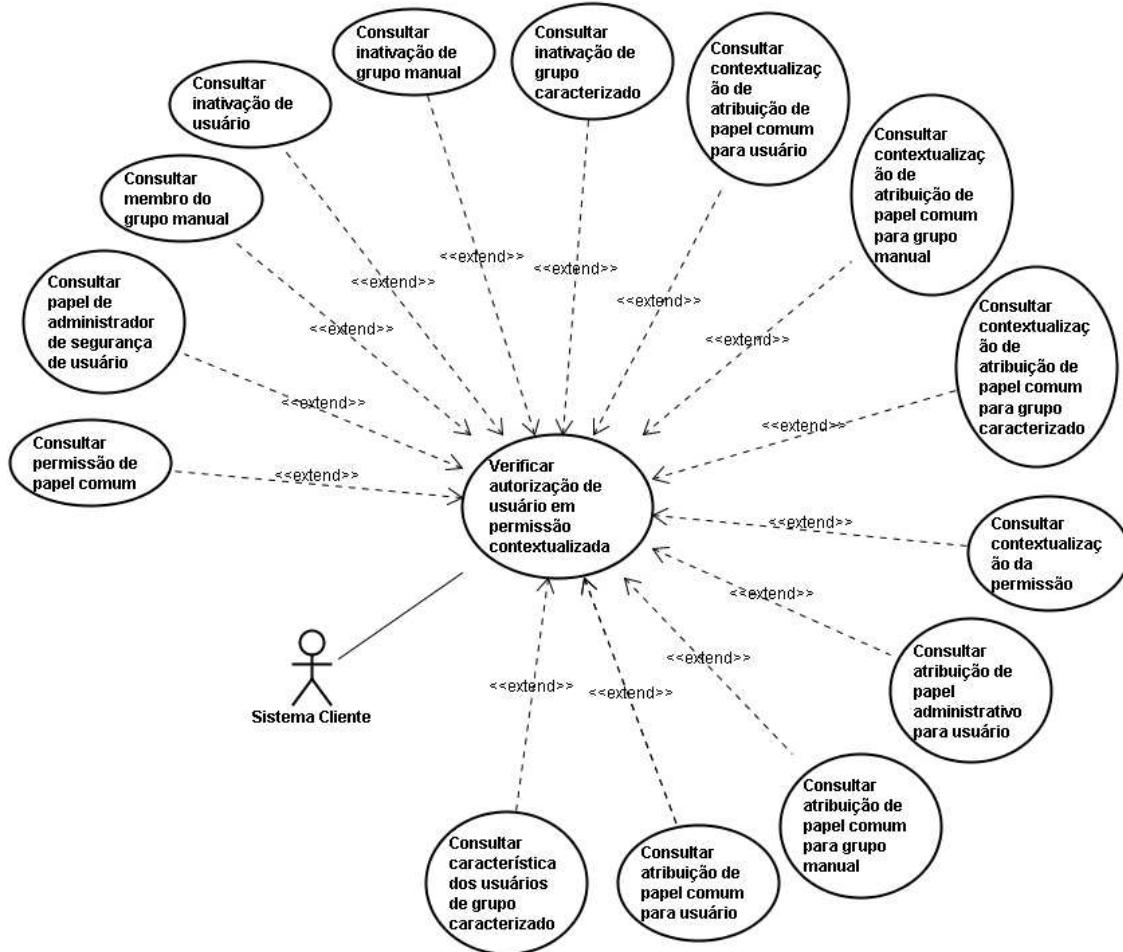


Figura 36: Caso de uso de verificação de autorização de usuário em permissão contextualizada

2.2.2.1.4.3. Conexão de sistema cliente

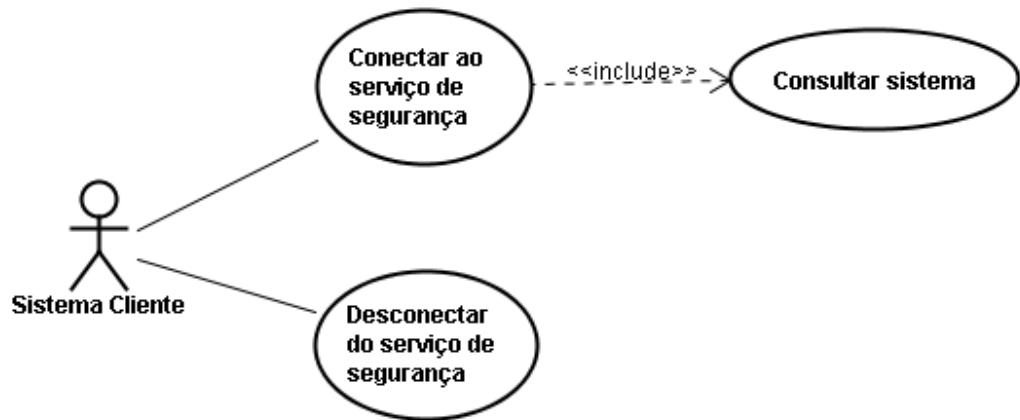


Figura 37: Casos de uso de conexão de sistema cliente

2.2.2.2. DESCRIÇÃO DOS CASOS DE USO

O Diagrama de Casos de Uso descreve as funcionalidades do sistema, ou seja, como ele deverá se comportar.

Este diagrama é composto por vários casos de uso, que estão listados a seguir:

Lista de Casos de Uso	
Ator	Caso de Uso
ADMINISTRADOR DE SEGURANÇA	Efetuar logon
	Efetuar logoff
	Alterar senha
	Incluir sistema
	Alterar sistema
	Excluir sistema
	Consultar sistema
	Incluir papel administrativo
	Alterar papel administrativo
	Excluir papel administrativo
	Consultar papel administrativo
	Incluir usuário
	Alterar usuário
	Excluir usuário
	Consultar usuário
	Incluir tipo de recurso
	Alterar tipo de recurso
	Excluir tipo de recurso
	Consultar tipo de recurso
	Inativar usuário
	Reativar usuário
	Consultar inativação de usuário
	Incluir valor de característica para usuário
	Excluir valor de característica de usuário
	Consultar valor de característica de usuário
SISTEMA CLIENTE	Conectar
	Desconectar
	Verificar autorização de usuário em permissão
	Verificar autorização de usuário em permissão contextualizada
USUÁRIO	Efetuar logon
	Efetuar logoff
	Alterar senha

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

ADMINISTRADOR DE SISTEMA	Efetuar logon Efetuar logoff Alterar senha Incluir recurso Alterar recurso Excluir recurso Consultar recurso Incluir operação Alterar operação Excluir operação Consultar operação Incluir permissão Alterar permissão Excluir permissão Consultar permissão Incluir papel comum Alterar papel comum Excluir papel comum Consultar papel comum Incluir grupo manual Alterar grupo manual Excluir grupo manual Consultar grupo manual Incluir grupo caracterizado Alterar grupo caracterizado Excluir grupo caracterizado Consultar grupo caracterizado Incluir característica Alterar característica Excluir característica Consultar característica Incluir valor da característica Alterar valor da característica Excluir valor da característica Consultar valor da característica Incluir permissões conflitantes Excluir permissões conflitantes Consultar permissões conflitantes Incluir contexto Alterar contexto Excluir contexto Consultar contexto Incluir valor de contexto Alterar valor de contexto Excluir valor de contexto Consulta valor de contexto Adicionar membro em grupo manual Remover membro de grupo manual Consultar membro de grupo manual Consultar membro de grupo caracterizado Inativar grupo manual Reativar grupo manual Consultar inativação de grupo manual
---------------------------------	---

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Inativar grupo caracterizado
Reativar grupo caracterizado
Consultar inativação de grupo caracterizado
Incluir valor de característica para grupo caracterizado
Excluir valor de característica de grupo caracterizado
Consultar valor de característica de grupo caracterizado

A seguir apresentam-se as descrições dos casos de uso do sistema proposto:

Caso de uso: realizar logon	
Autor(es)	Administrador de segurança Administrador do sistema Usuário
Descrição	Este caso de uso descreve a autenticação de um ator no Framework de Segurança.
Pré-condições	O ator não deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Entra no Console Administrativo.	
	2 – Exibe formulário de autenticação com seguintes campos: login, senha e sistema. Apenas o login e a senha são obrigatórios.
3 – Informa os dados e seleciona a opção “autenticar”.	
	4 – Valida os dados informados.
	5 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	6 – Guarda usuário autenticado na sessão.
	7 – Redireciona para a tela principal.
Fluxo alternativo #1 (login inexistente)	
	4 – Se não existir usuário com o login informado, grava um histórico do evento de tentativa de autenticação fracassada e exibe mensagem de falha na autenticação informando que as credenciais são inválidas.
Fluxo alternativo #2 (senha incorreta)	
	4 – Se a senha informada está incorreta, grava um histórico do evento de tentativa de autenticação fracassada e exibe mensagem de falha na autenticação informando que as credenciais são inválidas.
Fluxo alternativo #3 (campo obrigatório não preenchido)	
	4 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na autenticação pelo motivo de não ter informado valor em todos os campos obrigatórios.

Fluxo alternativo #4 (usuário esqueceu a senha)	
	4 – Se o usuário selecionou a opção “Esqueci minha senha”, executa o caso de uso “Solicitar nova senha por e-mail”.
Fluxo alternativo #5 (usuário informou o sistema)	
	4 – Se o usuário informou o sistema, verifica se o mesmo possui papel de administrador neste sistema e caso positivo, guarda o sistema selecionado na sessão e continua o fluxo básico.
Fluxo alternativo #6 (usuário não é administrador do sistema)	
	4 – Se o usuário informou o sistema, porém não possui papel de administrador no mesmo, exibe mensagem de erro informando que usuário não é administrador de sistema.
Fluxo alternativo #7 (usuário não é administrador de segurança)	
	4 – Se o usuário não informou o sistema e não possui papel de administrador de segurança, exibe mensagem de erro informando que usuário não é administrador de segurança.
Fluxo alternativo #8 (tentativa de acesso falhou pela décima vez consecutiva)	
	4 – Se foram tentados dez acessos com senha incorreta, a conta do usuário é bloqueada e uma mensagem de conta bloqueada é exibida.

Caso de uso: realizar logoff	
Autor(es)	Administrador de segurança Administrador do sistema Usuário
Descrição	Este caso de uso descreve a operação inversa da autenticação de um ator no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “sair”.	
	2 – Obtém usuário autenticado da sessão.
	3 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	4 – Remove usuário da sessão.
	5 – Remove sistema da sessão (caso exista).
	6 – Redireciona para a tela principal.
Fluxo alternativo #1 (sessão do usuário caiu)	
	2 – Se não existir usuário autenticado na sessão, redireciona para a tela principal.

Caso de uso: solicitar nova senha por e-mail	
Autor(es)	Administrador de segurança Administrador do sistema Usuário
Descrição	Este caso de uso descreve a solicitação de nova senha por um ator que esqueceu sua senha atual.
Pré-condições	O ator não deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Escolhe a opção “Esqueci minha senha”.	
	2 – Exibe formulário contendo um campo de login (obrigatório).
3 – Informa login e seleciona a opção “enviar”.	
	4 – Valida o login informado.
	5 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	6 – Envia um e-mail para o usuário contendo na mensagem um link temporário para uma página onde uma nova senha será gerada. Esta mensagem deverá informar ao usuário o tempo de validade do link.
	7 – Exibe mensagem para usuário solicitando que o mesmo acessasse seu e-mail para continuar o processo de geração de uma nova senha. Esta mensagem terá o e-mail para onde o link para página temporária foi enviado.
Fluxo alternativo #1 (login inexistente)	
	4 – Se não existir usuário com o login informado, grava um histórico do evento de tentativa de solicitação de nova senha fracassada e exibe mensagem de falha na solicitação informando que não existe usuário com o login informado.
Fluxo alternativo #2(campo obrigatório não preenchido)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	4 – Se o campo obrigatório não foi informado, exibe mensagem de falha na solicitação de nova senha pelo motivo de não ter informado valor em todos os campos obrigatórios.
Fluxo alternativo #3 (usuário acessa página temporária para geração de nova senha)	
1 – Entra na página temporária envia por e-mail.	
	2 – Verifica se o link ainda é válido
	3 – Gera uma senha aleatória, grava na base de dados.
	4 – Informa ao cliente que uma nova senha aleatória foi gerada e exibe uma opção para que o mesmo possa visualizá-la.
5 – Seleciona a opção “visualizar senha gerada”.	
	6 – Exibe a nova senha gerada.

Caso de uso: alterar senha	
Autor(es)	Usuário
Descrição	Este caso de uso descreve a operação de alteração de senha de um usuário.
Fluxo básico	
Autor	Sistema
1 – Seleciona a opção “alterar senha”.	
	2 – Exibe um formulário contendo os campos login, senha atual, nova senha e confirmação de nova senha. Todos obrigatórios.
3 – Informa o login, a senha atual, a nova senha, a confirmação da nova senha e seleciona a opção “alterar senha”.	
	4 – Verifica se a senha atual está correta. Se a nova senha e a confirmação da nova senha são iguais.
	5 – Atualiza a senha com a nova senha informada.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	7 – Exibe mensagem informando que a senha foi atualizada com sucesso.
Fluxo alternativo #1 (senha atual não é válida)	
	4 – Se a senha atual informada pelo usuário for inválida, exibe mensagem informando que a senha atual não é correta.
Fluxo alternativo #2 (nova senha e confirmação da nova senha não conferem)	
	4 – Se a nova senha e a confirmação de nova senha não conferem, exibe mensagem informando que a nova senha e a confirmação não são iguais.

Caso de uso: incluir sistema	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a inclusão de um sistema no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar sistema”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de sistema com os seguintes campos: código, nome e descrição do sistema, senha do sistema, estado da conta do sistema (ativado ou inativado). Todos os campos são obrigatórios.
4 – Preenche as informações e escolhe a opção “incluir”.	
	5 – Gera um identificador interno sequencial e uma senha aleatória para o sistema e grava as informações do mesmo.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do sistema, código de identificação, nome do sistema, descrição do sistema, tipo do evento, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na inclusão do sistema.
Fluxo alternativo #1 (sistema já existe)	
	5 – Se já existir sistema com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir sistema com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar sistema	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a alteração de um sistema no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar sistema”.	
2 – Seleciona o sistema que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do sistema selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do sistema.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do sistema, código de identificação do sistema, nome do sistema, descrição do sistema, tipo do evento, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do sistema.
Fluxo alternativo #1 (sistema já existe)	
	6 – Se já existir sistema com o novo código informado, exibe mensagem de falha na alteração pelo motivo de já existir sistema com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na alteração pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (foi gerada uma nova senha)	
	6 – Se uma nova senha foi gerada, envia esta nova senha para os administradores do sistema e volta para o passo 6 do fluxo básico.

Caso de uso: excluir sistema	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de um sistema no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar sistema”.	
2 – Seleciona o sistema que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o sistema selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do sistema, código do sistema, nome do sistema, descrição do sistema, estado, tipo do evento, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do sistema.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar sistema	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de sistemas no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “básico > sistemas”.	
	2 – Exibe a tela contendo os sistemas cadastrados.
Fluxo alternativo #1 (não existem sistemas cadastrados)	
	2 – Exibe mensagem informando que não existem sistemas cadastrados.

Caso de uso: conectar ao serviço de segurança	
Autor(es)	Sistema cliente
Descrição	Este caso de uso descreve o funcionamento de conexão de um sistema cliente no serviço de segurança do Framework de Segurança.
Pré-condições	O ator deverá não estar conectado.
Fluxo básico	
Autor	Sistema
1 – Informa o código e a senha do sistema.	
	2 – Valida os dados informados.
	3 – Grava um histórico do evento contendo os seguintes dados: identificador interno do sistema, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	4 – Guarda sistema conectado na sessão.
Fluxo alternativo #1 (não existe sistema com o código informado)	
	2 – Exibe mensagem informando que as credenciais são inválidas.
Fluxo alternativo #2 (senha informada é inválida)	
	2 – Exibe mensagem informando que as credenciais são inválidas.

Caso de uso: desconectar do serviço de segurança	
Autor(es)	Sistema cliente
Descrição	Este caso de uso descreve o funcionamento de desconexão de um sistema cliente do serviço de segurança do Framework de Segurança.
Pré-condições	O ator deverá estar conectado.
Fluxo básico	
Autor	Sistema
1 – Seleciona a opção “desconectar”.	
	2 – Grava um histórico do evento contendo os seguintes dados: identificador interno do sistema, tipo do evento, identificador interno do evento, data do evento e observação sobre o evento.
	3 – Remove sistema conectado da sessão.

Caso de uso: incluir usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a inclusão de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de usuário com os campos: login, nome, estado (ativado ou inativado) e e-mail. Os campos login, nome, estado e e-mail são obrigatórios.
4 – Preenche os campos.	
5 – Seleciona a opção “incluir”.	
	6 – Gera um identificador sequencial interno para o usuário, grava no banco os dados informados e envia a senha para o e-mail do usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, login do usuário, nome do usuário, estado do usuário, e-mail do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na inclusão do usuário.
Fluxo alternativo #1 (usuário já existe)	
	6 – Se já existir um usuário cadastrado com o login informado, exibe mensagem de falha na inclusão pelo motivo de já existir um usuário com o login informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (campo e-mail preenchido com valor incorreto)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	6 – Se o campo e-mail não foi preenchido corretamente, exibe mensagem de falha na inclusão pelo motivo de o campo e-mail não possuir um valor válido.
--	---

Caso de uso: alterar usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a alteração de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar usuário”.	
2 – Seleciona o usuário que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do usuário selecionado para edição. A senha informada anteriormente não será exibida.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, login do usuário, nome do usuário, estado do usuário, e-mail do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do usuário.
Fluxo alternativo #1 (usuário já existe)	
	6 – Se já existir um usuário cadastrado com o login informado, exibe mensagem de falha na inclusão pelo motivo de já existir um usuário com o login informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (campo e-mail preenchido com valor incorreto)	
	6 – Se o campo e-mail não foi preenchido corretamente, exibe mensagem de falha na inclusão pelo motivo de o campo e-mail não possuir um valor válido.

Caso de uso: excluir usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de um usuário do Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar usuário”.	
2 – Seleciona o usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o usuário selecionado e todos os seus relacionamentos.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do usuário, login do usuário, nome do usuário, estado do usuário, e-mail do usuário, validade do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”	
	6 - Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar usuário	
Autor(es)	Administrador de segurança Usuário Gestor
Descrição	Este caso de uso descreve a consulta de usuário do Framework de Segurança.
Pré-condições	Não possui.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “básico > usuários”	2 – Exibe a tela contendo os usuários cadastrados.
Fluxo alternativo #1 (não existem usuários cadastrados)	
	2 – Exibe mensagem informando que não existem usuários cadastrados.

Caso de uso: incluir tipo de recurso	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a inclusão de um tipo de recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar tipo de recurso”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de tipo de recurso com os campos: código, nome e descrição. Os campos código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o tipo de recurso e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do tipo de recurso, código do tipo de recurso, nome do tipo de recurso, descrição do tipo de recurso, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na inclusão do tipo de recurso.
Fluxo alternativo #1 (tipo de recurso já existe)	
	5 – Se já existir um tipo de recurso cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um tipo de recurso com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar tipo de recurso	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a alteração de um tipo de recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar tipo de recurso”.	
2 – Seleciona o tipo de recurso que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do tipo de recurso selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do tipo de recurso.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do tipo de recurso, código do tipo de recurso, nome do tipo de recurso, descrição do tipo de recurso, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do tipo de recurso.
Fluxo alternativo #1 (tipo de recurso já existe)	
	6 – Se já existir um tipo de recurso cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um tipo de recurso com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na alteração pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir tipo de recurso	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de um tipo de recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar tipo de recurso”.	
2 – Seleciona o tipo de recurso que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o tipo de recurso selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do tipo de recurso, código do tipo de recurso, nome do tipo de recurso, descrição do tipo de recurso, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do tipo de recurso.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem recursos do tipo selecionado)	
	6 – Se já existir algum recurso do mesmo tipo do selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum recurso do tipo do selecionado para exclusão.

Caso de uso: consultar tipo de recurso	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de tipos de recursos no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “básico > tipos de recursos”.	
	2 – Exibe a tela contendo os tipos de recursos cadastrados.
Fluxo alternativo #1 (não existem tipos de recursos cadastrados)	
	2 – Exibe mensagem informando que não existem tipos de recursos cadastrados.

Caso de uso: incluir característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de uma característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar característica de usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de característica de usuário com os campos: código, nome e descrição. Os campos código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a característica do usuário e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da característica do usuário, código da característica do usuário, nome da característica do usuário, descrição da característica do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão da característica de usuário.
Fluxo alternativo #1 (característica de usuário já existe)	
	5 – Se já existir uma característica de usuário cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir uma característica de usuário com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de uma característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar característica de usuário”.	
2 – Seleciona a característica de usuário que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados da característica do usuário selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da característica do usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da característica do usuário, código da característica do usuário, nome da característica do usuário, descrição da característica do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da característica do usuário.
Fluxo alternativo #1 (característica de usuário já existe)	
	6 – Se já existir uma característica de usuário cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir uma característica de usuário com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na alteração pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir característica de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de uma característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar característica de usuário”.	
2 – Seleciona a característica de usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a característica de usuário selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da característica de usuário, código da característica de usuário, nome da característica de usuário, descrição da característica de usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na exclusão da característica de usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem valores para característica de usuário selecionada)	
	6 – Se já existir algum valor para a característica de usuário selecionada para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum valor para a característica de usuário selecionada para exclusão.

Caso de uso: consultar característica de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “características”.	
	2 – Exibe a tela contendo as características de usuário cadastradas.
Fluxo alternativo #1 (não existem características de usuário cadastradas)	
	2 – Exibe mensagem informando que não existem características de usuário cadastradas.

Caso de uso: incluir valor de característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um valor de característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar valor de característica de usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de valor de característica de usuário com os campos: característica, código, nome e descrição. Os campos característica, código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o valor da característica do usuário e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno, código nome e descrição do valor da característica do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do valor da característica de usuário.
Fluxo alternativo #1 (valor da característica de usuário já existe)	
	5 – Se já existir um valor da característica de usuário cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um valor da característica de usuário com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar valor da característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um valor da característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar valor da característica de usuário”.	
2 – Seleciona o valor da característica de usuário que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do valor da característica do usuário selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do valor da característica do usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno, nova característica, novo código, novo nome e nova descrição do valor da característica do usuário alterada, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do valor da característica do usuário.
Fluxo alternativo #1 (valor da característica de usuário já existe)	
	6 – Se já existir um valor de característica de usuário cadastrado com o código informado para a característica selecionada, exibe mensagem de falha na alteração pelo motivo de já existir um valor de característica de usuário com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	6 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na alteração pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir valor da característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um valor da característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado. O ator deverá estar conectado ao sistema.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar valor da característica de usuário”.	
2 – Seleciona o valor da característica de usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o valor da característica de usuário selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno, característica, código, nome e descrição do valor da característica de usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na exclusão do valor da característica de usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar valor da característica de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de valor da característica de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado. O ator deverá estar conectado ao sistema.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “características > valores”.	
	2 – Exibe a tela contendo as características de usuário cadastradas.
3 – Seleciona uma das características de usuário cadastradas.	
	4 – Exibe a tela contendo os valores da característica de usuário selecionada.
Fluxo alternativo #1 (não existem características de usuário cadastradas)	
	2 – Exibe mensagem informando que não existem características de usuário cadastradas.
Fluxo alternativo #2 (não existem valores de características de usuário cadastradas)	
	2 – Exibe mensagem informando que não existem valores de características de usuário cadastradas para a característica de usuário selecionada.

Caso de uso: incluir papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um papel comum no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar papel comum”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de papel comum com os campos: código, nome, descrição e estado do papel comum (ativado ou desativado). Os campos código, nome e estado são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o papel comum e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, código do papel comum, nome do papel comum, descrição papel comum, estado do papel comum, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do papel comum.
Fluxo alternativo #1 (papel comum já existe)	
	5 – Se já existir um papel comum cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um papel comum com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um papel comum no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar papel comum”.	
2 – Seleciona o papel comum que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do papel comum selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do papel comum.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, código do papel comum, nome do papel comum, descrição papel comum, estado do papel comum, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do papel comum.
Fluxo alternativo #1 (papel comum já existe)	
	5 – Se já existir um papel comum cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um papel comum com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um papel comum no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar papel comum”.	
2 – Seleciona o papel comum que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o papel comum selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, código do papel comum, nome do papel comum, descrição do papel comum, estado do papel comum, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do papel comum.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem usuários com atribuição no papel comum selecionado)	
	6 – Se existir algum usuário com atribuição no papel comum selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum usuário com atribuição no papel comum selecionado para exclusão.
Fluxo alternativo #3 (existem permissões atribuídas ao papel comum selecionado)	
	6 – Se existir alguma permissão atribuída ao papel comum selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma permissão atribuída ao papel comum selecionado para exclusão.

Fluxo alternativo #4 (existem grupos com atribuição no papel comum selecionado)

	6 – Se existir algum grupo com atribuição no papel comum selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum grupo com atribuição no papel comum selecionado para exclusão.
--	---

Caso de uso: consultar papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de papéis comuns no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “papeis > papéis comuns”.	
	2 – Exibe a tela contendo os papéis comuns cadastrados.
Fluxo alternativo #1 (não existem papéis comuns cadastrados)	
	2 – Exibe mensagem informando que não existem papéis comuns cadastrados.

Caso de uso: incluir papel administrativo	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a inclusão de um papel administrativo no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar papel administrativo”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de papel administrativo com os campos: código, nome, descrição e estado do papel administrativo (ativado ou inativado). Os campos código, nome e estado são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	5 – Gera um identificador sequencial interno para o papel administrativo e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno, código, nome, descrição e estado do papel administrativo, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do papel administrativo.
Fluxo alternativo #1 (papel administrativo já existe)	
	5 – Se já existir um papel administrativo cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um papel administrativo com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar papel administrativo	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a alteração de um papel administrativo no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar papel administrativo”.	
2 – Seleciona o papel administrativo que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do papel administrativo selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do papel administrativo.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador, código, nome, descrição e estado do papel administrativo, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do papel administrativo.
Fluxo alternativo #1 (papel administrativo já existe)	
	5 – Se já existir um papel administrativo cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um papel administrativo com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir papel administrativo	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de um papel administrativo no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar papel administrativo”.	
2 – Seleciona o papel administrativo que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o papel administrativo selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno, código, nome, descrição e estado do papel administrativo, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do papel administrativo.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem usuários com atribuição no papel administrativo selecionado)	
	6 – Se existir algum usuário com atribuição no papel administrativo selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum usuário com atribuição no papel administrativo selecionado para exclusão.
Fluxo alternativo #3 (existem grupos com atribuição no administrativo comum selecionado)	
	6 – Se existir algum grupo com atribuição no papel administrativo selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum grupo com atribuição no papel administrativo selecionado para exclusão.

Caso de uso: consultar papel administrativo	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de papéis administrativos no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “papeis > papéis administrativos”.	
	2 – Exibe a tela contendo os papéis administrativos cadastrados.
Fluxo alternativo #1 (não existem papéis administrativos cadastrados)	
	2 – Exibe mensagem informando que não existem papéis administrativos cadastrados.

Caso de uso: incluir operação	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de uma operação no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar operação”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de operação com os campos: código, nome e descrição. Os campos código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a operação e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da operação, código da operação, nome da operação, descrição da operação, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão da operação.
Fluxo alternativo #1 (operação já existe)	
	5 – Se já existir uma operação cadastrada com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir uma operação com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar operação	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de uma operação no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar operação”.	
2 – Seleciona a operação que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados da operação selecionada para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da operação.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da operação, código da operação, nome da operação, descrição da operação, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da operação.
Fluxo alternativo #1 (operação já existe)	
	5 – Se já existir uma operação cadastrada com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir uma operação com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir operação	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de uma operação no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar operação”.	
2 – Seleciona a operação que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a operação selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador da operação, código da operação, nome da operação, descrição da operação, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na exclusão da operação.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem permissões para a operação selecionada)	
	6 – Se existir alguma permissão para a operação selecionada para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma permissão para a operação selecionada para exclusão.

Caso de uso: consultar operação	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de operações no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “mapeamentos > operações”.	
	2 – Exibe a tela contendo as operações cadastradas.
Fluxo alternativo #1 (não existem operações cadastradas)	
	2 – Exibe mensagem informando que não existem operações cadastradas.

Caso de uso: incluir recurso	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar recurso”.	
2 – Seleciona a opção “novo”.	3 – Exibe a tela de inclusão de recurso com os campos: código, nome, descrição, estado (ativado ou desativado), recurso pai e tipo do recurso. Os campos código, nome, estado e tipo são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o recurso e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do recurso, código do recurso, nome do recurso, descrição do recurso, tipo do recurso, recurso pai, estado do recurso, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do recurso.
Fluxo alternativo #1 (recurso já existe)	
	5 – Se já existir um recurso cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um recurso com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar recurso	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar recurso”.	
2 – Seleciona o recurso que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do recurso selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do recurso.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do recurso, código do recurso, nome do recurso, descrição recurso, estado do recurso, tipo do recurso, pai do recurso, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do recurso.
Fluxo alternativo #1 (recurso já existe)	
	5 – Se já existir um recurso cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um recurso com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir recurso	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um recurso no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar recurso”.	
2 – Seleciona o recurso que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o recurso selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do recurso, código do recurso, nome recurso, descrição do recurso, estado do recurso, tipo do recurso, recurso pai, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do recurso.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem recursos filhos do recurso selecionado)	
	6 – Se existir algum recurso, onde seu pai seja o recurso selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum recurso que possua como pai o recurso selecionado para exclusão.
Fluxo alternativo #3 (existem permissões com o recurso selecionado)	
	6 – Se existir alguma permissão com o recurso selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma permissão com o recurso selecionado para exclusão.

Caso de uso: consultar recurso	
Autor(es)	Administrador de segurança Administrador de sistema
Descrição	Este caso de uso descreve a consulta de recursos no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “mapeamentos > recursos”.	
	2 – Exibe a tela contendo os recursos cadastrados.
Fluxo alternativo #1 (não existem recursos cadastrados)	
	2 – Exibe mensagem informando que não existem recursos cadastrados.

Caso de uso: incluir permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de uma permissão no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar permissão”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de permissão com os campos: recurso, operação, estado (ativado ou desativado), “contextualizada”, “possui auditoria”. Todos os campos são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a permissão e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da permissão, recurso da permissão, operação da permissão, estado da permissão, atributo que indica se a permissão é contextualizada, atributo que indica se a permissão é auditada, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão da permissão.
Fluxo alternativo #1 (permissão já existe)	
	5 – Se já existir uma permissão cadastrada com o mesmo recurso e operação informados, exibe mensagem de falha na inclusão pelo motivo de já existir uma permissão com o mesmo recurso e operação informados.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de uma permissão no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar permissão”.	
2 – Seleciona a permissão que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados da permissão selecionada para edição. Os campos recurso e operação não estão disponíveis para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da permissão.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da permissão, recurso da permissão, operação da permissão, atributo que indica se a permissão é contextualizada, atributo que indica se a permissão é auditada, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da permissão.
Fluxo alternativo #1(campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de uma permissão no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar permissão”.	
2 – Seleciona a permissão que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a permissão selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador da permissão, recurso da permissão, operação da permissão, atributo que indica se a permissão é contextualizada, atributo que indica se a permissão é auditada, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da permissão.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem atribuições da permissão selecionada a papéis comuns)	
	6 – Se existir alguma atribuição da permissão selecionada para exclusão a algum papel comum, exibe mensagem de falha na exclusão pelo motivo de existir alguma atribuição da permissão selecionada para exclusão a algum papel comum.
Fluxo alternativo #3 (existe configuração de permissões conflitantes envolvendo a permissão selecionada)	

	6 – Se existir alguma configuração de permissões conflitantes envolvendo a permissão selecionada para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma configuração de permissões conflitantes envolvendo a permissão selecionada para exclusão.
<i>Fluxo alternativo #4 (existe configuração de permissões conflitantes envolvendo a permissão selecionada)</i>	
	6 – Se existir alguma configuração de permissões conflitantes envolvendo a permissão selecionada para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma configuração de permissões conflitantes envolvendo a permissão selecionada para exclusão.

Caso de uso: consultar permissão	
Autor(es)	Administrador de segurança Administrador de sistema
Descrição	Este caso de uso descreve a consulta de permissões no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “mapeamentos > permissões”.	
	2 – Exibe a tela contendo as permissões cadastradas.
Fluxo alternativo #1 (não existem permissões cadastradas)	
	2 – Exibe mensagem informando que não existem permissões cadastradas.

Caso de uso: incluir grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de grupo manual com os campos: código, nome, descrição e estado (ativado ou desativado). Os campos código, nome, estado são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	5 – Gera um identificador sequencial interno para o grupo manual e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo manual, código do grupo manual, nome do grupo manual, descrição do grupo manual, estado do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do grupo manual.
Fluxo alternativo #1 (grupo manual já existe)	
	5 – Se já existir um grupo manual cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um grupo manual com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar grupo manual”.	
2 – Seleciona o grupo manual que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do grupo manual selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do grupo manual.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo manual, código do grupo manual, nome do grupo manual, descrição grupo manual, estado do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do grupo manual.
Fluxo alternativo #1 (grupo manual já existe)	
	5 – Se já existir um grupo manual cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um grupo manual com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar grupo manual”.	
2 – Seleciona o grupo manual que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o grupo manual selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo manual, código do grupo manual, nome grupo manual, descrição do grupo manual, estado do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do grupo manual.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem usuários no grupo manual selecionado)	
	6 – Se existir algum usuário no grupo manual selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum usuário no grupo manual selecionado para exclusão.
Fluxo alternativo #3 (existem papéis atribuídos ao grupo manual selecionado)	
	6 – Se existir alguma papel (administrativo ou comum) atribuído ao grupo manual selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum papel atribuído ao grupo manual selecionado para exclusão.

Caso de uso: consultar grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de grupos manuais no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “grupos > grupos manuais”.	
	2 – Exibe a tela contendo os grupos manuais cadastrados.
Fluxo alternativo #1 (não existem grupos manuais cadastrados)	
	2 – Exibe mensagem informando que não existem grupos manuais cadastrados.

Caso de uso: incluir grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar grupo caracterizado”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de grupo caracterizado com os campos: código, nome, descrição e estado (ativado ou desativado). Os campos código, nome, estado são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o grupo caracterizado e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo manual, código do grupo caracterizado, nome do grupo caracterizado, descrição do grupo caracterizado, estado do grupo caracterizado, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do grupo caracterizado.
Fluxo alternativo #1 (grupo caracterizado já existe)	
	5 – Se já existir um grupo caracterizado cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um grupo caracterizado com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar grupo caracterizado”.	
2 – Seleciona o grupo caracterizado que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do grupo caracterizado selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do grupo caracterizado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo caracterizado, código do grupo caracterizado, nome do grupo caracterizado, descrição grupo caracterizado, estado do grupo caracterizado, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do grupo caracterizado.
Fluxo alternativo #1 (grupo caracterizado já existe)	
	5 – Se já existir um grupo caracterizado cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um grupo caracterizado com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar grupo caracterizado”.	
2 – Seleciona o grupo caracterizado que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o grupo caracterizado selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do grupo caracterizado, código do grupo caracterizado, nome grupo caracterizado, descrição do grupo caracterizado, estado do grupo caracterizado, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do grupo caracterizado.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem papéis atribuídos ao grupo caracterizado selecionado)	
	6 – Se existir alguma papel (administrativo ou comum) atribuído ao grupo caracterizado selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum papel atribuído ao grupo caracterizado selecionado para exclusão.

Caso de uso: consultar grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de grupos caracterizados no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “grupos > grupos caracterizados”.	
	2 – Exibe a tela contendo os grupos caracterizados cadastrados.
Fluxo alternativo #1 (não existem grupos caracterizados cadastrados)	
	2 – Exibe mensagem informando que não existem grupos caracterizados cadastrados.

Caso de uso: incluir característica em grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um valor de característica de usuário em um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar característica dos usuários de grupo caracterizado”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de valor de característica em grupo caracterizado com os campos: grupo caracterizado, valor da característica. Todos os campos são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno a nova caracterização do grupo caracterizado e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da caracterização, grupo caracterizado, valor da característica, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão da característica.
Fluxo alternativo #1 (grupo caracterizado já possui característica informada)	
	5 – Se o grupo caracterizado selecionado já possuir a característica selecionada, exibe mensagem de falha na inclusão pelo motivo de já existir a característica selecionada no grupo caracterizado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir característica em grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um valor de característica de usuário em um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar característica dos usuários de grupo caracterizado”.	
2 – Seleciona o valor da característica de usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	6 – Exclui o valor da característica de usuário do grupo caracterizado selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da caracterização, grupo caracterizado, valor da característica, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da característica.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: consultar característica dos usuários de grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta da característica dos usuários do grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “grupos > grupos caracterizados > características”.	
	2 – Exibe a tela contendo os grupos caracterizados cadastrados.
3 – Seleciona um dos grupos caracterizados exibidos.	
	4 – Exibe a característica dos usuários de grupo caracterizado.
Fluxo alternativo #1 (não existem grupos caracterizados cadastrados)	
	2 – Exibe mensagem informando que não existem grupos caracterizados cadastrados.
Fluxo alternativo #2 (não existem características dos usuários para o grupo caracterizado)	
	4 – Exibe mensagem informando que não existem características dos usuários do grupo caracterizado selecionado.

Caso de uso: adicionar valor da característica para usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a adição de um valor de característica para um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar valores de características dos usuários”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de adição de valores de características de usuários com os campos: usuário, característica e valor da característica. Todos os campos são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a adição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno, valor da característica e usuário da adição, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na adição do valor da característica para o usuário.
Fluxo alternativo #1 (valor da característica já adicionado para usuário)	
	5 – Se o usuário já possuir o valor da característica, exibe mensagem de falha na adição pelo motivo de já existir o valor da característica para o usuário informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: remover valor da característica de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a remoção de um valor de característica de usuário em um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar valores de características dos usuários”.	
2 – Seleciona o valor da característica de usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o valor da característica de usuário do grupo caracterizado selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da caracterização, grupo caracterizado, valor da característica, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da característica.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: consultar característica de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta das características dos usuários no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “básico > usuários > características”.	
	2 – Exibe a tela contendo as características dos usuários.
Fluxo alternativo #1 (não existem características de usuários)	
	2 – Exibe mensagem informando que não existem características de usuários.

Caso de uso: atribuir papel administrativo para usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a atribuição de papel administrativo para um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar atribuição de papel administrativo para usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de atribuição de papel administrativo para usuário com os campos: papel administrativo e usuário. Os campos papel administrativo e usuário são obrigatórios.
4 – Preenche os campos e escolhe a opção “atribuir”.	
	5 – Gera um identificador sequencial interno para a atribuição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel administrativo, identificador interno do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na atribuição de papel administrativo para usuário.
Fluxo alternativo #1 (usuário já possui atribuição ao papel administrativo)	
	5 – Se o usuário informado já possuir atribuição no papel administrativo, exibe mensagem de falha na atribuição pelo motivo de o usuário já possuir atribuição ao papel administrativo informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: revogar papel administrativo de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a revogação de papel administrativo de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar atribuição de papel administrativo para usuário”.	
2 – Seleciona a atribuição que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a atribuição do papel administrativo do usuário selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel administrativo, identificador interno do usuário, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação do papel administrativo do usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar atribuição de papel administrativo para usuário							
Autor(es)	Administrador de segurança						
Descrição	Este caso de uso descreve a consulta de atribuições de papéis administrativos para usuários no Framework de Segurança.						
Pré-condições	O ator deverá estar autenticado.						
Fluxo básico							
<table border="1"> <thead> <tr> <th>Autor</th><th>Sistema</th></tr> </thead> <tbody> <tr> <td>1 – Seleciona a opção “atribuições > papéis administrativos > usuários”.</td><td></td></tr> <tr> <td></td><td>2 – Exibe a tela contendo as atribuições de papéis administrativos para usuários.</td></tr> </tbody> </table>		Autor	Sistema	1 – Seleciona a opção “atribuições > papéis administrativos > usuários”.			2 – Exibe a tela contendo as atribuições de papéis administrativos para usuários.
Autor	Sistema						
1 – Seleciona a opção “atribuições > papéis administrativos > usuários”.							
	2 – Exibe a tela contendo as atribuições de papéis administrativos para usuários.						
Fluxo alternativo #1 (não existem atribuições de papéis administrativos para usuários)							
	2 – Exibe mensagem informando que não existem atribuições de papéis administrativos para usuários.						

Caso de uso: atribuir papel administrativo para grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atribuição de papel administrativo para um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel administrativo para grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de atribuição de papel administrativo para grupo manual com os campos: papel administrativo e grupo manual. Os campos papel administrativo e grupo manual são obrigatórios.
4 – Preenche os campos e escolhe a opção “atribuir”.	
	5 – Gera um identificador sequencial interno para a atribuição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel administrativo, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na atribuição de papel administrativo para grupo manual.
Fluxo alternativo #1 (grupo manual já possui atribuição ao papel administrativo)	
	5 – Se o grupo manual informado já possuir atribuição no papel administrativo, exibe mensagem de falha na atribuição pelo motivo de o grupo manual já possuir atribuição ao papel administrativo informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: revogar papel administrativo de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a revogação de papel administrativo de grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel administrativo para grupo manual”.	
2 – Seleciona a atribuição que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a atribuição do papel administrativo do grupo manual selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel administrativo, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação do papel administrativo do grupo manual.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar atribuição de papel administrativo para grupo manual	
Autor(es)	Administrador de segurança Administrador de sistema
Descrição	Este caso de uso descreve a consulta de atribuições de papéis administrativos para grupos manuais no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “atribuições > papéis administrativos > grupos manuais”.	
	2 – Exibe a tela contendo as atribuições de papéis administrativos para grupos manuais.
Fluxo alternativo #1 (não existem atribuições de papéis administrativos para grupos manuais)	
	2 – Exibe mensagem informando que não existem atribuições de papéis administrativos para grupos manuais.

Caso de uso: atribuir papel de administrador de segurança para usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a atribuição de papel de administrador de segurança para usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar atribuição de papel de administrador de segurança para usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de atribuição de papel de administrador de segurança para usuário com os campos: usuário e validade. O campo usuário é obrigatório.
4 – Preenche os campos e escolhe a opção “atribuir”.	
	5 – Gera um identificador sequencial interno para a atribuição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da atribuição, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na atribuição de papel de administrador para usuário.
Fluxo alternativo #1 (usuário já possui atribuição ao papel de administrador de segurança)	
	5 – Se o usuário informado já possuir atribuição no papel de administrador de segurança, exibe mensagem de falha na atribuição pelo motivo de o usuário já possuir atribuição ao papel de administrador de segurança.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: atualizar atribuição de papel de administrador de segurança de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a atualização da atribuição de papel de administrador de segurança de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel de administrador de segurança para usuário”.	
2 – Seleciona a atribuição que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados da atribuição de papel de administrador de segurança selecionada para edição, porém apenas o campo validade pode ser editado.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da atribuição de papel de administrador de segurança do usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da atribuição, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da atribuição de papel de administrador de segurança do usuário.

Caso de uso: revogar papel de administrador de segurança de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a revogação de papel de administrador de segurança de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel de administrador de segurança para usuário”.	
2 – Seleciona a atribuição que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a atribuição do papel de administrador de segurança do usuário selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da atribuição, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação do papel de administrador de segurança do usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar atribuição de papel de administrador de segurança do usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de atribuições de papéis de administrador de segurança para usuários no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Seleciona a opção “atribuições > papel de segurança > usuários”.	
	2 – Exibe a tela contendo as atribuições de papéis de administrador de segurança para usuários.
Fluxo alternativo #1 (não existem atribuições de papéis de administrador de segurança para usuários)	
	2 – Exibe mensagem informando que não existem atribuições de papéis de administrador de segurança para usuários.

Caso de uso: incluir conflito de permissões	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um conflito de permissões.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar conflito de permissões”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de conflito de permissões com os campos: permissão, permissão conflitante, nome e descrição, os campos permissão, permissão conflitante e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o conflito de permissões e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do conflito de permissões, identificador interno da permissão, identificador interno da permissão conflitante, nome e descrição do conflito, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do conflito de permissões.
Fluxo alternativo #1 (conflito de permissões já existe)	
	5 – Se já existir um conflito de permissões com as mesmas permissões informadas, exibe mensagem de falha na inclusão pelo motivo de já existir um conflito de permissões com as mesmas permissões informadas.
Fluxo alternativo #2 (já existem usuários com as duas permissões informadas)	
	5 – Se já existir algum usuário com as duas permissões informadas, exibe mensagem de falha na inclusão pelo motivo de já existir um usuário com o conflito que está sendo incluído.
Fluxo alternativo #3 (campo obrigatório não preenchido)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	<p>5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.</p>
--	---

Caso de uso: alterar conflito de permissões	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um conflito de permissões no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar conflito de permissões”.	
2 – Seleciona o conflito de permissões que deseja alterar.	
3 – Seleciona a opção “editar”.	4 – Exibe os dados do conflito de permissões selecionado para edição. Porém, apenas o nome e a descrição podem ser editados.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do conflito de permissões.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do conflito de permissões, identificador interno da permissão, identificador interno da permissão conflitante, nome e descrição do conflito, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do conflito de permissões.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na alteração pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir conflito de permissões	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um conflito de permissões no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar conflito de permissões”.	
2 – Seleciona o conflito de permissões que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o conflito de permissões selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do conflito de permissões, identificador interno da permissão, identificador interno da permissão conflitante, nome e descrição do conflito, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do conflito de permissões.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar conflito de permissões	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de conflitos de permissões no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “mapeamentos > conflito de permissões”.	
	2 – Exibe a tela contendo os conflitos de permissões cadastrados.
Fluxo alternativo #1 (não existem conflitos de permissões cadastrados)	
	2 – Exibe mensagem informando que não existem conflitos de permissões cadastrados.

Caso de uso: conceder permissão para papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a concessão de permissão para papel comum no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar concessão de permissão para papel comum”.	
2 – Seleciona a opção “nova”.	
	3 – Exibe a tela de concessão de permissão para papel comum com os campos: papel comum e permissão. Todos obrigatórios.
4 – Preenche os campos e escolhe a opção “conceder”.	
	5 – Gera um identificador sequencial interno para a concessão e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno da permissão, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na concessão de permissão para papel comum.
Fluxo alternativo #1 (papel comum já possui concessão na permissão)	
	5 – Se o papel comum informado já possuir concessão na permissão, exibe mensagem de falha na concessão pelo motivo de papel comum já possuir concessão na permissão informada.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (conflito de permissões)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	5 – Se existir algum usuário com atribuição ao papel comum e o mesmo possuir uma permissão que conflita com a permissão que se deseja conceder para o papel comum, exibe mensagem de falha.
--	---

Caso de uso: revogar permissão de papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a revogação de permissão de um papel comum no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar concessão de permissão para papel comum”.	
2 – Seleciona a concessão que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a concessão de permissão de papel comum selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno da permissão, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação da concessão de permissão de papel comum.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar concessão de permissão para papel comum	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de concessões de permissões para papéis comuns no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “concessões > não contextualizadas”.	
	2 – Exibe a tela contendo as concessões de permissões para papéis comuns.
Fluxo alternativo #1 (não existem concessões de permissões para papéis comuns)	
	2 – Exibe mensagem informando que não existem concessões de permissões para papéis comuns.

Caso de uso: atribuir papel comum para usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atribuição de papel comum para um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel comum para usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de atribuição de papel comum para usuário com os campos: papel comum, usuário e validade. Os campos papel comum e usuário são obrigatórios.
4 – Preenche os campos e escolhe a opção “atribuir”.	
	5 – Gera um identificador sequencial interno para a atribuição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na atribuição de papel comum para usuário.
Fluxo alternativo #1 (usuário já possui atribuição ao papel comum)	
	5 – Se o usuário informado já possuir atribuição no papel comum, exibe mensagem de falha na atribuição pelo motivo de o usuário já possuir atribuição ao papel comum informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (conflito de permissões)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	5 – Se o usuário já possuir atribuição em outro papel que possua concessão em alguma permissão que conflita com as permissões concedidas para o papel comum que está sendo atribuído, exibe mensagem de falha.
--	--

Caso de uso: atualizar atribuição de papel comum de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atualização da atribuição de papel comum de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel comum para usuário”.	
2 – Seleciona a atribuição que deseja alterar.	
3 – Seleciona a opção “editar”.	4 – Exibe os dados da atribuição de papel comum selecionada para edição, porém apenas o campo validade pode ser editado.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da atribuição de papel comum de usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da atribuição, identificador interno do papel comum, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da atribuição de papel comum do usuário.

Caso de uso: revogar papel comum de usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a revogação de papel comum de usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar atribuição de papel comum para usuário”.	
2 – Seleciona a atribuição que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a atribuição do papel comum do usuário selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação do papel comum do usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar atribuição de papel comum para usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de atribuições de papéis comuns para usuários no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “atribuições > papéis comuns > usuários”.	
	2 – Exibe a tela contendo as atribuições de papéis comuns para usuários.
Fluxo alternativo #1 (não existem atribuições de papéis comuns para usuários)	
	2 – Exibe mensagem informando que não existem atribuições de papéis comuns para usuários.

