MIDDLEWARE PARA FORNECIMENTO DE SERVIÇO DE SEGURANÇA EM CONFORMIDADE COM A ISO/IEC 15.408

astellani Gucowski

do da Silva - Orientador

Roteiro

- Introdução
- Objetivos do trabalho
- Fundamentação teórica
- Desenvolvimento do Middleware
- Resultados e discussões
- Conclusão
- Extensões

Introdução

- Segurança da informação
- Desenvolvimento do software sem segurança
- Desenvolvimento do middleware
- Norma ISO/IEC 15.408
- Remote Method Invocation (RMI)

Objetivos do trabalho

- Desenvolver um middleware em conformidade com algumas classes da norma ISO/IEC 15.408, que garanta a segurança dos softwares e auxilie/facilite o desenvolvimento dos mesmo.

Fundamentação teórica

Aspectos de segurança

- Confidencialidade;
- Integridade dos dados;
- Disponibilidade;
- Autentitação;
- Não repúdio;
- Legalidade;
- Privacidade;
- Auditoria.

ISO/IEC 15.408

- **Objetivos da norma**

  ✓ Fornecer um conjunto de critérios fixos que permitem especificar a segurança de uma aplicação (ALBUQUERQUE; RIBEIRO, 2002, p. 7). A norma é composta de 7 níveis de avaliação: 1 à 4, para produtos comerciais e 5 à 7 para produtos militares.

ISO/IEC 15.408

- **Classes da norma**

Classe	Sigla
Auditoria	FAU
Proteção de dados do usuário	FDP
Criptografia	FCS
Autoproteção	FPT
Canais seguros	FTP
Autenticação	FIA
Acesso ao sistema	FTA
Gerenciamento de segurança	FMT
Utilização de recursos	FRU
Privacidade	FPR