Caso de uso: atribuir papel comum para grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atribuição de papel comum para um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar atribuição de papel comum para grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de atribuição de papel comum para grupo manual com os campos: papel comum e grupo manual. Todos os campos são obrigatórios.
4 – Preenche os campos e escolhe a opção “atribuir”.	
	5 – Gera um identificador sequencial interno para a atribuição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na atribuição de papel comum para grupo manual.
Fluxo alternativo #1 (grupo manual já possui atribuição ao papel comum)	
	5 – Se o usuário informado já possuir atribuição no papel comum, exibe mensagem de falha na atribuição pelo motivo de o usuário já possuir atribuição ao papel comum informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na atribuição pelo motivo de não ter informado valor em um dos campos obrigatórios.
Fluxo alternativo #3 (conflito de permissões)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	5 – Se o grupo manual possui algum usuário com atribuição em outro papel que possua concessão em alguma permissão que conflita com as permissões concedidas para o papel comum que está sendo atribuído, exibe mensagem de falha.
--	---

Caso de uso: revogar papel comum de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a revogação de papel comum de grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar atribuição de papel comum para grupo manual”.	
2 – Seleciona a atribuição que deseja revogar.	
3 – Seleciona a opção “revogar”.	
	4 – Pede confirmação para iniciar a revogação.
5 – Seleciona a opção “confirmar”.	
	6 – Revoga a atribuição do papel comum do grupo manual selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do papel comum, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na revogação do papel comum do grupo manual.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar atribuição de papel comum para grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de atribuições de papéis comuns para grupos manuais no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “atribuições > papéis comuns > grupos manuais”.	
	2 – Exibe a tela contendo as atribuições de papéis comuns para grupos manuais.
Fluxo alternativo #1 (não existem atribuições de papéis comuns para grupos manuais)	
	2 – Exibe mensagem informando que não existem atribuições de papéis comuns para grupos manuais.

Caso de uso: adicionar membro em grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a adição de um membro em um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar membro do grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de adição de membro em grupo manual com os campos: grupo e usuário. Todos os campos obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a adição e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da adição, identificador interno do usuário, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na adição do membro no grupo manual.
Fluxo alternativo #1 (usuário já é membro do grupo manual)	
	5 – Se o usuário já é membro do grupo manual, exibe mensagem de falha na adição pelo motivo de o usuário já ser membro do grupo informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na adição pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: remover membro de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a remoção de um membro de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar membro do grupo manual”.	
2 – Seleciona o membro do grupo manual que deseja excluir.	
3 – Seleciona a opção “remover”.	
	4 – Pede confirmação para iniciar a remoção.
5 – Seleciona a opção “confirmar”.	
	6 – Remove o membro do grupo manual selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da adição, identificador interno do usuário, identificador interno do grupo manual, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na remoção do membro do grupo manual.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar membro do grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de membros dos grupos manuais no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “grupos > grupos manuais > membros”.	
	2 – Exibe a tela contendo os membros dos grupos manuais cadastrados.
Fluxo alternativo #1 (não existem membros dos grupos manuais cadastrados)	
	2 – Exibe mensagem informando que não existem membros dos grupos manuais cadastrados.

Caso de uso: incluir inativação de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a inclusão de uma inativação de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de inativação de usuário com os campos: usuário, motivo da inativação e validade. Os campos usuário e motivo são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a inativação e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na inclusão de inativação do usuário.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão da inativação pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: atualizar inativação de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a atualização da inativação de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de usuário”.	
2 – Seleciona a inativação que deseja alterar.	
3 – Seleciona a opção “editar”.	4 – Exibe os dados da inativação do usuário selecionada para edição, porém apenas o campo validade pode ser editado.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da inativação de usuário.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da inativação do usuário.

Caso de uso: excluir inativação de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a exclusão de uma inativação de um usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de usuário”.	
2 – Seleciona a inativação de usuário que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a inativação do usuário selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do usuário, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da inativação de usuário.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar inativação de usuário	
Autor(es)	Administrador de segurança
Descrição	Este caso de uso descreve a consulta de inativações de usuários no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “inativações > usuários”.	
	2 – Exibe a tela contendo as inativações de usuários cadastradas.
Fluxo alternativo #1 (não existem inativações de usuários cadastradas)	
	2 – Exibe mensagem informando que não existem inativações de usuários cadastradas.

Caso de uso: incluir inativação de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de uma inativação de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de inativação de grupo manual com os campos: grupo manual, motivo da inativação e validade. Os campos grupo manual e motivo são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a inativação e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo manual, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na inclusão de inativação do grupo manual.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão da inativação pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: atualizar inativação de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atualização da inativação de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo manual”.	
2 – Seleciona a inativação que deseja alterar.	
3 – Seleciona a opção “editar”.	4 – Exibe os dados da inativação do grupo manual selecionada para edição, porém apenas o campo validade pode ser editado.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da inativação de grupo manual.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo manual, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da inativação do grupo manual.

Caso de uso: excluir inativação de grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de uma inativação de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo manual”.	
2 – Seleciona a inativação de grupo manual que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a inativação do grupo manual selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo manual, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da inativação de grupo manual.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar inativação de grupo manual							
Autor(es)	Administrador de sistema						
Descrição	Este caso de uso descreve a consulta de inativações de grupos manuais no Framework de Segurança.						
Pré-condições	O ator deverá estar autenticado.						
Fluxo básico							
<table border="1"> <thead> <tr> <th>Autor</th><th>Sistema</th></tr> </thead> <tbody> <tr> <td>1 – Seleciona a opção “inativações > grupos manuais”.</td><td></td></tr> <tr> <td></td><td>2 – Exibe a tela contendo as inativações de grupos manuais cadastradas.</td></tr> </tbody> </table>		Autor	Sistema	1 – Seleciona a opção “inativações > grupos manuais”.			2 – Exibe a tela contendo as inativações de grupos manuais cadastradas.
Autor	Sistema						
1 – Seleciona a opção “inativações > grupos manuais”.							
	2 – Exibe a tela contendo as inativações de grupos manuais cadastradas.						
Fluxo alternativo #1 (não existem inativações de grupos manuais cadastradas)							
	2 – Exibe mensagem informando que não existem inativações de grupos manuais cadastradas.						

Caso de uso: incluir inativação de grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de uma inativação de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo caracterizado”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de inativação de caracterizado com os campos: grupo caracterizado, motivo da inativação e validade. Os campos grupo caracterizado e motivo são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a inativação e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo caracterizado, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na inclusão de inativação do grupo caracterizado.
Fluxo alternativo #1 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão da inativação pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: atualizar inativação de grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a atualização da inativação de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo caracterizado”.	
2 – Seleciona a inativação que deseja alterar.	
3 – Seleciona a opção “editar”.	4 – Exibe os dados da inativação do grupo caracterizado selecionada para edição, porém apenas o campo validade pode ser editado.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações da inativação de grupo caracterizado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo caracterizado, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração da inativação do grupo caracterizado.

Caso de uso: excluir inativação de grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de uma inativação de um grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar inativação de grupo caracterizado”.	
2 – Seleciona a inativação de grupo caracterizado que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui a inativação do grupo caracterizado selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da inativação, identificador interno do grupo caracterizado, identificador interno da validade, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão da inativação de grupo caracterizado.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar inativação de grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de inativações de grupos caracterizados no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “inativações > grupos caracterizados”.	
	2 – Exibe a tela contendo as inativações de grupos caracterizados cadastradas.
Fluxo alternativo #1 (não existem inativações de grupos caracterizados cadastradas)	
	2 – Exibe mensagem informando que não existem inativações de grupos caracterizados cadastradas.

Caso de uso: incluir contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um contexto no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar contexto”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de contexto com os campos: código, nome, descrição. Os campos código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o contexto e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno do contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do contexto.
Fluxo alternativo #1 (contexto já existe)	
	5 – Se já existir um contexto cadastrado com o código informado, exibe mensagem de falha na inclusão pelo motivo de já existir um contexto com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar contexto”.	
2 – Seleciona o contexto que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do contexto selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do contexto.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do contexto.
Fluxo alternativo #1 (contexto já existe)	
	5 – Se já existir um contexto cadastrado com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um contexto com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um contexto no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar contexto”.	
2 – Seleciona o contexto que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o contexto selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno do contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do contexto.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem valores de contexto para o contexto selecionado)	
	6 – Se existir algum valor de contexto para o contexto selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir algum valor de contexto para o contexto selecionado para exclusão.
Fluxo alternativo #3 (existem permissões contextualizadas com o contexto selecionado)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	<p>6 – Se existir alguma permissão contextualizada com o contexto selecionado para exclusão, exibe mensagem de falha na exclusão pelo motivo de existir alguma permissão contextualizada que depende do contexto selecionado para exclusão.</p>
--	---

Caso de uso: consultar contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de contextos no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “contextos”.	
	2 – Exibe a tela contendo os contextos cadastrados.
Fluxo alternativo #1 (não existem contextos cadastrados)	
	2 – Exibe mensagem informando que não existem contextos cadastrados.

Caso de uso: incluir valor de contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a inclusão de um valor de contexto no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar valor de contexto”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de inclusão de valor de contexto com os campos: contexto, código do valor do contexto, nome do valor do contexto, descrição do valor do contexto. Os campos contexto, código e nome são obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para o valor de contexto e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno valor do contexto, contexto do valor de contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	7 – Exibe mensagem de sucesso na inclusão do valor de contexto.
Fluxo alternativo #1 (valor de contexto já existe)	
	5 – Se já existir um valor de contexto cadastrado com o código para o contexto informado, exibe mensagem de falha na inclusão pelo motivo de já existir um valor de contexto com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: alterar valor de contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a alteração de um valor de no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar valor de contexto”.	
2 – Seleciona o valor de contexto que deseja alterar.	
3 – Seleciona a opção “editar”.	
	4 – Exibe os dados do valor de contexto selecionado para edição.
5 – Edita os dados e seleciona a opção “atualizar”.	
	6 – Grava as novas informações do valor de contexto.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno valor do contexto, contexto do valor de contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na alteração do valor do contexto.
Fluxo alternativo #1 (valor do contexto já existe)	
	5 – Se já existir um valor de contexto cadastrado para o contexto com o código informado, exibe mensagem de falha na alteração pelo motivo de já existir um valor de contexto com o código informado.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: excluir valor de contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a exclusão de um valor de contexto no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar valor de contexto”.	
2 – Seleciona o valor de contexto que deseja excluir.	
3 – Seleciona a opção “excluir”.	
	4 – Pede confirmação para iniciar a exclusão.
5 – Seleciona a opção “confirmar”.	
	6 – Exclui o valor de contexto selecionado.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno valor do contexto, contexto do valor de contexto, código do contexto, nome do contexto, descrição do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na exclusão do valor de contexto.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.
Fluxo alternativo #2 (existem atribuições contextualizadas com o valor de contexto)	
	6 – Se existir alguma atribuição de papel comum para usuário, grupo manual ou caracterizado e está for contextualizada com o valor de contexto selecionado para exclusão, exibe mensagem de falha na exclusão.

Caso de uso: consultar valor de contexto	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de valores de contextos no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	
1 – Seleciona a opção “contextos > valores”.	
	2 – Exibe a tela contendo os valores de contextos cadastrados.
Fluxo alternativo #1 (não existem valores de contextos cadastrados)	
	2 – Exibe mensagem informando que não existem valores de contextos cadastrados.

Caso de uso: contextualizar atribuição de papel comum para usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a contextualização de uma atribuição de papel comum para usuário.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para usuário”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de contextualização de atribuição de papel comum para usuário com os campos: atribuição de papel comum para usuário, concessão de permissão para papel comum e valor de contexto. Todos os campos obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a contextualização e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para usuário, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na contextualização de atribuição de papel comum para usuário.
Fluxo alternativo #1 (contextualização já existe)	
	5 – Se já existir uma contextualização cadastrada com os valores informados, exibe mensagem de erro na inclusão.
Fluxo alternativo #2 (campo obrigatório não preenchido)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	<p>5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.</p>
--	---

Caso de uso: remover contextualização de atribuição de papel comum para usuário	
Fluxo básico	
Ator(es)	Administrador de sistema
Descrição	Este caso de uso descreve a remoção de uma contextualização de atribuição de papel comum para usuário no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Ator	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para usuário”.	
2 – Seleciona a contextualização que deseja excluir.	
3 – Seleciona a opção “remover”.	
	4 – Pede confirmação para iniciar a remoção.
5 – Seleciona a opção “confirmar”.	
	6 – Remove a contextualização selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para usuário, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na remoção da contextualização.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar contextualização de atribuição de papel comum para usuário	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de contextualizações de atribuições de papéis comuns para usuários no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Seleciona a opção “atribuições > papéis comuns > usuários > contextualizadas”.	
	2 – Exibe a tela contendo as contextualizações de atribuições de papéis comuns para usuários cadastradas.
Fluxo alternativo #1 (não existem contextualizações cadastradas)	
	2 – Exibe mensagem informando que não existem contextualizações cadastradas.

Caso de uso: contextualizar atribuição de papel comum para grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a contextualização de uma atribuição de papel comum para grupo manual.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para grupo manual”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de contextualização de atribuição de papel comum para grupo manual com os campos: atribuição de papel comum para grupo manual, concessão de permissão para papel comum e valor de contexto. Todos os campos obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a contextualização e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para grupo manual, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na contextualização de atribuição de papel comum para grupo manual.
Fluxo alternativo #1 (contextualização já existe)	
	5 – Se já existir uma contextualização cadastrada com os valores informados, exibe mensagem de erro na inclusão.
Fluxo alternativo #2 (campo obrigatório não preenchido)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.
--	--

Caso de uso: remover contextualização de atribuição de papel comum para grupo manual	
Fluxo básico	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a remoção de uma contextualização de atribuição de papel comum para grupo manual no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Autor	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para grupo manual”.	
2 – Seleciona a contextualização que deseja excluir.	
3 – Seleciona a opção “remover”.	
	4 – Pede confirmação para iniciar a remoção.
5 – Seleciona a opção “confirmar”.	
	6 – Remove a contextualização selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para grupo manual, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na remoção da contextualização.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar contextualização de atribuição de papel comum para grupo manual	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de contextualizações de atribuições de papéis comuns para grupos manuais no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “atribuições > papéis comuns > grupos manuais > contextualizadas”.	
	2 – Exibe a tela contendo as contextualizações de atribuições de papéis comuns para grupos manuais cadastradas.
Fluxo alternativo #1 (não existem contextualizações cadastradas)	
	2 – Exibe mensagem informando que não existem contextualizações cadastradas.

Caso de uso: contextualizar atribuição de papel comum para grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a contextualização de uma atribuição de papel comum para grupo caracterizado.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para grupo caracterizado”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de contextualização de atribuição de papel comum para grupo manual com os campos: atribuição de papel comum para grupo caracterizado, concessão de permissão para papel comum e valor de contexto. Todos os campos obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a contextualização e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para grupo caracterizado, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na contextualização de atribuição de papel comum para grupo caracterizado.
Fluxo alternativo #1 (contextualização já existe)	
	5 – Se já existir uma contextualização cadastrada com os valores informados, exibe mensagem de erro na inclusão.
Fluxo alternativo #2 (campo obrigatório não preenchido)	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.
--	--

Caso de uso: remover contextualização de atribuição de papel comum para grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a remoção de uma contextualização de atribuição de papel comum para grupo caracterizado no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar contextualização de papel comum para grupo caracterizado”.	
2 – Seleciona a contextualização que deseja excluir.	
3 – Seleciona a opção “remover”.	
	4 – Pede confirmação para iniciar a remoção.
5 – Seleciona a opção “confirmar”.	
	6 – Remove a contextualização selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da atribuição de papel comum para grupo caracterizado, identificador interno da concessão de permissão para papel comum e valor de contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na remoção da contextualização.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar contextualização de atribuição de papel comum para grupo caracterizado	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de contextualizações de atribuições de papéis comuns para grupos caracterizados no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Seleciona a opção “atribuições > papéis comuns > grupos caracterizados > contextualizadas”.	
	2 – Exibe a tela contendo as contextualizações de atribuições de papéis comuns para grupos caracterizados cadastradas.
Fluxo alternativo #1 (não existem contextualizações cadastradas)	
	2 – Exibe mensagem informando que não existem contextualizações cadastradas.

Caso de uso: contextualizar permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a contextualização de uma permissão.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Executa o caso de uso “consultar contextualização da permissão”.	
2 – Seleciona a opção “novo”.	
	3 – Exibe a tela de contextualização da permissão com os campos: permissão e contexto. Todos os campos obrigatórios.
4 – Preenche os campos e escolhe a opção “incluir”.	
	5 – Gera um identificador sequencial interno para a contextualização e grava no banco os dados informados.
	6 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da permissão, identificador interno do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	9 – Exibe mensagem de sucesso na contextualização da permissão.
Fluxo alternativo #1 (contextualização já existe)	
	5 – Se já existir uma contextualização cadastrada com os valores informados, exibe mensagem de erro na inclusão.
Fluxo alternativo #2 (campo obrigatório não preenchido)	
	5 – Se um dos campos obrigatórios não foi informado, exibe mensagem de falha na inclusão pelo motivo de não ter informado valor em um dos campos obrigatórios.

Caso de uso: remover contextualização da permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a remoção de uma permissão no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Executa o caso de uso “consultar contextualização da permissão”.	
2 – Seleciona a contextualização que deseja excluir.	
3 – Seleciona a opção “remover”.	
	4 – Pede confirmação para iniciar a remoção.
5 – Seleciona a opção “confirmar”.	
	6 – Remove a contextualização selecionada.
	7 – Grava um histórico do evento contendo os seguintes dados: identificador interno da contextualização, identificador interno da permissão, identificador interno do contexto, identificador interno do evento, data do evento, autor do evento e observação sobre o evento.
	8 – Exibe mensagem de sucesso na remoção da contextualização.
Fluxo alternativo #1 (ator não confirma a exclusão)	
5 – Seleciona a opção “cancelar”.	
	6 – Retorna para o passo 1 do fluxo básico.

Caso de uso: consultar contextualização da permissão	
Autor(es)	Administrador de sistema
Descrição	Este caso de uso descreve a consulta de contextualizações das permissões no Framework de Segurança.
Pré-condições	O ator deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Seleciona a opção “concessões > contextualizadas”.	
	2 – Exibe a tela contendo as contextualizações das permissões cadastradas.
Fluxo alternativo #1 (não existem contextualizações cadastradas)	
	2 – Exibe mensagem informando que não existem contextualizações cadastradas.

Caso de uso: verificar autorização de usuário em permissão	
Autor(es)	Sistema cliente
Descrição	Este caso de uso descreve a verificação de autorização de um usuário em permissão no Framework de Segurança.
Pré-condições	O ator deverá estar conectado. O usuário deverá estar autenticado.
Fluxo básico	
Ator	Sistema
1 – Informa o recurso, a operação e usuário autenticado.	
2 – Executa a funcionalidade de verificação de autorização de usuário em permissão.	
	3 – Verifica a autorização do usuário na permissão informada.
	4 – Retorna o resultado da verificação.
Fluxo alternativo #1 (usuário está inativado)	
	3 – Exibe mensagem informando que o usuário está inativado.

Caso de uso: verificar autorização de usuário em permissão contextualizada	
Autor(es)	Sistema cliente
Descrição	Este caso de uso descreve a verificação de autorização de um usuário em permissão contextualizada no Framework de Segurança.
Pré-condições	O ator deverá estar conectado. O usuário deverá estar autenticado.
Fluxo básico	
Autor	Sistema
1 – Informa o recurso, a operação, o usuário autenticado e o contexto da execução.	
2 – Executa a funcionalidade de verificação de autorização de usuário em permissão.	
	3 – Verifica a autorização do usuário na permissão informada baseado no contexto de execução.
	4 – Retorna o resultado da verificação.
Fluxo alternativo #1 (usuário está inativado)	
	3 – Exibe mensagem informando que o usuário está inativado.

2.2.3. DESCRIÇÃO DOS ATORES

Um ator, de acordo com a UML é toda entidade externa que interage com o sistema, sendo ela uma pessoa, um hardware ou até outro sistema. Segue abaixo a descrição dos atores especificados no Diagrama de Casos de Uso:

- Usuário

Refere-se a qualquer pessoa que interaja com o sistema.

- Administrador de Segurança

Refere-se a um Usuário responsável pelo Framework de Segurança. Suas funções são realizar as operações básicas necessárias para o funcionamento da ferramenta.

- Administrador de Sistema

Refere-se a um Usuário responsável pela configuração de um Sistema Cliente, como definição dos recursos e operações existentes no sistema, papéis comuns, grupos etc.

- Sistema Cliente

Refere-se a qualquer sistema que utilize o serviço de segurança provido pelo Framework.

2.2.4. DESCRIÇÃO DOS ATRIBUTOS DAS CLASSES

Classe	SISTEMA
Descrição	Sistema que utiliza o Framework de Segurança.
Atributos	Código, nome e conta.
Volume inicial	Zero.
Taxa de crescimento	50 por ano

Classe	CONTA DO SISTEMA
Descrição	Conta do sistema.
Atributos	Senha e ativada.
Volume inicial	Zero.
Taxa de crescimento	50 por ano

Classe	USUÁRIO
Descrição	Usuário dos sistemas.
Atributos	Nome e conta.
Volume inicial	Um.
Taxa de crescimento	400/ano.

Classe	CONTA DO USUÁRIO
Descrição	Conta do usuário.
Atributos	Login, senha, ativada e e-mail.
Volume inicial	Um.
Taxa de crescimento	400/ano.

Classe	INATIVADA
Descrição	Configuração de inatividade de um usuário ou grupo.
Atributos	Motivo e validade.
Volume inicial	Um.
Taxa de crescimento	600/ano.

Classe	VALIDADE
Descrição	Configuração de validade de uma inativação ou atribuição.
Atributos	Início e término.
Volume inicial	Um.
Taxa de crescimento	600/ano.

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Classe	TIPO DE RECURSO
Descrição	Tipos que um recurso pode assumir.
Atributos	Código, nome e descrição.
Volume inicial	Zero.
Taxa de crescimento	300/ano.

Classe	RECURSO
Descrição	Qualquer recurso que possa ser controlado em um sistema.
Atributos	Código, nome, descrição, ativado, pai, tipo e sistema.
Volume inicial	Zero.
Taxa de crescimento	300/ano.

Classe	OPERAÇÃO
Descrição	Qualquer operação que possa ser realizada em um recurso de um sistema.
Atributos	Código, nome, descrição e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	PERMISSÃO
Descrição	É o relacionamento entre o recurso e a operação.
Atributos	Recurso, operação auditável, contextualizada e ativada.
Volume inicial	Zero.
Taxa de crescimento	400/ano.

Classe	CONFLITO DE PERMISSÕES
Descrição	É uma configuração que impede que um mesmo usuário possua autorização em permissões conflitantes.
Atributos	Permissão, permissão conflitante, nome e descrição.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	PAPEL
Descrição	Agrupamento de permissões concedidas.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	400/ano.

Classe	PAPEL ADMINISTRATIVO
Descrição	Uma especificação de papel. É um papel que tem concessão em qualquer permissão do sistema.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	PAPEL COMUM
Descrição	Uma especificação de papel. É um papel que para ter concessão em uma permissão do sistema, precisa estar relacionado com ela.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	GRUPO
Descrição	Agrupamento de usuários.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	400/ano.

Classe	GRUPO MANUAL
Descrição	Uma especificação de grupo. É um grupo onde os usuários para serem considerados membros devem ser adicionados manualmente por um administrador de sistema.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	GRUPO CARACTERIZADO
Descrição	Uma especificação de grupo. É um grupo onde os usuários para serem considerados membros devem possuir as mesmas características que descrevem o grupo caracterizado.
Atributos	Código, nome, descrição, ativado e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	CARACTERÍSTICA
Descrição	Representa a característica de um usuário.
Atributos	Código, nome, descrição e sistema.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	VALOR DA CARACTERÍSTICA
Descrição	Valor que uma característica de um usuário pode assumir.
Atributos	Código, nome, descrição e característica.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	CONTEXTO
Descrição	Contexto onde uma permissão contextualizada pode ser inserida.
Atributos	Código, nome, descrição e sistema.
Volume inicial	Zero.
Taxa de crescimento	200/ano.

Classe	VALOR DO CONTEXTO
Descrição	Valor que um contexto pode assumir.
Atributos	Código, nome, descrição e contexto.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO
Descrição	Representa a atribuição de um papel comum para um usuário.
Atributos	Papel comum e usuário.
Volume inicial	Zero.
Taxa de crescimento	600/ano.

Classe	CONCESSÃO DE PERMISSÃO PARA PAPEL COMUM
Descrição	Representa a concessão de uma permissão para um papel comum.
Atributos	Papel comum e permissão
Volume inicial	Zero.
Taxa de crescimento	600/ano.

Classe	CONTEXTUALIZAÇÃO DE ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO
Descrição	Contextualização de uma atribuição e papel comum para um usuário.
Atributos	Atribuição de papel comum para usuário, valor do contexto e atribuição de permissão para papel comum.
Volume inicial	Zero.
Taxa de crescimento	300/ano.

Classe	ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO
Descrição	Representa a atribuição de um papel comum para um grupo.
Atributos	Papel comum e grupo.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA USUÁRIO
Descrição	Representa a atribuição de um papel administrativo para um usuário.
Atributos	Papel administrativo, usuário e validade.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA GRUPO
Descrição	Representa a atribuição de um papel administrativo para um grupo.
Atributos	Papel administrativo, grupo e validade.
Volume inicial	Zero.
Taxa de crescimento	100/ano.

Classe	ATRIBUIÇÃO DE PAPEL DE ADMINISTRADOR DE SEGURANÇA PARA USUÁRIO
Descrição	Representa a atribuição de um papel de administrador de segurança para um usuário.
Atributos	Usuário e validade.
Volume inicial	Um.
Taxa de crescimento	5/ano.

Classe	ATRIBUIÇÃO DE PAPEL DE ADMINISTRADOR DE SEGURANÇA PARA USUÁRIO
Descrição	Representa a atribuição de um papel de administrador de segurança para um usuário.
Atributos	Usuário e validade.
Volume inicial	Um.
Taxa de crescimento	50/ano.

2.2.5. PROJETO DE INTERFACES

A seguir encontram-se as telas que mostram o padrão da interface adotada para o console administrativo do Framework de Segurança.

Tela	Boas vindas
Objetivo	Ser a tela de boas vindas para qualquer usuário que acesse o sistema.
Usuários atingidos	Todos os usuários do sistema.
Frequência de uso	Toda vez que o usuário for acessar o sistema.

[ALTERAR SENHA] [ENTRAR]

Framework de Segurança

Bem vindo ao Framework de Segurança

O Framework de Segurança é um software de reuso utilizado como ferramenta para autenticar, autorizar e auditar qualquer sistema corporativo.

Ele funciona como um serviço centralizado onde os demais sistemas se conectam a ele para verificar a autenticidade e as permissões de seus usuários.

Tela	Autenticação
Objetivo	Permitir que o usuário se autentique no console administrativo.
Usuários atingidos	Administradores de segurança e sistemas.
Frequência de uso	Toda vez que o usuário precisar acessar o console administrativo.

[ALTERAR SENHA] [ENTRAR]

Framework de Segurança

Autenticação

Login*:

Senha*:

Sistema:

[Esqueci minha senha]

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Esqueci senha
Objetivo	Permitir que o usuário solicite uma nova senha.
Usuários atingidos	Todos os usuários do sistema.
Frequência de uso	Toda vez que o usuário esquecer sua senha e precisar solicitar uma nova.

The screenshot shows a web page titled "Framework de Segurança". At the top right are links for "ALTERAR SENHA" and "ENTRAR". Below the title is a blue header bar with a lock icon and two user icons. The main content area has a green header "Esqueceu sua senha?". A green box contains the text: "Clicando no botão enviar, uma confirmação será enviada para seu e-mail. Siga as instruções contidas nele para gerar uma nova senha.". Below this is a form with a "Login*" input field and a "Enviar" button.

Tela	Alterar senha
Objetivo	Permitir que o usuário altere sua senha.
Usuários atingidos	Todos os usuários do sistema.
Frequência de uso	Toda vez que o usuário precisar alterar sua senha.

The screenshot shows a web page titled "Framework de Segurança". At the top right are links for "ALTERAR SENHA" and "ENTRAR". Below the title is a blue header bar with a lock icon and two user icons. The main content area has a green header "Alterar senha". A form with four input fields: "Login*", "Senha atual*", "Nova senha*", and "Confirme*". Below the form is a "Alterar" button.

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Cadastro de sistema
Objetivo	Cadastrar sistemas.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que um novo sistema cliente começar a utilizar o Framework de Segurança.

[PHELIPE PERBORES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

Incluir Sistema	
Básico	→
Papéis	→
Atribuições	→
Inativações	→
<input type="text"/> Código*: <input type="text"/> <input type="text"/> Nome*: <input type="text"/> <input type="text"/> Senha*: <input type="text"/> <input type="checkbox"/> Ativado*: <input type="checkbox"/> <input type="button" value="Incluir"/>	

Tela	Cadastro de usuário
Objetivo	Cadastrar usuários.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que um novo funcionário entrar na empresa.

[PHELIPE PERBORES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

Incluir Usuário	
Básico	→
Papéis	→
Atribuições	→
Inativações	→
<input type="text"/> Nome*: <input type="text"/> <input type="text"/> Login*: <input type="text"/> <input type="text"/> Senha*: <input type="text"/> <input type="checkbox"/> Ativado*: <input type="checkbox"/> <input type="text"/> E-mail*: <input type="text"/> <input type="button" value="Incluir"/>	

Tela	Cadastro de característica de usuário
Objetivo	Cadastrar características de usuários.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que as características dos usuários sofrer alteração.

Tela	Cadastro de tipo de recurso
Objetivo	Cadastrar tipos de recursos.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que um novo tipo de recurso for necessário.

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Cadastro de papel administrativo
Objetivo	Cadastrar papéis administrativos.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que o administrador de sistemas solicitar um novo tipo de papel administrativo para seu sistema.

[PHELIPE PERBOURES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

Básico Papéis Atribuições Inativações	Incluir Papel Administrativo Código*: <input type="text"/> Nome*: <input type="text"/> Descrição: <input type="text"/> Sistema*: Sistema Integrado Acadêmico
<input type="button" value="Incluir"/>	

Tela	Atribuição de papel administrativo para usuário
Objetivo	Atribuir papéis administrativos para usuários.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que precisar adicionar um novo administrador de sistema.

[PHELIPE PERBOURES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

Básico Papéis Atribuições Inativações	Incluir Atribuição de Papel Administrativo para Usuário Papel Administrativo*: Administrador Usuário*: Phelipe Perboires
<input type="button" value="Incluir"/>	

Tela	Atribuição de papel de segurança para usuário
Objetivo	Atribuir papel de segurança para usuários.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que um novo administrador de segurança for necessário.

[PHELIPE PERBOIRES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Básico Papéis Atribuições Inativações

Incluir Atribuição de Papel de Segurança para Usuário

Usuário*: Phelipe Perboires

Início da Validade:

Término da Validade:

Incluir

Tela	Inativação de usuário
Objetivo	Incluir motivos de inativação para um usuário.
Usuários atingidos	Administradores de segurança.
Frequência de uso	Toda vez que existir um motivo para se inativar um usuário.

[PHELIPE PERBOIRES] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Básico Papéis Atribuições Inativações

Incluir Inativação de Usuário

Usuário*: Phelipe Perboires

Motivo*:

Início da Inativação:

Terminio da Inativação:

Incluir

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Cadastro de papel comum
Objetivo	Cadastrar papéis comuns.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar de um novo papel comum.

[\[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO \]](#) | [\[ALTERAR SENHA \]](#) | [\[SAIR \]](#)



Framework de Segurança



▼ Incluir Papel Comum

Código*:	<input type="text"/>
Nome*:	<input type="text"/>
Descrição:	<input type="text"/>

Incluir



Tela	Cadastro de grupo manual
Objetivo	Cadastrar grupos manuais.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar de um novo grupo manual.

[\[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO \]](#) | [\[ALTERAR SENHA \]](#) | [\[SAIR \]](#)



Framework de Segurança



▼ Incluir Grupo Manual

Código*:	<input type="text"/>
Nome*:	<input type="text"/>
Descrição:	<input type="text"/>

Incluir



UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Membro de grupo manual
Objetivo	Incluir membros em grupos manuais.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que um usuário precisar fazer parte de um grupo manual.

[THAMIRES RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]



Framework de Segurança

[BR | EN | PT]

	Incluir Membro de Grupo Manual Grupo Manual*: Professores de Sistemas Usuário*: Phelipe Perboires <input style="width: 100%;" type="button" value="Incluir"/>
--	---

Tela	Cadastro de grupo caracterizado
Objetivo	Cadastrar grupos caracterizados.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar de um grupo caracterizado.

[THAMIRES RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]



Framework de Segurança

[BR | EN | PT]

	Incluir Grupo Caracterizado Código*: <input type="text"/> Nome*: <input type="text"/> Descrição: <input type="text"/> Ativado*: <input type="checkbox"/> <input style="width: 100%;" type="button" value="Incluir"/>
---	--

Tela	Caracterização de grupo caracterizado
Objetivo	Caracterizar grupos caracterizados.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar caracterizar um grupo caracterizado.

Tela	Cadastro de recurso
Objetivo	Cadastrar recursos.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar mapear um novo recurso do sistema no Framework de Segurança.

Tela	Cadastro de operação
Objetivo	Cadastrar operações.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar de uma nova operação para um recurso.

THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO | [ALTERAR SENHA] | [SAIR]

Framework de Segurança

Incluir Operação

Código*:

Nome*:

Descrição:

Incluir

Tela	Cadastro de permissão
Objetivo	Cadastrar permissões.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que precisar definir uma nova permissão no Framework de Segurança.

THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO | [ALTERAR SENHA] | [SAIR]

Framework de Segurança

Incluir Permissão

Recurso*: Módulo Básico

Operação*: Clicar

Contextualizada*:

Auditada*:

Ativada*:

Incluir

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Contextualização de Permissão
Objetivo	Contextualizar uma permissão.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que uma permissão precisar ser contextualizada.


Framework de Segurança

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

BR USA ES

 <ul style="list-style-type: none">  Papéis →  Grupos →  Mapeamentos →  Contextos →  Características →  Atribuições →  Concessões →  Inativações → 	<p>Incluir Contexto de Permissão</p> <p>Permissão*: Lançar Nota > Executar</p> <p>Contexto*: Turma</p> <p>Incluir</p>
--	---

Tela	Cadastro de conflito de permissões
Objetivo	Cadastrar conflitos de permissões.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que um conflito entre permissões for detectado e precisar ser mapeado no Framework de Segurança.


Framework de Segurança

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

BR USA ES

 <ul style="list-style-type: none">  Papéis →  Grupos →  Mapeamentos →  Contextos →  Características →  Atribuições →  Concessões →  Inativações → 	<p>Incluir Conflito de Permissões</p> <p>Permissão*: Lançar Nota > Executar</p> <p>Conflitante*: Lançar Nota > Executar</p> <p>Nome*: </p> <p>Descrição: </p> <p>Incluir</p>
---	---

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Cadastro de contexto
Objetivo	Cadastrar contextos.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar cadastrar um contexto para controlar uma permissão contextualizada.

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

Incluir Contexto	
Código*:	<input type="text"/>
Nome*:	<input type="text"/>
Descrição:	<input type="text"/>
Incluir	

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

BR USA ES

incluir Valor do Contexto	
Contexto*:	Turma
Código*:	<input type="text"/>
Nome*:	<input type="text"/>
Descrição:	<input type="text"/>
Incluir	

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Tela	Cadastro de característica
Objetivo	Cadastrar características.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que uma nova característica de usuário precisar ser usada dentro do Framework de Segurança.

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Tela	Cadastro de valor de característica
Objetivo	Cadastrar valor de característica.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que um novo valor surgir para uma característica.

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Tela	Atribuição de papel comum para usuário
Objetivo	Atribuir papéis comuns para usuários.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que um usuário precisar ganhar um papel comum.

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [[ALTERAR SENHA](#)] [[SAIR](#)]

Framework de Segurança







 Papéis  Grupos  Mapeamentos  Contextos  Características  Atribuições  Concessões  Inativações	<p>Incluir Atribuição de Papel Comum para Usuário</p> <p>Papel Comum*: Professor</p> <p>Usuário*: Phelipe Perboires</p> <p>Início da Validade: <input type="text"/></p> <p>Término da Validade: <input type="text"/></p> <p style="text-align: center;">Incluir</p>
--	---

Tela	Contextualização de atribuição de papel comum para usuário
Objetivo	Contextualizar atribuições de papéis comuns para usuários.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que uma atribuição de papel comum para usuário precisar ser contextualizada.

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [[ALTERAR SENHA](#)] [[SAIR](#)]

Framework de Segurança







 Papéis  Grupos  Mapeamentos  Contextos  Características  Atribuições  Concessões  Inativações	<p>Incluir Contextuação de Atribuição de Papel Comum para Usuário</p> <p>Atribuição de Papel Comum*: Professor > Millan</p> <p>Concessão da Permissão*: Coordenador > Cadastrar Turma > Ex</p> <p>Valor do Contexto*: Plataforma > P-51</p> <p style="text-align: center;">Incluir</p>
---	--

Tela	Atribuição de papel comum para grupo manual
Objetivo	Atribuir papéis comuns para grupos manuais.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que precisar atribuir um papel comum para um grupo manual.

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Incluir Atribuição de Papel Comum para Grupo Manual

Grupo Manual*: Professores de Sistemas

Papel Comum*: Professor

Incluir

Tela	Atribuição de papel comum para grupo caracterizado
Objetivo	Atribuir papel comum para grupo caracterizado.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que precisar atribuir um papel comum para um grupo caracterizado.

[THAMIRE RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Incluir Atribuição de Papel Comum para Grupo Caracterizado

Grupo Caracterizado*: Professores de Niterói

Papel Comum*: Professor

Incluir

Tela	Atribuição de papel administrativo para grupo manual
Objetivo	Atribuir papéis administrativos para grupos manuais.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar atribuir um papel administrativo para um grupo manual.

Tela	Concessão de permissão para papel comum
Objetivo	Conceder permissões para papéis comuns.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que precisar definir quais permissões devem ser concedidas para um determinado papel comum.

Tela	Inativação de grupo manual
Objetivo	Incluir motivo de inativação para grupo manual.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar incluir um motivo de inativação para um grupo manual.

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Painel de Controle

Incluir Inativação de Grupo Manual

Grupo Manual*: Professores de Sistemas

Motivo*:

Início da Inativação:

Início da Inativação:

Incluir

Papéis Grupos Mapeamentos Contextos Características Atribuições Concessões Inativações

Tela	Inativação de grupo caracterizado
Objetivo	Incluir motivo de inativação para grupo caracterizado.
Usuários atingidos	Administradores de sistema.
Frequência de uso	Toda vez que necessitar incluir um motivo de inativação para um grupo caracterizado.

[THAMIRE S RAMOS - SISTEMA INTEGRADO ACADÉMICO] [ALTERAR SENHA] [SAIR]

Framework de Segurança

Painel de Controle

Incluir Inativação de Grupo Caracterizado

Grupo Caracterizado*: Professores de Niterói

Motivo*:

Início da Inativação:

Início da Inativação:

Incluir

Papéis Grupos Mapeamentos Contextos Características Atribuições Concessões Inativações

2.2.6. DIAGRAMAS DE ESTADO

2.2.6.1. Usuário



2.2.6.2. Sistema



2.2.6.3. Papel



2.2.6.4. Grupo



2.2.6.5. Permissão



2.2.6.6. Recurso



2.2.7. DIAGRAMA DE CLASSES DO MODELO

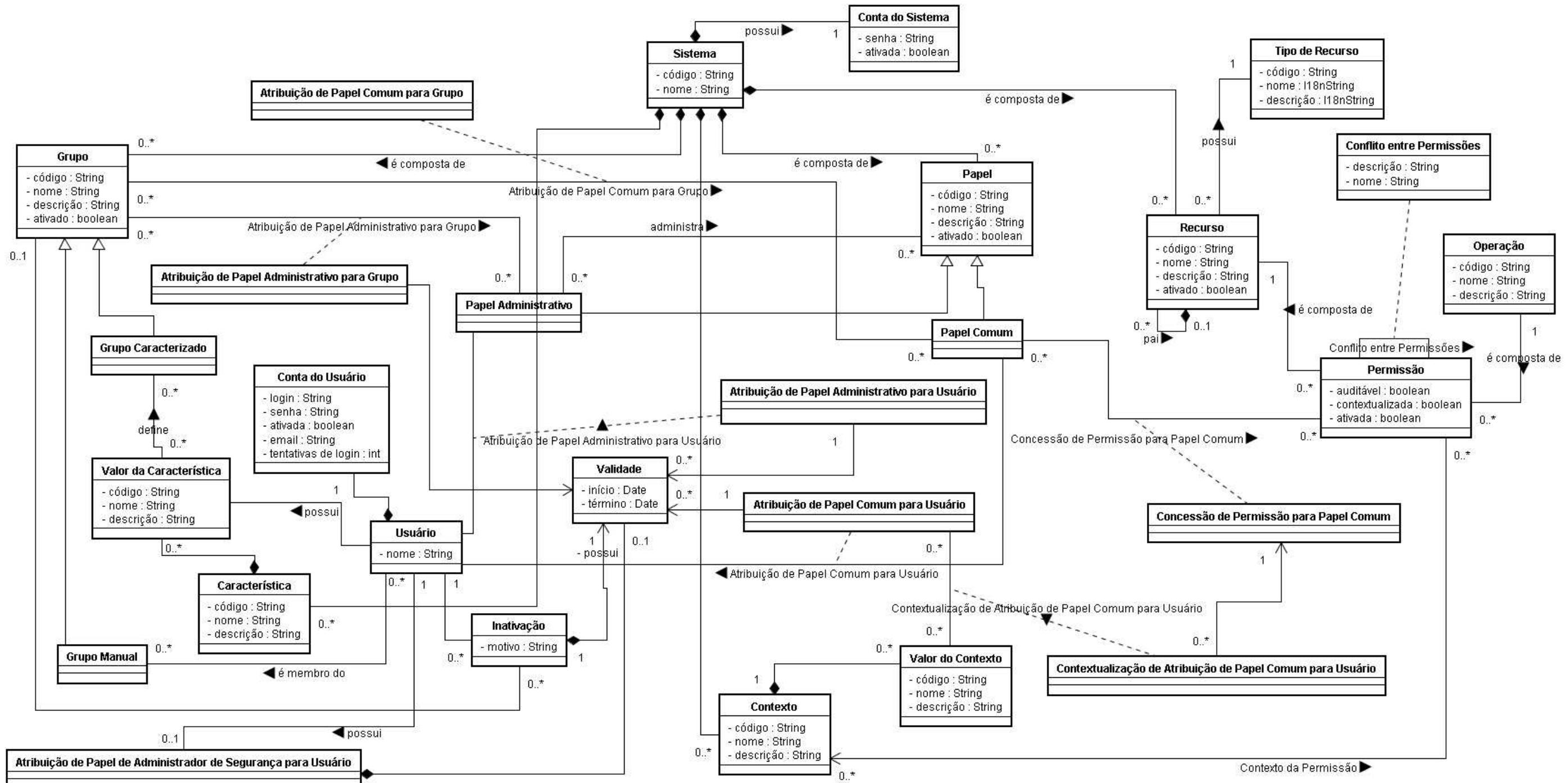


Figura 38: Diagrama de Classes do Modelo

2.2.8. DIAGRAMAS DE SEQUÊNCIA

2.2.8.1. Conectar sistema cliente ao serviço de segurança

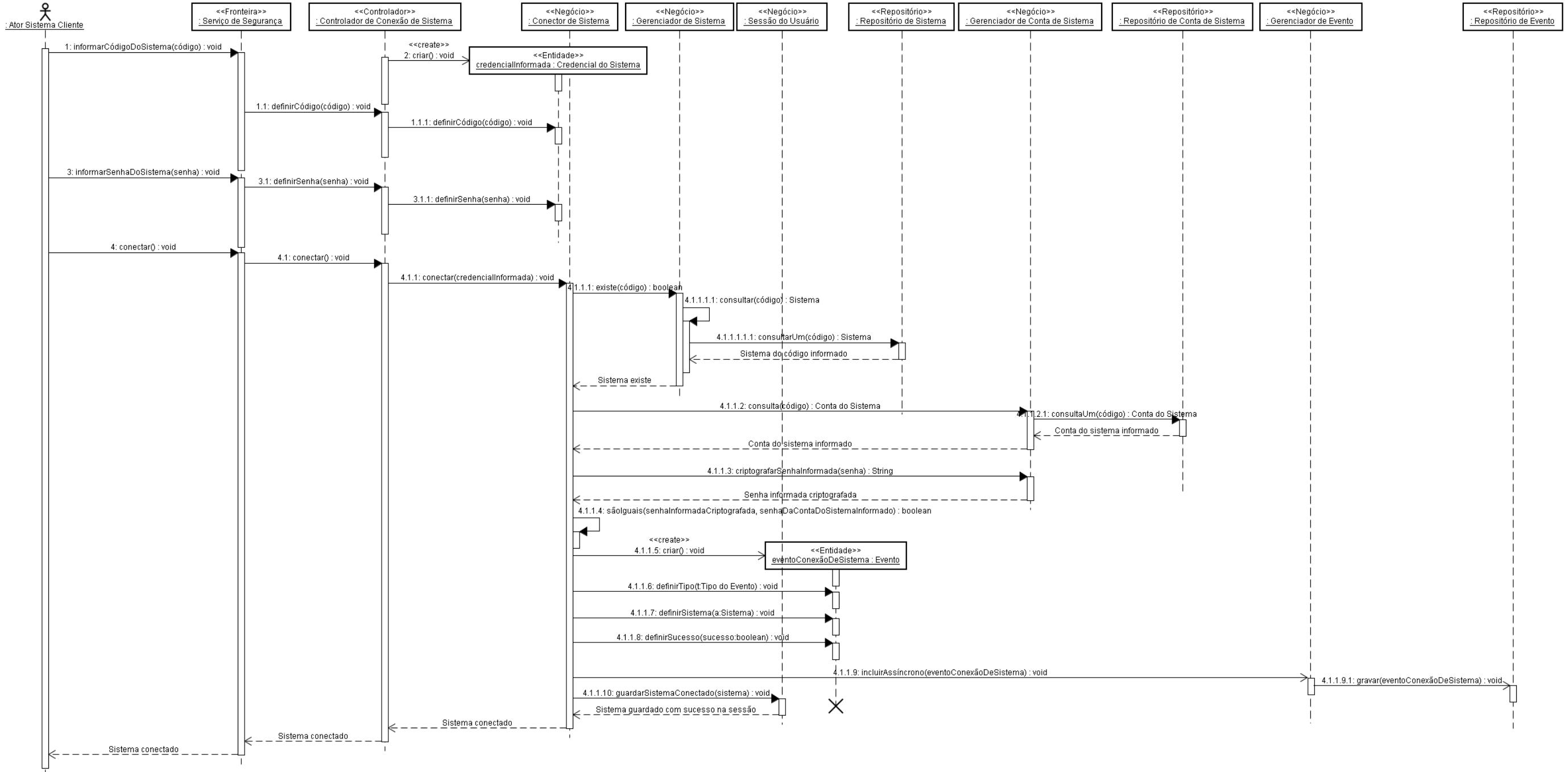


Figura 39: Diagrama de sequência conectar sistema cliente ao serviço de segurança

2.2.8.2. Desconectar sistema cliente do serviço de segurança

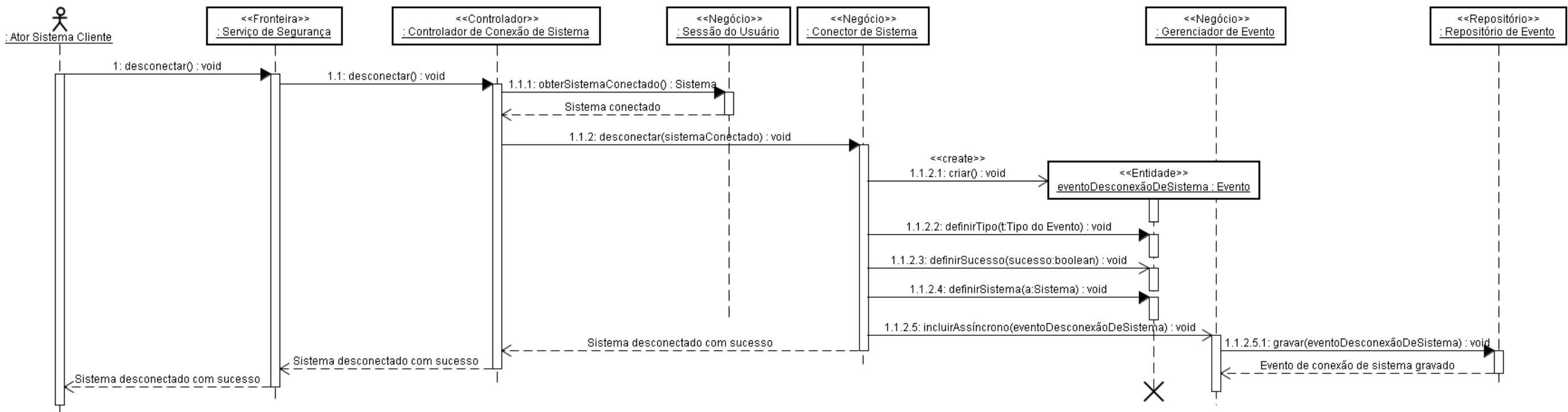


Figura 40: Diagrama de sequência desconectar sistema cliente do serviço de segurança

2.2.8.3. Realizar logon do usuário

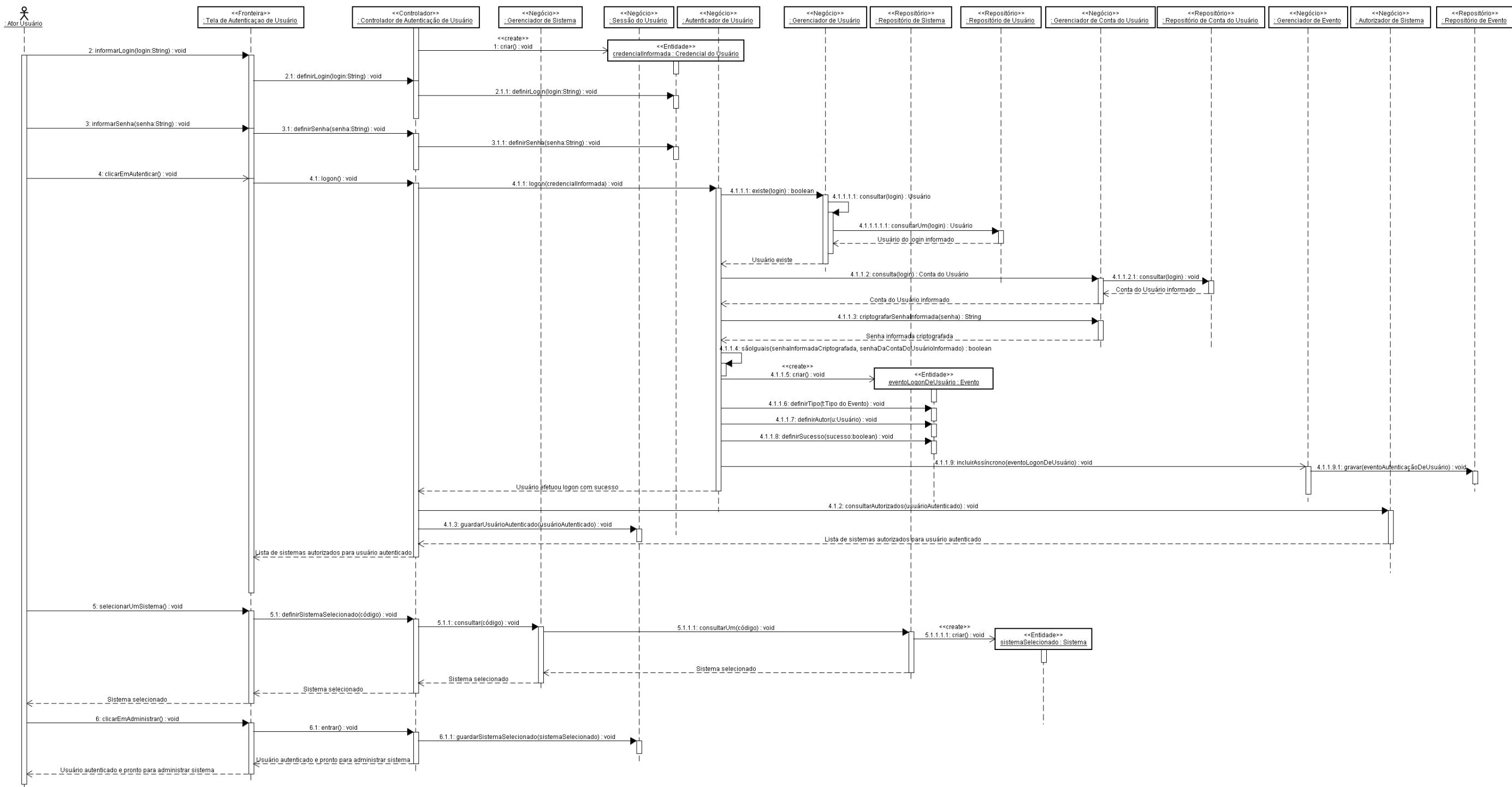


Figura 41: Diagrama de sequência realizar logon do usuário

2.2.8.4. Realizar logoff de usuário

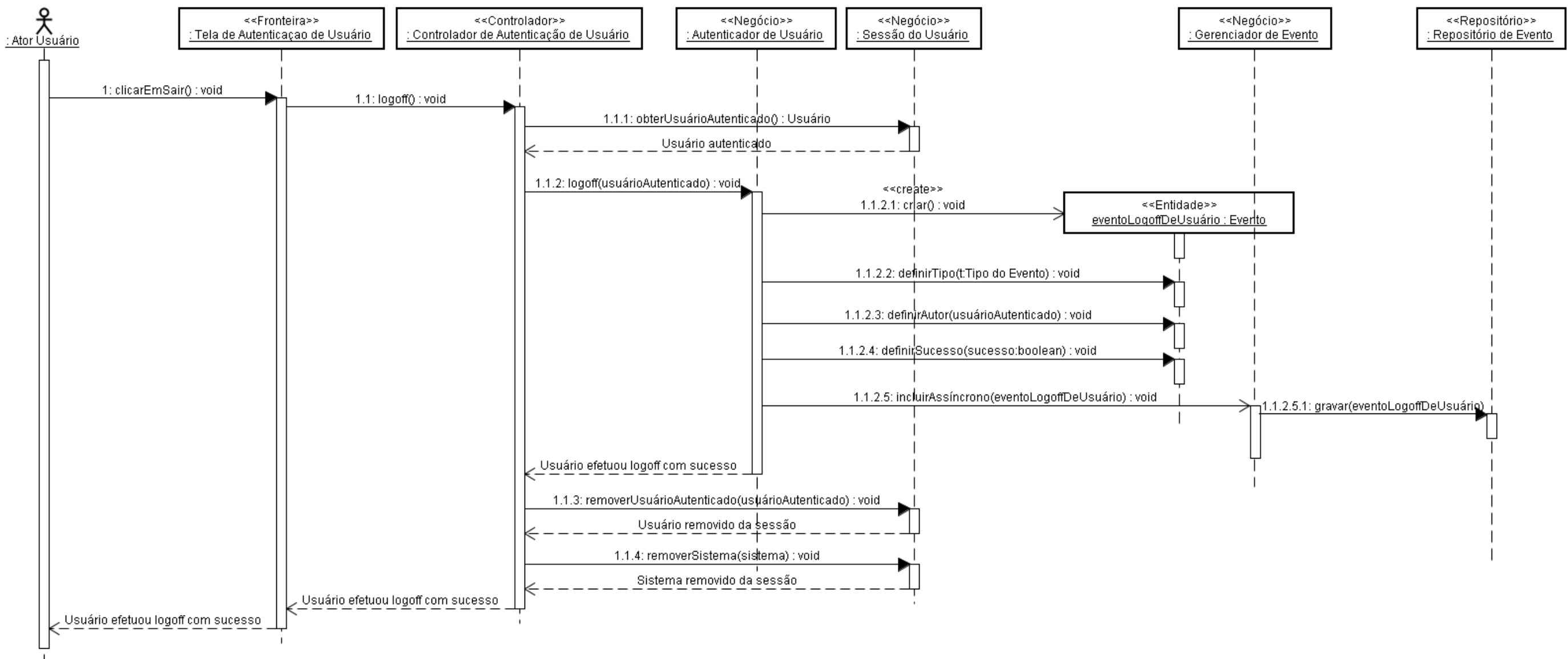


Figura 42: Diagrama de sequência realizar logoff do usuário

2.2.8.5. Solicitar nova senha por e-mail

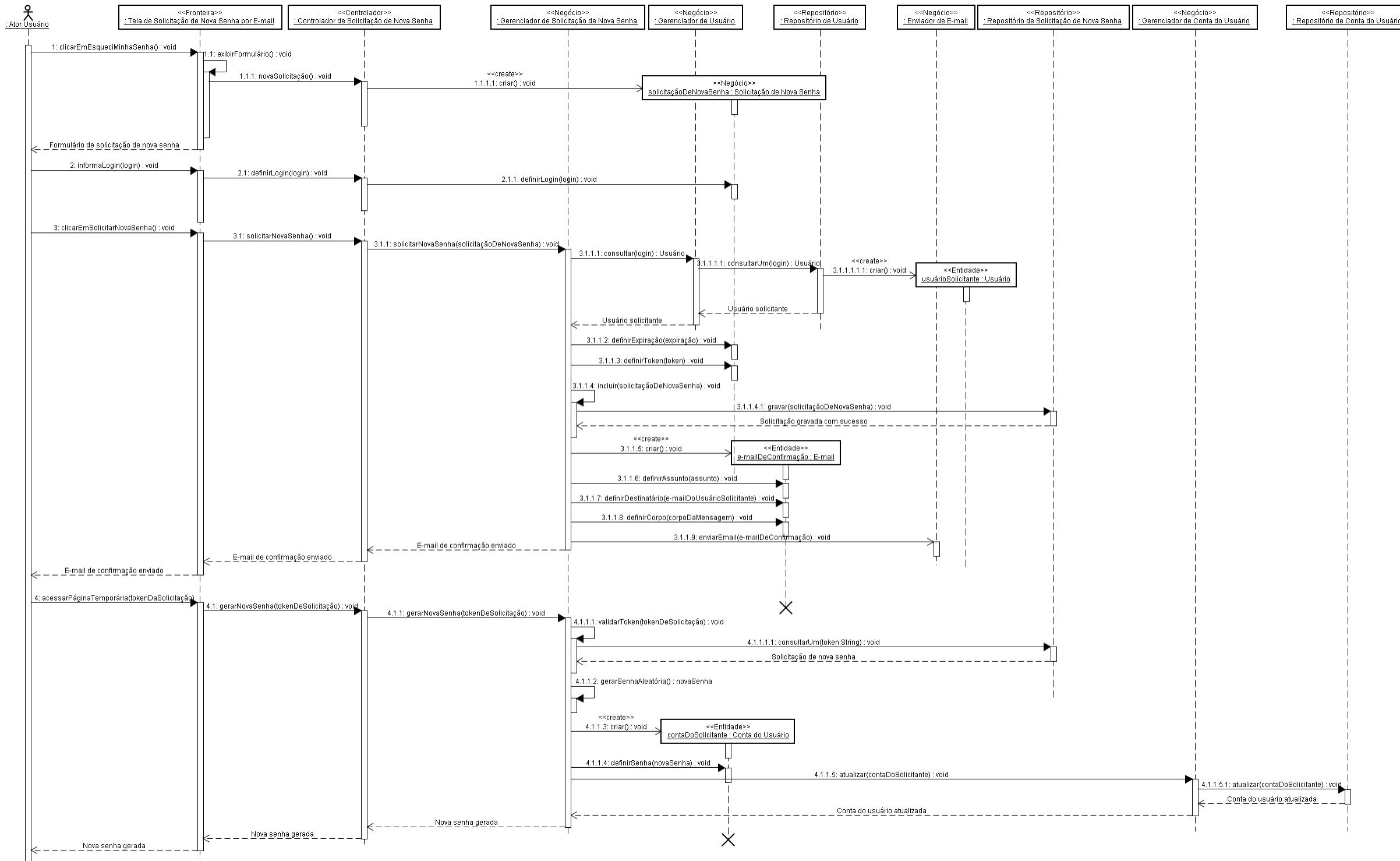


Figura 43: Diagrama de sequência solicitar nova senha por e-mail

2.2.8.6. Alterar senha

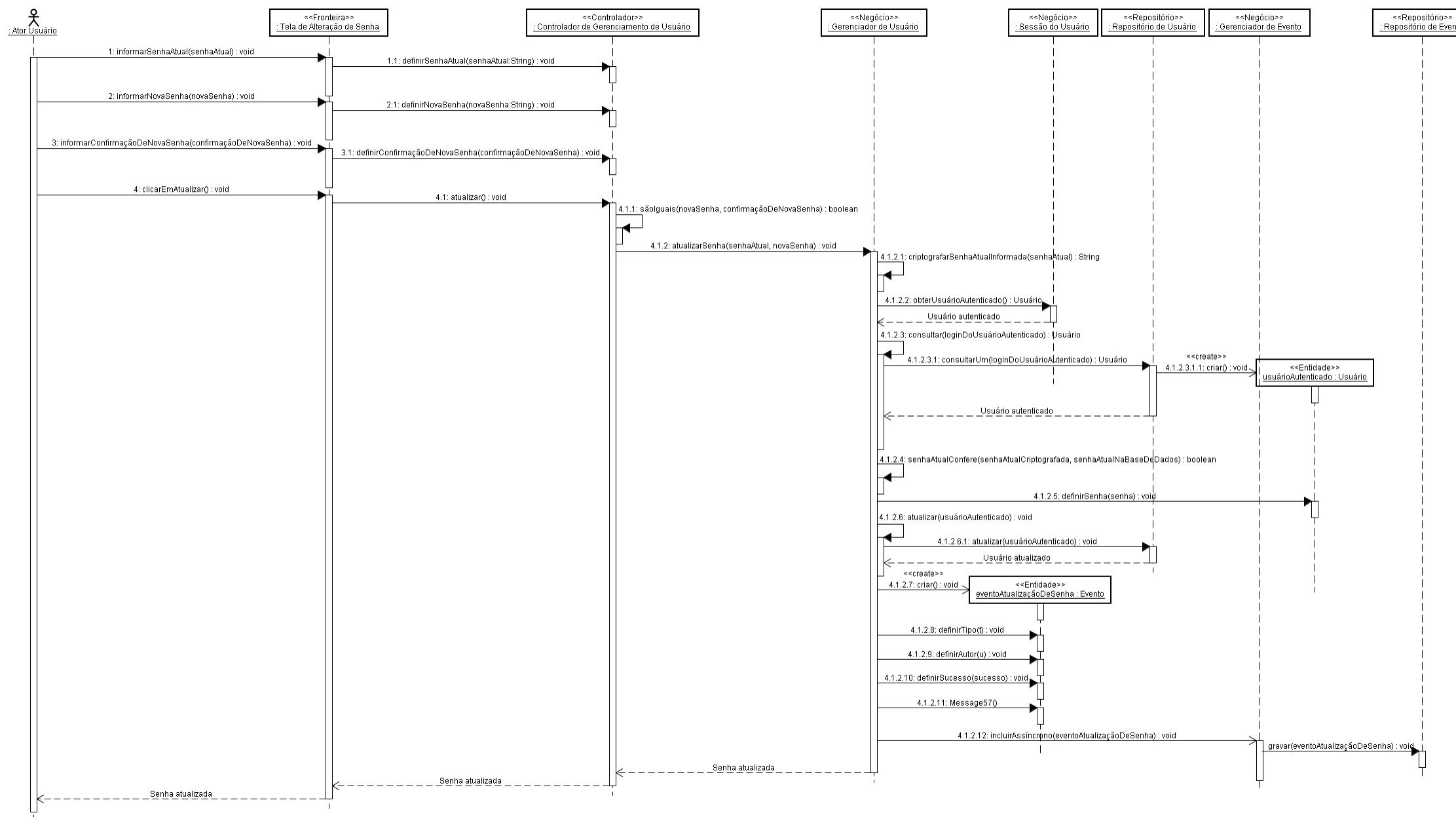


Figura 44: Diagrama de sequência alterar senha

2.2.8.7. Incluir recurso

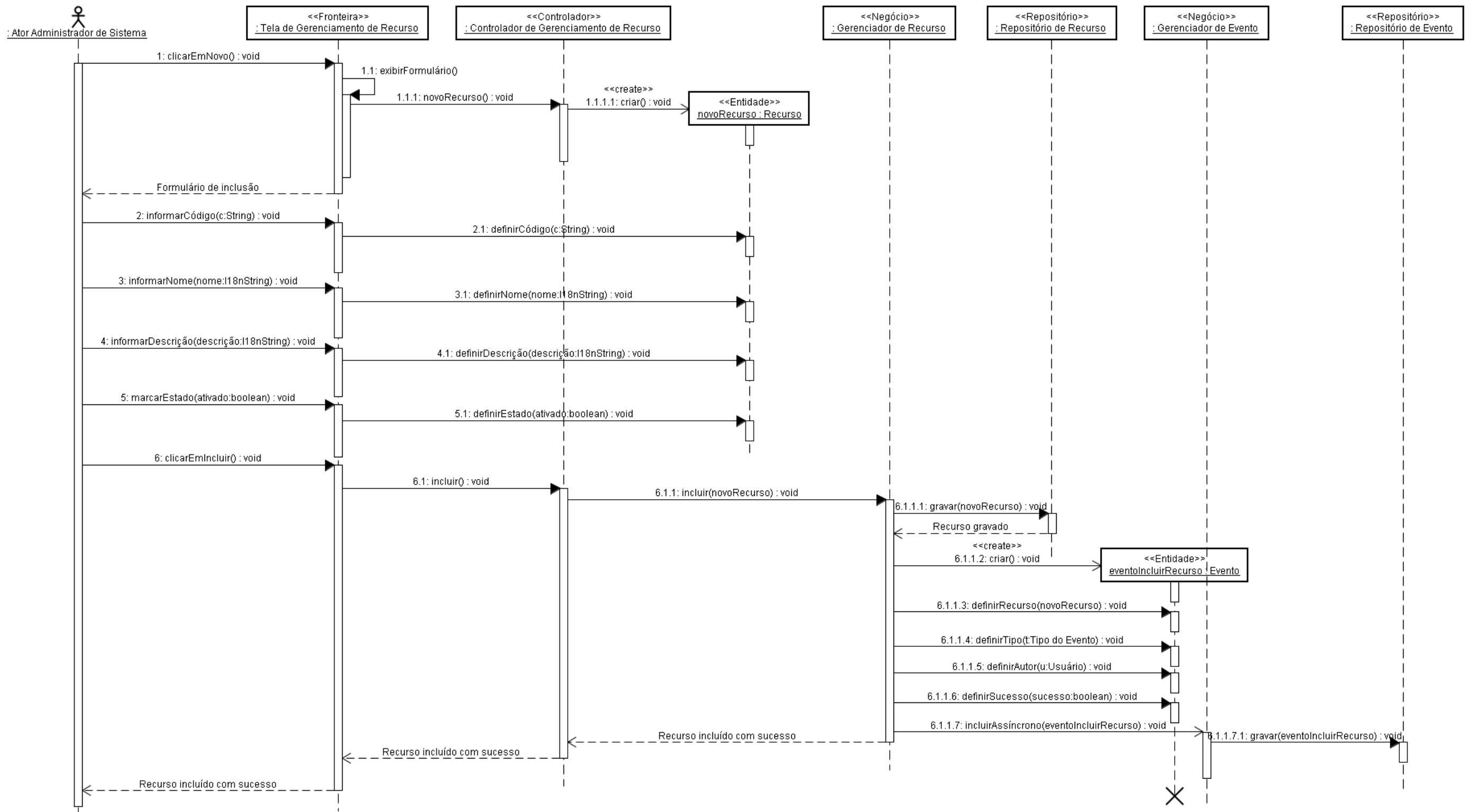


Figura 45: Diagrama de sequência incluir recurso

2.2.8.8. Alterar recurso

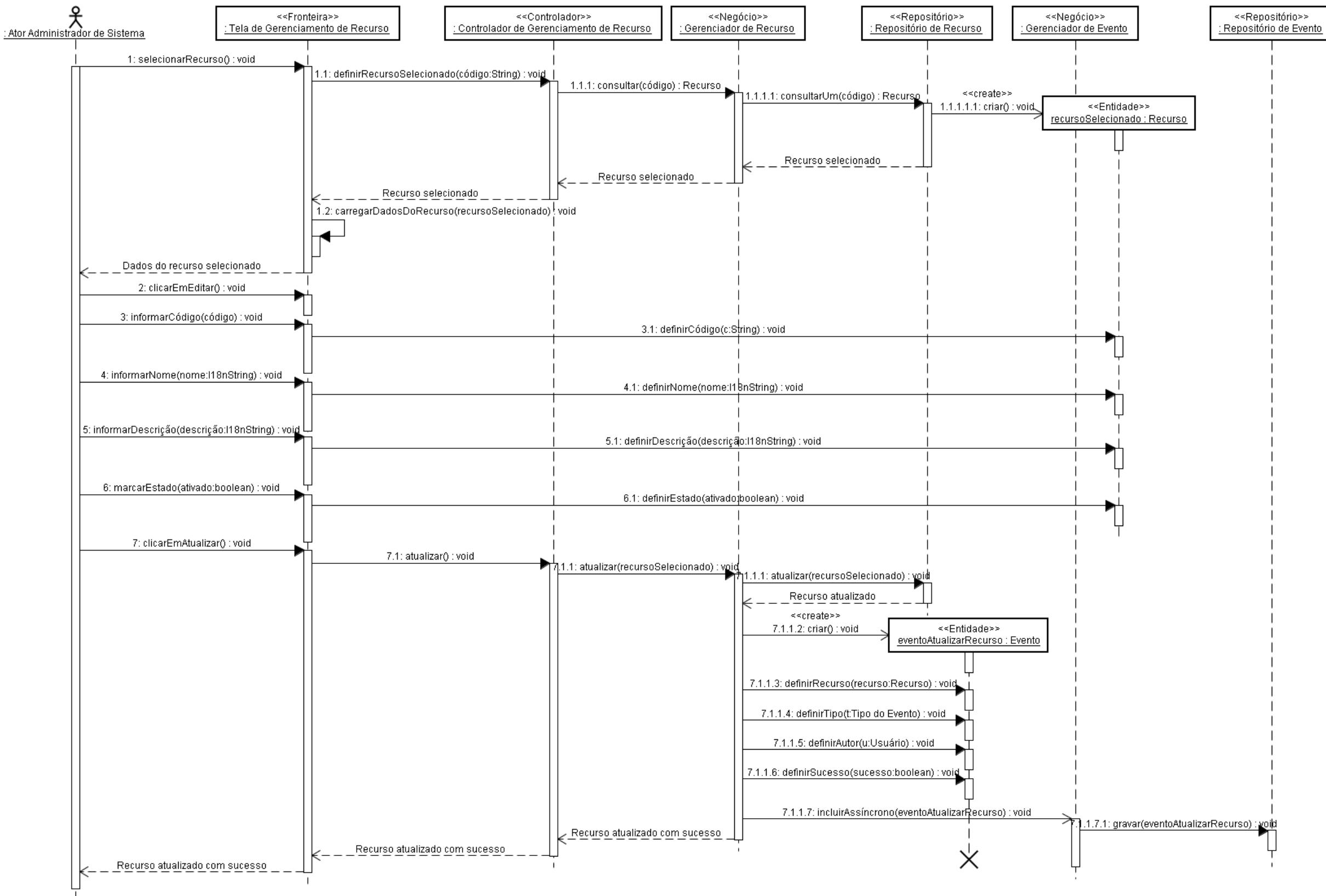


Figura 46: Diagrama de sequência alterar recurso

2.2.8.9. Excluir recurso

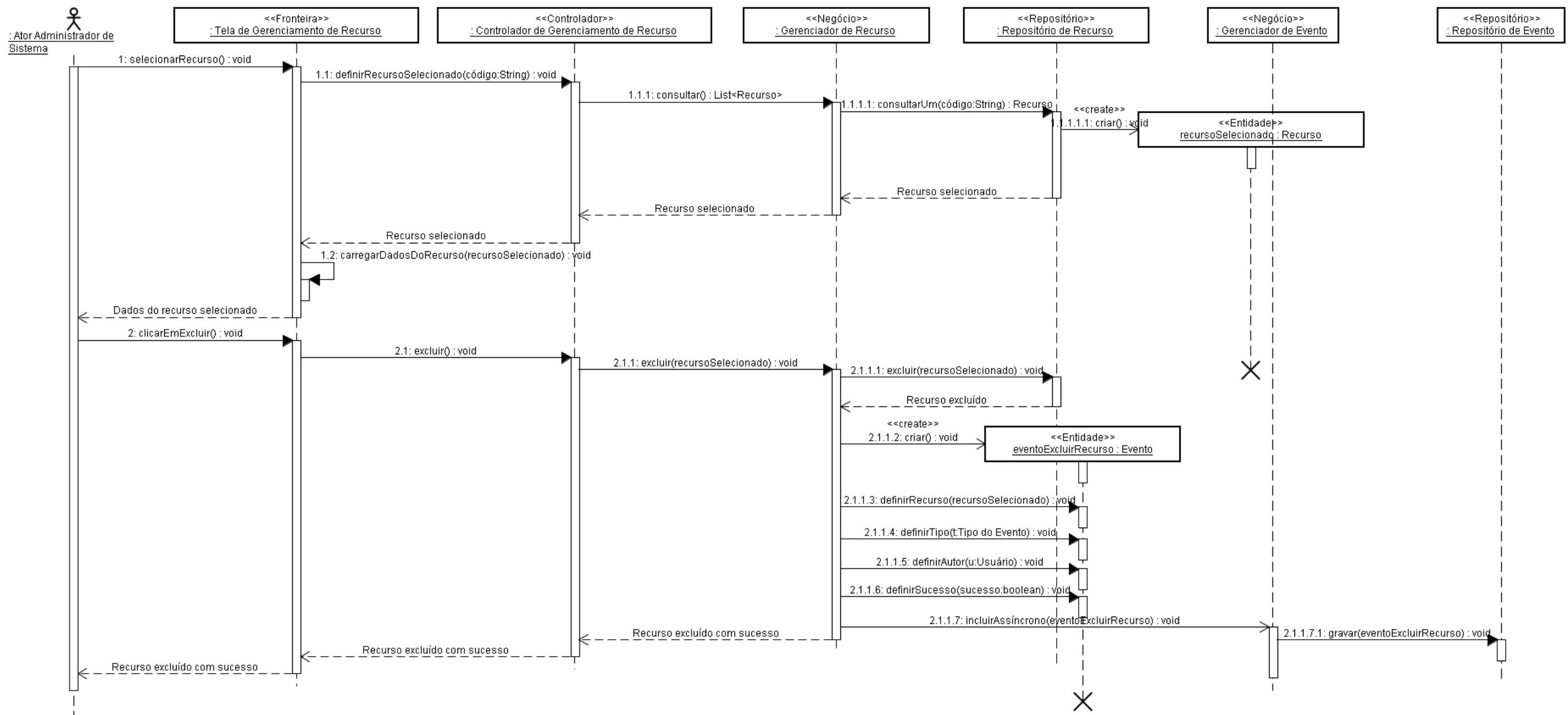


Figura 47: Diagrama de sequência excluir recurso

2.2.8.10. Consultar recurso

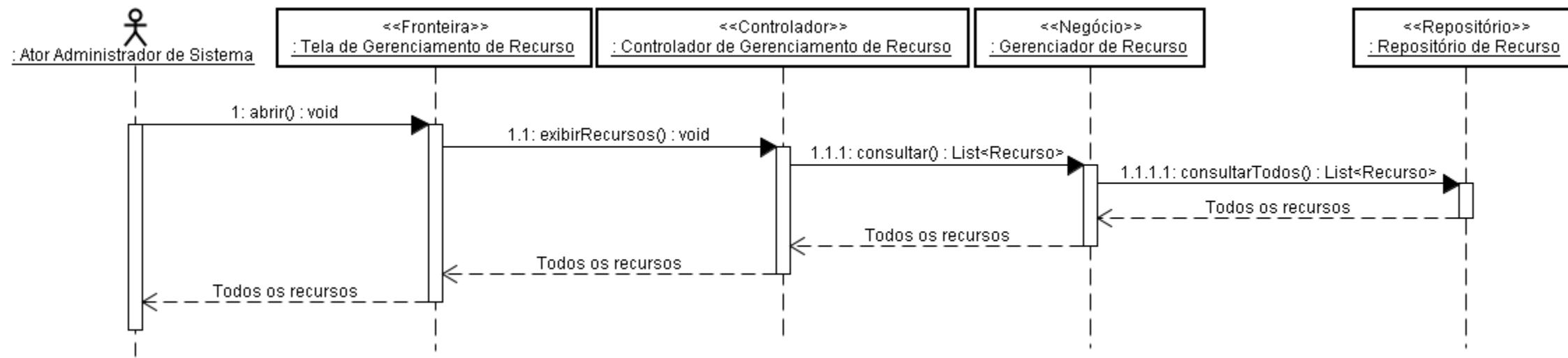


Figura 48: Diagrama de sequência consultar recurso

2.2.8.11. Incluir operação

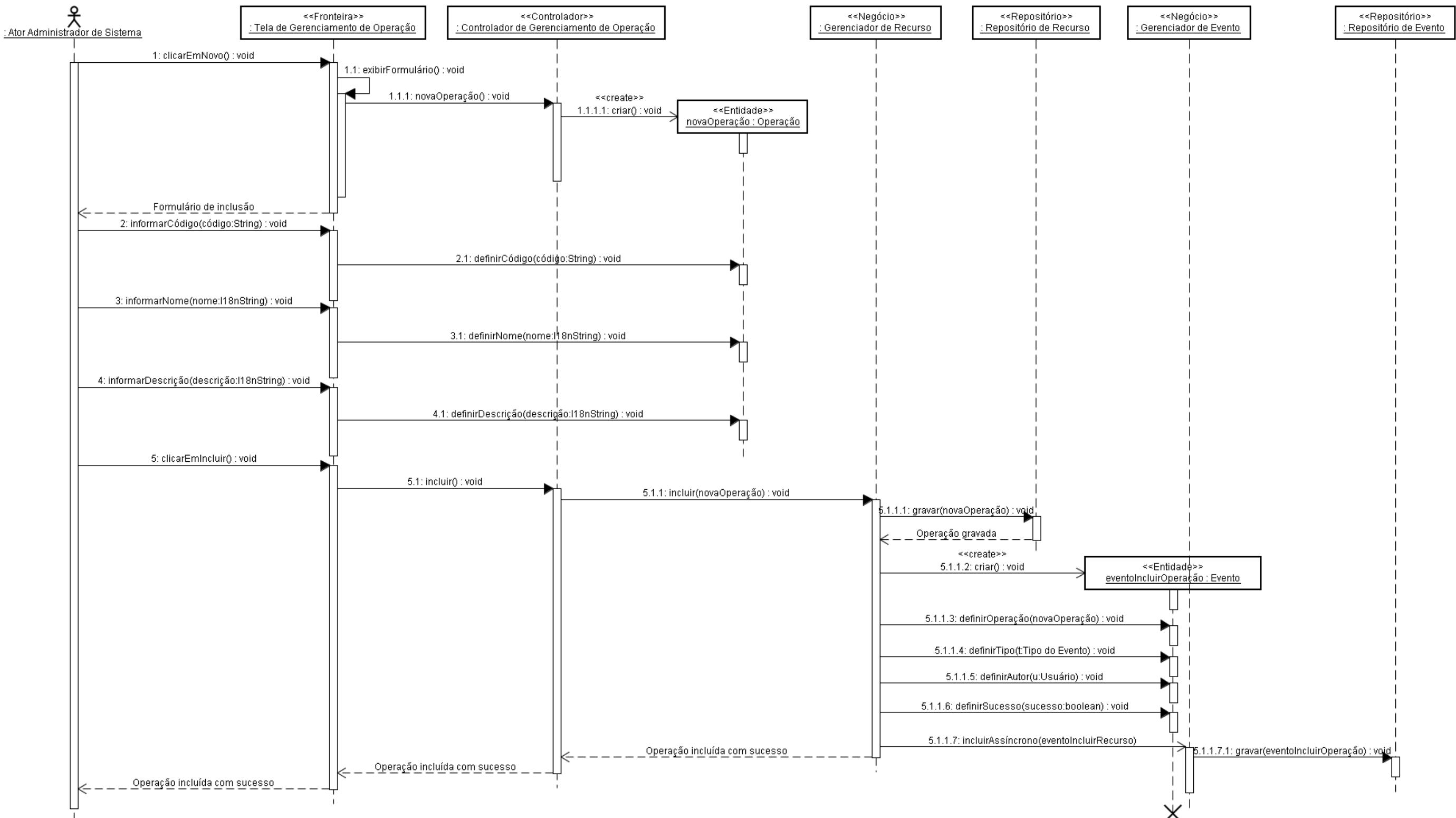


Figura 49: Diagrama de sequência incluir operação

2.2.8.12. Alterar operação

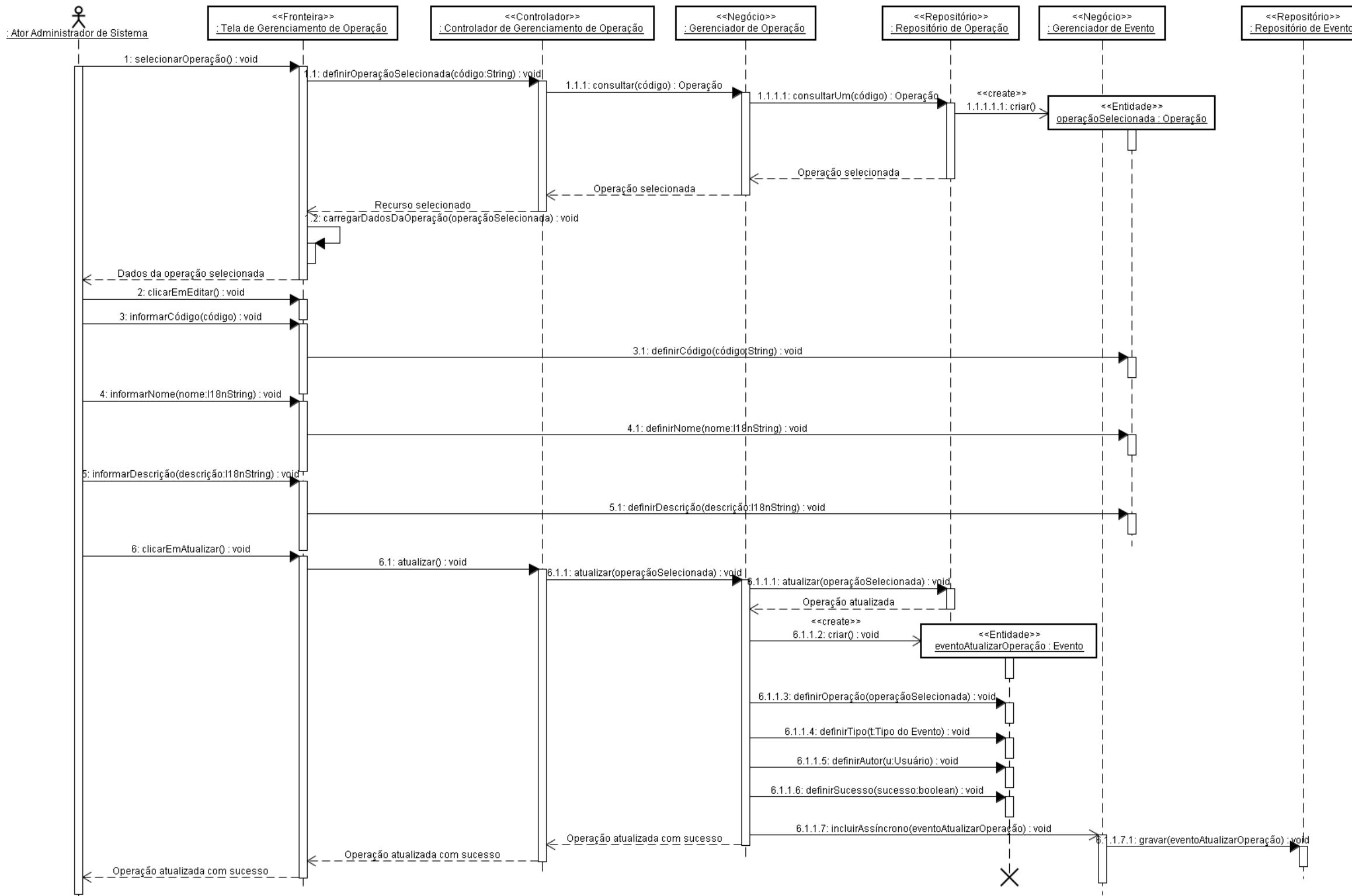


Figura 50: Diagrama de sequência alterar operação

2.2.8.13. Excluir operação

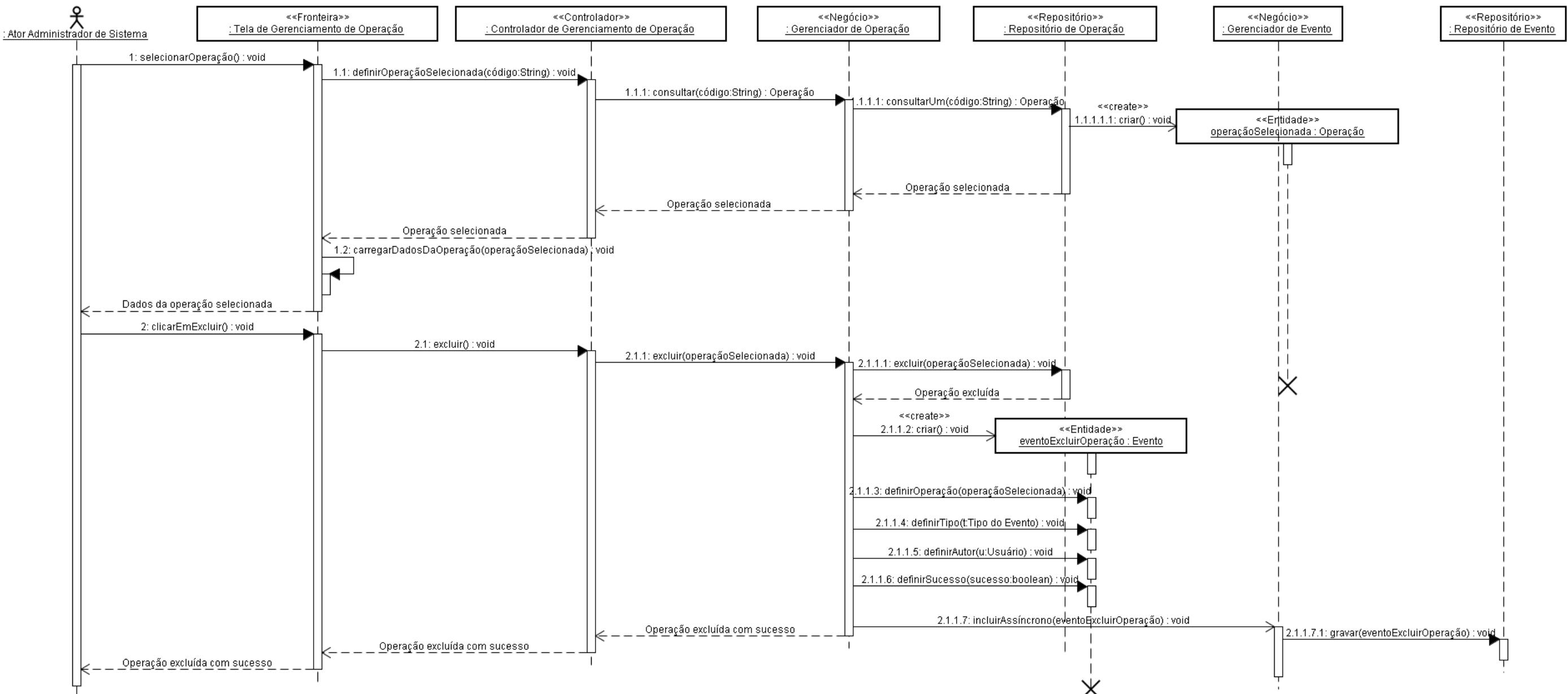


Figura 51: Diagrama de sequência excluir operação

2.2.8.14. Consultar operação

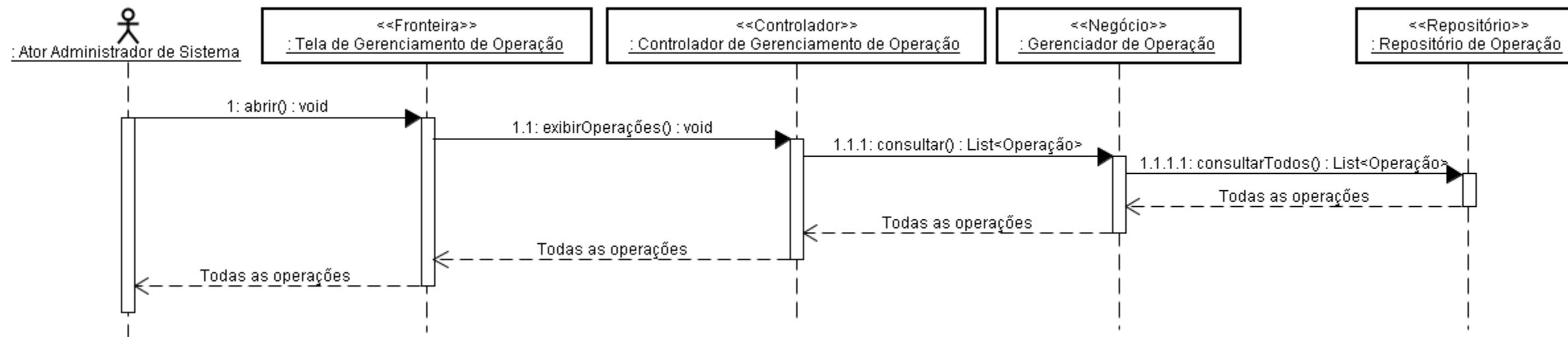


Figura 52: Diagrama de sequência consultar operação

2.2.8.15. Incluir permissão

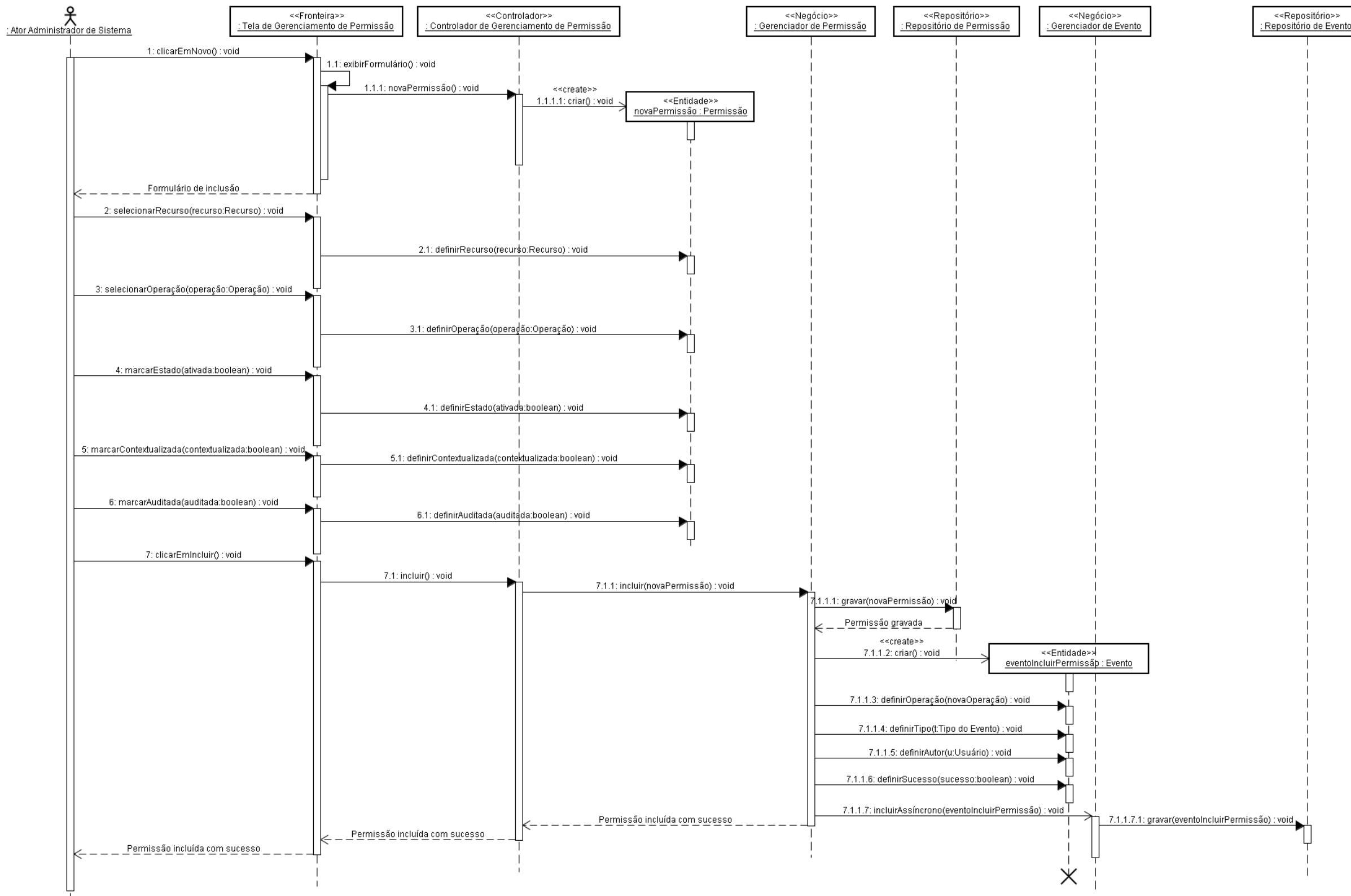


Figura 53: Diagrama de sequência incluir permissão

2.2.8.16. Alterar permissão

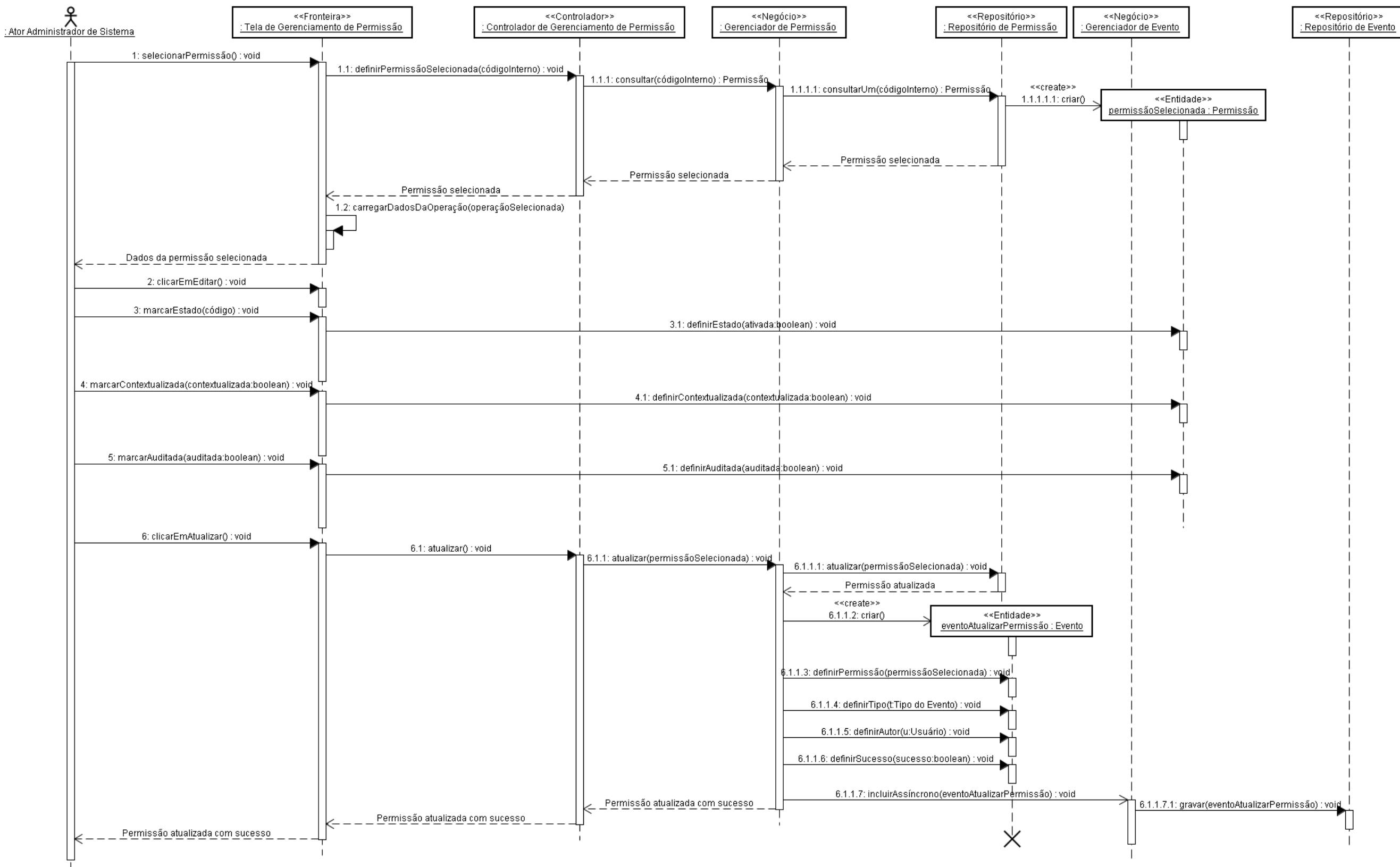


Figura 54: Diagrama de sequência alterar permissão

2.2.8.17. Excluir permissão

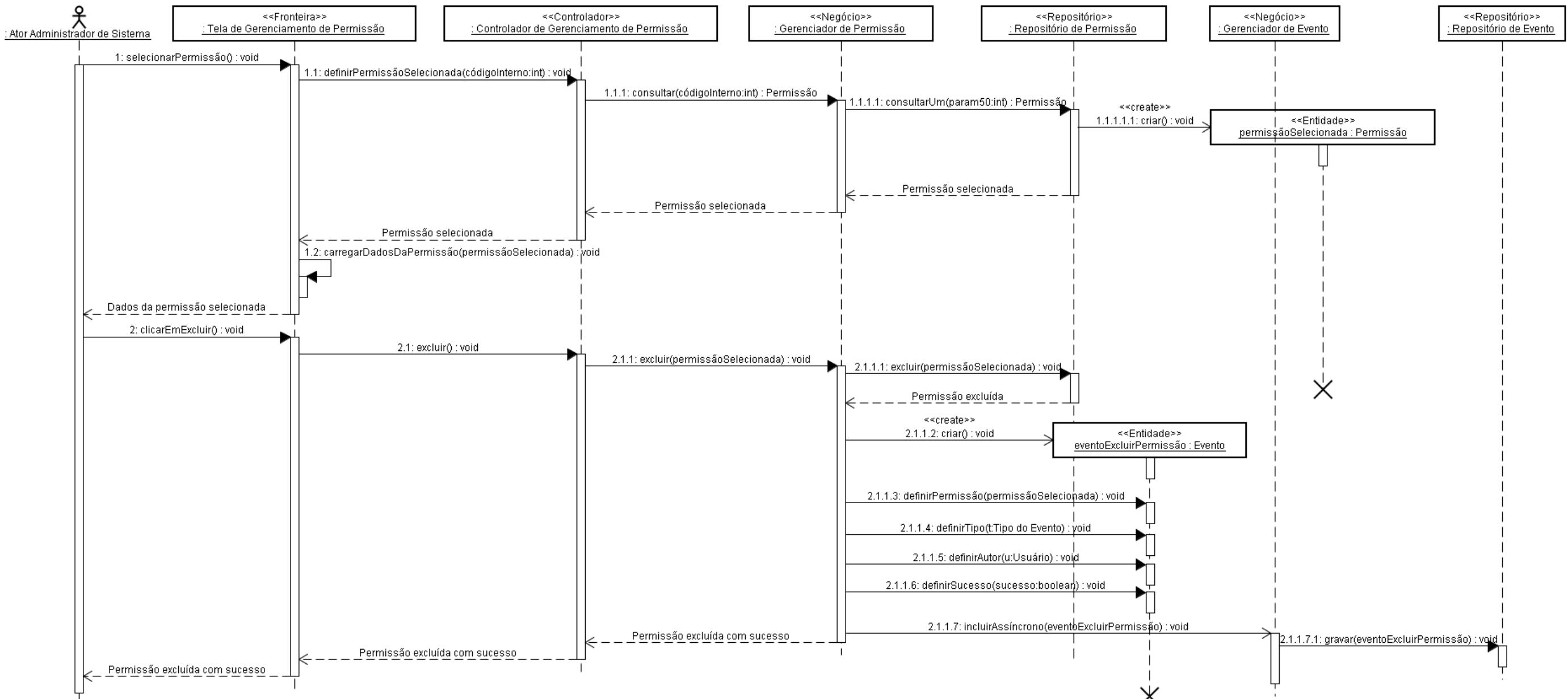


Figura 55: Diagrama de sequência excluir permissão

2.2.8.18. Consultar permissão

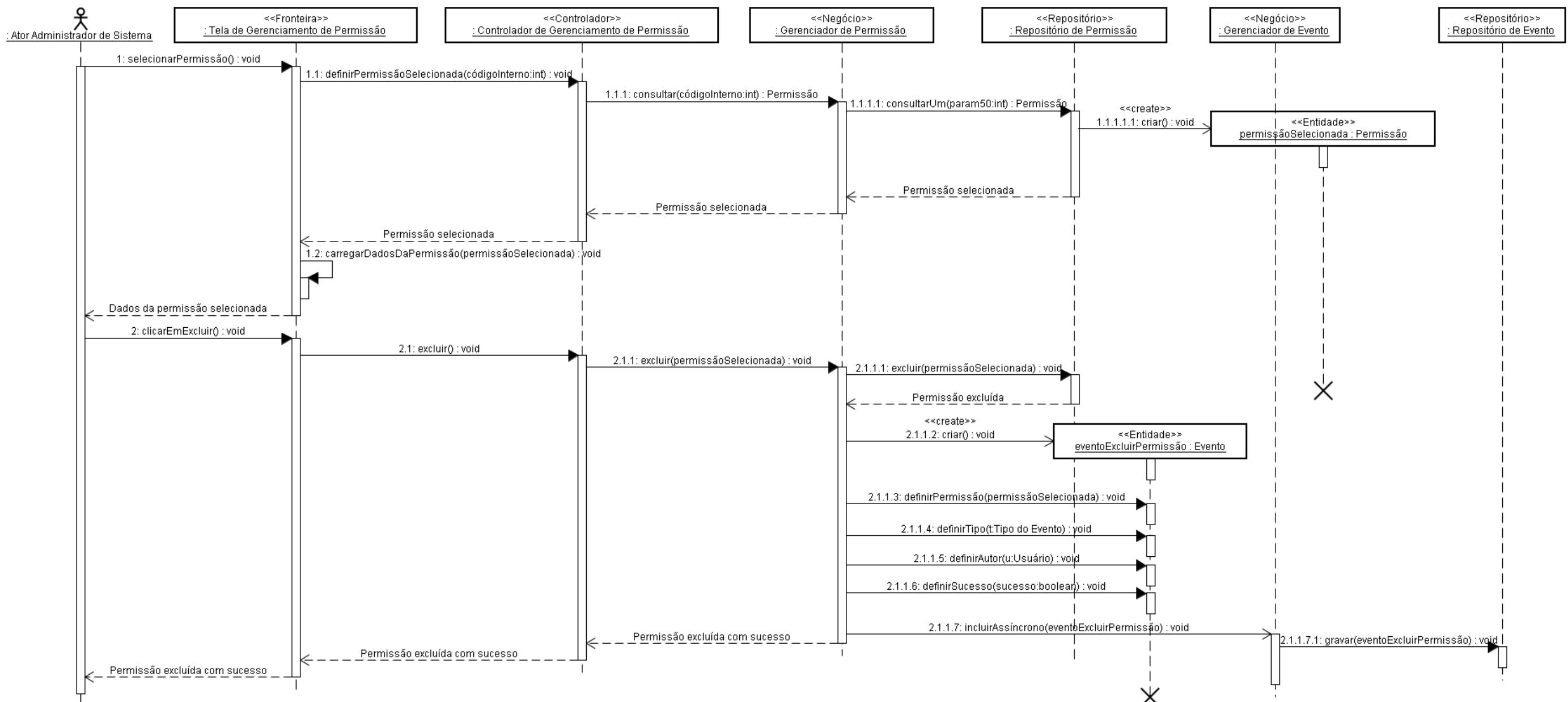


Figura 56: Diagrama de sequência consultar permissão

2.2.8.19. Incluir papel comum

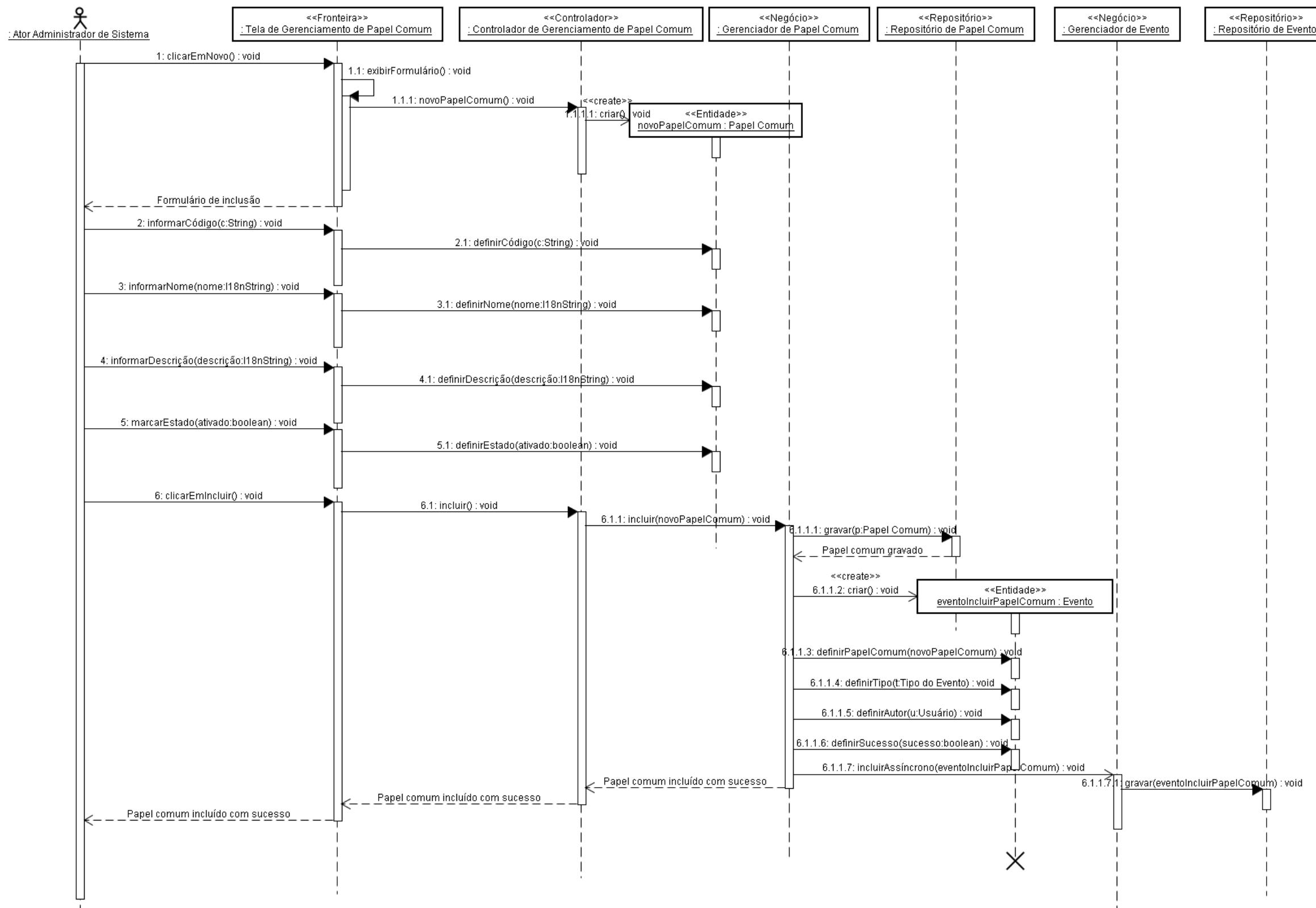


Figura 57: Diagrama de sequência papel comum

2.2.8.20. Alterar papel comum

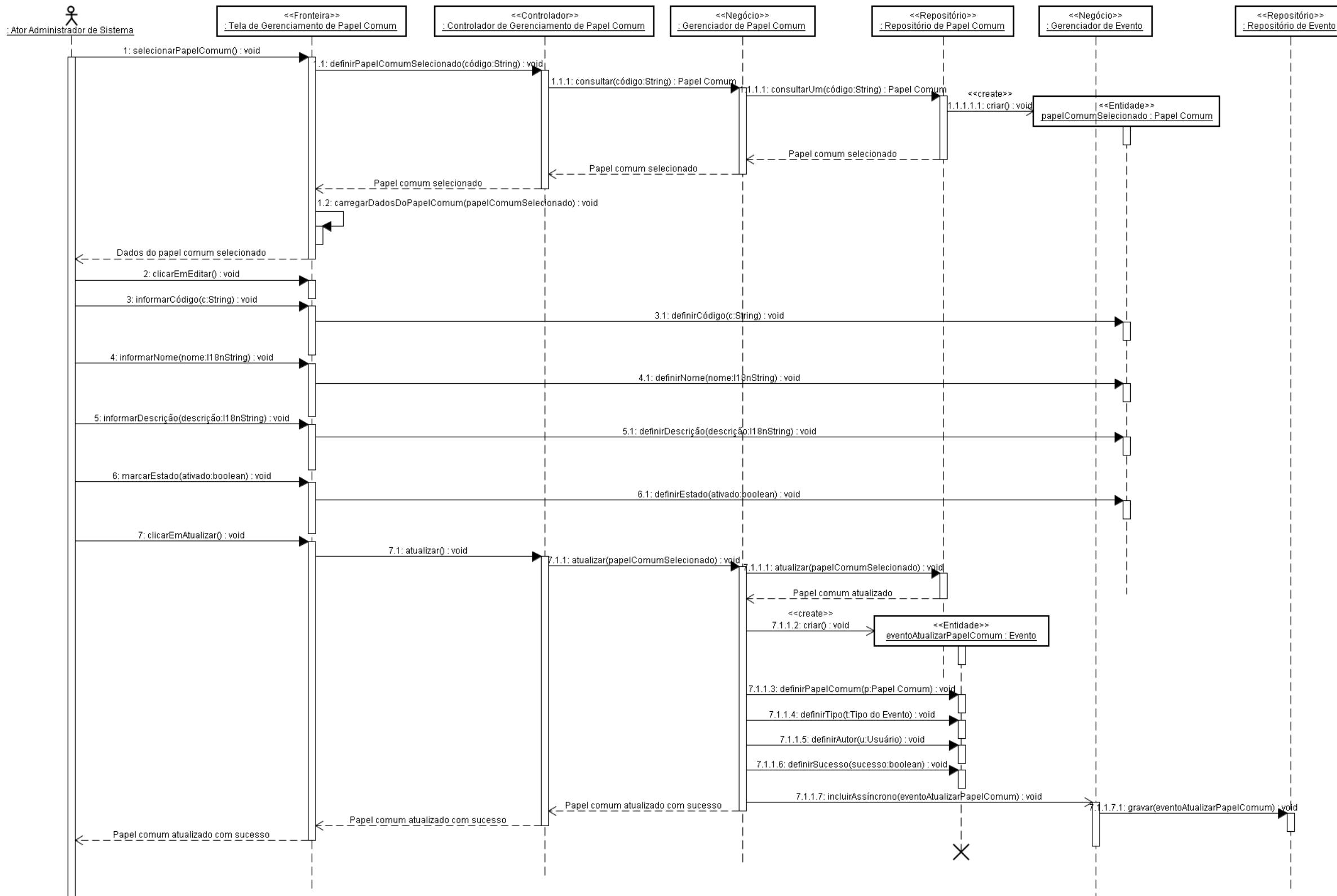


Figura 58: Diagrama de sequência alterar papel comum

2.2.8.21. Excluir papel comum

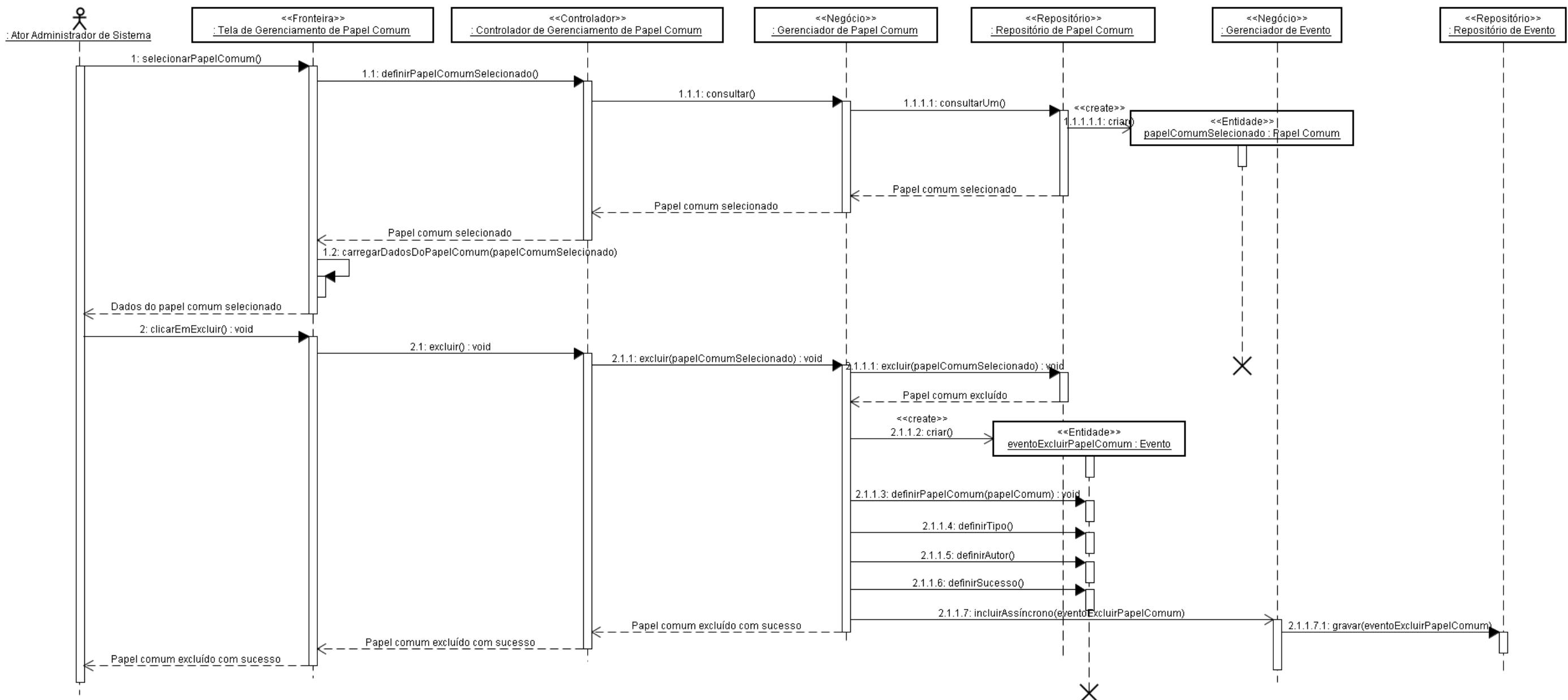


Figura 59: Diagrama de sequência excluir papel comum

2.2.8.22. Consultar papel comum

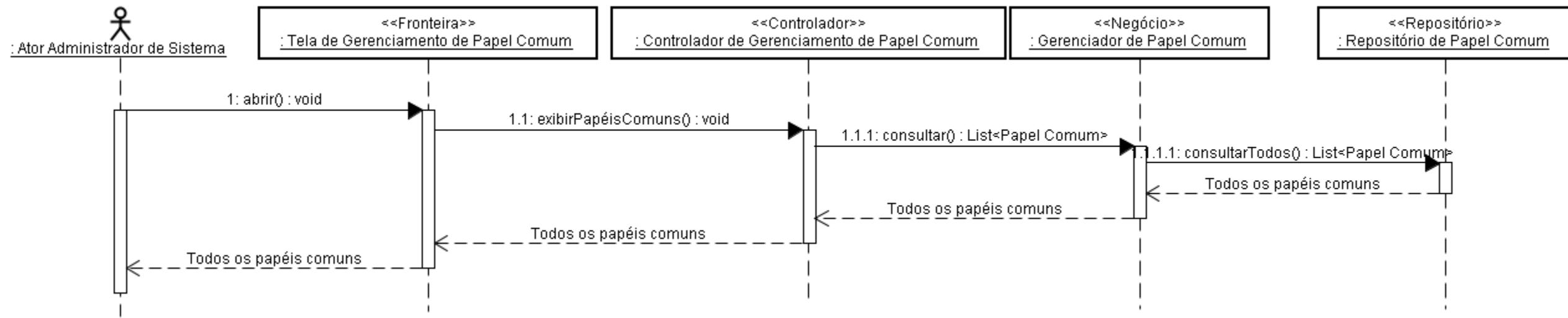


Figura 60: Diagrama de sequência consultar papel comum

2.2.8.23. Incluir papel administrativo

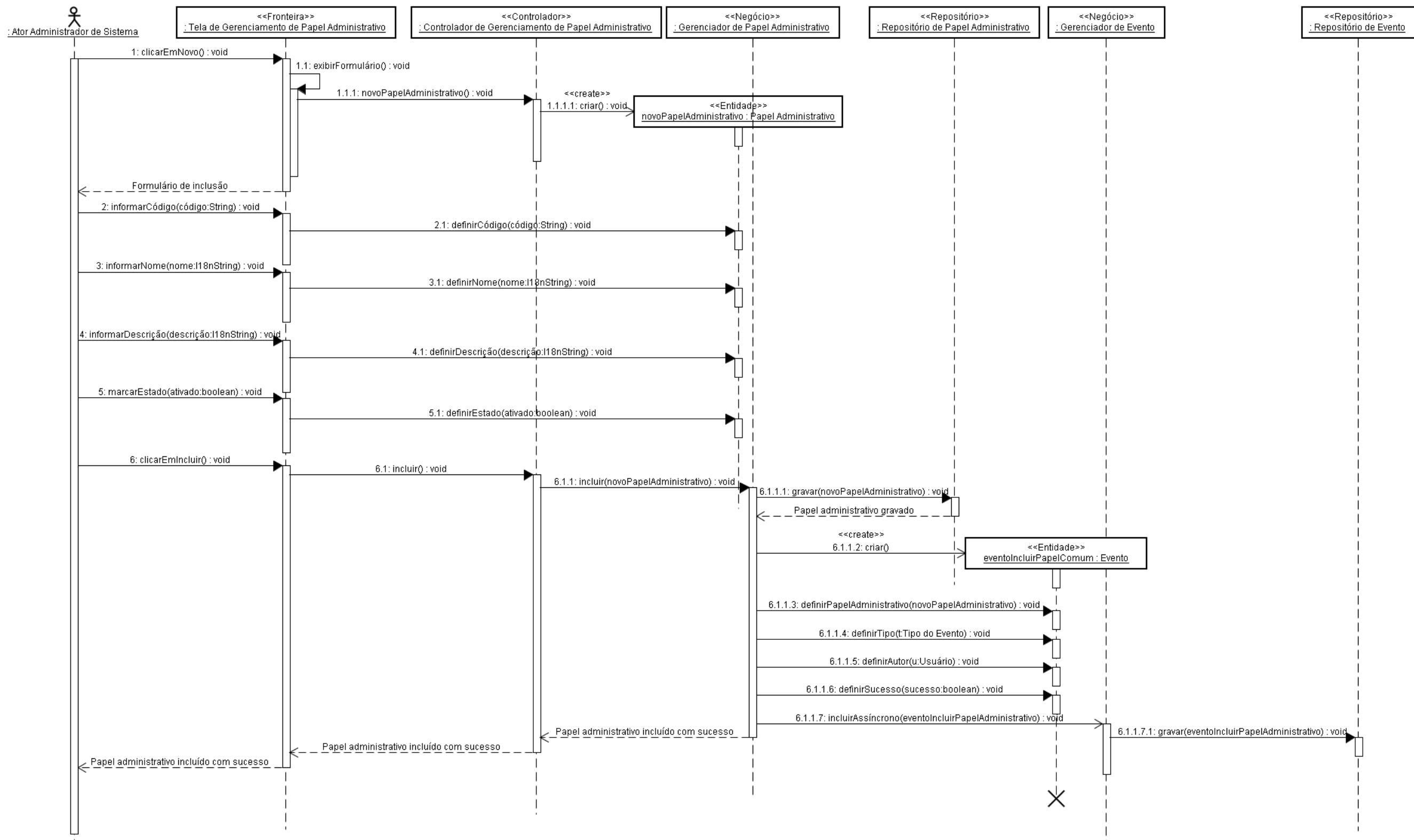


Figura 61: Diagrama de sequência incluir papel administrativo

2.2.8.24. Alterar papel administrativo

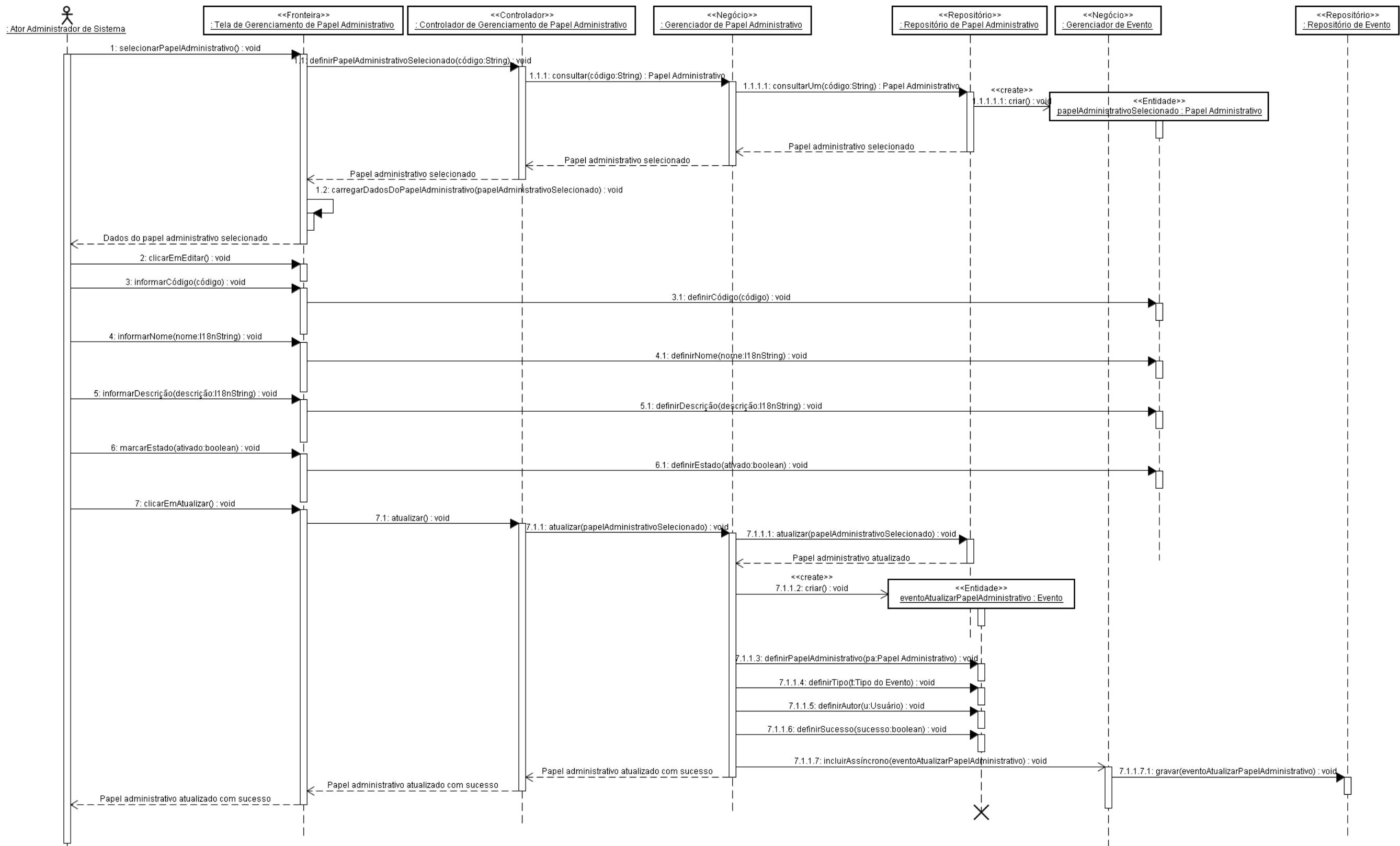


Figura 62: Diagrama de sequência alterar papel administrativo

2.2.8.25. Excluir papel administrativo

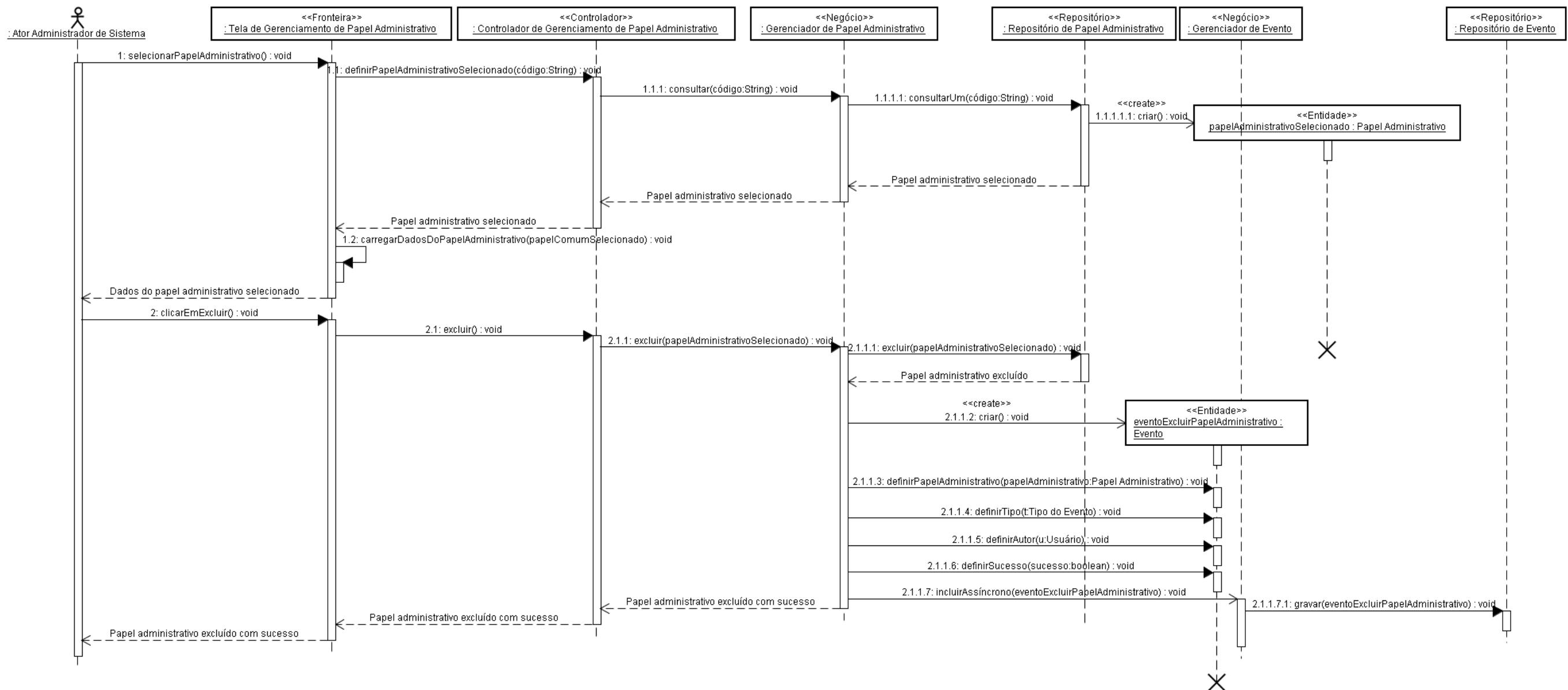


Figura 63: Diagrama de sequência excluir papel administrativo

2.2.8.26. Consultar papel administrativo

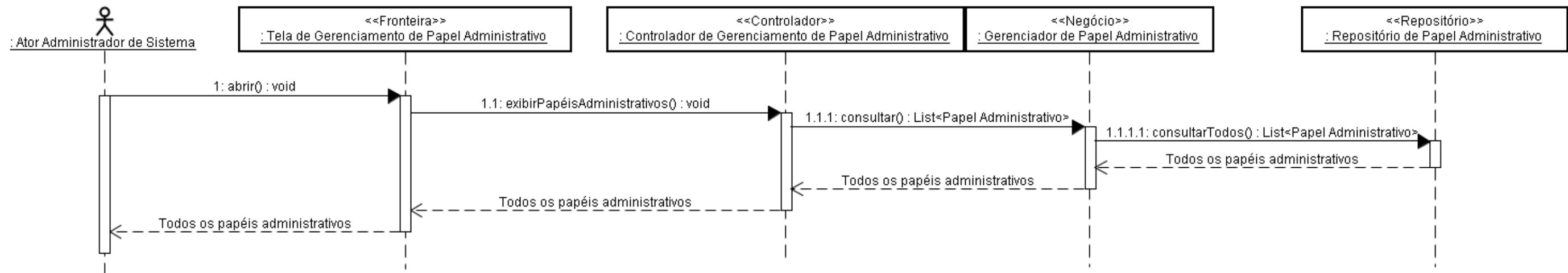


Figura 64: Diagrama de sequência consultar papel administrativo

2.2.8.27. Incluir usuário

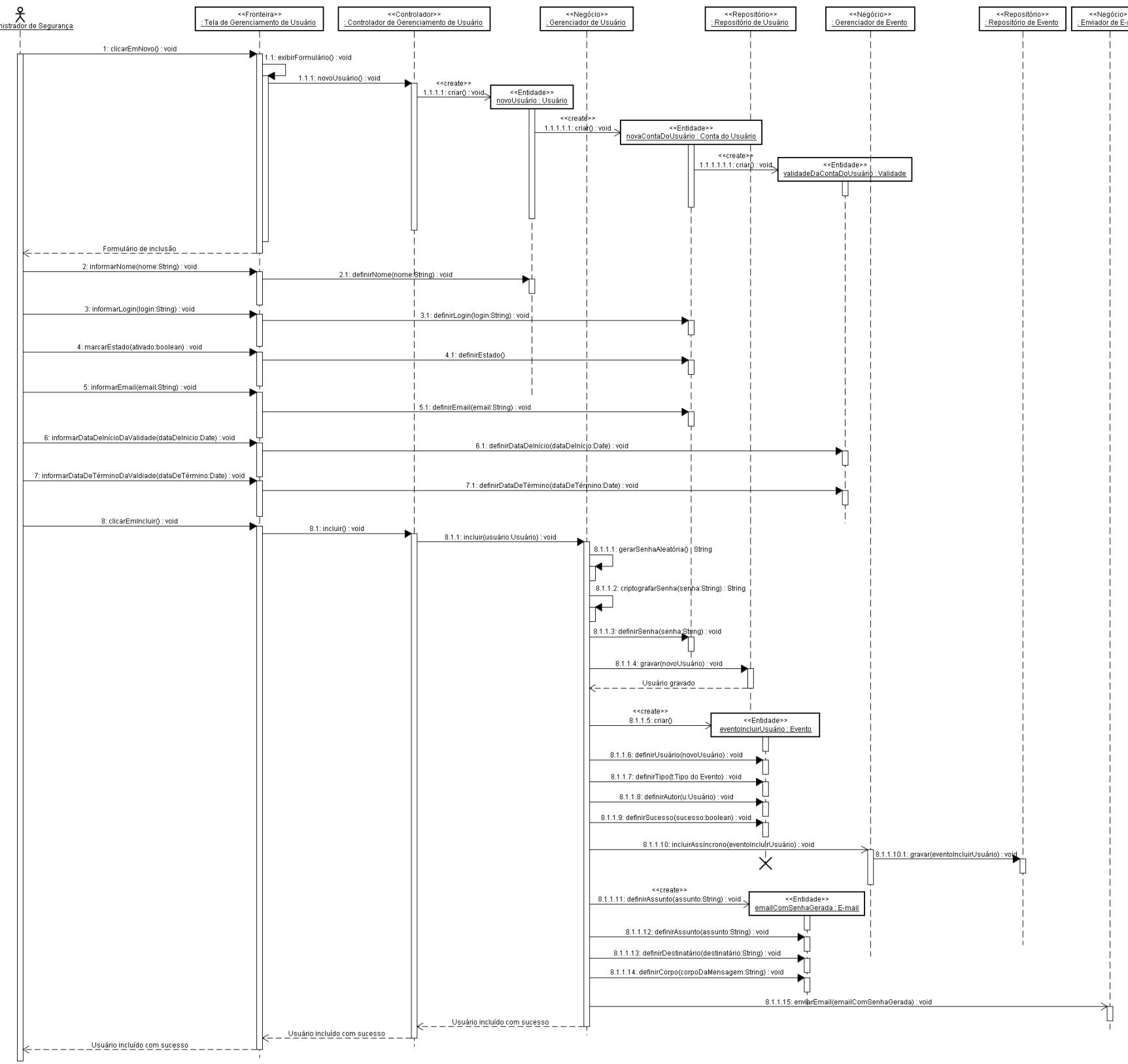


Figura 65: Diagrama de sequência incluir usuário

2.2.8.28. Alterar usuário

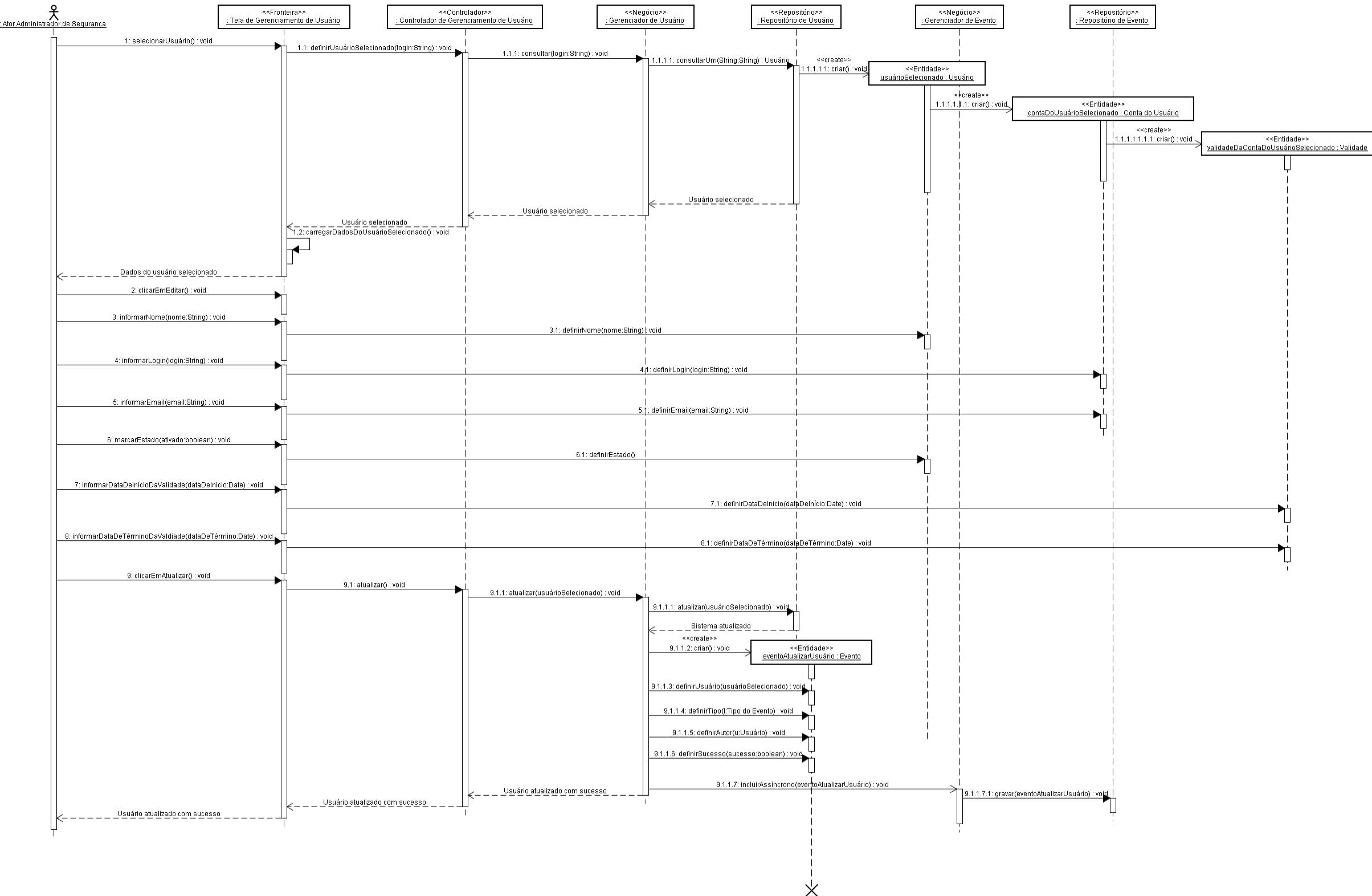


Figura 66: Diagrama de sequência alterar usuário

2.2.8.29. Excluir usuário

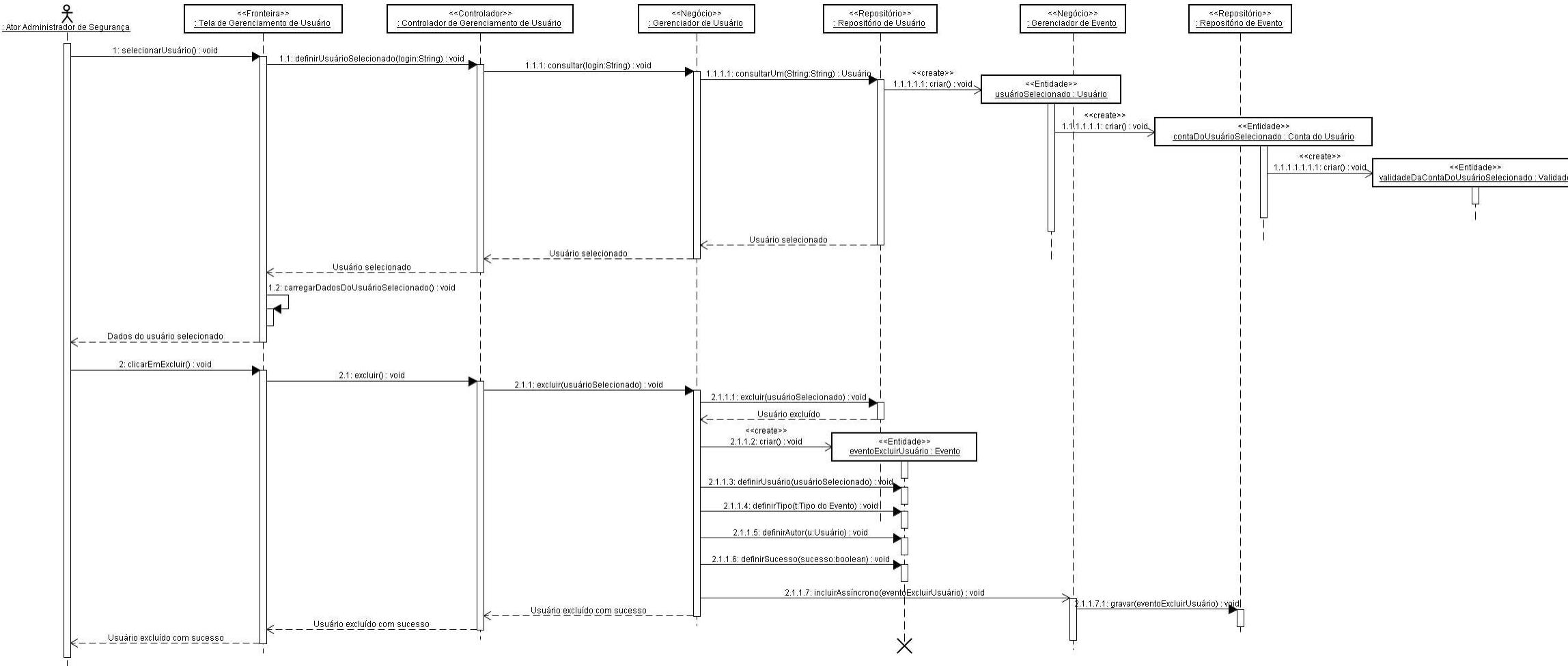


Figura 67: Diagrama de sequência excluir usuário

2.2.8.30. Consultar usuário

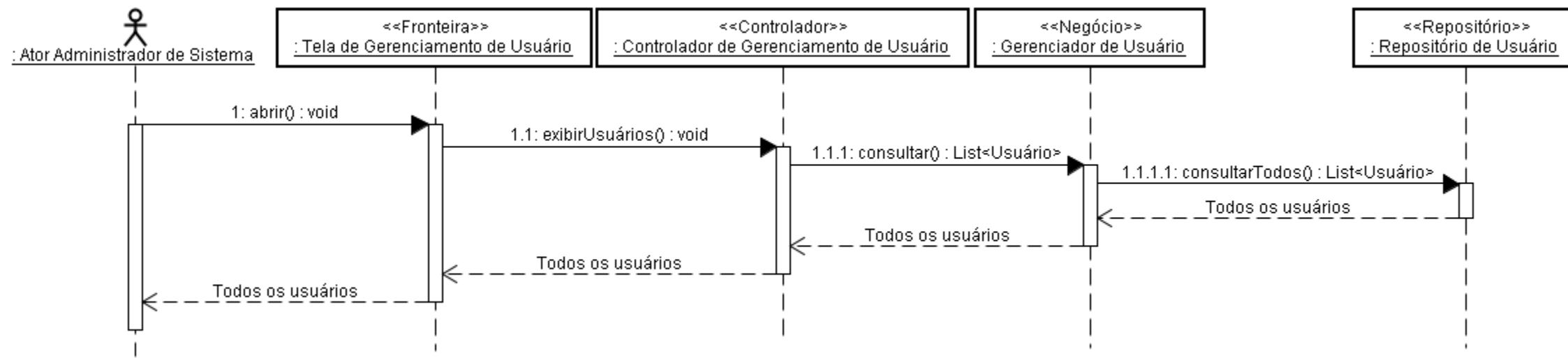


Figura 68: Diagrama de sequência consultar usuário

2.2.8.31. Incluir sistema

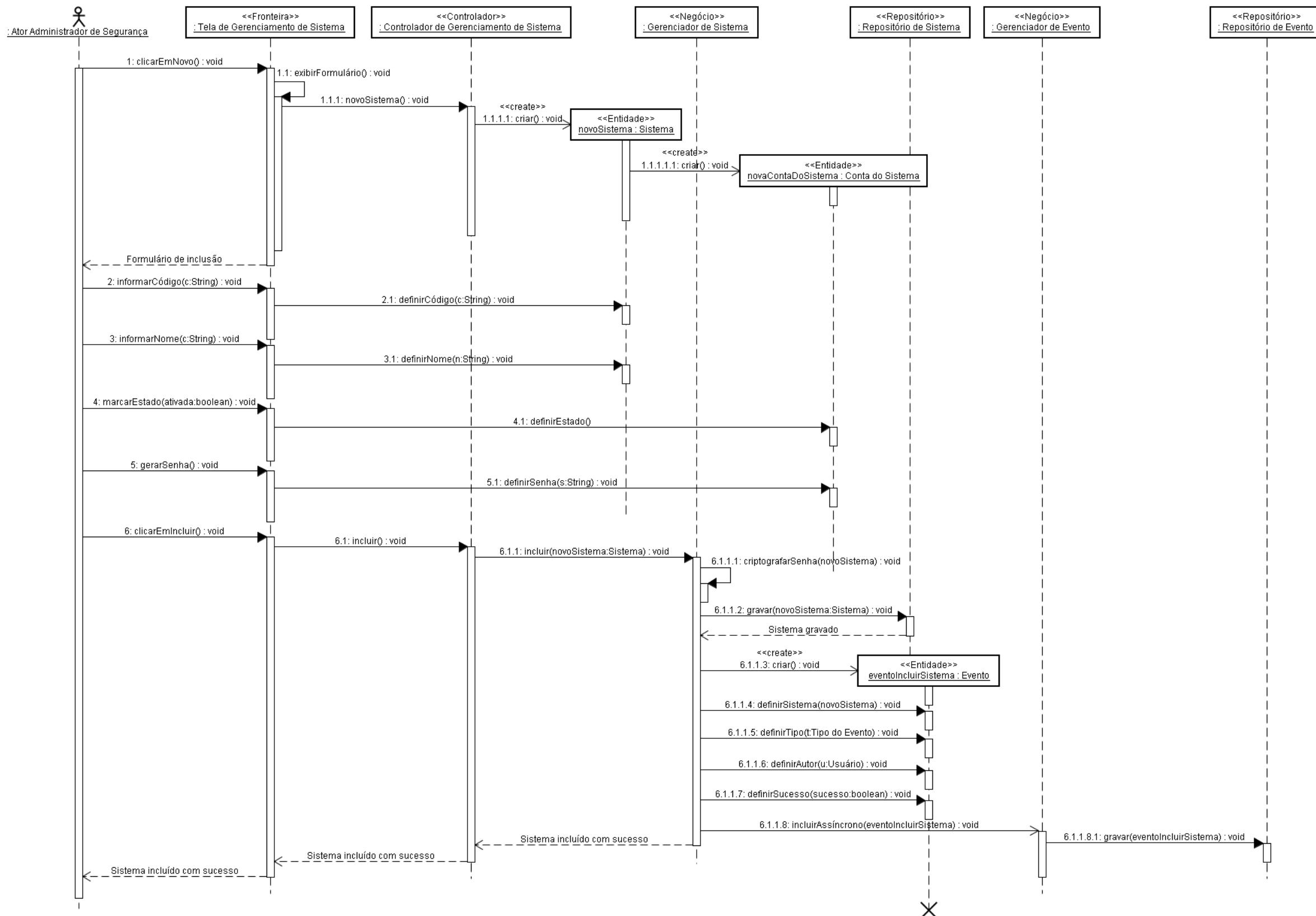


Figura 69: Diagrama de sequência incluir sistema

2.2.8.32. Alterar sistema

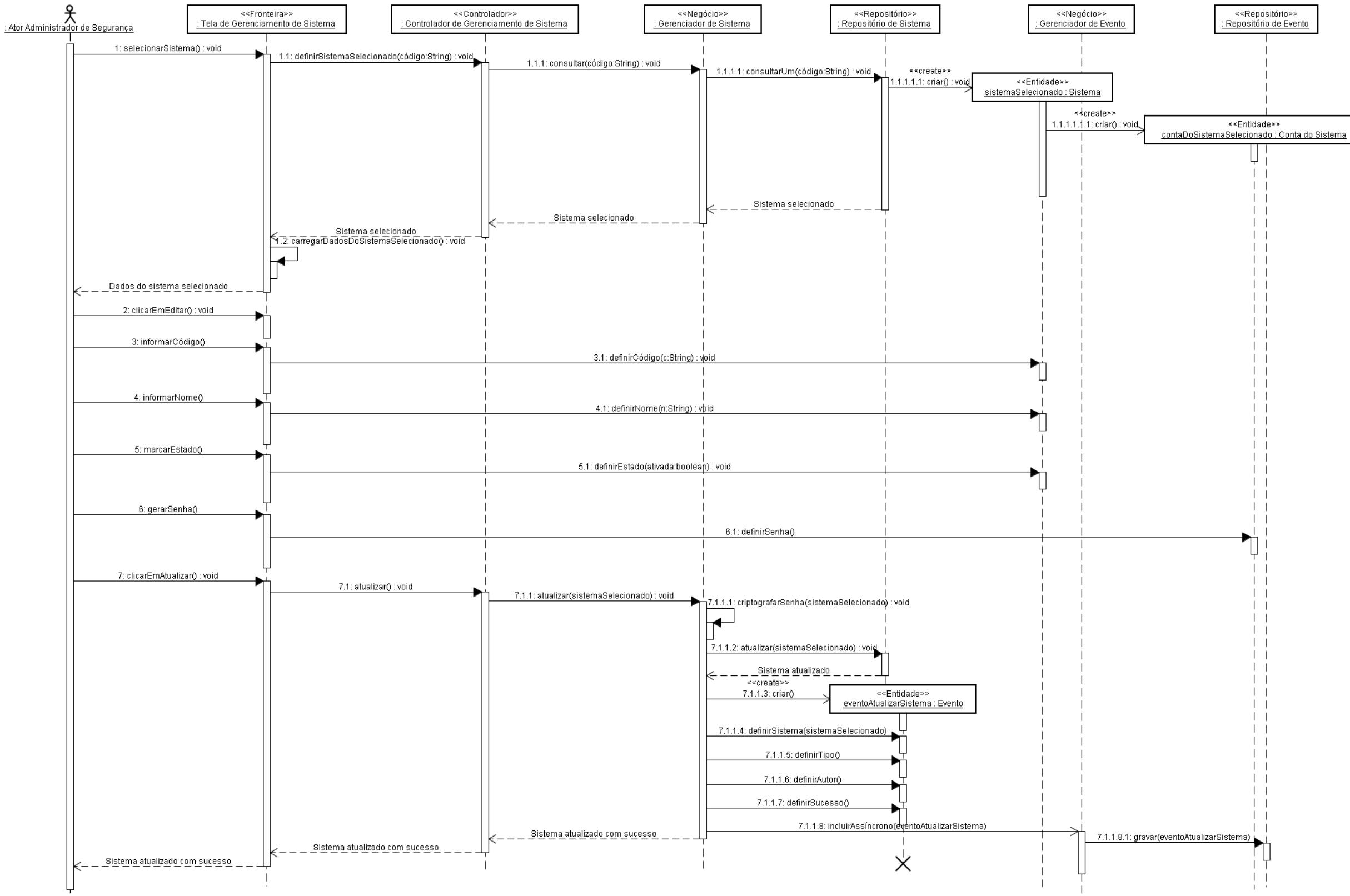


Figura 70: Diagrama de sequência alterar sistema

2.2.8.33. Excluir sistema

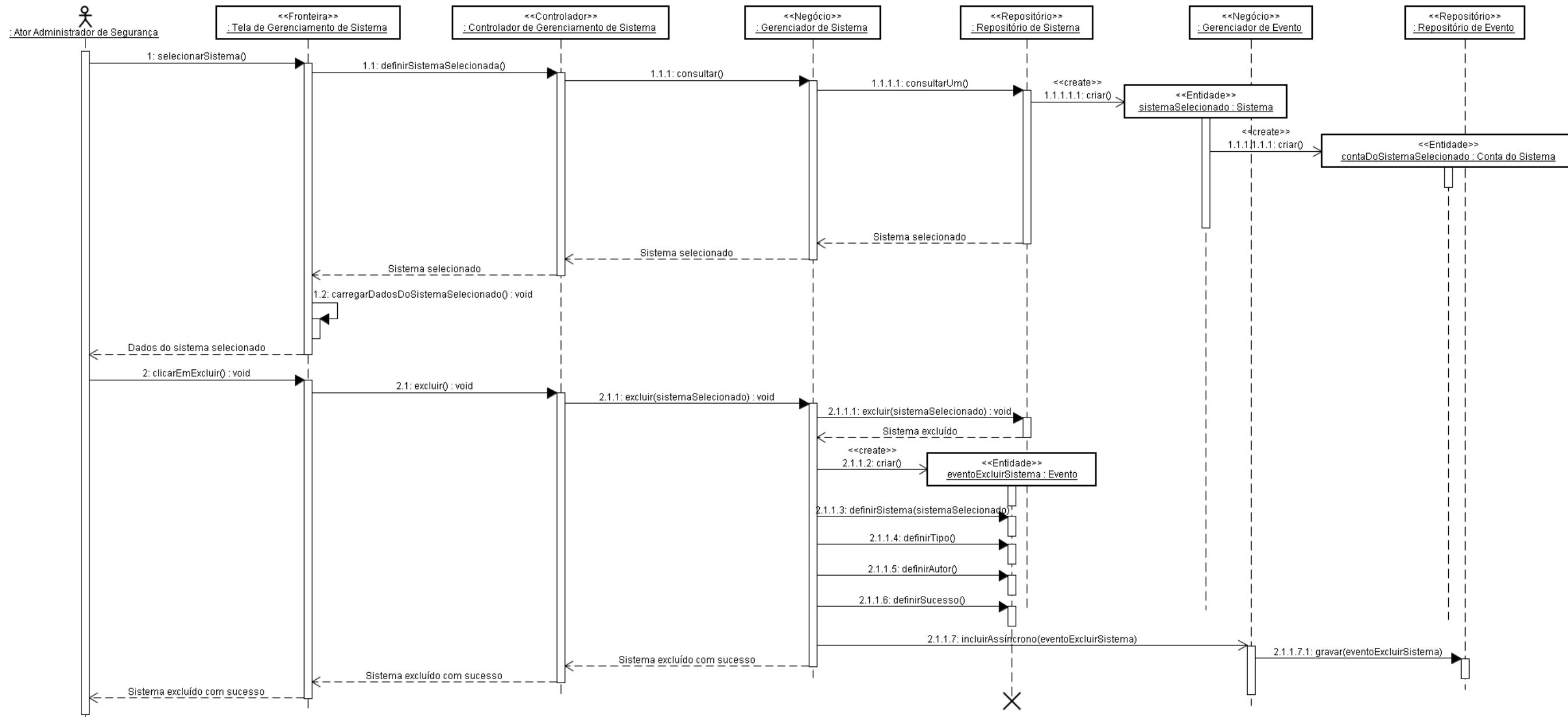


Figura 71: Diagrama de sequência excluir sistema

2.2.8.34. Consultar sistema

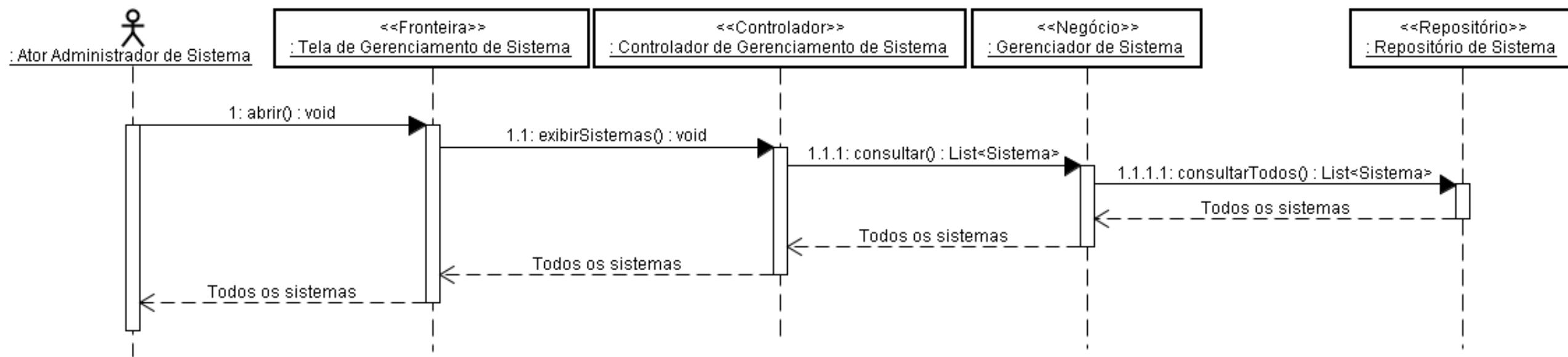
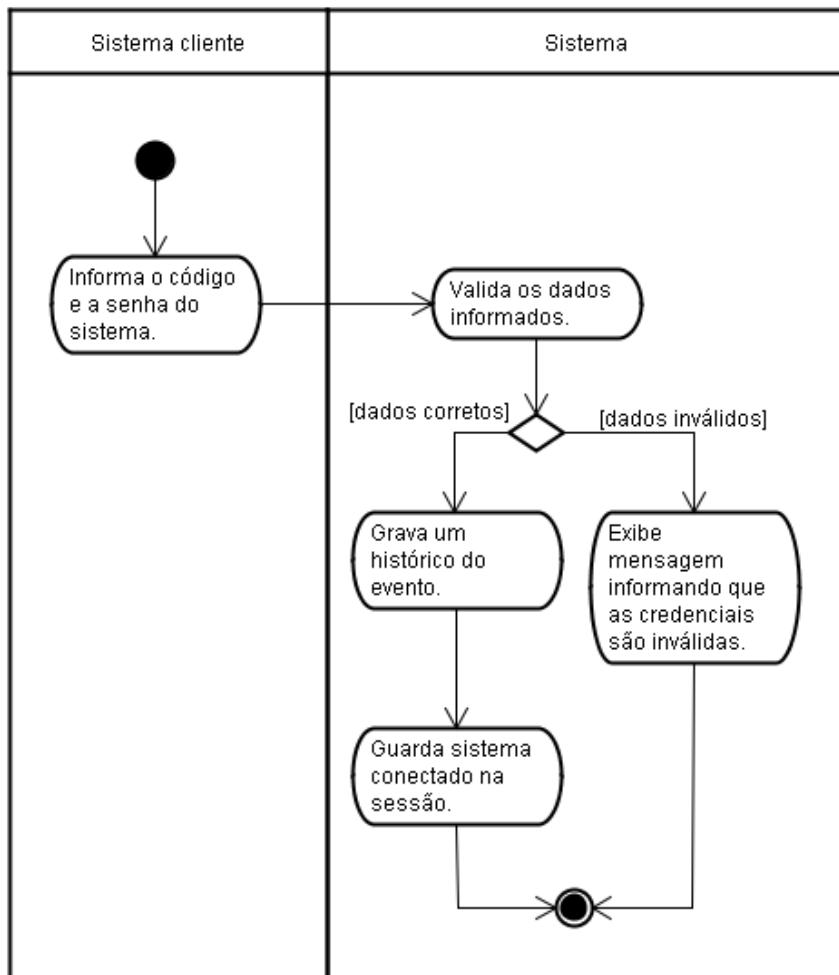


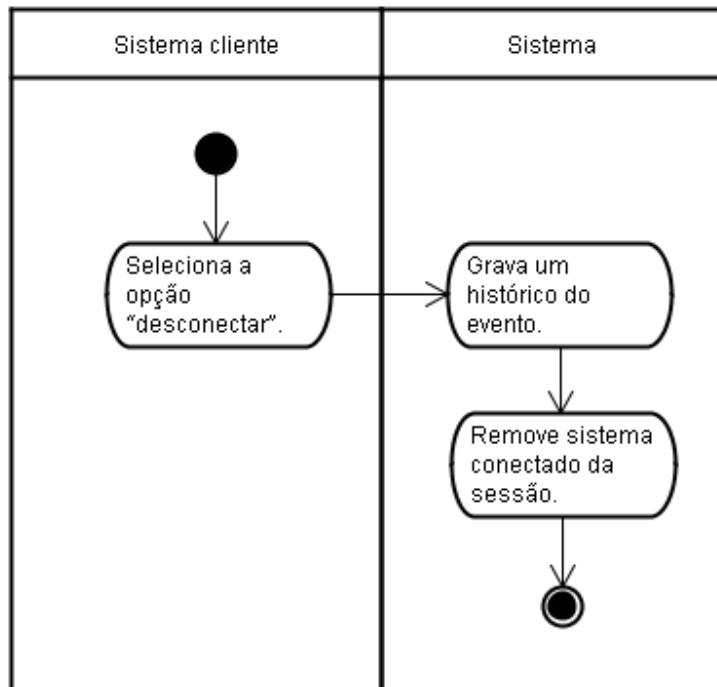
Figura 72: Diagrama de sequência consultar sistema

2.2.9. DIAGRAMAS DE ATIVIDADE

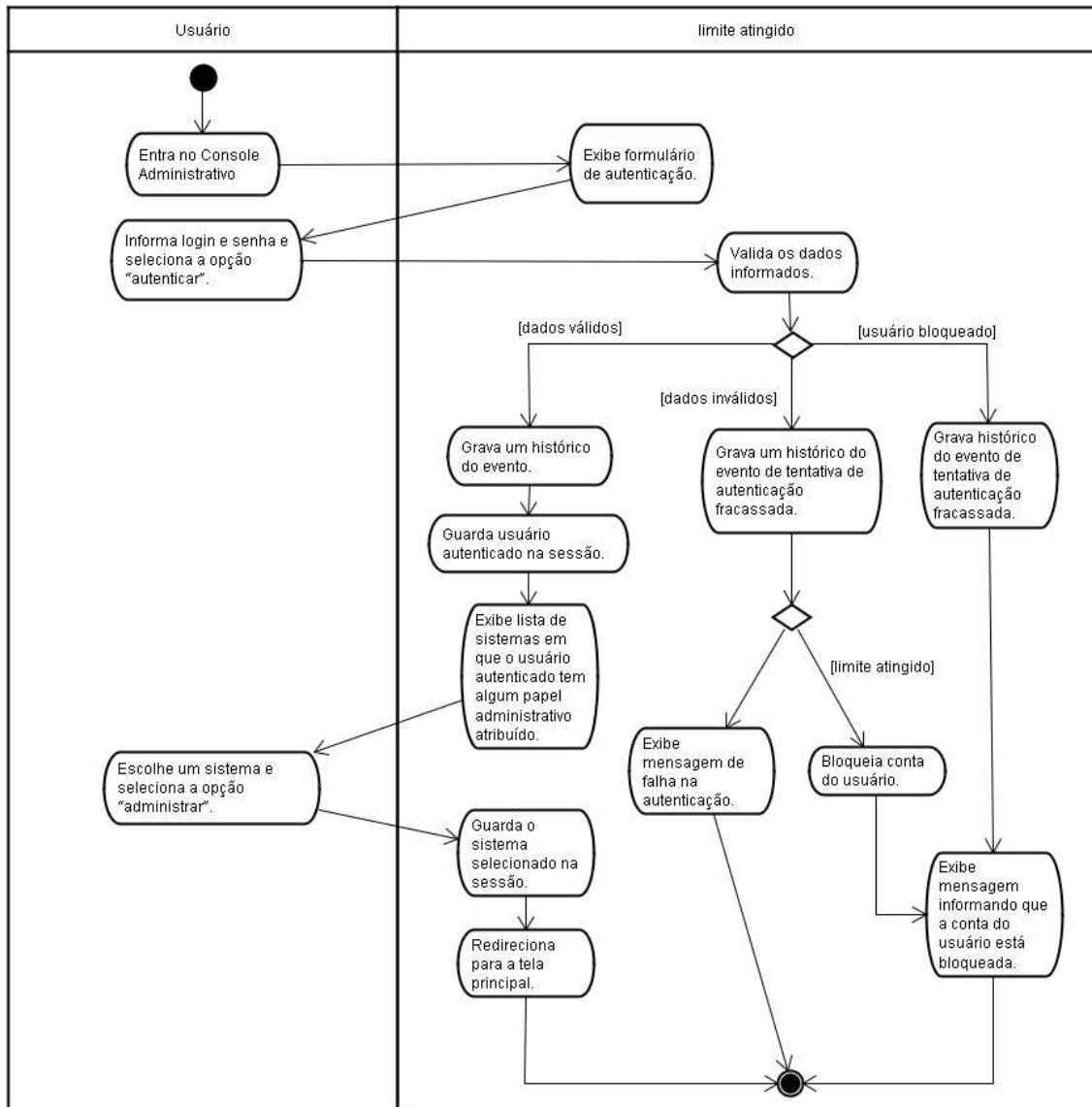
2.2.9.1. Conectar sistema cliente ao serviço de segurança



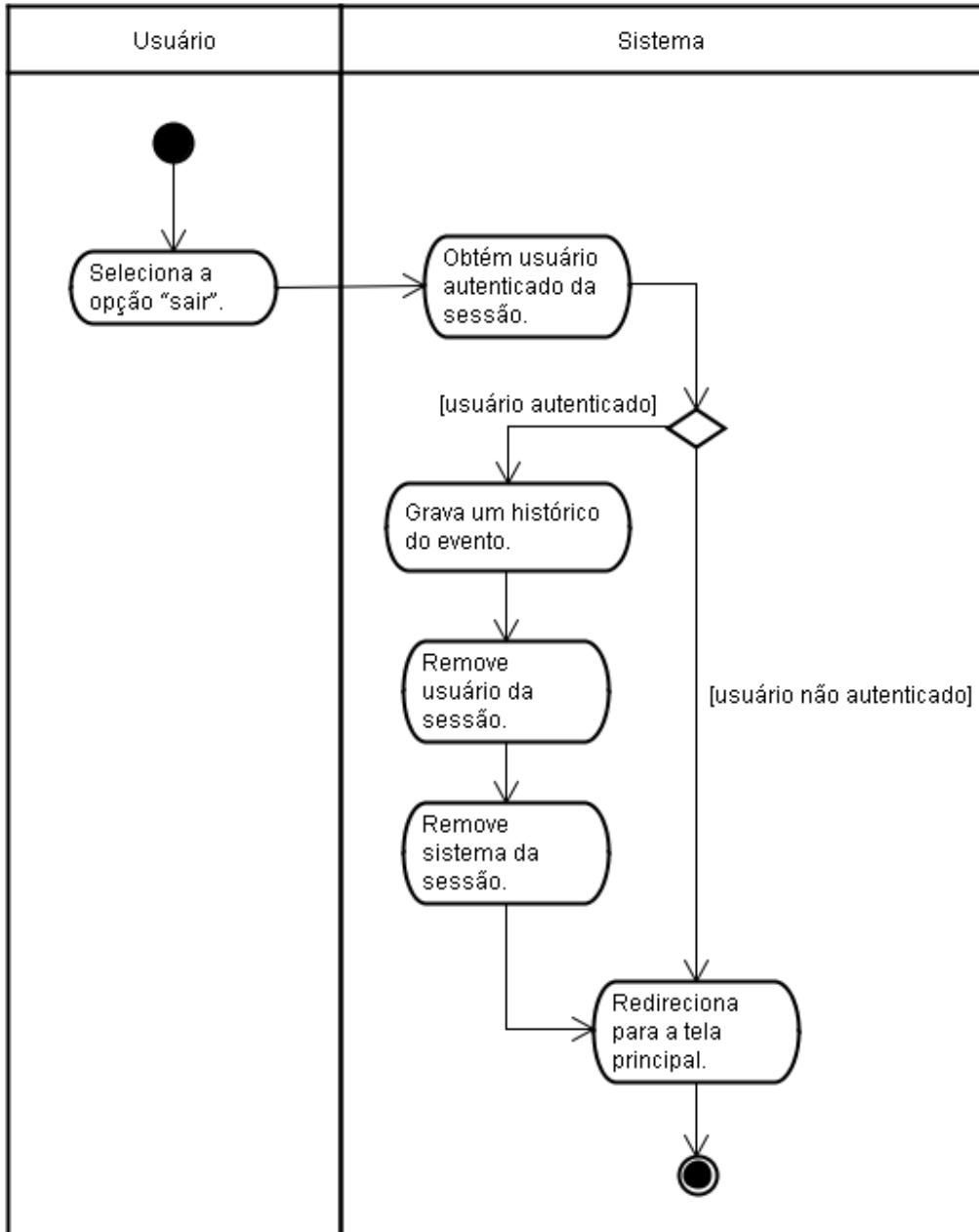
2.2.9.2. Desconectar sistema cliente do serviço de segurança



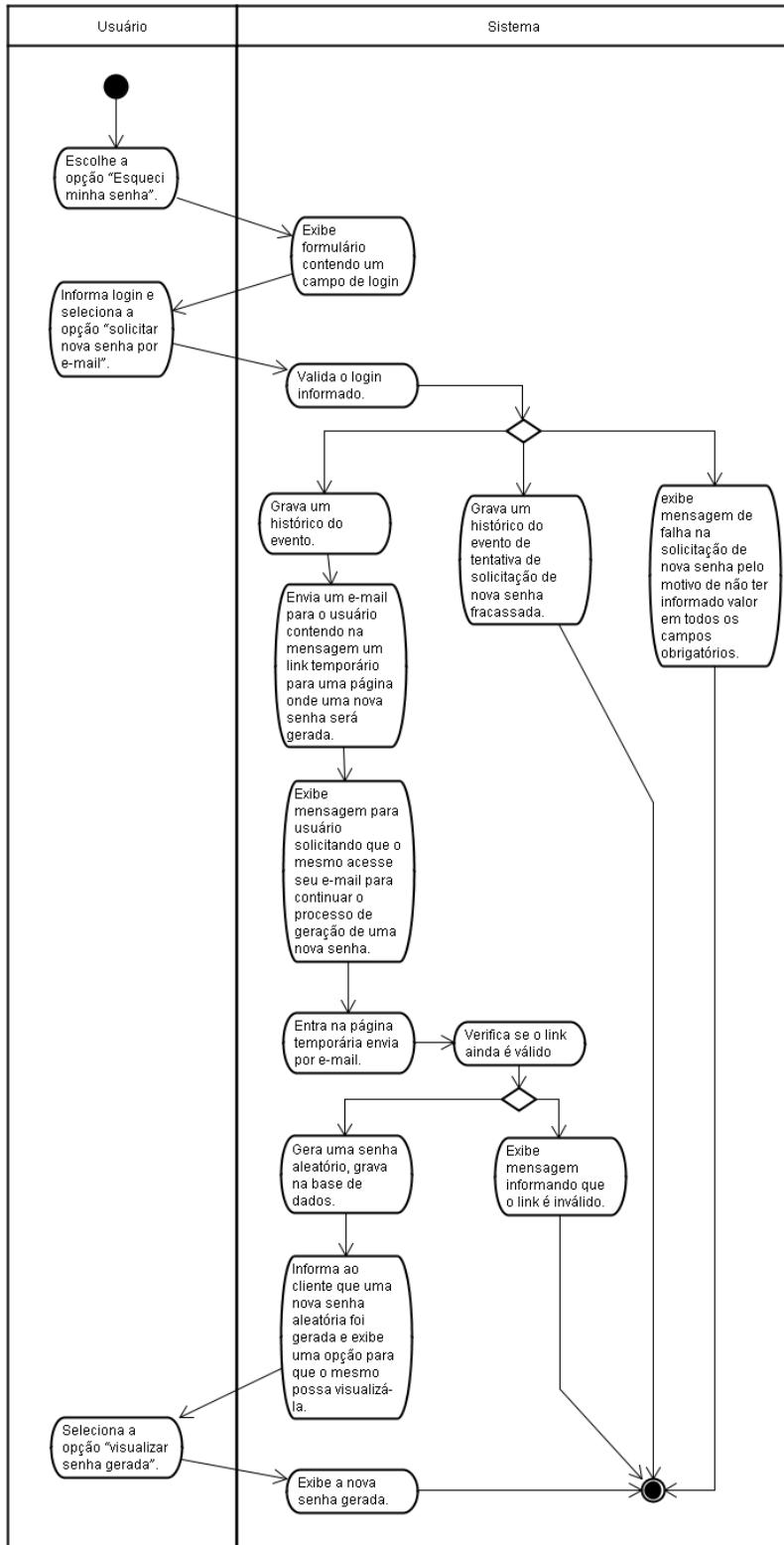
2.2.9.3. Realizar logon do usuário



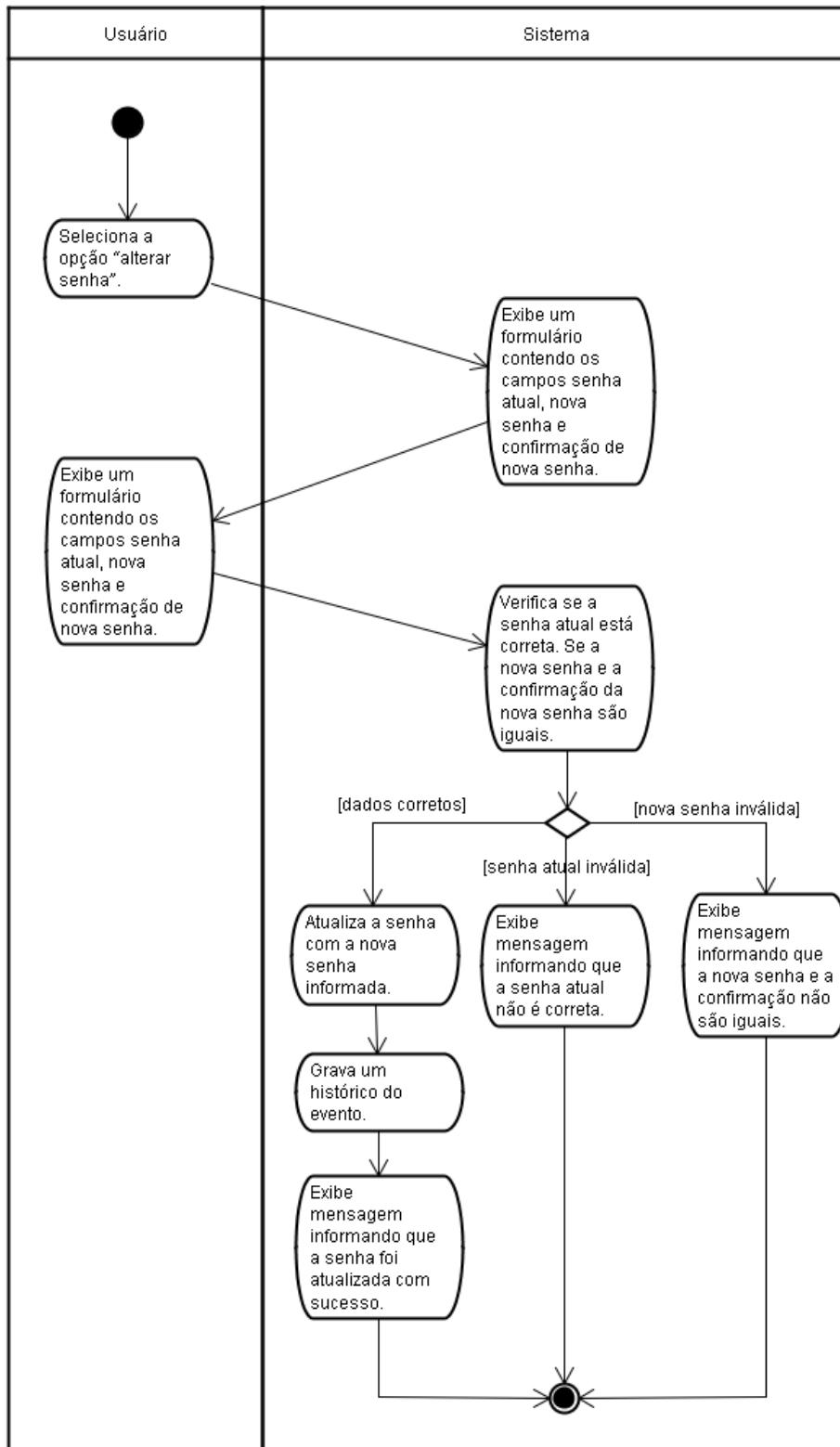
Realizar logoff de usuário



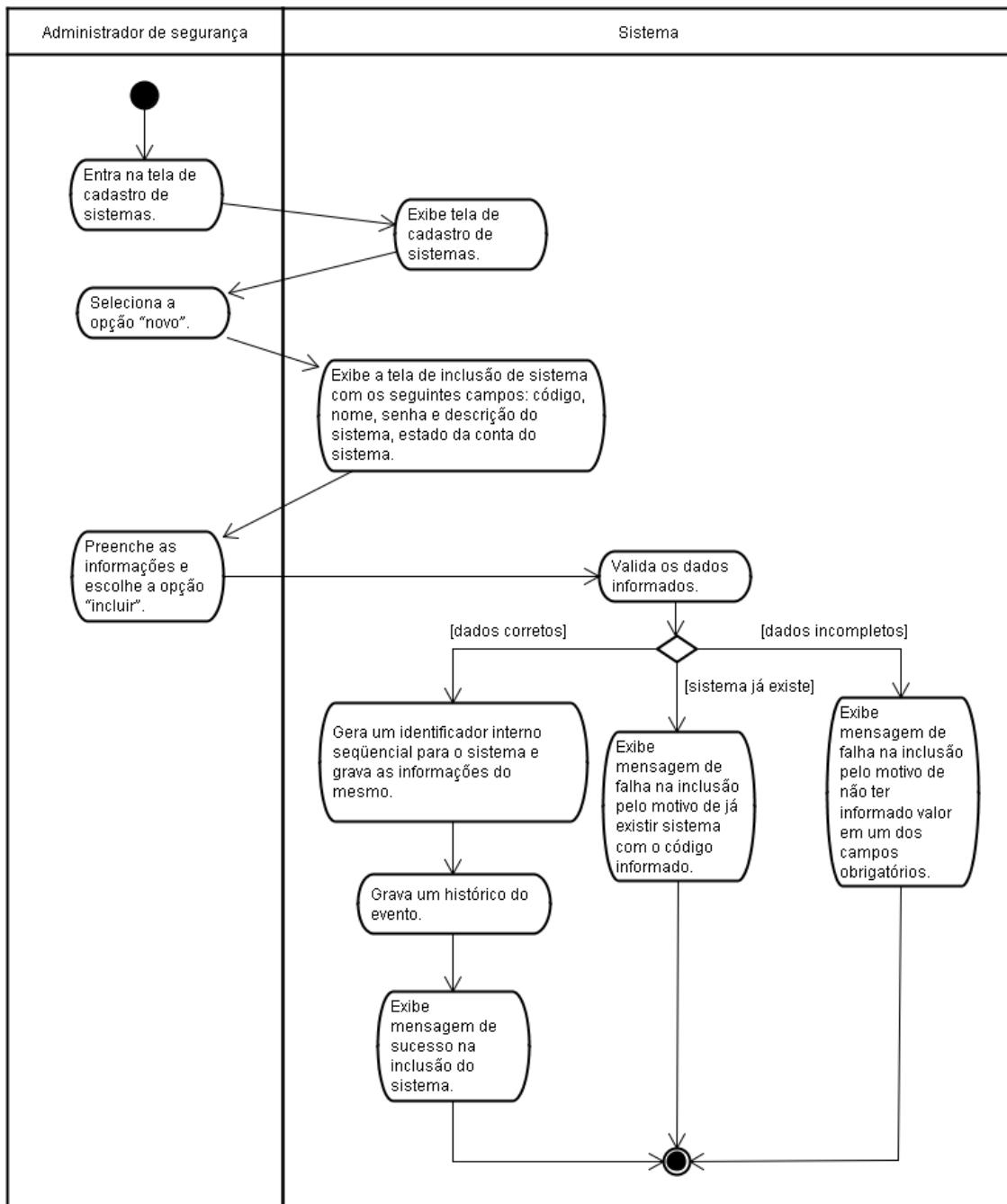
2.2.9.4. Solicitar nova senha por e-mail



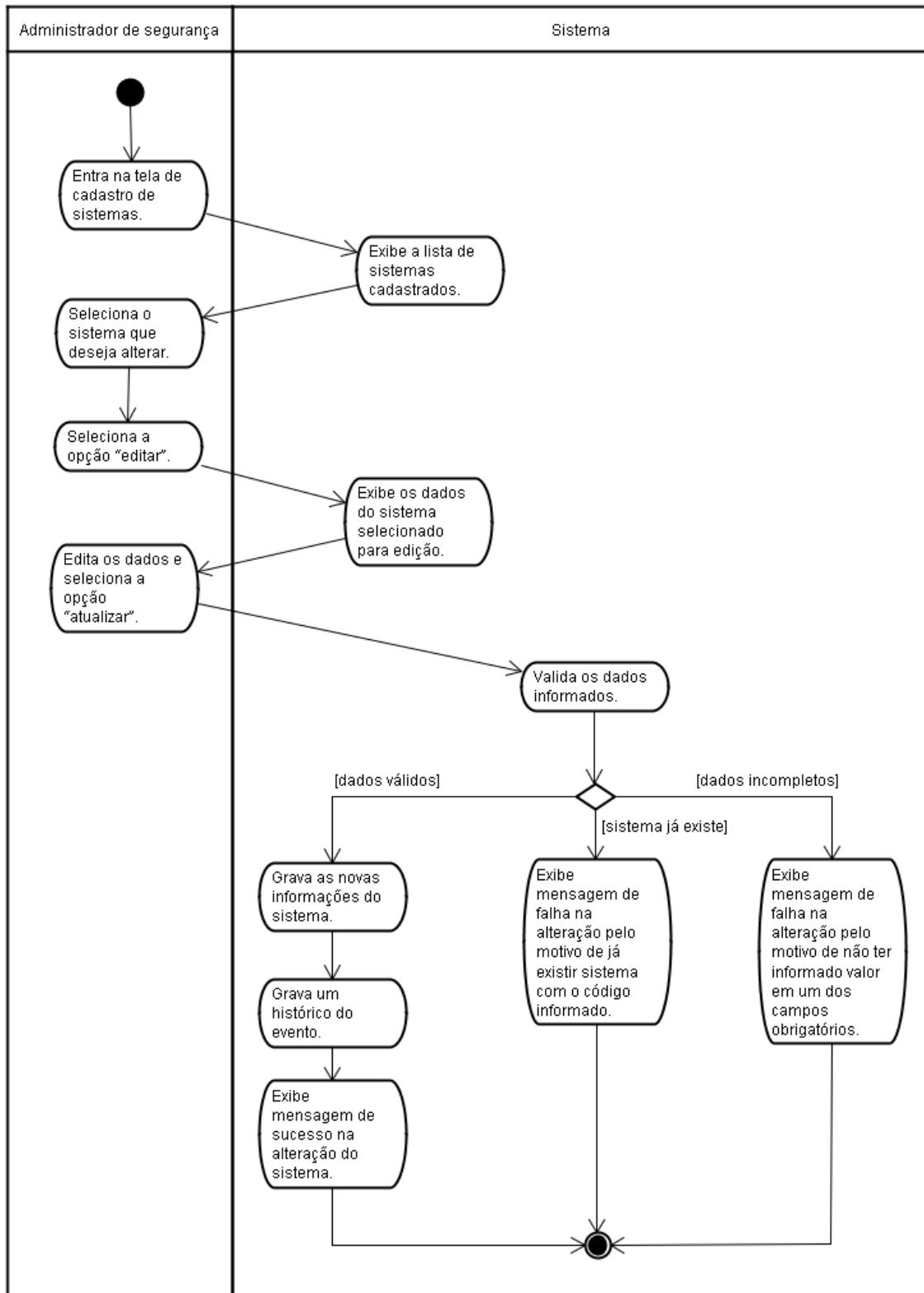
2.2.9.5. Alterar senha



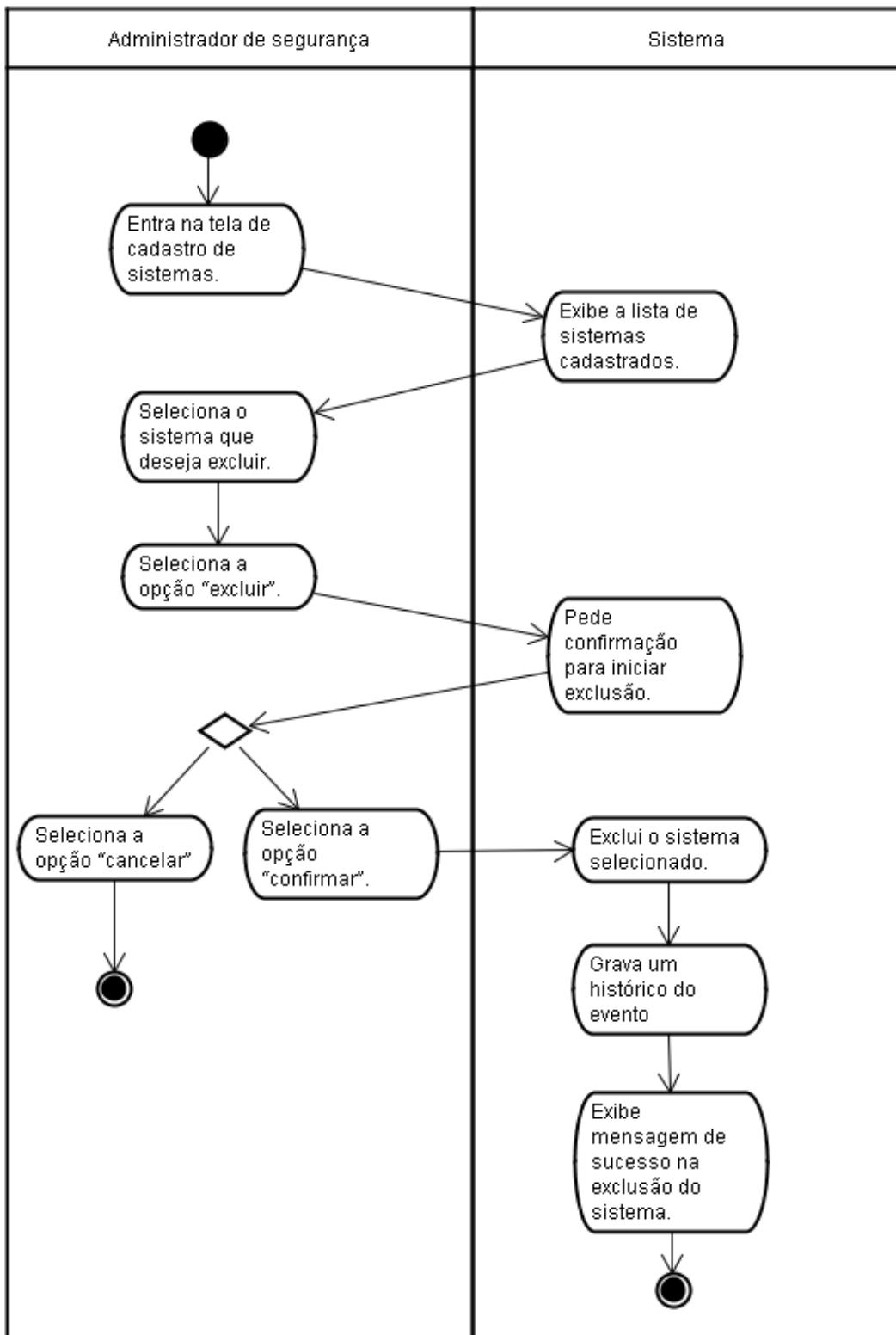
2.2.9.6. Incluir sistema



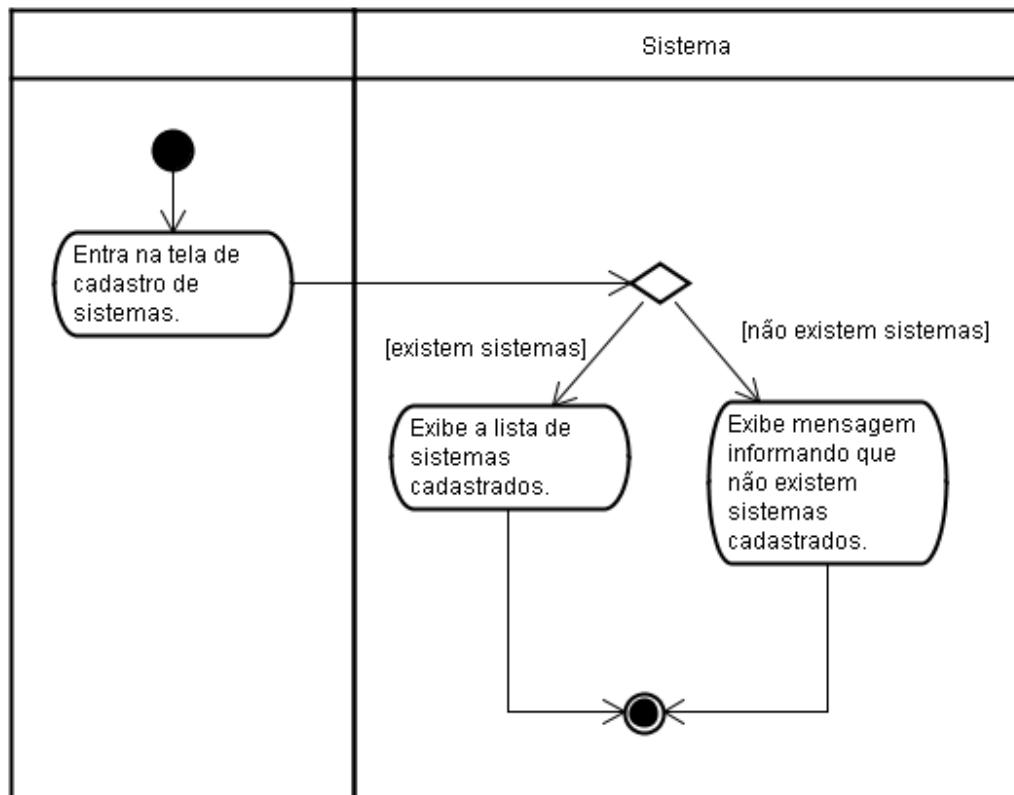
2.2.9.7. Alterar sistema



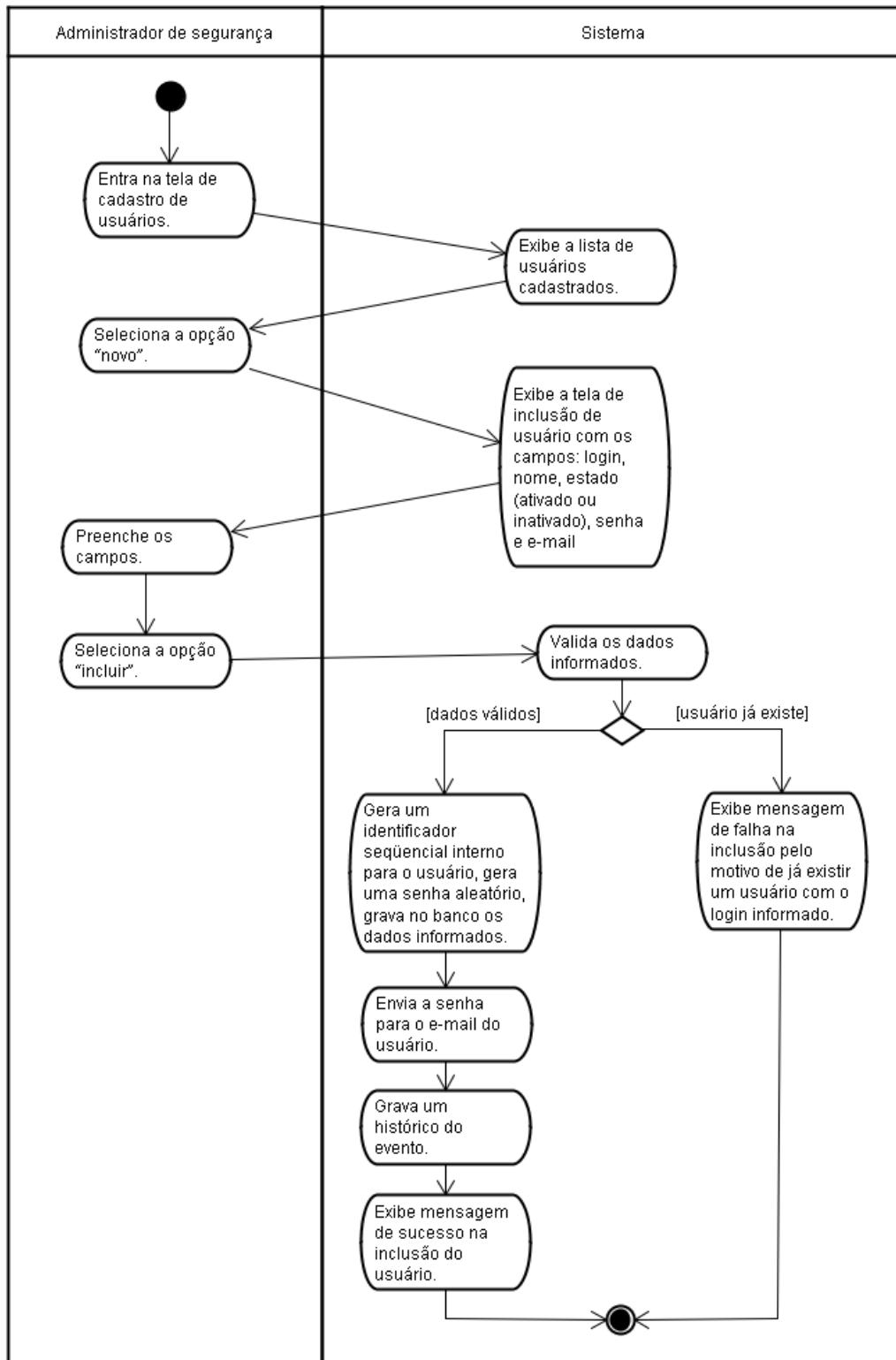
2.2.9.8. Excluir sistema



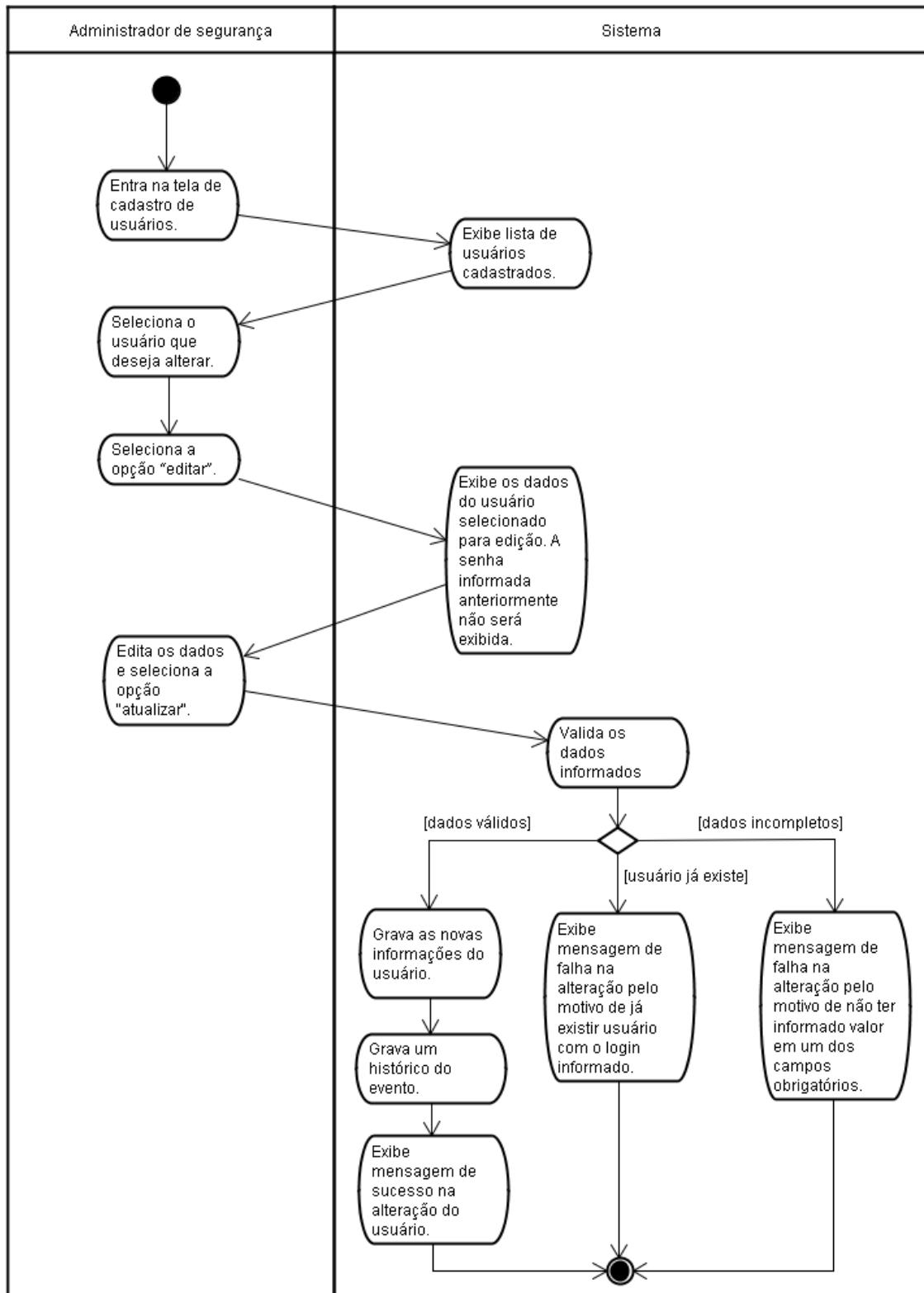
2.2.9.9. Consultar sistema



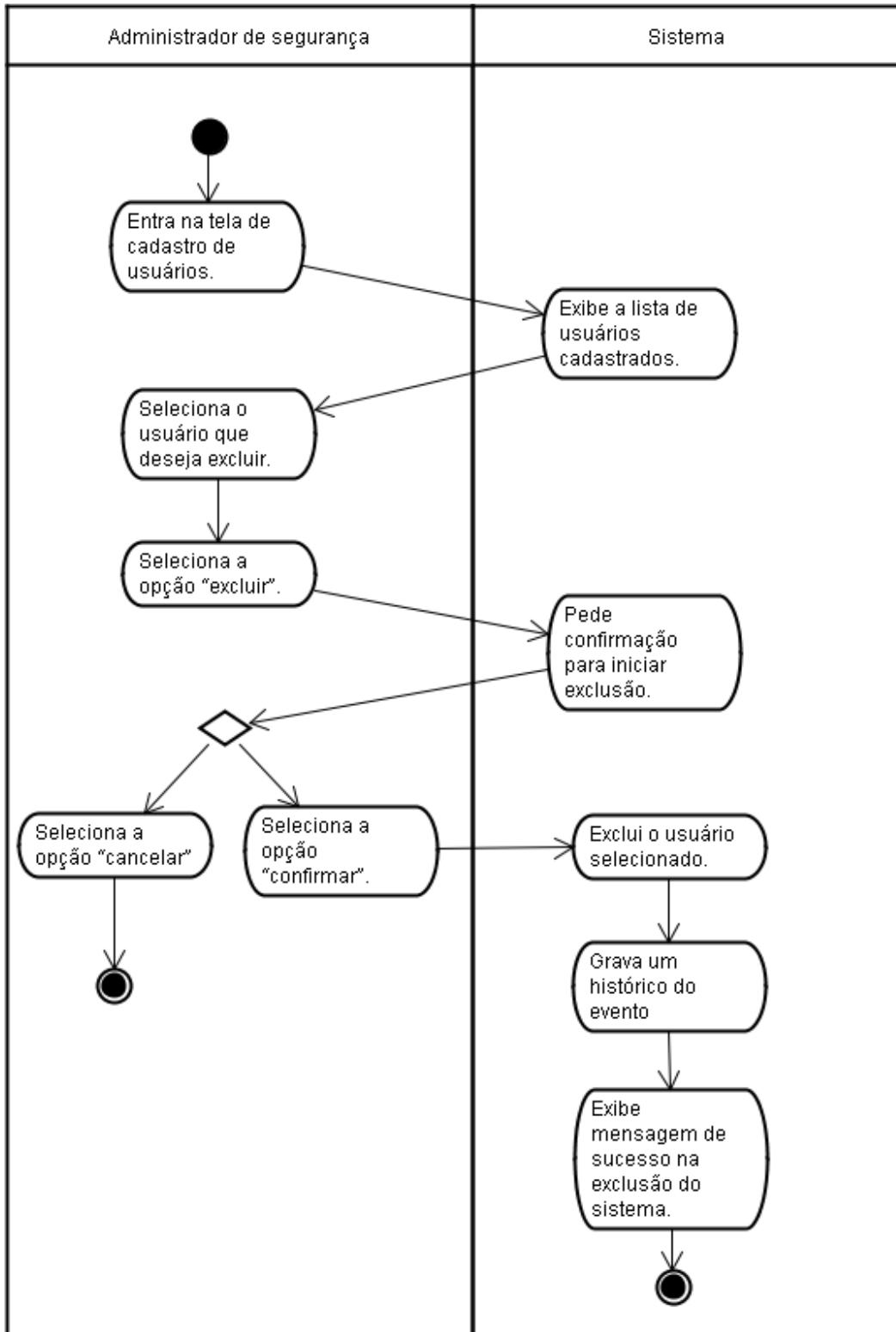
2.2.9.10. Incluir usuário



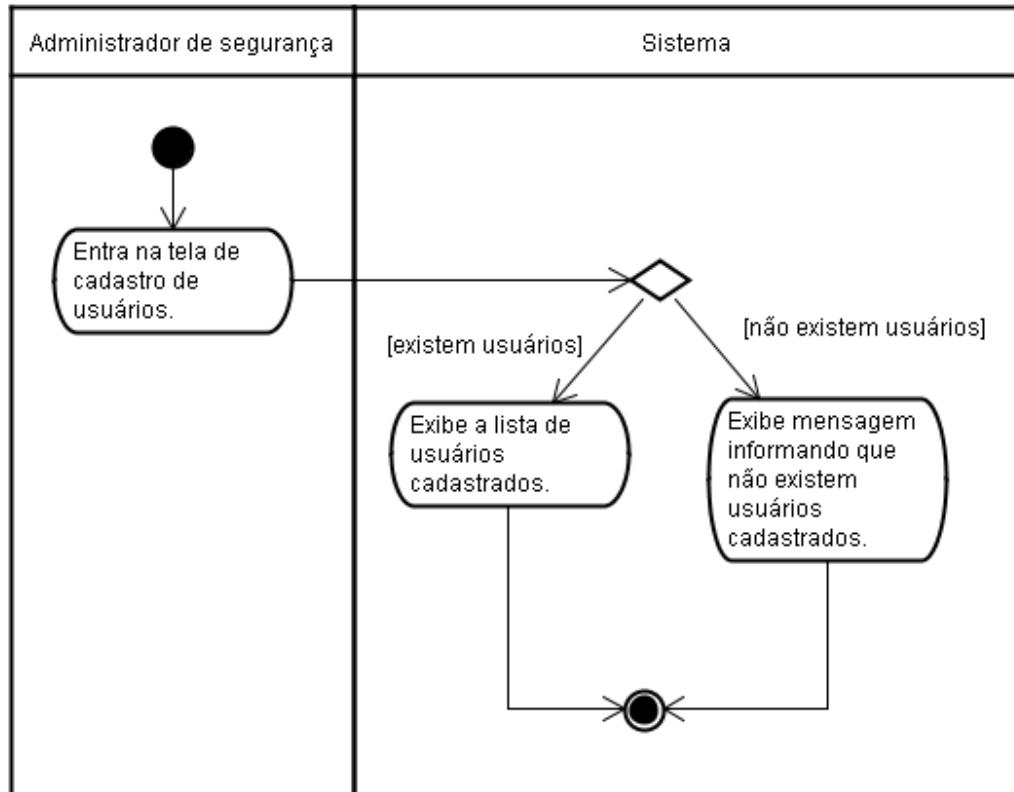
2.2.9.11. Alterar usuário



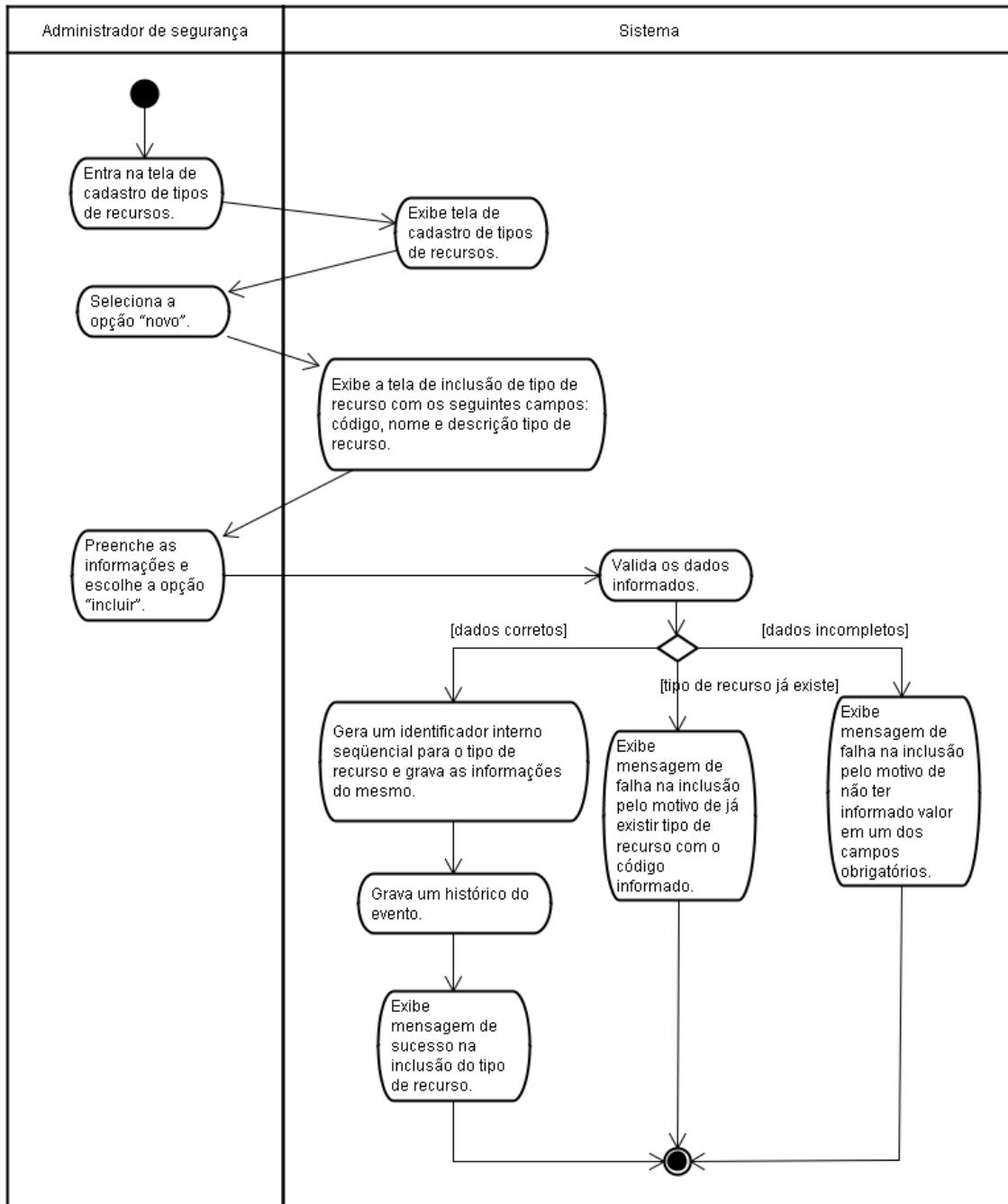
2.2.9.12. Excluir usuário



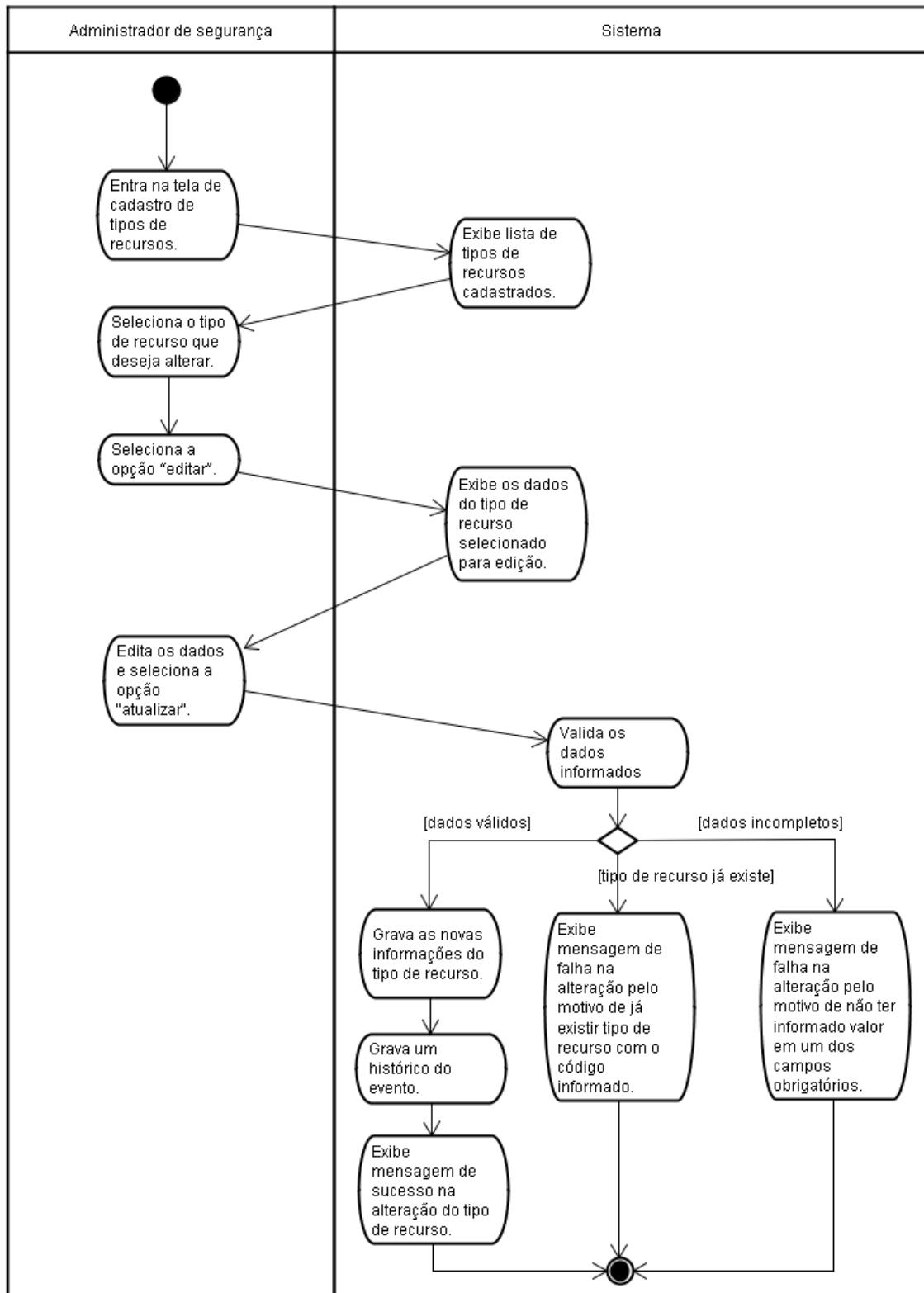
2.2.9.13. Consultar usuário



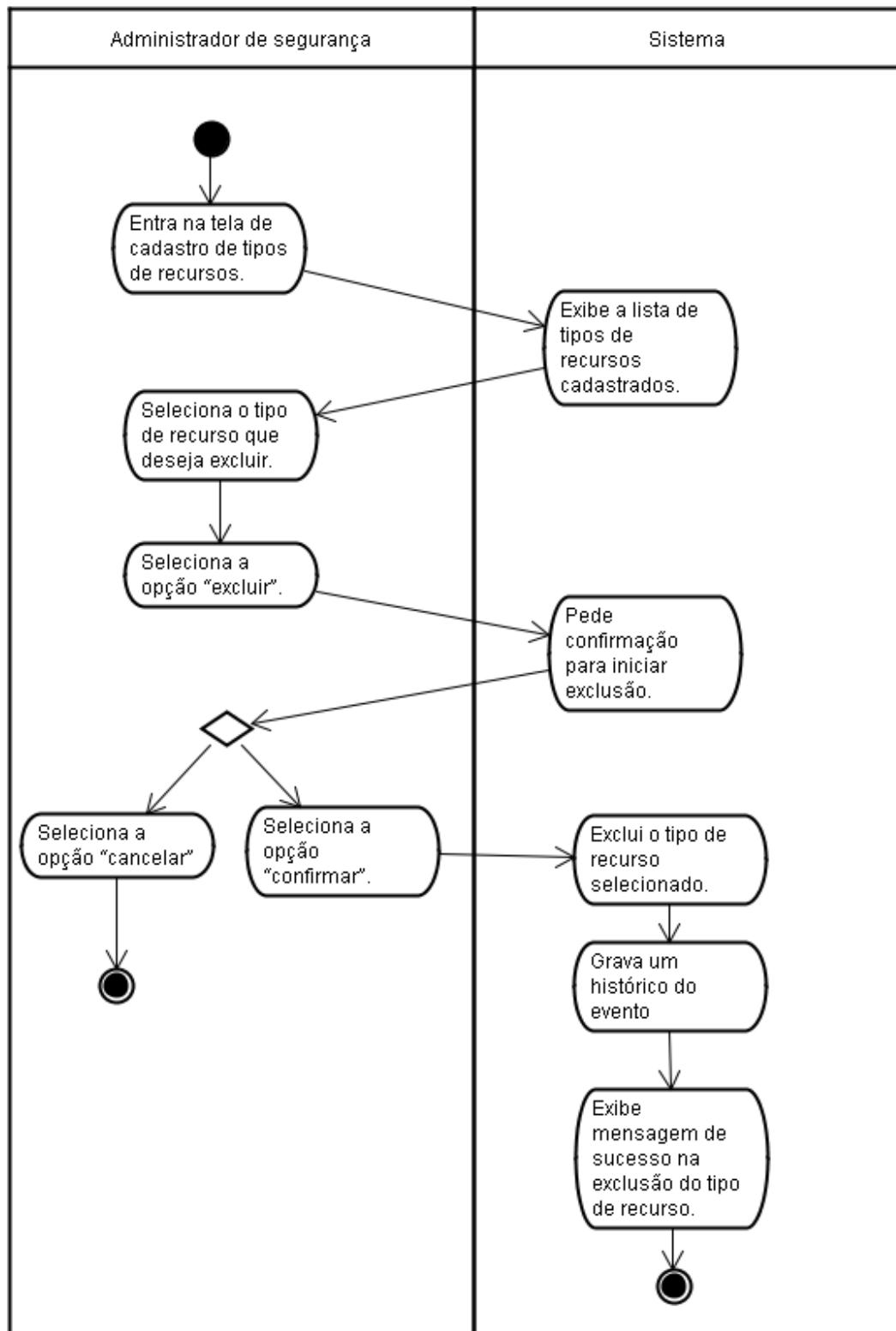
2.2.9.14. Incluir tipo de recurso



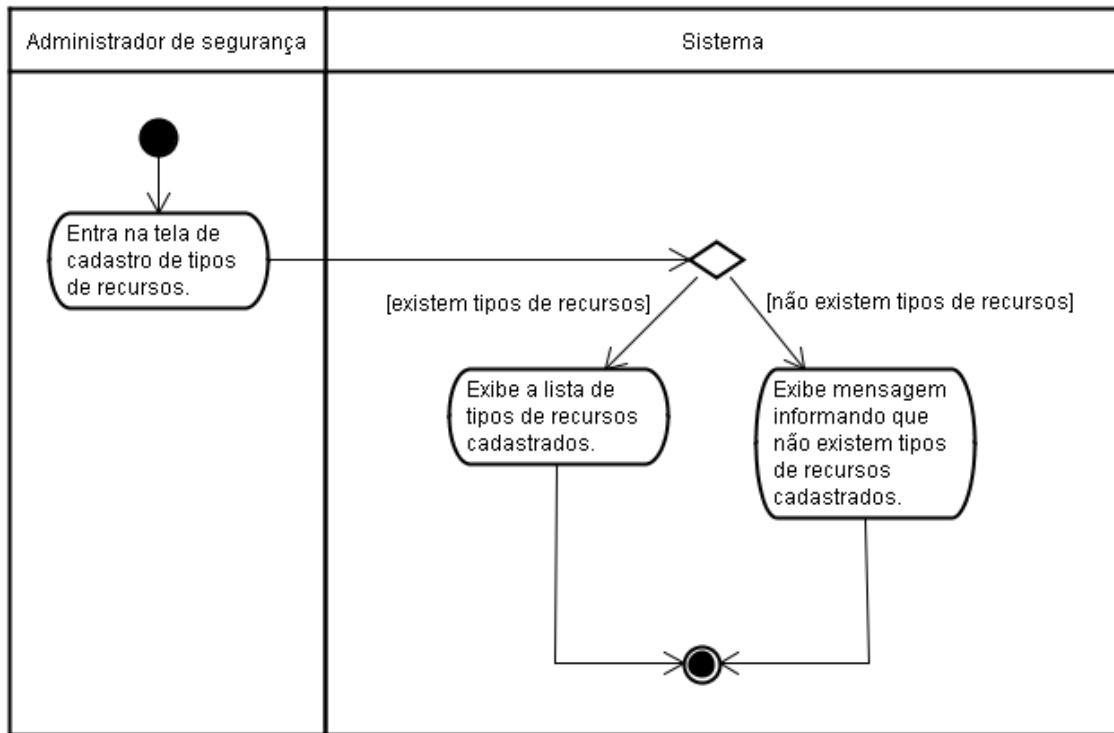
2.2.9.15. Alterar tipo de recurso



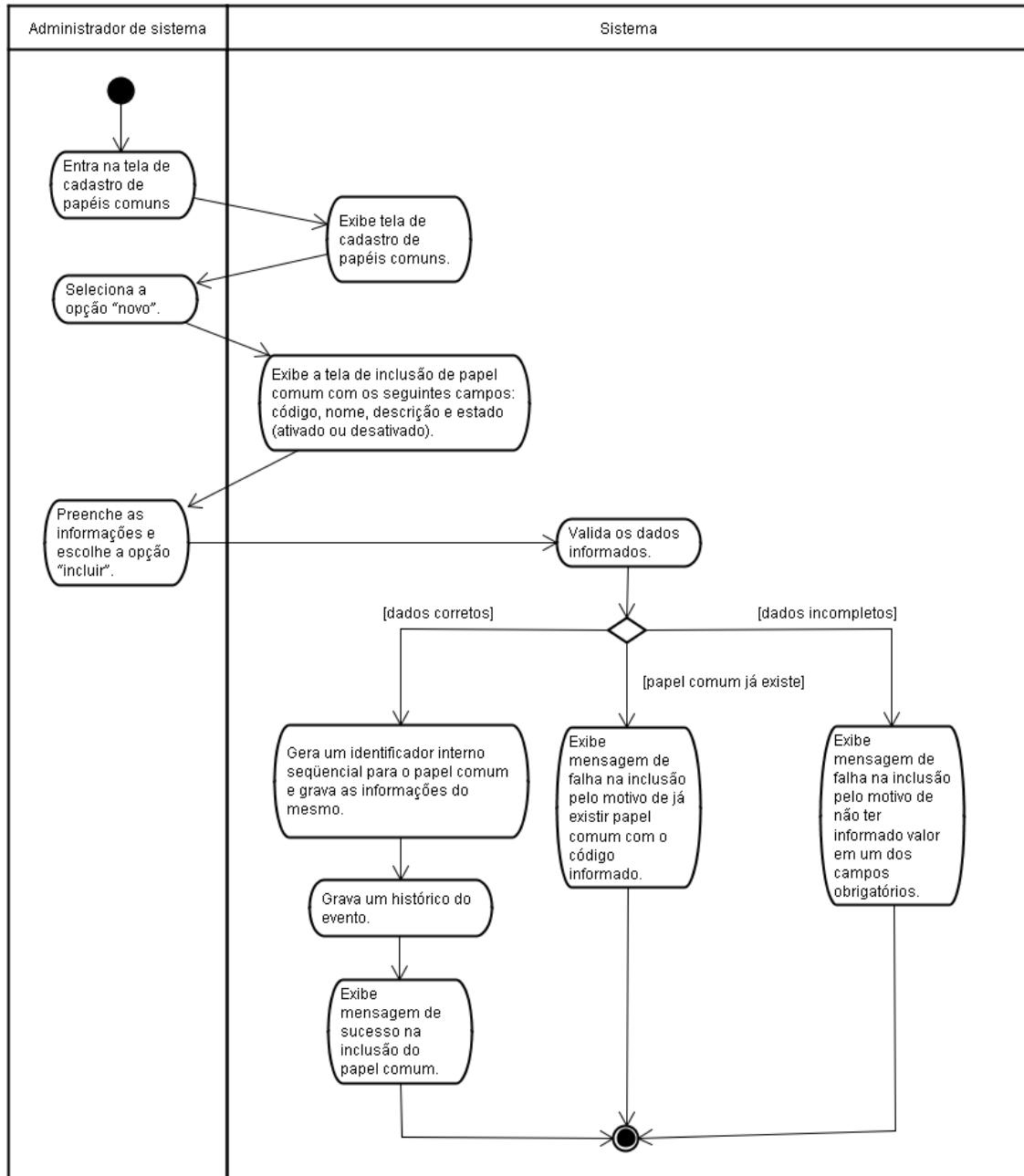
2.2.9.16. Excluir tipo de recurso



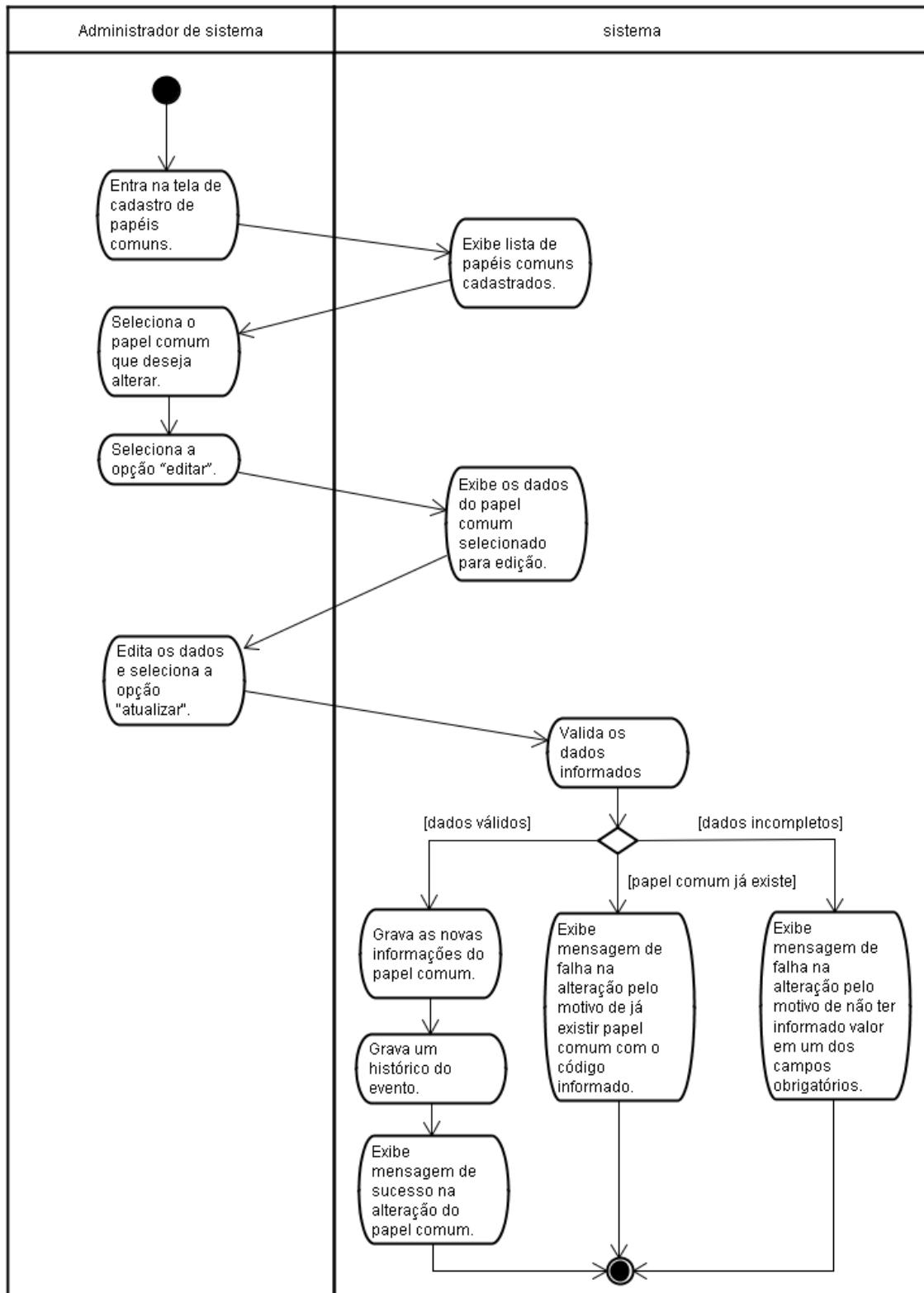
2.2.9.17. Consultar tipo de recurso



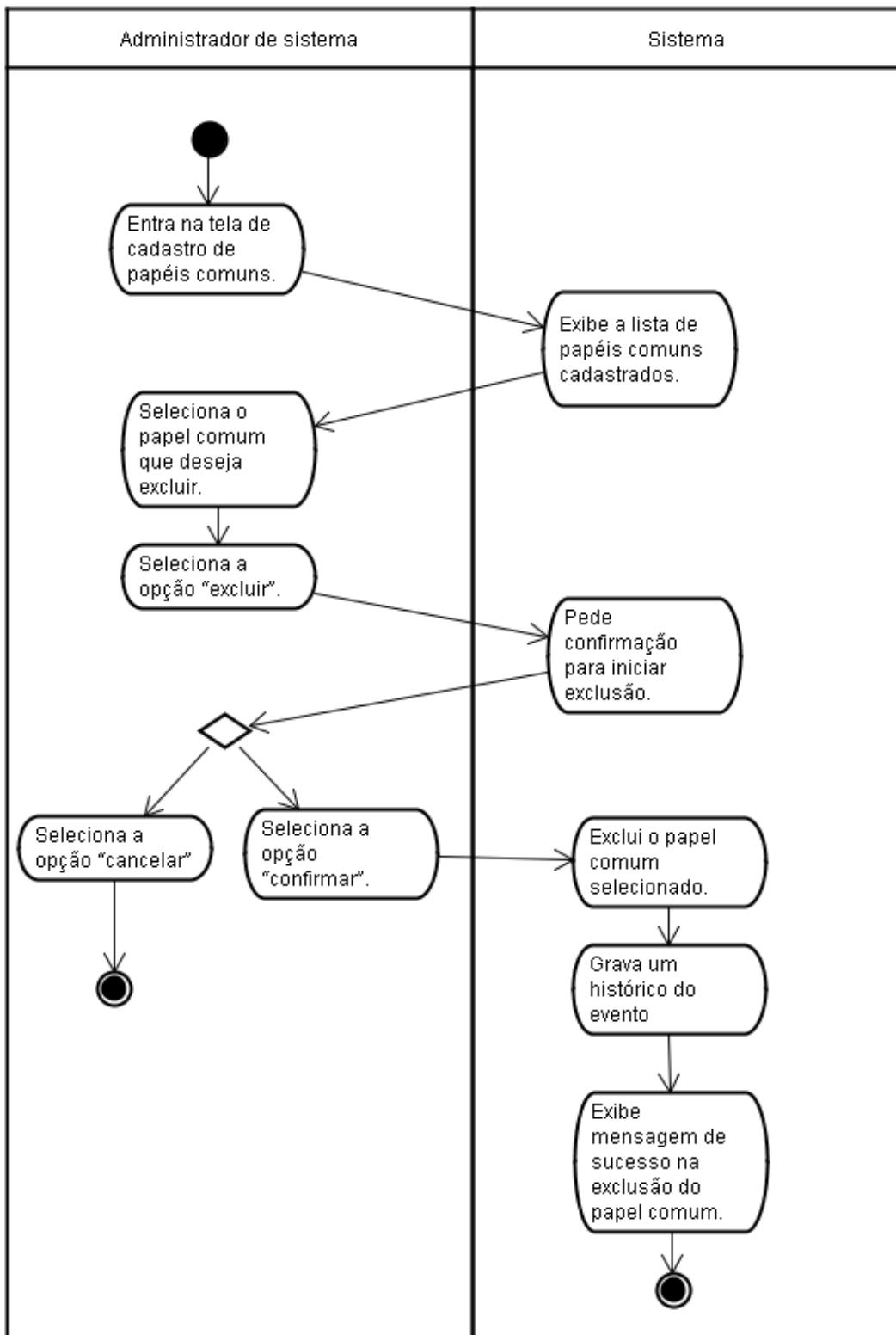
2.2.9.18. Incluir papel comum



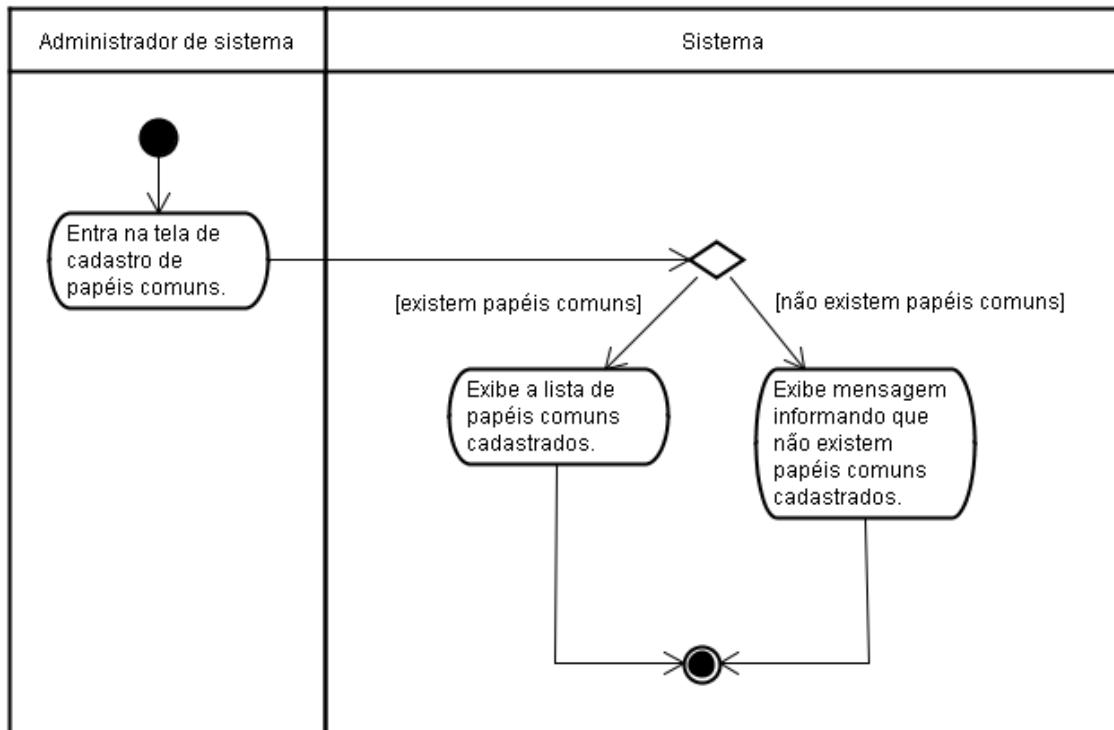
2.2.9.19. Alterar papel comum



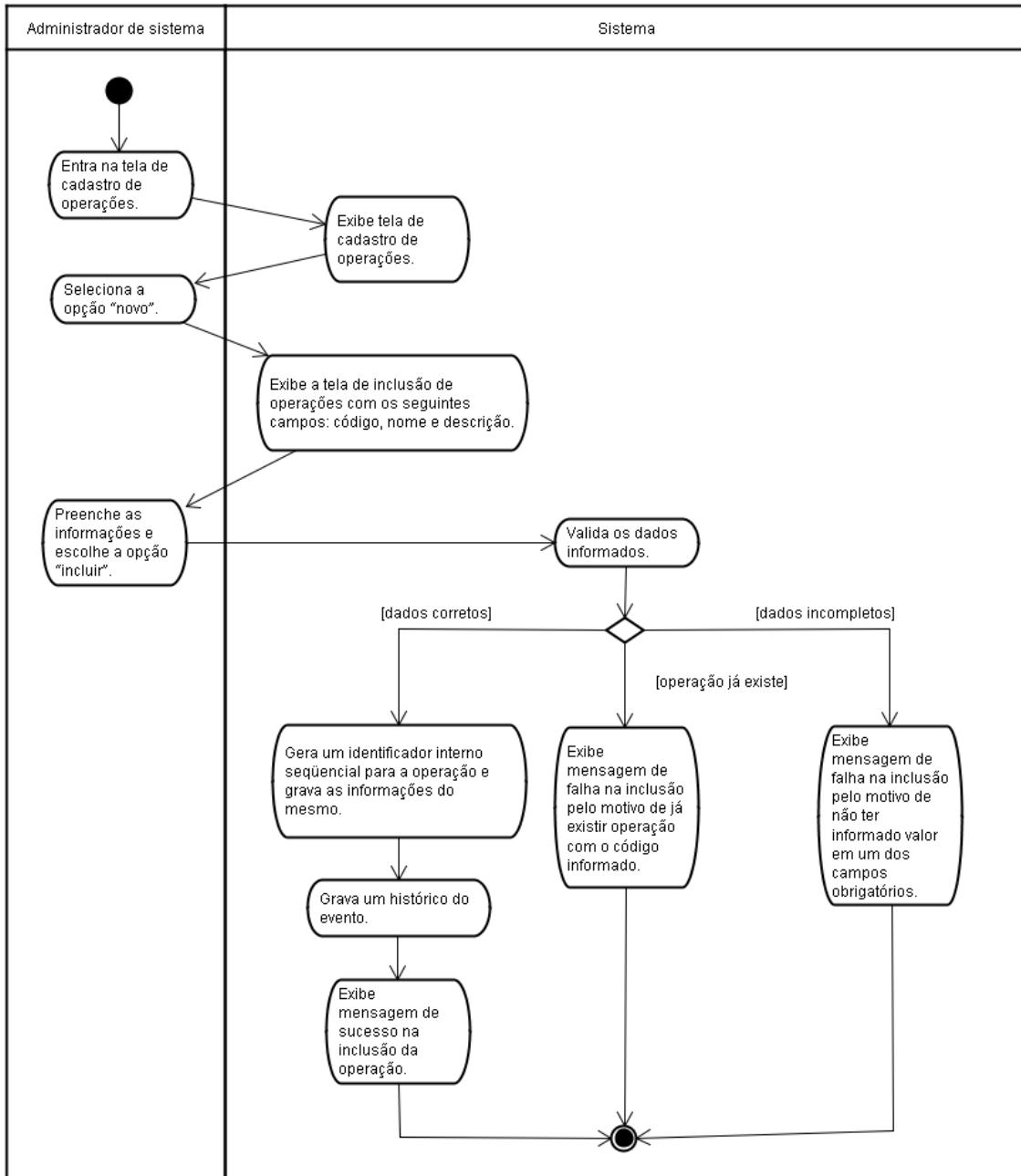
2.2.9.20. Excluir papel comum



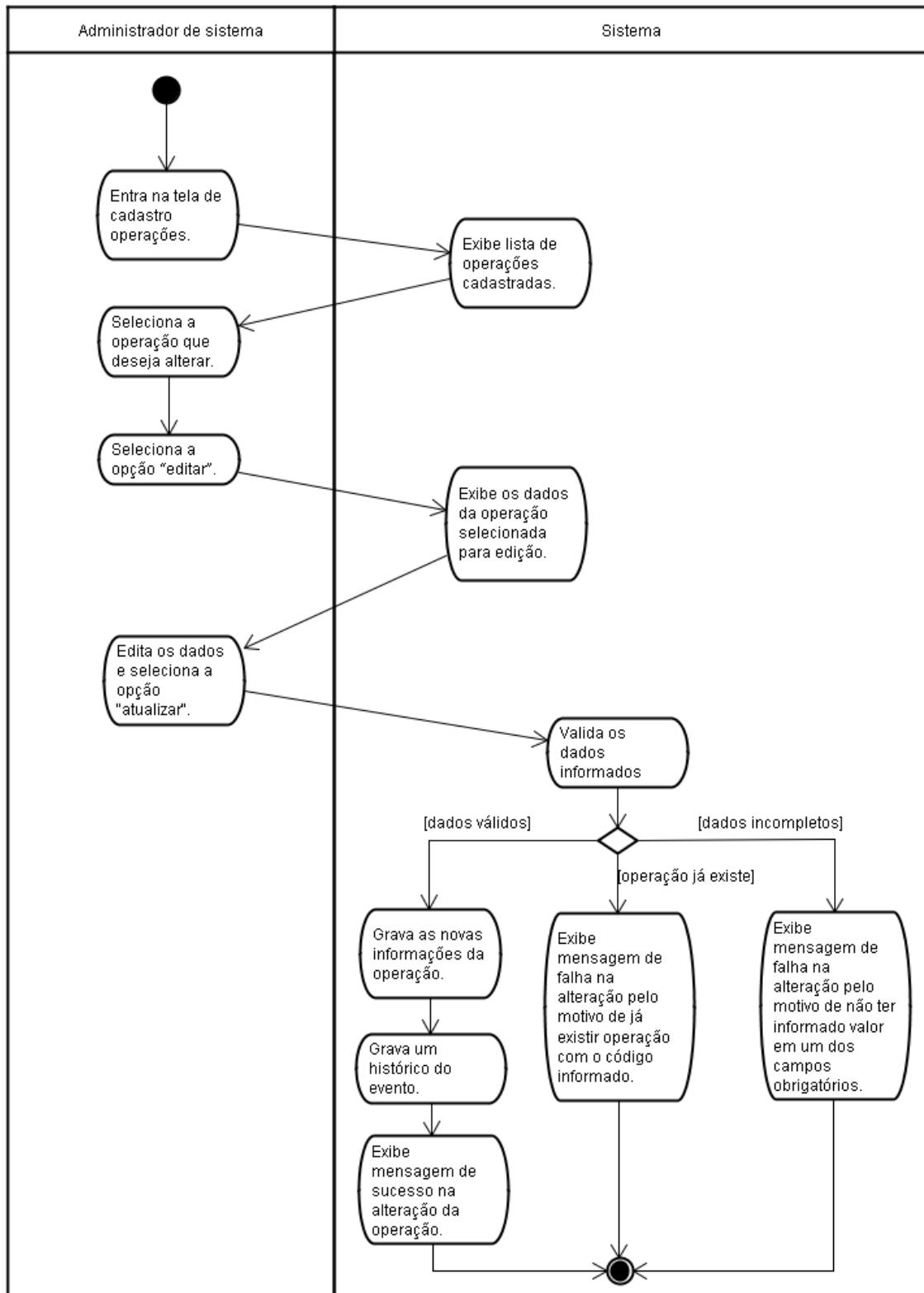
2.2.9.21. Consultar papel comum



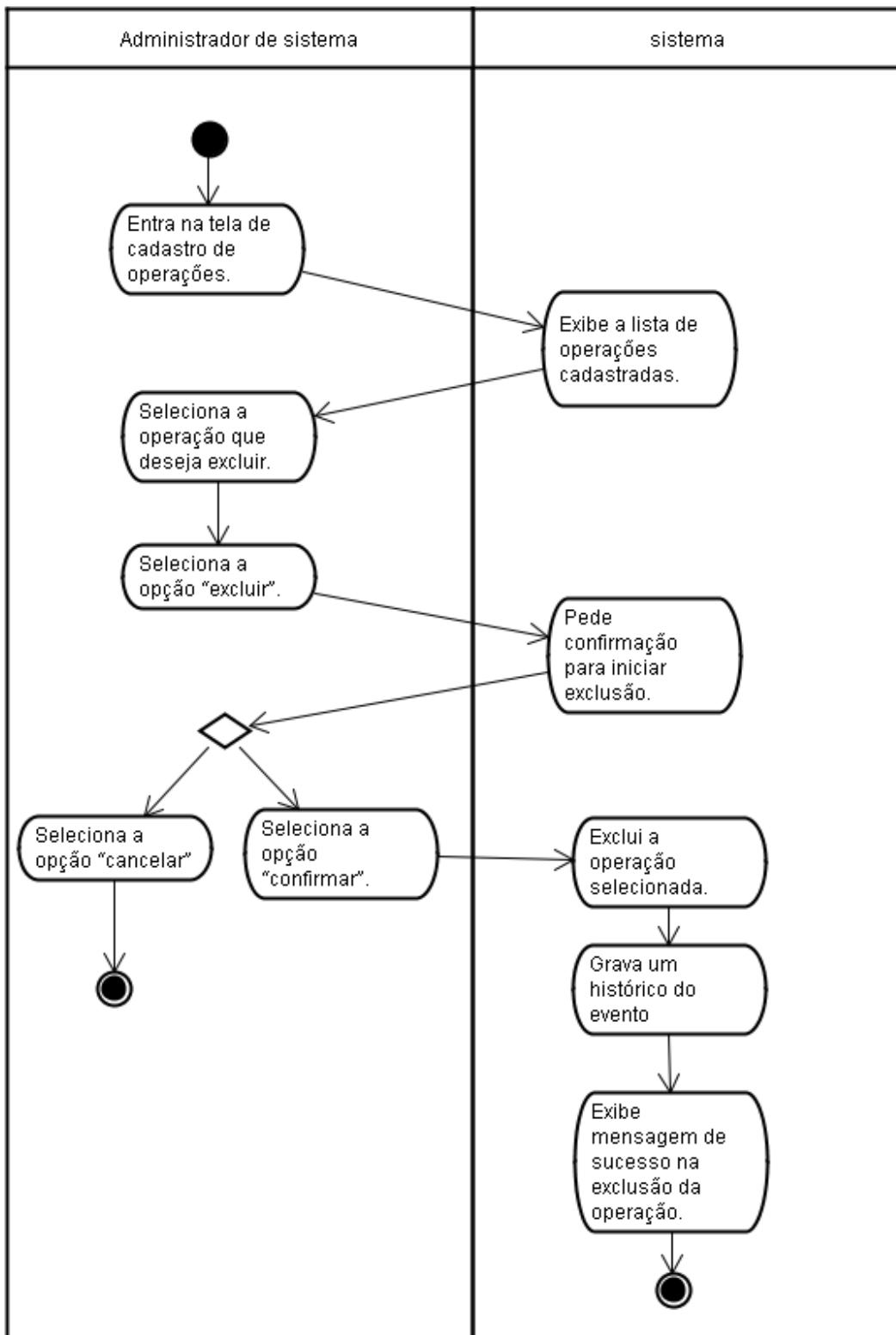
2.2.9.22. Incluir operação



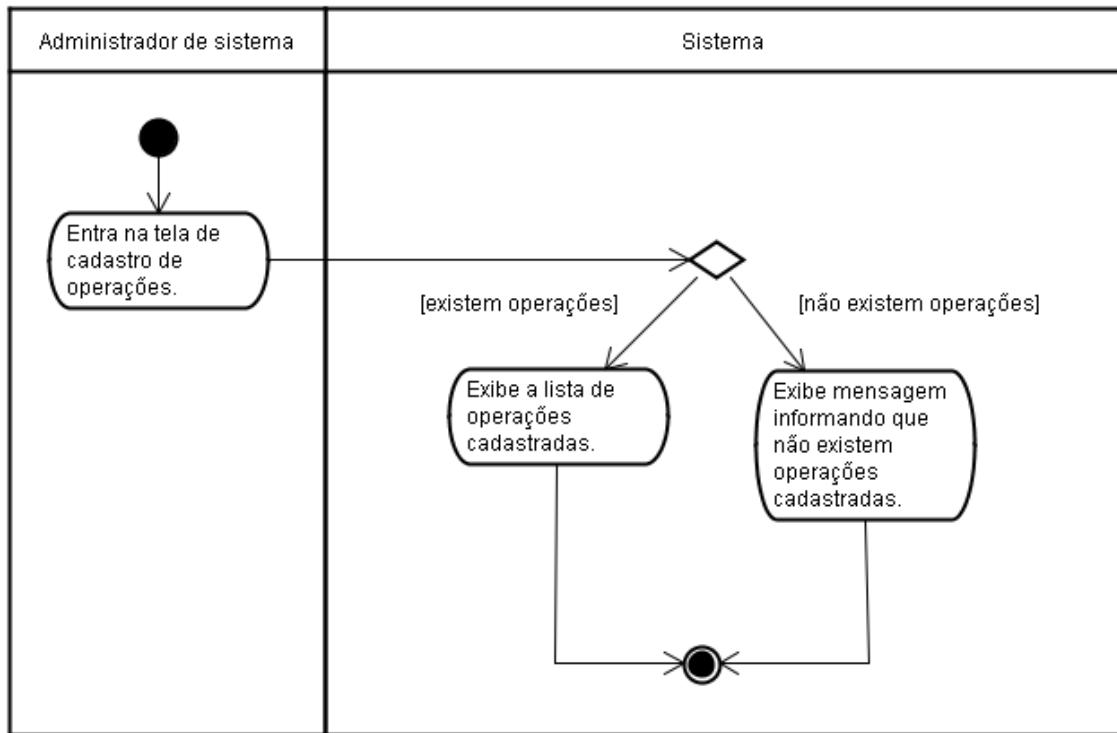
2.2.9.23. Alterar operação



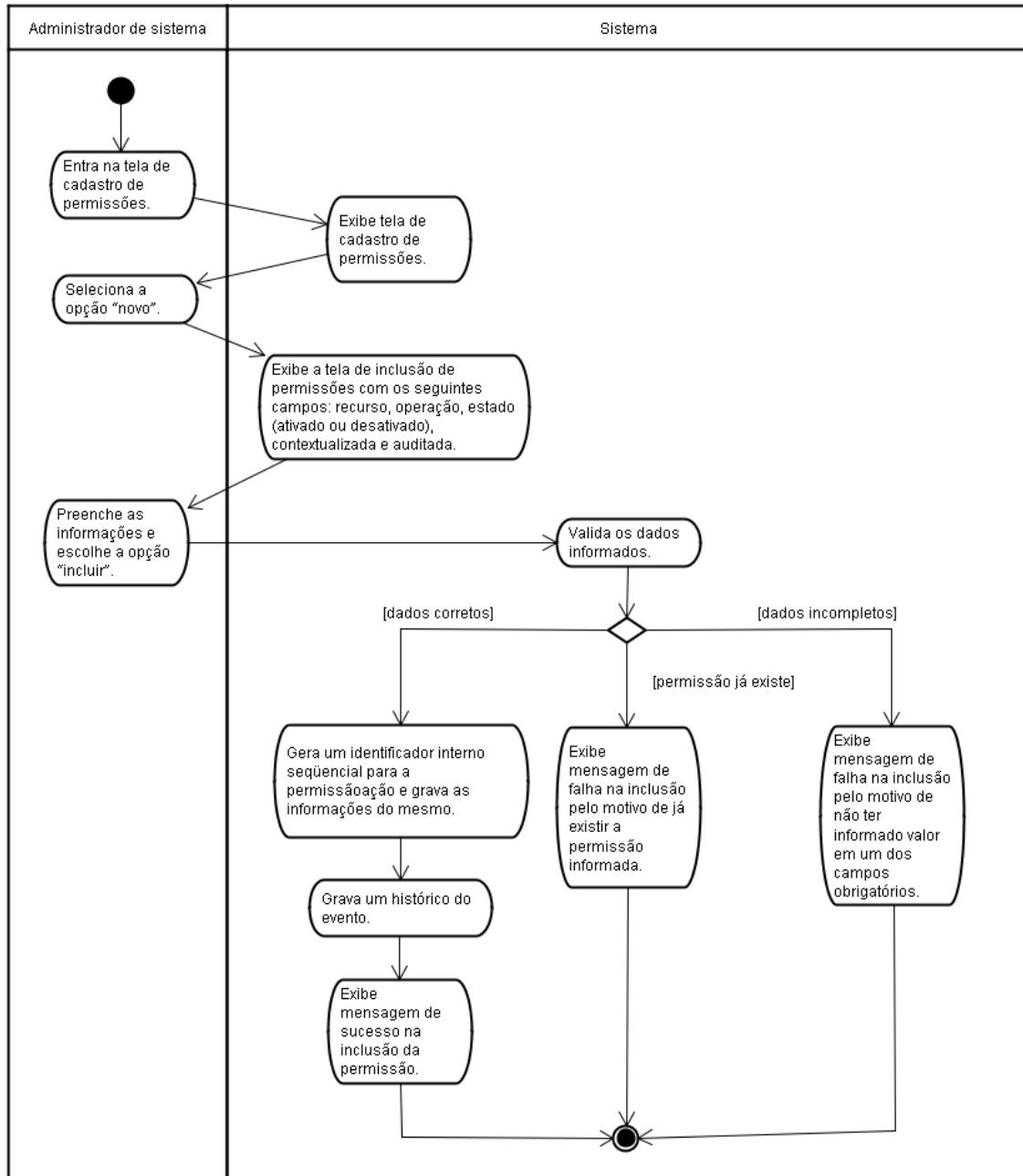
2.2.9.24. Excluir operação



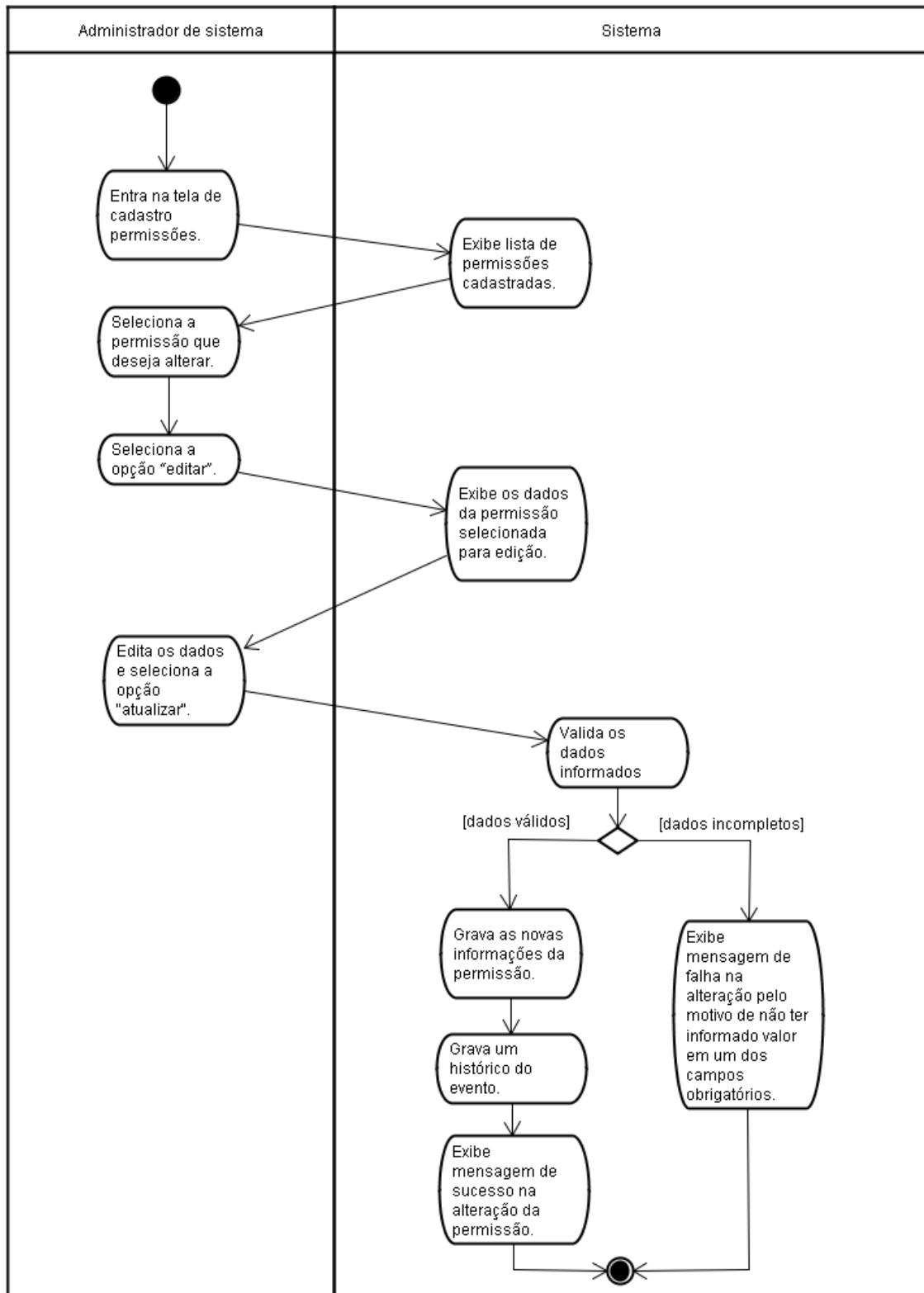
2.2.9.25. Consultar operação



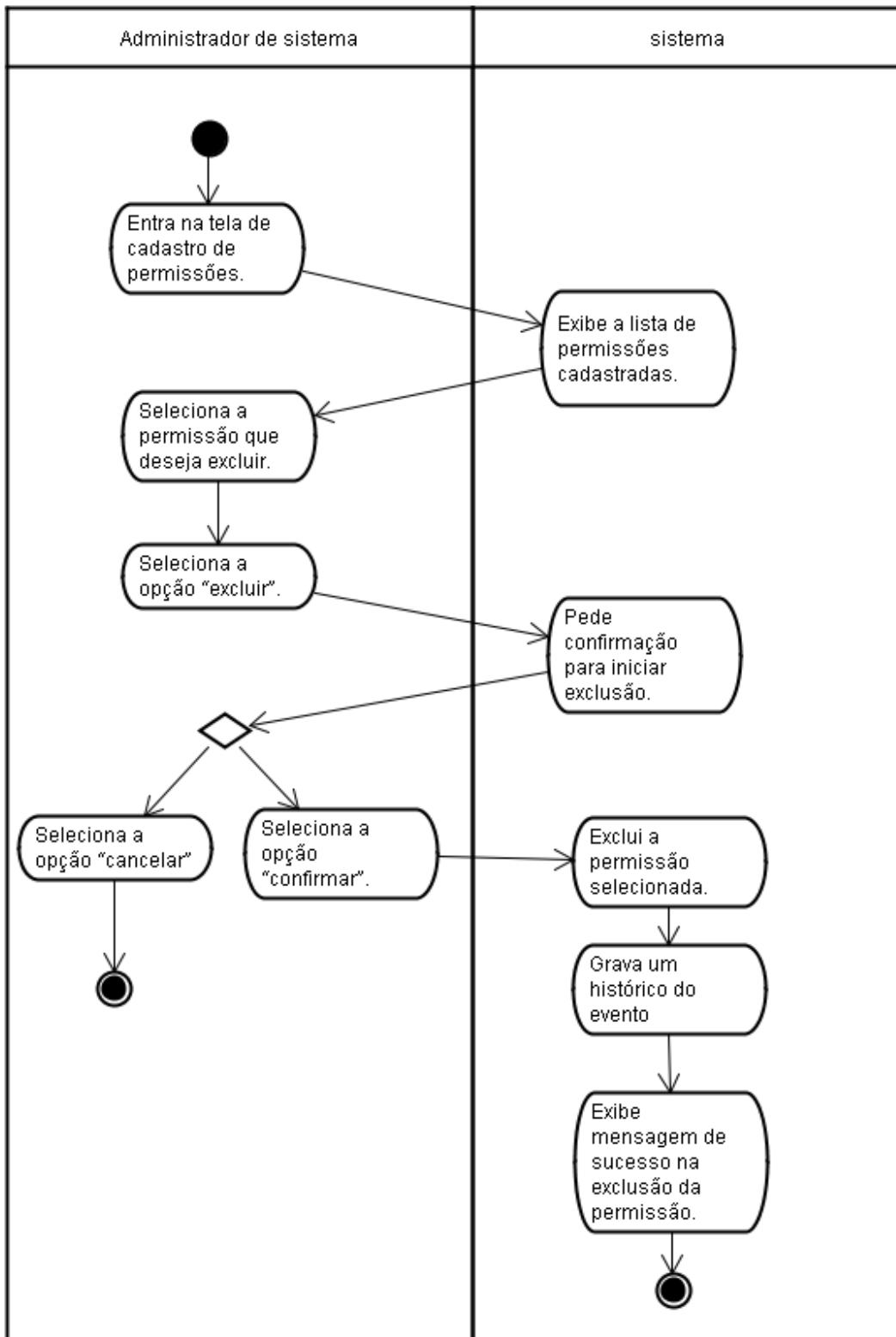
2.2.9.26. Incluir permissão



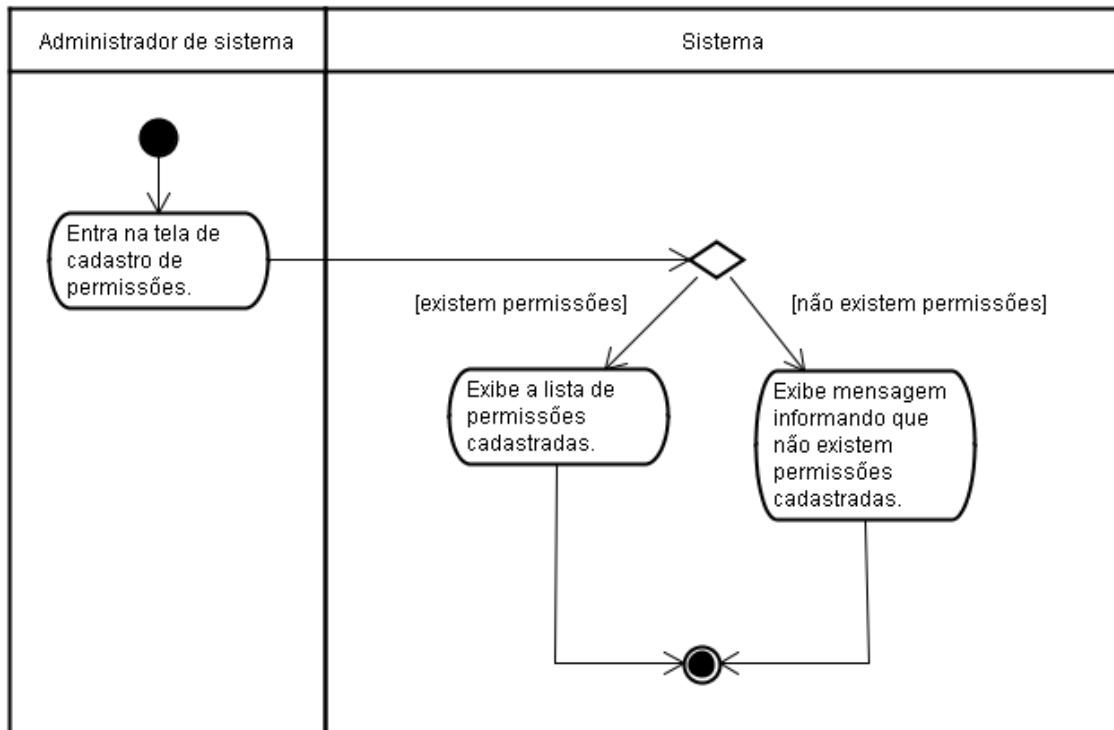
2.2.9.27. Alterar permissão



2.2.9.28. Excluir permissão



2.2.9.29. Consultar permissão



2.2.10. PROJETO DE TABELAS/ARQUIVOS

A base de dados do Framework de Segurança foi construída com base na definição do modelo de dados. Cada entidade foi transformada em tabela e seus principais relacionamentos também. A seguir as tabelas e seus respectivos scripts de criação:

PAPEL ADMINISTRATIVO						
Nome Físico: tb_administrative_role						
Objetivo: Armazenar os papéis administrativos de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Ativado	enabled	BOOLEAN	N		1
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Versão	version	INTENGER	S		10
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_administrative_role
(
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_administrative_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_administrative_role_un
        UNIQUE (id, application_uid)
);

ALTER TABLE tb_administrative_role ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

SISTEMA						
Nome Físico: tb_application						
Objetivo: Armazenar os sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Nome	name	VARCHAR	N		255
	Código	id	VARCHAR	N		255
FK	ID Interno da Conta do Sistema	application_account_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_application (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    name VARCHAR(255) NOT NULL,
    application_account_uid BIGINT NOT NULL,
    CONSTRAINT tb_application_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_application_un
        UNIQUE (id)
);

ALTER TABLE tb_application ADD CONSTRAINT fk_application_account
FOREIGN KEY (application_account_uid)
REFERENCES tb_application_account (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONTA DO SISTEMA						
Nome Físico: tb_application_account						
Objetivo: Armazenar as contas dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Ativada	enabled	BOOLEAN	N		1
	Senha	password	VARCHAR	N		255

Script:

```
CREATE TABLE tb_application_account (
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    password VARCHAR(255) NOT NULL,
    CONSTRAINT tb_application_account_pkey
        PRIMARY KEY (uid)
);
```

CARACTERÍSTICA						
Nome Físico: tb_characteristic						
Objetivo: Armazenar as características que podem ser atribuídas para os usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characteristic (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_characteristic_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characteristic_un
        UNIQUE (id, application_uid)

);

ALTER TABLE tb_characteristic ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

VALOR DA CARACTERÍSTICA						
Nome Físico: tb_characteristic_value						
Objetivo: Armazenar os valores para as características que podem ser atribuídas para os usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno da Característica	characteristic_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characteristic_value (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    characteristic_uid BIGINT NOT NULL,
    CONSTRAINT tb_characteristic_value_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characteristic_value_un
        UNIQUE (id, characteristic_uid)

);

ALTER TABLE tb_characteristic_value ADD CONSTRAINT fk_characteristic
FOREIGN KEY (characteristic_uid)
REFERENCES tb_characteristic (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

GRUPO CARACTERIZADO						
Nome Físico: tb_characterized_group						
Objetivo: Armazenar os grupos caracterizados de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Ativado	enabled	BOOLEAN	N		1
	Código	id	VARCHAR	S		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characterized_group (
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_characterized_group_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characteristic_un
        UNIQUE (id, application_uid)
);

ALTER TABLE tb_characterized_group ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA GRUPO CARACTERIZADO						
Nome Físico: tb_characterized_group_assigned_administrative_role						
Objetivo: Armazenar as atribuições de papéis administrativos para os grupos caracterizados de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Administrativo	administrative_role_uid	BIGINT	N		100
FK	ID Interno do Grupo Caracterizado	characterized_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characterized_group_assigned_administrative_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    administrative_role_uid BIGINT NOT NULL,
    characterized_group_uid BIGINT NOT NULL,
    CONSTRAINT tb_characterized_group_assigned_administrative_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characterized_group_assigned_administrative_role_un
        UNIQUE (administrative_role_uid, characterized_group_uid)
) ;

ALTER TABLE tb_characterized_group_assigned_administrative_role ADD
CONSTRAINT fk_characterized_group
FOREIGN KEY (characterized_group_uid)
REFERENCES public.tb_characterized_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_characterized_group_assigned_administrative_role ADD
CONSTRAINT fk_administrative_role
FOREIGN KEY (administrative_role_uid)
REFERENCES public.tb_administrative_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO CARACTERIZADO						
Nome Físico: tb_characterized_group_assigned_common_role						
Objetivo: Armazenar as atribuições de papéis comuns para os grupos caracterizados de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Comum	common_role_uid	BIGINT	N		100
FK	ID Interno do Grupo Caracterizado	characterized_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characterized_group_assigned_common_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    characterized_group_uid BIGINT NOT NULL,
    common_role_uid BIGINT NOT NULL,
    CONSTRAINT tb_characterized_group_assigned_common_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characterized_group_assigned_common_role_un
        UNIQUE (common_role_uid, characterized_group_uid)
) ;

ALTER TABLE tb_characterized_group_assigned_common_role ADD CONSTRAINT
fk_common_role
FOREIGN KEY (common_role_uid)
REFERENCES tb_common_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_characterized_group_assigned_common_role ADD CONSTRAINT
fk_characterized_group
FOREIGN KEY (characterized_group_uid)
REFERENCES tb_characterized_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

VALOR DA CARACTERÍSTICA DE GRUPO CARACTERIZADO						
Nome Físico: tb_characterized_group_characteristic_value						
Objetivo: Armazenar os valores das características dos grupos caracterizados de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Valor da Característica	characteristic_value_uid	BIGINT	N		100
FK	ID Interno do Grupo Caracterizado	characterized_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characterized_group_characteristic_value (
    uid BIGINT NOT NULL,
    version INTEGER,
    characteristic_value_uid BIGINT NOT NULL,
    characterized_group_uid BIGINT NOT NULL,
    CONSTRAINT tb_characterized_group_characteristic_value_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characterized_group_characteristic_value_un
        UNIQUE (characteristic_value_uid, characterized_group_uid)
);

ALTER TABLE tb_characterized_group_characteristic_value ADD CONSTRAINT
fk_characteristic_value
FOREIGN KEY (characteristic_value_uid)
REFERENCES tb_characteristic_value (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_characterized_group_characteristic_value ADD CONSTRAINT
fk_characterized_group
FOREIGN KEY (characterized_group_uid)
REFERENCES tb_characterized_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

INATIVAÇÃO DE GRUPO CARACTERIZADO						
Nome Físico: tb_characterized_group_inactivation						
Objetivo: Armazenar as inativações dos grupos caracterizados de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno da Inativação	inactivation_uid	BIGINT	N		100
FK	ID Interno do Grupo Caracterizado	characterized_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_characterized_group_inactivation (
    uid BIGINT NOT NULL,
    version INTEGER,
    characterized_group_uid BIGINT NOT NULL,
    inactivation_uid BIGINT NOT NULL,
    CONSTRAINT tb_characterized_group_inactivation_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_characterized_group_inactivation_un
        UNIQUE (inactivation_uid, characterized_group_uid)
);

ALTER TABLE tb_characterized_group_inactivation ADD CONSTRAINT
fk_inactivation
FOREIGN KEY (inactivation_uid)
REFERENCES tb_inactivation (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_characterized_group_inactivation ADD CONSTRAINT
fk_characterized_group
FOREIGN KEY (characterized_group_uid)
REFERENCES tb_characterized_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

PAPEL COMUM						
Nome Físico: tb_common_role						
Objetivo: Armazenar os papéis comuns de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Ativado	enabled	BOOLEAN	N		1
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_common_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_common_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_common_role_un
        UNIQUE (application_uid, id)
);

ALTER TABLE tb_common_role ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONCESSÃO DE PERMISSÃO PARA PAPEL COMUM						
Nome Físico: tb_common_role_assigned_permission						
Objetivo: Armazenar as concessões de permissões para papéis comuns.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Comum	common_role_uid	BIGINT	N		100
FK	ID Interno da Permissão	permission_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_common_role_assigned_permission (
    uid BIGINT NOT NULL,
    version INTEGER,
    common_role_uid BIGINT NOT NULL,
    permission_uid BIGINT NOT NULL,
    CONSTRAINT tb_common_role_assigned_permission_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_common_role_assigned_permission_un
        UNIQUE (permission_uid, common_role_uid)
) ;

ALTER TABLE tb_common_role_assigned_permission ADD CONSTRAINT
fk_common_role
FOREIGN KEY (common_role_uid)
REFERENCES tb_common_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_common_role_assigned_permission ADD CONSTRAINT
fk_permission
FOREIGN KEY (permission_uid)
REFERENCES tb_permission (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONTEXTO						
Nome Físico: tb_context						
Objetivo: Armazenar os contextos de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_context (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_context_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_context_un
        UNIQUE (application_uid, id)
);

ALTER TABLE tb_context ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

VALOR DE CONTEXTO						
Nome Físico: tb_context_value						
Objetivo: Armazenar os valores dos contextos de um sistema.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	Id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Contexto	context_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_context_value (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    context_uid BIGINT NOT NULL,
    CONSTRAINT tb_context_value_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_context_value_un
        UNIQUE (context_uid, id)
);

ALTER TABLE tb_context_value ADD CONSTRAINT fk_context
FOREIGN KEY (context_uid)
REFERENCES tb_context (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

INATIVAÇÃO						
Nome Físico: tb_inactivation						
Objetivo: Armazenar as inativações.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Motivo	reason	VARCHAR	N		255
FK	ID Interno da Validade	validity_uid	BIGINT	S		100

Script:

```

CREATE TABLE tb_inactivation (
    uid BIGINT NOT NULL,
    version INTEGER,
    validity_uid BIGINT,
    reason VARCHAR(255) NOT NULL,
    CONSTRAINT tb_inactivation_pkey
        PRIMARY KEY (uid)
);

ALTER TABLE tb_inactivation ADD CONSTRAINT fk_validity
FOREIGN KEY (validity_uid)
REFERENCES tb_validity (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

GRUPO MANUAL						
Nome Físico: tb_manual_group						
Objetivo: Armazenar os grupos manuais dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Ativado	enabled	BOOLEAN	N		1
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_manual_group (
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_manual_group_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_manual_group_un
        UNIQUE (application_uid, id)
);

ALTER TABLE tb_manual_group ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA GRUPO MANUAL						
Nome Físico: tb_manual_group_assigned_administrative_role						
Objetivo: Armazenar as atribuições de papéis administrativos para os grupos manuais dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID do Papel Administrativo	administrative_role_uid	BIGINT	N		100
FK	ID do Grupo Manual	manual_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_manual_group_assigned_administrative_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    administrative_role_uid BIGINT NOT NULL,
    manual_group_uid BIGINT NOT NULL,
    CONSTRAINT tb_manual_group_assigned_administrative_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_manual_group_assigned_administrative_role_un
        UNIQUE (administrative_role_uid, manual_group_uid)
) ;

ALTER TABLE tb_manual_group_assigned_administrative_role ADD CONSTRAINT
fk_manual_group
FOREIGN KEY (manual_group_uid)
REFERENCES tb_manual_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_manual_group_assigned_administrative_role ADD CONSTRAINT
fk_administrative_role
FOREIGN KEY (administrative_role_uid)
REFERENCES tb_administrative_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

ATRIBUIÇÃO DE PAPEL COMUM PARA GRUPO MANUAL						
Nome Físico: tb_manual_group_assigned_common_role						
Objetivo: Armazenar as atribuições de papéis comuns para os grupos manuais dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Comum	common_role_uid	BIGINT	N		100
FK	ID Interno do Grupo Manual	manual_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_manual_group_assigned_common_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    common_role_uid BIGINT NOT NULL,
    manual_group_uid BIGINT NOT NULL,
    CONSTRAINT tb_manual_group_assigned_common_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_manual_group_assigned_common_role_un
        UNIQUE (common_role_uid, manual_group_uid)
) ;

ALTER TABLE tb_manual_group_assigned_common_role ADD CONSTRAINT
fk_common_role
FOREIGN KEY (common_role_uid)
REFERENCES tb_common_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_manual_group_assigned_common_role ADD CONSTRAINT
fk_manual_group
FOREIGN KEY (manual_group_uid)
REFERENCES tb_manual_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

INATIVAÇÃO DE GRUPO MANUAL						
Nome Físico: tb_manual_group_inactivation						
Objetivo: Armazenar as inativações dos grupos manuais dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno da Inativação	inactivation_uid	BIGINT	N		100
FK	ID Interno do Grupo Manual	manual_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_manual_group_inactivation (
    uid BIGINT NOT NULL,
    version INTEGER,
    manual_group_uid BIGINT NOT NULL,
    inactivation_uid BIGINT NOT NULL,
    CONSTRAINT tb_manual_group_inactivation_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_manual_group_inactivation_un
        UNIQUE (manual_group_uid, inactivation_uid)
) ;

ALTER TABLE tb_manual_group_inactivation ADD CONSTRAINT
tb_manual_group_inactivation_inactivation_uid_fkey
FOREIGN KEY (inactivation_uid)
REFERENCES tb_inactivation (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_manual_group_inactivation ADD CONSTRAINT fk_manual_group
FOREIGN KEY (manual_group_uid)
REFERENCES tb_manual_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

OPERAÇÃO						
Nome Físico: tb_operation						
Objetivo: Armazenar as operações dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Sistema	application_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_operation (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    CONSTRAINT tb_operation_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_operation_un
        UNIQUE (application_uid, id)
);

ALTER TABLE tb_operation ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

PERMISSÃO						
Nome Físico: tb_permission						
Objetivo: Armazenar as permissões dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Auditada	audited	BOOLEAN	N		1
	Contextualizada	contextualized	BOOLEAN	N		1
	Ativada	enabled	BOOLEAN	N		1
FK	ID Interno da Operação	operation_uid	BIGINT	N		100
FK	ID Interno do Recurso	resource_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_permission (
    uid BIGINT NOT NULL,
    version INTEGER,
    audited BOOLEAN NOT NULL,
    contextualized BOOLEAN NOT NULL,
    enabled BOOLEAN NOT NULL,
    operation_uid BIGINT NOT NULL,
    resource_uid BIGINT NOT NULL,
    CONSTRAINT tb_permission_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_permission_un
        UNIQUE (resource_uid, operation_uid)
);

ALTER TABLE tb_permission ADD CONSTRAINT fk_resource
FOREIGN KEY (resource_uid)
REFERENCES tb_resource (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_permission ADD CONSTRAINT fk_permission
FOREIGN KEY (operation_uid)
REFERENCES tb_operation (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONFLITO DE PERMISSÃO						
Nome Físico: tb_permission_conflict						
Objetivo: Armazenar os conflitos de permissões dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno da Permissão	permission_uid	BIGINT	N		100
FK	ID Interno da Permissão Conflitada	Permission_conflicted	BIGINT	N		100

Script:

```

CREATE TABLE tb_permission_conflict (
    uid BIGINT NOT NULL,
    version INTEGER,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    permission_uid BIGINT NOT NULL,
    permission_conflicted_uid BIGINT NOT NULL,
    CONSTRAINT tb_permission_conflict_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_permission_conflict_un
        UNIQUE (permission_uid, permission_conflicted_uid)
);

ALTER TABLE tb_permission_conflict ADD CONSTRAINT
fk_permission_conflicted
FOREIGN KEY (permission_conflicted_uid)
REFERENCES tb_permission (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_permission_conflict ADD CONSTRAINT fk_permission
FOREIGN KEY (permission_uid)
REFERENCES tb_permission (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONTEXTO DA PERMISSÃO						
Nome Físico: tb_permission_context						
Objetivo: Armazenar os contextos das permissões dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno da Permissão	permission_uid	BIGINT	N		100
FK	ID Interno do Contexto	context_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_permission_context (
    uid BIGINT NOT NULL,
    version INTEGER,
    context_uid BIGINT NOT NULL,
    permission_uid BIGINT NOT NULL,
    CONSTRAINT tb_permission_context_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_permission_conflict_translation_un
        UNIQUE (context_uid, permission_uid)
) ;

ALTER TABLE tb_permission_context ADD CONSTRAINT fk_context
FOREIGN KEY (context_uid)
REFERENCES tb_context (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_permission_context ADD CONSTRAINT fk_permission
FOREIGN KEY (permission_uid)
REFERENCES tb_permission (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

RECURSO						
Nome Físico: tb_resource						
Objetivo: Armazenar os recursos dos sistemas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Ativado	enabled	BOOLEAN	N		1
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255
FK	ID Interno do Tipo de Recurso	type_uid	BIGINT	N		100
FK	ID Interno do Sistema	application_uid	BIGINT	N		100
FK	ID Interno do Recurso pai	parent_uid	BIGINT	S		100

Script:

```

CREATE TABLE tb_resource (
    uid BIGINT NOT NULL,
    version INTEGER,
    enabled BOOLEAN NOT NULL,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    application_uid BIGINT NOT NULL,
    parent_uid BIGINT NOT NULL,
    type_uid BIGINT NOT NULL,
    CONSTRAINT tb_resource_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_resource_un
        UNIQUE (application_uid, id)
);

ALTER TABLE tb_resource ADD CONSTRAINT fk_type
FOREIGN KEY (type_uid)
REFERENCES tb_resource_type (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_resource ADD CONSTRAINT fk_application
FOREIGN KEY (application_uid)
REFERENCES tb_application (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_resource ADD CONSTRAINT fk_parent
FOREIGN KEY (parent_uid)

```

```
REFERENCES tb_resource (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;
```

TIPO DE RECURSO						
Nome Físico: tb_resource_type						
Objetivo: Armazenar os tipos de recursos.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Código	id	VARCHAR	N		255
	Nome	name	VARCHAR	N		255
	Descrição	description	VARCHAR	S		255

Script:

```
CREATE TABLE tb_resource_type (
    uid BIGINT NOT NULL,
    version INTEGER,
    id VARCHAR(255) NOT NULL,
    description VARCHAR(255),
    name VARCHAR(255) NOT NULL,
    CONSTRAINT tb_resource_type_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_resource_type_un
        UNIQUE (id)
);
```

USUÁRIO						
Nome Físico: tb_user						
Objetivo: Armazenar os usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	Nome	name	VARCHAR	N		255
FK	ID Interno da Conta do Usuário	account_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_user (
    uid BIGINT NOT NULL,
    version INTEGER,
    name VARCHAR(255) NOT NULL,
    account_uid BIGINT NOT NULL,
    CONSTRAINT tb_user_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_un
        UNIQUE (account_uid)
) ;

ALTER TABLE tb_user ADD CONSTRAINT fk_locale
FOREIGN KEY (preferred_locale_uid)
REFERENCES tb_locale (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user ADD CONSTRAINT fk_account
FOREIGN KEY (account_uid)
REFERENCES tb_user_account (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONTA DE USUÁRIO						
Nome Físico: tb_user_account						
Objetivo: Armazenar as contas dos usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
	E-mail	email	VARCHAR	N		255
	Ativada	enabled	BOOLEAN	N		1
	Login	login	VARCHAR	N		255
	Senha	password	VARCHAR	N		255
	Tentativas Inválidas	invalid_attempts	INTEGER	N		10

Script:

```
CREATE TABLE tb_user_account (
    uid BIGINT NOT NULL,
    version INTEGER,
    email VARCHAR(255) NOT NULL,
    enabled BOOLEAN NOT NULL,
    login VARCHAR(255) NOT NULL,
    password VARCHAR(255) NOT NULL,
    invalid_attempts INTEGER NOT NULL,
    CONSTRAINT tb_user_account_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_account_un
        UNIQUE (login)
);
```

ATRIBUIÇÃO DE PAPEL ADMINISTRATIVO PARA USUÁRIO						
Nome Físico: tb_user_assigned_administrative_role						
Objetivo: Armazenar as atribuições de papéis administrativos para usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Administrativo	administrative_role_uid	BIGINT	N		100
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno da Validade	validity_uid	BIGINT	S		100

Script:

```

CREATE TABLE tb_user_assigned_administrative_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    administrative_role_uid BIGINT NOT NULL,
    user_uid BIGINT NOT NULL,
    validity_uid BIGINT,
    CONSTRAINT tb_user_assigned_administrative_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_assigned_administrative_role_un
        UNIQUE (user_uid, administrative_role_uid)
) ;

ALTER TABLE tb_user_assigned_administrative_role ADD CONSTRAINT
fk_validity
FOREIGN KEY (validity_uid)
REFERENCES tb_validity (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_administrative_role ADD CONSTRAINT fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_administrative_role ADD CONSTRAINT
fk_administrative_role
FOREIGN KEY (administrative_role_uid)
REFERENCES tb_administrative_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO						
Nome Físico: tb_user_assigned_common_role						
Objetivo: Armazenar as atribuições de papéis comuns para usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Papel Comum	common_role_uid	BIGINT	N		100
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno da Validade	validity_uid	BIGINT	S		100

Script:

```

CREATE TABLE tb_user_assigned_common_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    common_role_uid BIGINT NOT NULL,
    permission_uid BIGINT NOT NULL,
    user_uid BIGINT NOT NULL,
    validity_uid BIGINT,
    CONSTRAINT tb_user_assigned_common_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_assigned_common_role_un
        UNIQUE (user_uid, common_role_uid)
) ;

ALTER TABLE tb_user_assigned_common_role ADD CONSTRAINT fk_validity
FOREIGN KEY (validity_uid)
REFERENCES tb_validity (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_common_role ADD CONSTRAINT fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_common_role ADD CONSTRAINT fk_common_role
FOREIGN KEY (common_role_uid)
REFERENCES tb_common_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

CONTEXTUALIZAÇÃO DE ATRIBUIÇÃO DE PAPEL COMUM PARA USUÁRIO						
Nome Físico: tb_user_assigned_common_role_contextualization						
Objetivo: Armazenar as contextualizações das atribuições de papéis comuns para usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno da Concessão de Permissão para Papel Comum	common_role_assigned_permission_uid	BIGINT	N		100
FK	ID Interno do Valor de Contexto	context_value_uid	BIGINT	N		100
FK	ID Interno da Atribuição de Papel Comum para Usuário	user_assigned_common_role_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_user_assigned_common_role_contextualization (
    uid BIGINT NOT NULL,
    version INTEGER,
    common_role_assigned_permission_uid BIGINT NOT NULL,
    context_value_uid BIGINT NOT NULL,
    user_assigned_common_role_uid BIGINT NOT NULL,
    CONSTRAINT tb_user_assigned_common_role_contextualization_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_assigned_administrative_role_un
        UNIQUE (user_assigned_common_role_uid,
                common_role_assigned_permission_uid,
                context_value)
) ;

```

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

```
ALTER TABLE tb_user_assigned_common_role_contextualization ADD CONSTRAINT
fk_context_value
FOREIGN KEY (context_value_uid)
REFERENCES tb_context_value (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_common_role_contextualization ADD CONSTRAINT
fk_user_assigned_common_role
FOREIGN KEY (user_assigned_common_role_uid)
REFERENCES tb_user_assigned_common_role (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_common_role_contextualization ADD CONSTRAINT
fk_common_role_assigned_permission
FOREIGN KEY (common_role_assigned_permission_uid)
REFERENCES tb_common_role_assigned_permission (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;
```

ATRIBUIÇÃO DE PAPEL DE ADMINISTRAÇÃO DE SEGURANÇA PARA USUÁRIO						
Nome Físico: tb_user_assigned_security_administrative_role						
Objetivo: Armazenar as atribuições de papel de administração de segurança para usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno da Validade	validity_uid	BIGINT	S		100

Script:

```

CREATE TABLE tb_user_assigned_security_administrative_role (
    uid BIGINT NOT NULL,
    version INTEGER,
    user_uid BIGINT NOT NULL,
    validity_uid BIGINT,
    CONSTRAINT tb_user_assigned_security_administrative_role_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_assigned_security_administrative_role_un
        UNIQUE (user_uid)
) ;

ALTER TABLE tb_user_assigned_security_administrative_role ADD CONSTRAINT
fk_validity
FOREIGN KEY (validity_uid)
REFERENCES tb_validity (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_assigned_security_administrative_role ADD CONSTRAINT
fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

VALOR DE CARACTERÍSTICA DE USUÁRIO						
Nome Físico: tb_user_characteristic_value						
Objetivo: Armazenar os valores de características dos usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	Uid	BIGINT	N		100
	Versão	Version	INTEGER	S		10
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno do Valor de Característica	characteristic_value_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_user_characteristic_value (
    uid BIGINT NOT NULL,
    version INTEGER,
    characteristic_value_uid BIGINT NOT NULL,
    user_uid BIGINT NOT NULL,
    CONSTRAINT tb_user_characteristic_value_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_characteristic_value _un
        UNIQUE (user_uid, characteristic_value_uid)
);

ALTER TABLE tb_user_characteristic_value ADD CONSTRAINT
fk_characteristic_value
FOREIGN KEY (characteristic_value_uid)
REFERENCES tb_characteristic_value (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_characteristic_value ADD CONSTRAINT fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

INATIVAÇÃO DE USUÁRIO						
Nome Físico: tb_user_inactivation						
Objetivo: Armazenar as inativações de usuários.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	uid	BIGINT	N		100
	Versão	version	INTEGER	S		10
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno da Inativação	inactivation_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_user_inactivation (
    uid BIGINT NOT NULL,
    version INTEGER,
    inactivation_uid BIGINT NOT NULL,
    user_uid BIGINT NOT NULL,
    CONSTRAINT tb_user_inactivation_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_inactivation_un
        UNIQUE (user_uid, inactivation_uid)
);

ALTER TABLE tb_user_inactivation ADD CONSTRAINT fk_inactivation
FOREIGN KEY (inactivation_uid)
REFERENCES tb_inactivation (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_inactivation ADD CONSTRAINT fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

USUÁRIO MEMBRO DE GRUPO MANUAL						
Nome Físico: tb_user_manual_group_membership						
Objetivo: Armazenar os usuários membros dos grupos manuais.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	Uid	BIGINT	N		100
	Versão	Version	INTEGER	S		10
FK	ID Interno do Usuário	user_uid	BIGINT	N		100
FK	ID Interno do Grupo Manual	manual_group_uid	BIGINT	N		100

Script:

```

CREATE TABLE tb_user_manual_group_membership (
    uid BIGINT NOT NULL,
    version INTEGER,
    manual_group_uid BIGINT NOT NULL,
    user_uid BIGINT NOT NULL,
    CONSTRAINT tb_user_manual_group_membership_pkey
        PRIMARY KEY (uid),
    CONSTRAINT tb_user_manual_group_membership_un
        UNIQUE (user_uid, manual_group_uid)
) ;

ALTER TABLE tb_user_manual_group_membership ADD CONSTRAINT fk_user
FOREIGN KEY (user_uid)
REFERENCES tb_user (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

ALTER TABLE tb_user_manual_group_membership ADD CONSTRAINT
fk_manual_group
FOREIGN KEY (manual_group_uid)
REFERENCES tb_manual_group (uid)
ON DELETE NO ACTION
ON UPDATE NO ACTION
NOT DEFERRABLE;

```

VALIDADE						
Nome Físico: tb_validity						
Objetivo: Armazenar as validades.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	Uid	BIGINT	N		100
	Versão	Version	INTEGER	S		10
	Início	begin_date	TIMESTAMP	S		12
	Término	end_date	TIMESTAMP	S		12

Script:

```
CREATE TABLE tb_validity (
    uid BIGINT NOT NULL,
    version INTEGER,
    begin_date TIMESTAMP,
    end_date TIMESTAMP,
    CONSTRAINT tb_validity_pkey
        PRIMARY KEY (uid)
);
```

HISTÓRICO						
Nome Físico: tb_history						
Objetivo: Armazenar o histórico das operações realizadas.						
Chave	Nome Lógico	Nome Físico	Tipo	Nulo	Domínio	Tamanho
PK	ID Interno	Uid	BIGINT	N		100
	Versão	Version	INTEGER	S		10
	Data	date_history	TIMESTAMP	N		12
	Nome do autor	author_name	VARCHAR	S		255
	Nome do sistema	application_name	VARCHAR	S		255
	Descrição	Description	VARCHAR	N		255

Script:

```
CREATE TABLE tb_history (
    uid BIGINT NOT NULL,
    version INTEGER,
    date_history TIMESTAMP NOT NULL,
    author_name VARCHAR(255),
    application_name VARCHAR(255),
    description VARCHAR(255) NOT NULL,
    CONSTRAINT tb_history_pkey
        PRIMARY KEY (uid)
);
```

Script da sequência utilizada por todas as tabelas:

```
CREATE SEQUENCE hibernate_sequence
INCREMENT 1
MINVALUE 1
MAXVALUE 9223372036854775807
START 1470
CACHE 1;
```

2.2.11. DIAGRAMA DE MODELO DE DADOS FÍSICO

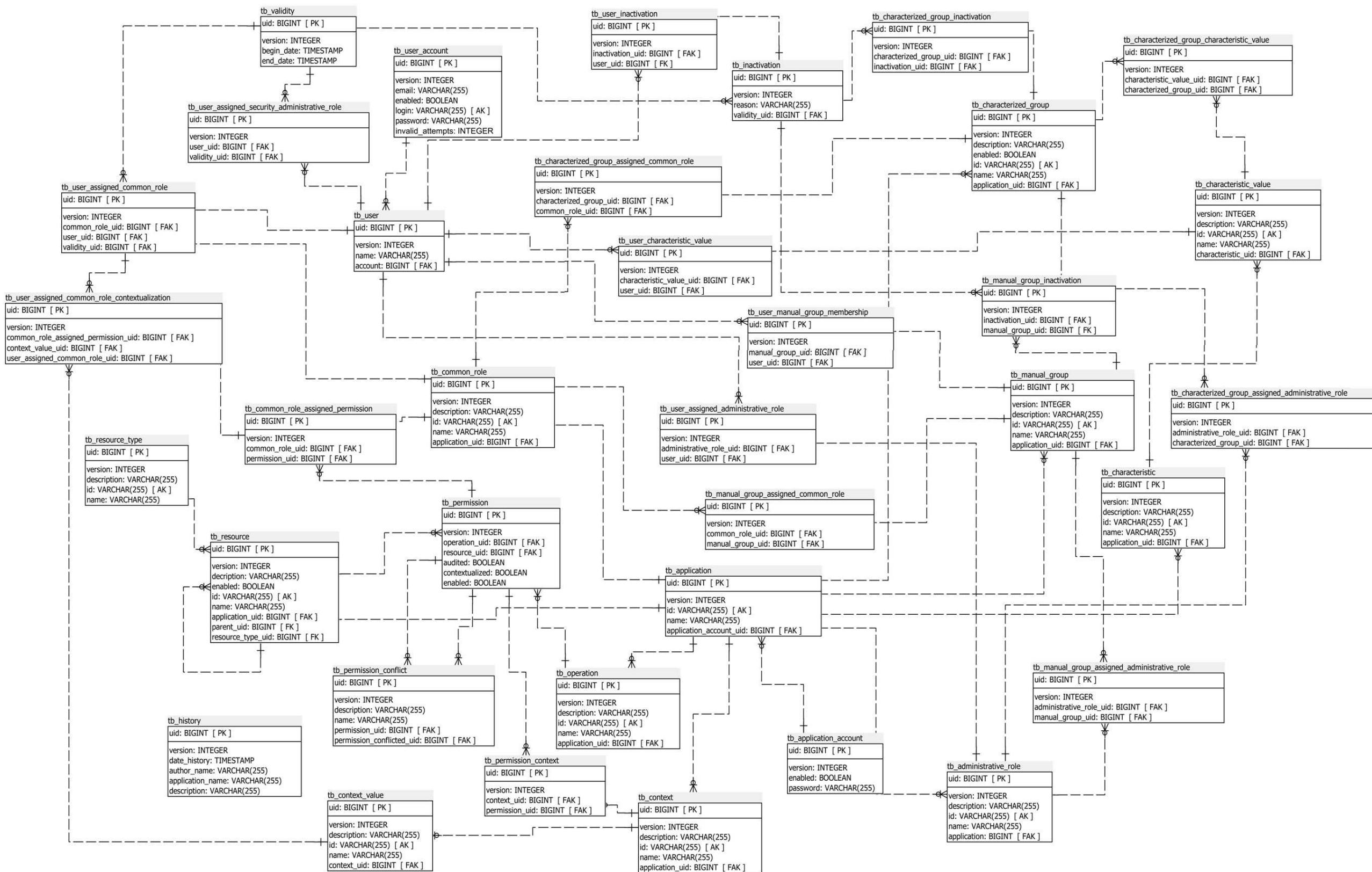


Figura 73: Diagrama de modelo de dados físico

2.2.12. DIAGRAMA DE MODELO DE DADOS LÓGICO

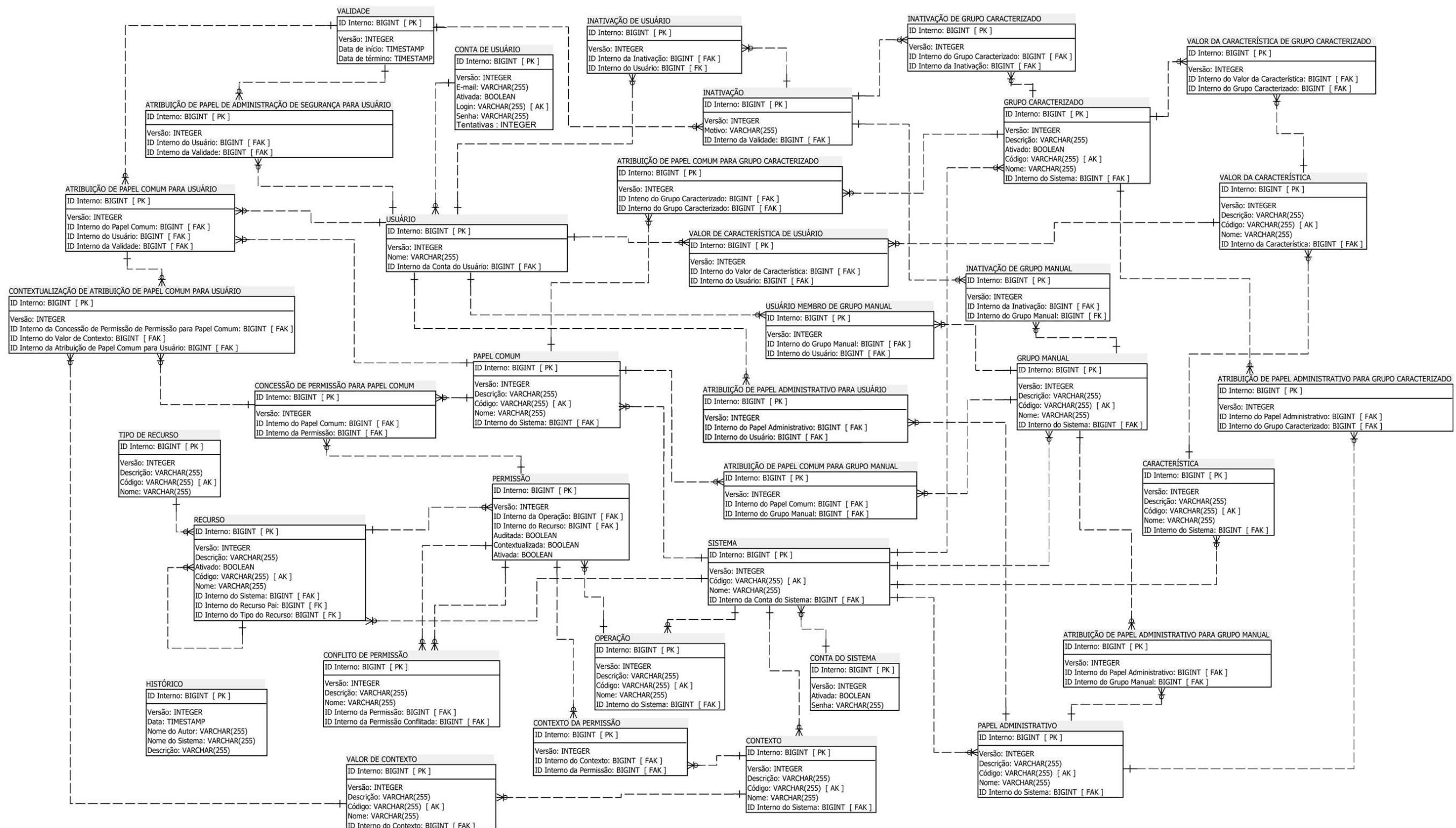


Figura 74: Diagrama de modelo de dados lógico

2.2.13. CONTROLES

2.2.13.1. Controle de Acesso

- Controle lógico

Os acessos as diferentes funcionalidades do sistema serão todas protegidas por login e senha, deste modo cada profissional fará somente as tarefas de sua competência. Por questão de segurança todas as senhas serão armazenadas utilizando um algoritmo de criptografia confiável e sem volta.

As alterações feitas ao sistema serão registradas com o usuário responsável por tal alteração e o dia e hora em que tal operação ocorreu.

O sistema possuirá dois níveis de acesso. Com isto, os usuários do sistema poderão assumir os seguintes papéis:

Administrador de segurança

Possui acesso às funcionalidades básicas do sistema que são:

- Cadastro de sistemas;
- Cadastro de usuários;
- Cadastro de papéis administrativos;
- Cadastro de tipos de recursos;
- Caracterização de usuários;
- Inativação de usuários;
- Atribuição de papéis administrativos para usuários;
- Atribuição de papel de segurança para usuários.

Administrador de sistema

Possui acesso às demais funcionalidades do sistema que são:

- Cadastro de papéis comuns;
- Cadastro de grupos manuais e caracterizados;
- Cadastro de membros em grupos manuais;
- Caracterização de grupos caracterizados;
- Atribuição de papéis comuns para usuários, grupos manuais e caracterizados;
- Contextualização de atribuição de papéis comuns para usuários;
- Atribuição de papéis administrativos para grupos manuais e caracterizados;
- Cadastro de recursos, operações e permissões;
- Contextualização de permissões;
- Cadastro de conflito de permissões;
- Cadastro de contextos e valores de contextos;
- Cadastro de características e valores de características;
- Concessão de permissões para papéis comuns;
- Inativação de grupos manuais e caracterizados.

A definição de quais usuários terão o papel de administrador de segurança caberá ao setor de Segurança da Informação.

A definição de quais usuários terão o papel de administrador de sistema deverá ser decidida pela equipe que estiver desenvolvendo o sistema que consumirá o Framework de Segurança.

Ainda sobre o controle de acesso lógico, apenas a porta 80 (HTTP) do servidor onde o sistema está hospedado é liberada para qualquer usuário da empresa. As demais portas ou são bloqueadas por um firewall, ou somente podem ser acessadas através de autenticação por chave e token de acesso.

- Controle físico

O sistema ficará hospedado em um servidor que está localizado em uma sala cofre na sede da empresa. O acesso físico a esta sala é restrito a alguns funcionários da operação. A autenticidade e a autorização são garantidas através de cartão magnético e reconhecimento de íris.

- Controle de execução

O controle de execução do sistema visa manter o sistema em funcionamento o maior tempo possível.

O local onde o sistema estará hospedado conta com equipamentos capazes de garantir, caso haja falta de energia elétrica, o fornecimento de energia elétrica por até um mês.

- Controle de recuperação

Para que não haja perda das informações a equipe de infraestrutura da empresa fará backup incremental diariamente da base de dados e ao final de cada semana, será feito um agrupamento dos backups realizados durante a semana. Ao final de cada mês, será feito um novo backup que será o agrupamento dos backups semanais. E este backup mensal ficará guardado por cinco anos.

Caso seja necessário voltar alguma versão, a equipe de infraestrutura da empresa estará apta a fazer esta operação e restabelecer a base de dados em até duas horas.

2.2.14. PLANO DE CONTINGÊNCIA

- **Sobrecarga**

O sistema será implantando em uma infraestrutura de TI com balanceamento de carga. Dessa forma, as solicitações serão distribuídas entre os servidores disponíveis na infraestrutura dando preferência para as máquinas mais ociosas.

- **Falha no servidor**

O sistema será implantando em um uma infraestrutura com redundância de servidores de aplicações e banco de dados. Caso haja uma falha em um dos servidores, a equipe de operação será informada e enquanto este servidor é reparado o sistema continuará funcionando através dos demais servidores que não apresentaram problema.

Além da replicação dos dados entre os servidores existentes na infraestrutura principal, será realizada uma replicação entre os demais servidores existentes na empresa. Dessa forma, caso haja problemas em todos os servidores da infraestrutura principal (da sede), as requisições serão redirecionadas para os servidores de outra infraestrutura mais próxima. Porém as operações do sistema serão reduzidas a apenas consultas.

- **Falta de energia elétrica**

O local onde o sistema será implantando conta com equipamentos capazes de garantir, caso haja falta de energia elétrica, o fornecimento de energia elétrica por até um mês.

- **Falha na rede**

Devido à possibilidade de falha na rede será utilizada redundância em todos os equipamentos de rede (switches, cabos, fibras ópticas etc.) evitando que a falha em um equipamento não atrapalhe o uso do sistema. Além da redundância, todos os equipamentos que necessitam de energia elétrica estarão conectados a um no-break.

- **Testes**

Mensalmente, todos os equipamentos utilizados para garantir o pleno funcionamento do sistema serão testados por uma equipe especializada. Nestes testes, serão verificados quais equipamentos não estão funcionando corretamente e serão substituídos por novos equipamentos.

3. PLANO DE IMPLEMENTAÇÃO

3.1. ESTRATÉGIA DE TRABALHO

3.1.1. DESENVOLVIMENTO

O desenvolvimento do sistema será dividido em três etapas:

- Console administrativo

Primeiramente, será desenvolvida toda a parte administrativa e visual do sistema, para que haja maior tempo hábil para testes de carga de dados.

Esta primeira etapa será realizada com o auxílio de uma ferramenta conhecida como Spring Roo. Trata-se de uma ferramenta de interface baseada em texto onde é possível digitar comandos que criam as classes do sistema em linguagem Java e a partir destas classes são criados esboços de telas e o banco de dados. Além disso, ela gera automaticamente os testes de integração e funcionais dos casos de uso de cadastro.

O uso desta ferramenta permitirá entregar rapidamente todas as funcionalidades previstas para esta primeira etapa.

- Serviço de segurança

Após o desenvolvimento do console administrativo, será desenvolvido o serviço de segurança que conterá no primeiro momento as funcionalidades básicas que os sistemas clientes necessitarão (autenticação e autorização). Este serviço será disponibilizado através de web-services para garantir a interoperabilidade entre o serviço e qualquer outra tecnologia que necessite utilizá-lo.

- Clientes nas principais tecnologias

Por último, será desenvolvida uma biblioteca capaz de consumir o serviço de segurança desenvolvido na etapa anterior. Permitindo que o sistema seja usado pelos desenvolvedores das principais tecnologias da forma mais transparente possível.

3.1.2. VERSIONAMENTO DOS ARTEFATOS

Todos os artefatos produzidos pelo projeto serão versionados em uma ferramenta que permita a qualquer momento verificar o histórico de revisões de qualquer artefato, seja ele código fonte ou documento. Esta ferramenta deverá ser capaz de informar também quem, o que e por qual motivo um determinado documento ou trecho de código foi modificado por um integrante do projeto.

Também deverá ser capaz de garantir o acesso aos artefatos do projeto apenas a pessoas autorizadas.

3.1.3. TESTES

Durante o desenvolvimento do sistema, será utilizado um servidor de integração contínua conhecido como Hudson que será responsável por realizar diversos testes todas as vezes que o código fonte do sistema for alterado. Com isto, será possível identificar rapidamente qualquer problema inserido pelo desenvolvedor.

Os testes de integração, funcionais, unitários e de cobertura serão executados automaticamente pelo servidor de integração contínua. Ao final de cada teste, o servidor de integração contínua irá gerar relatórios que podem ser analisados por qualquer pessoa da equipe.

Para aumentar a qualidade do sistema, além dos testes funcionais executados automaticamente pela ferramenta de integração contínua, uma equipe dedicada à realização de testes da empresa também executarão os testes funcionais.

3.1.4. CARGA INICIAL

Será necessário elaborar um script para cadastrar todos os funcionários da empresa que utilizam computador. Essa informação será obtida a partir do repositório de dados de funcionários.

Além disto, será preciso atribuir manualmente o papel de administrador de segurança para o primeiro funcionário da empresa que foi escolhido para ter esse papel. Esta atribuição será feita através de script executado diretamente em banco de dados.

3.1.5. TREINAMENTO

Serão aplicados treinamentos quinzenais até que todos os desenvolvedores da empresa sejam treinados. Estes treinamentos utilizarão um sistema exemplo de fácil entendimento e contarão também com o manual do usuário.

Será criada uma área em um fórum interno já existente da empresa para discutir assuntos ligados à utilização da ferramenta. Possibilitando a troca de conhecimento entre os desenvolvedores da empresa com relação ao sistema.

3.1.6. IMPLANTAÇÃO

A implantação do sistema será feita através da abertura de chamado para equipe de operações existente na empresa. Esta equipe é responsável por executar os scripts de instalação que serão fornecidos neste chamado.

Para execução desta tarefa, o prazo acordado entre a área de desenvolvimento e infraestrutura é de três dias úteis.

No dia após a finalização da tarefa realizada pela equipe de infraestrutura, serão realizados os testes de carga e stress para garantir a operacionalidade do sistema em ambiente de homologação.

Após o aceite dos testes de carga e stress, o sistema será liberado para operação em homologação. Com isto, os usuários serão habilitados a utilizar o sistema e, em paralelo, o desempenho será monitorado pela equipe de infraestrutura por uma semana. Ao final desta semana, será emitido um parecer alegando que o sistema não apresentou instabilidade e que poderá ser implantado em produção.

A implantação no ambiente de produção será feita automaticamente por meio de replicação dos dados presentes no ambiente de homologação para produção em horário não comercial e será transparente para os usuários.

3.2. RECURSOS ESTIMADOS

A proposta para implementação do sistema conta com os seguintes recursos humanos e materiais:

3.2.1. FASE DE DESENVOLVIMENTO

- Recursos humanos

Quantidade	Recurso
1	Analista de sistemas
1	Desenvolvedor

Tabela 12: Previsão de alocação de recursos humanos na fase de desenvolvimento

- Recursos materiais

Hardware	
Quantidade	Recurso
1	Notebook MacBook Intel Core 2 Dual, 2GHz, 2GB de memória.

Tabela 13: Previsão de recursos de hardware na fase de desenvolvimento

Software	
Quantidade	Recurso
1	Microsoft Windows XP Professional
1	Eclipse IDE
1	PostgreSQL 8.4
1	pgAdmin III
1	JBoss Application Server
1	Hudson Continuous Integration Server
1	Spring Roo
1	TortoiseSVN
1	Navegador Mozilla Firefox 3.6

Tabela 14: Previsão de recursos de software na fase de desenvolvimento

3.2.2. FASE DE TESTES

- Recursos humanos

Quantidade	Recurso
1	Analista de sistemas

Tabela 15: Previsão de alocação de recursos humanos na fase de testes

- Recursos materiais

Hardware	
Quantidade	Recurso
1	Computador Intel Core 2 Dual, 4GHz, 16GB de memória.

Tabela 16: Previsão de recursos de hardware na fase de testes

Software	
Quantidade	Recurso
1	Linux Red Hat 9
1	PostgreSQL 8.4
1	Hudson Continuous Integration Server
1	Navegador Mozilla Firefox 3.6

Tabela 17: Previsão de recursos de software na fase de testes

3.2.3. FASE DE TREINAMENTO

- Recursos humanos

Quantidade	Recurso
1	Analista de sistemas
-	Todos os desenvolvedores da empresa

Tabela 18: Previsão de alocação de recursos humanos na fase de desenvolvimento

- Recursos materiais

Hardware	
Quantidade	Recurso
1	Notebook Intel Core 2 Dual, 2GHz, 2GB de memória
20	Microcomputadores Intel Core 2 Dual, 2GHz, 2GB de memória
1	Projetor multimídia EPSON PowerLite S8

Tabela 19: Previsão de recursos de hardware na fase de desenvolvimento

Software	
Quantidade	Recurso
1	Microsoft Windows XP
1	PostgreSQL 8.4
1	Navegador Mozilla Firefox 3.6
1	MS Office 2007 Professional

Tabela 20: Previsão de recursos de software na fase de desenvolvimento

Material de Escritório	
Quantidade	Recurso
100	Manual do usuário
20	Folha de papel A4
1	Flip chart
1	Quadro branco
5	Caneta Pillot
6	Cartucho de tinta para impressora
2	Caneta preta
2	Caneta azul

Tabela 21: Previsão de materiais de escritório na fase de desenvolvimento

3.2.4. FASE DE HOMOLOGAÇÃO

- Recursos humanos

Quantidade	Recurso
1	Analista de sistemas
1	Técnico de infraestrutura
-	Analistas e desenvolvedores da empresa

Tabela 22: Previsão de alocação de recursos humanos na fase de homologação

- Recursos materiais

Software	
Quantidade	Recurso
1	Linux Red Hat 9
1	PostgreSQL 8.4

Tabela 23: Previsão de recursos de hardware na fase de homologação

3.2.5. FASE DE IMPLANTAÇÃO

- Recursos humanos

Quantidade	Recurso
1	Analista de sistemas
1	Técnico de infraestrutura

Tabela 24: Previsão de alocação de recursos humanos na fase de homologação

- Recursos materiais

Software	
Quantidade	Recurso
1	Linux Red Hat 9
1	PostgreSQL 8.4

Tabela 25: Previsão de recursos de hardware na fase de homologação

3.3. CRONOGRAMA

O cronograma para realização das fases prevista para o plano de implementação é apresentado a seguir. Serão considerados apenas dias úteis.

#	Nome da tarefa	Duração (dias)	Início	Término
1	Desenvolvimento	9	01/06/2010	09/06/2010
1.1	Cadastro básico	1	01/06/2010	01/06/2010
1.2	Cadastro de papeis	1	02/06/2010	02/06/2010
1.3	Cadastro de atribuições	1	03/06/2010	03/06/2010
1.4	Cadastro de inativações	1	04/06/2010	04/06/2010
1.5	Cadastro de grupos	1	07/06/2010	07/06/2010
1.6	Cadastro de concessões	1	08/06/2010	08/06/2010
1.7	Cadastro de mapeamentos	1	09/06/2010	09/06/2010
1.8	Cadastro de contextos	1	10/06/2010	10/06/2010
1.9	Cadastro de características	1	11/06/2010	11/06/2010
2	Testes	2	14/06/2010	15/06/2010
3	Treinamento	5	16/06/2010	22/06/2010
4	Homologação	2	23/06/2010	24/06/2010
5	Implantação	2	25/06/2010	28/06/2010

Tabela 26: Cronograma do plano de implementação

3.4. ORÇAMENTO

Todos os valores a seguir serão expressos em reais (R\$).

- Cálculo de salário

Para o cálculo de salário dos integrantes do projeto por hora será utilizada a fórmula a seguir:

$$(\text{SBM} / \text{CHM}) \text{ EM}$$

Fórmula 2: Cálculo do salário

Onde:

- **SBM** corresponde ao salário bruto mensal.
- **CHM** corresponde a carga horária mensal. Será definido o valor 240 para esta variável.
- **EM** corresponde ao valor dos encargos mensais. Será definido o valor 2,54 para esta variável.

Os valores levam em consideração os cursos indiretos do salário, tais como FGTS, impostos, férias etc.

- Cálculo de depreciação

Bens e equipamentos depreciam por lei em 5 anos. Com a base de cálculo sendo de 20% por ano. Para isto, foi elaborada a seguinte tabela para calcular a depreciação de cada equipamento em cada mês:

Recurso material	Valor	Depreciação por mês
Notebook	3.000,00	50,00
Servidor	20.000,00	333,33
MS Office 2007 Professional	1.500,00	25,00

Tabela 27: Depreciação dos recursos materiais por mês

- Cálculo de despesas diversas

Calcula-se que as despesas diversas de um projeto giram em torno de 10% (dez por cento) do total de todas as despesas. O cálculo é feito somando todas as demais despesas e dividindo o total desta soma por 9 (nove).

- Cálculo do custo do dinheiro

Sobre um bem ou equipamento quando de sua aquisição, é gerado de imediato, uma despesa referindo-se ao dinheiro. Quando aplicado este dinheiro no mercado financeiro é estimado que renda cerca de 1% ao mês.

- Cálculo do orçamento final

Representa todo o somatório de investimentos e despesas

- Totalização dos cursos

Custo total do projeto, somatório de todos os meses.

- Consolidação dos cálculos.

Abaixo serão apresentadas diversas tabelas que foram usadas para calcular o custo da implementação.

Recurso humano	Junho
Analista de sistemas	50h
Gerente de projeto	10h
Técnico de infraestrutura	24h
Desenvolvedor	72h
Testador	16h

Tabela 28: Utilização dos recursos humanos ao longo da fase de implementação

A tabela a seguir representa os valores e o cálculo usado para obtenção do valor por hora de cada recurso humano que participará do projeto na fase de implementação. O cálculo do valor por hora utiliza a fórmula explicada no item “Cálculo do salário”.

Recurso humano	Salário Bruto Mensal	Valor por hora no projeto
Analista de sistemas	6.000,00	63,50
Gerente de projetos	9.000,00	95,25
Técnico de infraestrutura	3.000,00	31,75
Testador	3.000,00	31,75
Desenvolvedor	5.000,00	52,91

Tabela 29: Valor por hora dos recursos humanos no projeto

Multiplicando as horas de cada recurso humano pelo seu custo por hora no projeto, obtém-se a tabela a seguir:

Recurso humano	Junho
Analista de sistemas	3.175,00
Gerente de projeto	952,50
Técnico de infraestrutura	762,00
Testador	508
Desenvolvedor	3.809,52
Total	9.207,02

Tabela 30: Despesas com recursos humanos durante a fase de implementação

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

Usando os valores obtidos no cálculo da depreciação e levando em consideração que os recursos materiais a seguir já foram obtidos durante a primeira fase, temos os seguintes gastos com recurso material na segunda fase:

Recurso material	Junho
Notebook	50,00
Impressora colorida	5,00
MS Windows XP Pro	9,17
MS Office 2007 Pro	25,00
Servidor	333,33
Total	422,50

Tabela 31: Despesas com recursos materiais durante a fase de implementação

O projetor multimídia e os computadores utilizados nos treinamentos não entrarão nos custos do projeto, pois são recursos oferecidos pela empresa em suas salas de treinamento sem custo para o projeto.

Despesa	Junho
Despesas recursos humanos	9.207,02
Despesas recursos materiais	422,50
Despesas diversas	1.069,95
Custo do dinheiro	106,70
Total	10.806,46

Tabela 32: Cálculo do orçamento final para a fase de implementação

3.5. PLANO DE TESTES

O desenvolvimento de software é uma atividade complexa, justamente por estar suscetível a erros de diversas naturezas, tais como: especificação errada ou incompleta, requisitos impossíveis de serem implementados por limitações de hardware ou software, ou até um simples erro de digitação durante a implementação. Por esta razão, serão executados testes de várias naturezas com intuito de identificar e corrigir os erros existentes.

Serão abortadas as seguintes técnicas de teste de software:

- Teste funcional (caixa preta)

Serão realizados testes nas interfaces do console administrativo para demonstrar a operacionalidade das funções (entrada de dados aceita e saída corretamente produzida). Um teste de caixa preta examina um sistema sem se preocupar muito com estrutura lógica interna do software. Para estes testes serão criados casos de testes que serão executados pela equipe de testes da empresa. Além de executados por esta equipe, os testes serão automatizados na ferramenta Selenium que permite gravar uma sequência de passos dentro do sistema que simula a navegação de um usuário no mesmo. Esta ferramenta gera relatórios dos testes executados como mostrado a seguir:

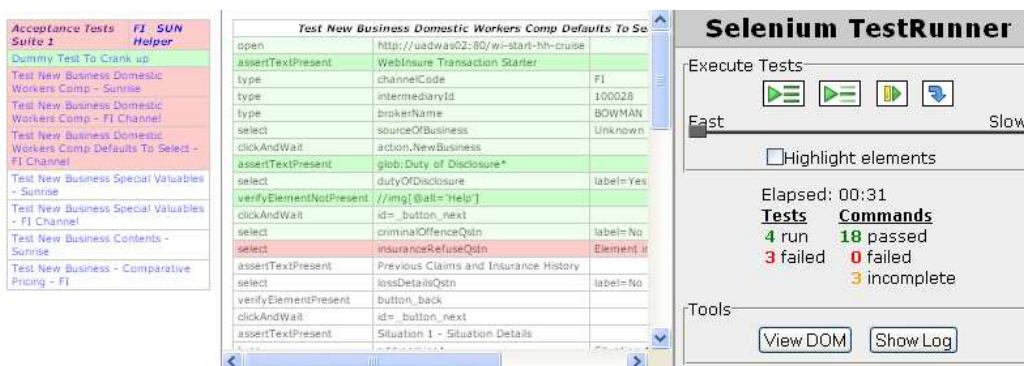


Figura 75 - Exemplo de relatório de testes gerado pelo Selenium

- Teste estrutural (caixa branca)

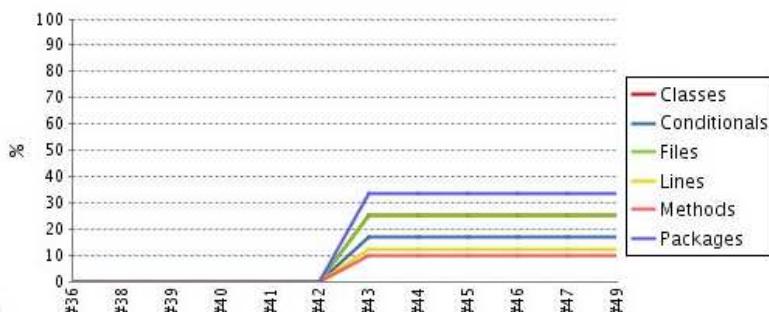
Diferentemente dos testes de caixa preta, os de caixa branca buscam a verificação da estrutura interna (implementação) do sistema, de forma que possa garantir sua validade. O objetivo é derivar todos os casos de teste possíveis, de forma a percorrer todas as opções condicionais e a exercitar as derivações lógicas. Para estes testes serão utilizados os testes unitários e de integração.

Para estes testes será utilizada a ferramenta JUnit, que permite escrever código que testam a implementação. Porém, para garantir a precisão destes testes, será utilizada a ferramenta Cobertura que analisa se os testes executados passaram por todo o código do sistema. Dessa forma, ela indica quais trechos de código não foram testados, permitindo que o desenvolvedor analise o resultado e decida se o código não testado deveria existir ou se será preciso escrever um código para testá-lo. A seguir, será exibido o relatório gerado pelas duas ferramentas citadas dentro do servidor de integração continua Hudson.

Code Coverage

Cobertura Coverage Report

Trend



Project Coverage Summary

Name	Packages	Files	Classes	Methods	Lines	Conditionals
Cobertura Coverage Report	33% (1/3)	25% (1/4)	25% (1/4)	10% (3/31)	12% (10/82)	17% (4/24)

Coverage Breakdown by Package

Name	Files	Classes	Methods	Lines	Conditionals
surveys.view	0% (0/1)	0% (0/1)	0% (0/5)	0% (0/16)	0% (0/8)
surveys.persistence	0% (0/2)	0% (0/2)	0% (0/7)	0% (0/17)	0% (0/8)
surveys.domain	100% (1/1)	100% (1/1)	16% (3/19)	20% (10/49)	50% (4/8)

Figura 76 - Exemplo de relatório de testes de cobertura gerado pelo Cobertura

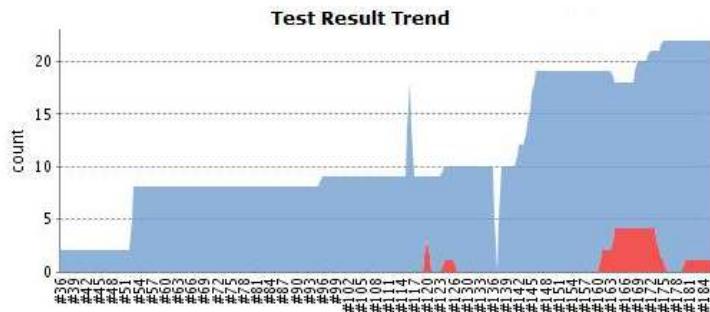


Figura 77 - Exemplo de relatório de testes unitários e de integração gerado pelo JUnit

- **Teste de validação**

Este teste tem como objetivo verificar se as funcionalidades desenvolvidas estão atendendo aos requisitos especificados. Este teste será realizado durante a fase de homologação, onde os usuários ao utilizar o sistema constatarão se o mesmo está de acordo com o que foi solicitado.

- **Teste de segurança**

Serão realizados testes para verificar os mecanismos de segurança do sistema. No sistema proposto, será verificado se usuários terão acesso a áreas onde não possuem autorização.

- **Teste de stress**

O teste de stress é utilizado para verificar o comportamento do sistema quando submetido a uma massa de dados muito superior à que será usualmente observada. Espera-se que não haja comprometimento das informações e que o desempenho não seja depreciado. Para este teste, será utilizada a ferramenta JMeter que será responsável por executá-lo e gerar relatórios que serão exibidos pelo servidor de integração continua, como mostrado na imagem a seguir:

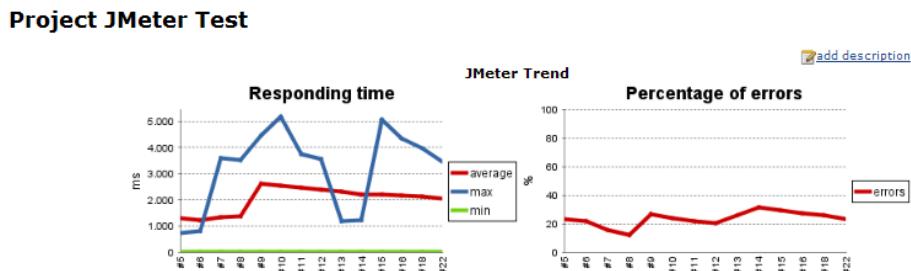


Figura 78 - Exemplo de relatório de testes de stress gerado pelo JMeter

Além destes testes, serão feitos também testes alfas e testes betas para garantir que não existirão problemas no ambiente do cliente.

Os testes de caixa preta serão executados seguindo um plano de teste. Seu grau de complexidade será avaliado, seguindo os cálculos da complexidade ciclomática.

O programa escolhido para esta etapa foi o de autenticação de usuário. A seguir o código em português estruturado, o fluxograma o grafo de fluxo, o cálculo da complexidade ciclomática e a identificação dos caminhos independentes.

UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

- Português estruturado

	<pre> ALGORITMO "AUTENTICAÇÃO DE USUÁRIO" VARIÁVEIS 1 V_LOGIN : TEXTO; 2 V_SENHA : TEXTO; 3 V_SISTEMA : TEXTO; 4 V_ADMIN_SEGURANCA = FALSO : LÓGICO; 5 V_SENHA_VALIDA = FALSO : LÓGICO; 6 V_ADMIN_SISTEMA = FALSO : LÓGICO; INÍCIO 7 ESCREVA("INFORME O LOGIN: "); 8 LEIA(V_LOGIN); 9 ESCREVA("INFORME A SENHA: "); 10 LEIA(V_SENHA); 11 ESCREVA("INFORME O SISTEMA: "); 12 LEIA(V_SISTEMA); 13 RESGATAR EM "INATIVAÇÕES DE USUÁRIOS" (VALIDADE) ONDE LOGIN = V_LOGIN; 14 FAÇA PARA CADA "INATIVAÇÃO" EM "R.INATIVAÇÕES DE USUÁRIOS" 15 SE "INATIVAÇÃO.VALIDADE.INÍCIO" < DATA_ATUAL E 16 "INATIVAÇÃO.VALIDADE.TÉRMINO" > DATA_ATUAL ENTÃO 17 RETORNE ERRO "USUÁRIO INATIVADO"; 18 FIM SE 19 PRÓXIMO; 20 SE V_SISTEMA = "" ENTÃO 21 RESGATAR EM 22 "ATRIBUIÇÕES DE PAPEL DE ADMINISTRADOR DE SEGURANÇA" (VALIDADE) 23 ONDE LOGIN = V_LOGIN; 24 FAÇA PARA CADA "ATRIBUIÇÃO" EM 25 "R.ATRIBUIÇÕES DE PAPEL DE ADMINISTRADOR DE SEGURANÇA" 26 27 SE "ATRIBUIÇÃO.VALIDADE.INÍCIO" < DATA_ATUAL E 28 "ATRIBUIÇÃO.VALIDADE.TÉRMINO" > DATA_ATUAL ENTÃO 29 V_ADMIN_SEGURANCA <- VERDADEIRO; 30 31 FIM SE 32 PRÓXIMO; 33 SE V_ADMIN_SEGURANCA = FALSO ENTÃO 34 RETORNE ERRO "USUÁRIO NÃO É ADMINISTRADOR DE SEGURANÇA"; 35 36 SENÃO 37 RESGATAR EM "USUÁRIOS" (TENTATIVAS_COM_ERRO) 38 ONDE LOGIN = V_LOGIN; 39 FAÇA PARA CADA "USUÁRIO" EM "R.USUÁRIOS" 40 SE "USUÁRIO.TENTATIVAS_COM_ERRO" > 10 ENTÃO 41 RETORNE ERRO "CONTA DO USUÁRIO BLOQUEADA"; 42 SENÃO SE "USUÁRIO.SENHA" = V_SENHA ENTÃO 43 V_SENHA_VALIDA <- VERDADEIRO; 44 TENTATIVAS_COM_ERRO <- 0; 45 PARE; 46 SENÃO 47 TENTATIVAS_COM_ERRO <- TENTATIVAS_COM_ERRO + 1; 48 PARE; 49 FIM SE 50 PRÓXIMO; </pre>
--	---

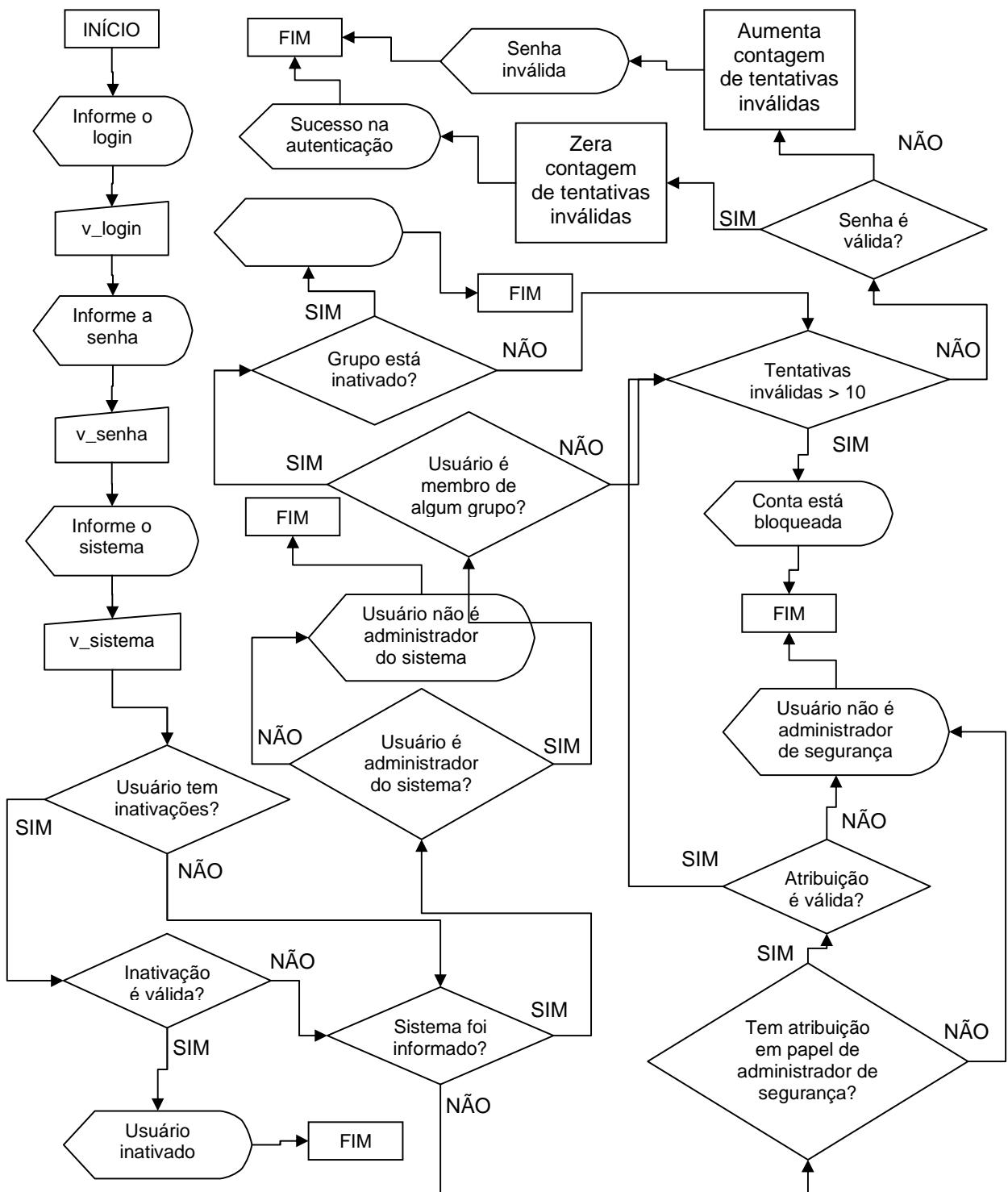
UNIVERSIDADE ESTÁCIO DE SÁ
SISTEMAS DE INFORMAÇÃO

```

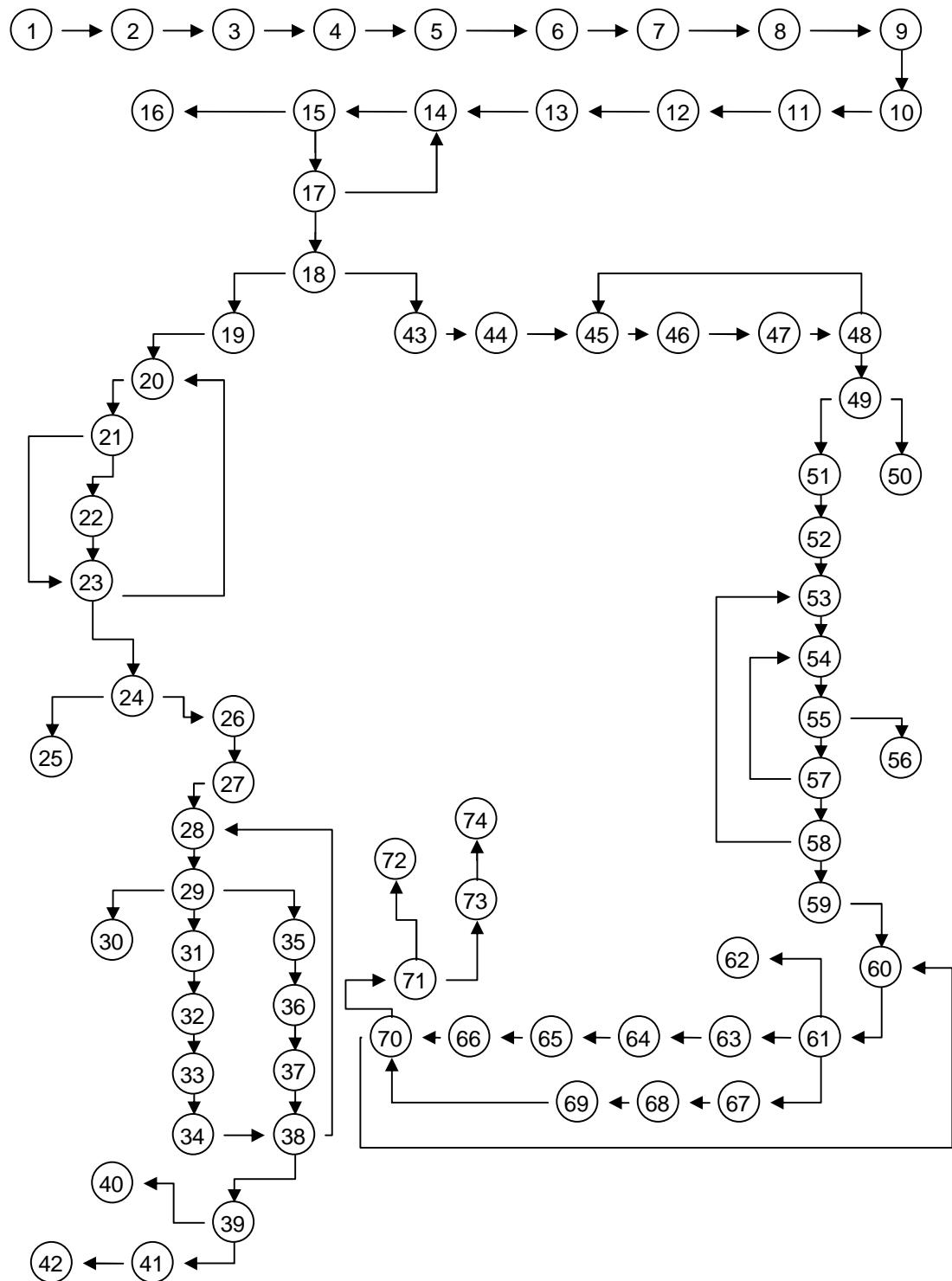
38      SE V_SENHA_VALIDA = FALSO ENTÃO
40          RETORNE ERRO "SENHA INVÁLIDA";
41      SENÃO
42          ESCREVA "SUCESSO NA AUTENTICAÇÃO";
43          FIM SE
44      FIM SE
45      SENÃO
46          RESGATAR EM
47              "ATRIBUIÇÕES DE PAPEL DE ADMINISTRADOR DE SISTEMA"
48                  ONDE LOGIN = V_LOGIN E SISTEMA = V_SISTEMA;
49                  FAÇA PARA CADA "ATRIBUIÇÃO" EM
50                      "R.ATRIBUIÇÕES DE PAPEL DE ADMINISTRADOR DE SISTEMA"
51                      V_ADMIN_SISTEMA <- VERDADEIRO;
52                      PARE;
53                      PRÓXIMO;
54
55          SE V_ADMIN_SISTEMA = FALSO ENTÃO
56              RETORNE ERRO "USUÁRIO NÃO É ADMINISTRADOR DO SISTEMA";
57
58          SENÃO
59              RESGATAR EM "MEMBROS DO GRUPO DE USUÁRIOS" ONDE LOGIN = V_LOGIN;
60              FAÇA PARA CADA "MEMBRO" EM "R.MEMBROS DO GRUPO DE USUÁRIOS"
61                  RESGATAR EM
62                      "INATIVAÇÕES DE GRUPO DE USUÁRIOS"
63                          ONDE GRUPO = "MEMBRO.GRUPO" E
64                          "MEMBRO.GRUPO.SISTEMA" = V_SISTEMA;
65                  FAÇA PARA CADA "INATIVAÇÃO" EM
66                      "R.INATIVAÇÕES DE GRUPO DE USUÁRIOS"
67                      SE "INATIVAÇÃO.VALIDADE.INÍCIO" < DATA_ATUAL E
68                          "INATIVAÇÃO.VALIDADE.TÉRMINO" > DATA_ATUAL ENTÃO
69                          RETORNE ERRO "USUÁRIO INATIVADO";
70                      FIM SE
71                      PRÓXIMO;
72
73          RESGATAR EM "USUÁRIOS" (TENTATIVAS_COM_ERRO) ONDE LOGIN = V_LOGIN;
74          FAÇA PARA CADA "USUÁRIO" EM "R.USUÁRIOS"
75              SE "USUÁRIO.TENTATIVAS_COM_ERRO" > 10 ENTÃO
76                  RETORNE ERRO "CONTA DO USUÁRIO BLOQUEADA";
77              SENÃO SE "USUÁRIO.SENHA" = V_SENHA ENTÃO
78                  V_SENHA_VALIDA <- VERDADEIRO;
79                  TENTATIVAS_COM_ERRO <- 0;
80                  PARE;
81              SENÃO
82                  TENTATIVAS_COM_ERRO <- TENTATIVAS_COM_ERRO + 1;
83                  PARE;
84              FIM SE
85          PRÓXIMO;
86
87          SE V_SENHA_VALIDA = FALSO ENTÃO
88              RETORNE ERRO "SENHA INVÁLIDA";
89          SENÃO
90              ESCREVA "SUCESSO NA AUTENTICAÇÃO";
91              FIM SE
92          FIM SE
93
94      FIM.

```

- Fluxograma



- Grafo de fluxo



- Cálculo da complexidade ciclomática

Nós predicativos: 11

Regiões: 10

Nós: 74

Arrestas: 83

Prova real: $82 - 74 + 2 = 10$

- Caminhos independentes
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-25
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-25
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-26-27-28-29-30
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-26-27-28-29-31-32-33-34-38-39-40
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-26-27-28-29-31-32-33-34-38-39-41-42
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-26-27-28-29-35-36-37-38-39-40
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-22-23-24-26-27-28-29-35-36-37-38-39-41-42
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-26-27-28-29-30
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-26-27-28-29-31-32-33-34-38-39-40
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-26-27-28-29-31-32-33-34-38-39-41-42
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-26-27-28-29-35-36-37-38-39-40
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-19-20-21-23-24-26-27-28-29-35-36-37-38-39-41-42
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-50
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-56
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-57-58-59-60-61-62
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-57-58-59-60-61-63-34-65-66-70-71-72
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-57-58-59-60-61-63-34-65-66-70-71-73-74
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-57-58-59-60-61-67-68-69-70-71-72
 - 1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-17-18-43-44-45-46-47-48-49-51-52-53-54-55-57-58-59-60-61-67-68-69-70-71-73-74

- Plano de testes

Tipo de Teste	Caso de Teste	Condições	Ações	Resultados Esperados
Interface	Não preenchimento dos campos obrigatórios	-	Tentar autenticar um usuário sem preencher os campos login e senha.	Que o sistema exiba uma alerta informando que os campos login e senha são obrigatórios.
Funcionalidade	Cadastramento de sistema já existente	Que já exista sistema com o mesmo código do que será cadastrado no teste.	Cadastrar sistema com mesmo código de um já existente na base de dados.	Que o sistema exiba mensagem de erro informando que já existe sistema com o código informado.
Desempenho	Tempo de resposta	Que existam ao menos 50.000 registros de usuários, papéis, recursos, operações, grupos, usuários e atribuições.	Verificar autorização de usuário em permissão.	Que o sistema retorne o resultado em menos de 1 segundo.
Conteúdo da Informação	Veracidade da resposta	Que usuário esteja inativado.	Verificar autorização de usuário inativo em permissão.	Que o sistema negue a autorização.

4. CONCLUSÃO

O Framework de Segurança foi desenvolvido com o objetivo de atender aos requisitos solicitados pelos envolvidos no projeto. Todas as áreas que participaram das reuniões contribuíram com ideias e ajudaram a dar soluções para alguns problemas que surgiram, principalmente os tecnológicos.

Por ter sido um projeto pioneiro com o objetivo de aumentar reuso durante o desenvolvimento de software na empresa, inicialmente sofreu preconceitos por alguns funcionários, principalmente gerentes. Porém, após o cálculo de economia que o projeto poderia dar para a área de desenvolvimento, os gerentes passaram a olhá-lo com outros olhos. Isto foi bom, pois ganhamos apoio de diversas áreas e, consequentemente, nos deu forças para prosseguir com o projeto.

Diante das necessidades levantadas, o módulo desenvolvido até o momento conta com as seguintes funcionalidades:

- Autenticação de usuários;
- Cadastro de sistemas;
- Cadastro de usuários;
- Cadastro de tipos de recursos;
- Caracterização de usuários
- Cadastro de papéis administrativos;
- Cadastro de papéis comuns;
- Cadastro de grupos manuais;
- Cadastro de grupos caracterizados;
- Atribuição de papéis administrativos para usuários;
- Atribuição de papéis administrativos para grupos manuais;
- Atribuição de papéis administrativos para grupos caracterizados;
- Atribuição de papel de segurança para usuários;
- Atribuição de papéis comuns para usuários;
- Atribuição de papéis comuns para grupos manuais;
- Atribuição de papéis comuns para grupos caracterizados;
- Inativação de usuários;
- Inativação de grupos manuais;
- Inativação de grupos caracterizados;
- Cadastro de características e valores de características;
- Cadastro de contextos e valores de contextos;
- Cadastro de recursos;
- Cadastro de operações;
- Cadastro de permissões;
- Contextualização de permissões;
- Cadastro permissões conflitantes;
- Concessões de permissões.

- **Benefícios tangíveis**

- Erros relacionados à segurança nos projetos tiveram uma diminuição de 80%;
- Redução de 20% dos custos no desenvolvimento dos novos sistemas;
- Redução de 10% do escopo dos novos sistemas;
- Diminuição de 25% os prazos para desenvolvimento dos novos sistemas;

- **Benefícios intangíveis**

- Reforço na segurança dos sistemas;
- Melhoria na qualidade dos sistemas desenvolvidos;
- Aumento da produtividade dos desenvolvedores;
- Equipes passaram a focar mais os problemas de negócio do que os de segurança;
- Satisfação dos clientes finais, pois agora, eles têm apenas uma interface gráfica para administrar a segurança de todos os seus sistemas.

5. TRABALHOS FUTUROS

A seguir, serão listados os possíveis trabalhos futuros identificados para este projeto:

- Desenvolvimento do Serviço de Segurança com as operações básicas de autenticação e autorização;
- Desenvolvimento do Cliente Java;
- Desenvolvimento do Cliente .NET;
- Expansão das funcionalidades presentes no Console Administrativo para o Serviço de Segurança e consequentemente para os Clientes Java e .NET.
- Criação de mecanismos de cache no Serviço de Segurança para aumentar a performance do sistema;
- Criação de mecanismos de cache nos Clientes para diminuir a quantidade de requisições feitas ao Serviço de Segurança.

6. GLOSSÁRIO

Palavra	Significado
.NET	Plataforma de desenvolvimento de aplicações da empresa Microsoft Corporativa.
Atribuir	Ato de conferir o direito a alguém.
Cache	Área de armazenamento de dados de acesso rápido.
COBERTURA	Software utilizado para analisar a taxa de cobertura dos testes unitários e de integração.
Conceder	Ato de dar privilégio, direito, vantagem de alguma coisa para alguém.
ECLIPSE IDE	Ferramenta para desenvolvimento de aplicações, principalmente Java.
Firewall	Programa que controla o tráfego de dados em uma rede.
Framework	É uma abstração que une códigos comuns entre vários projetos de software provendo uma funcionalidade genérica.
HUDSON	Servidor de integração contínua.
Java	Linguagem de programação orientada a objetos desenvolvida na década de 90 pela empresa Sun Microsystems.
Java EE	Plataforma corporativa da linguagem Java.
JBOSS	Servidor de aplicações da plataforma Java EE.
JMETER	Software utilizado para realizar testes de carga e stress em aplicações.
JUNIT	Framework utilizado para realização de testes unitários e de integração na linguagem Java.
No-break	Fonte de alimentação ininterrupta. Destinado a suprir a alimentação elétrica dos equipamentos a ele acoplados, quando é interrompido o fornecimento pela concessionária de energia elétrica.
Offshore	Localizado ou operado no mar.
Revogar	Ato de retirar o privilégio, direito ou vantagem de alguém.
SELENIUM	Software utilizado para realização de testes funcionais em aplicações web.
SVN/Subversion	Repositório de versionamento de artefatos de projeto.
Token de acesso	Dispositivo eletrônico gerador de senhas, sem conexão física com o computador.
TORTOISE SVN	Software para manipulação de repositórios de versionamentos Subversion.
UML	Sigla de Unified Modeling Language. É uma linguagem de modelagem não proprietária de terceira geração.

7. BIBLIOGRAFIA

DEITEL, H. M.; DEITEL, P.J. Java: Como programar; tradução e revisão técnica Carlos Arthur Lang Lisboa. 4 ed., 2003.

FOWLER, Martin, KOBRYN, Cris, BOOCH, Grady – UML Essencial: Um breve guia para linguagem padrão de modelagem de objetos. 3 ed. – Porto Alegre: Bookman, 2005.

LARMAN, Craig – Utilizando UML e Padrões: uma introdução à análise e ao projeto orientados a objetos e AP desenvolvimento iterativo; tradução Rosana Vaccare Brava ...[et AL.]. 3 ed. – Porto Alegre: Bookman, 2007.

FERRAIOLI, David – Role-based Access control: Artech house computer security sense.
1 ed. – Norwood, MA: British Library, 2003.

8. ANEXO I – MANUAL DO USUÁRIO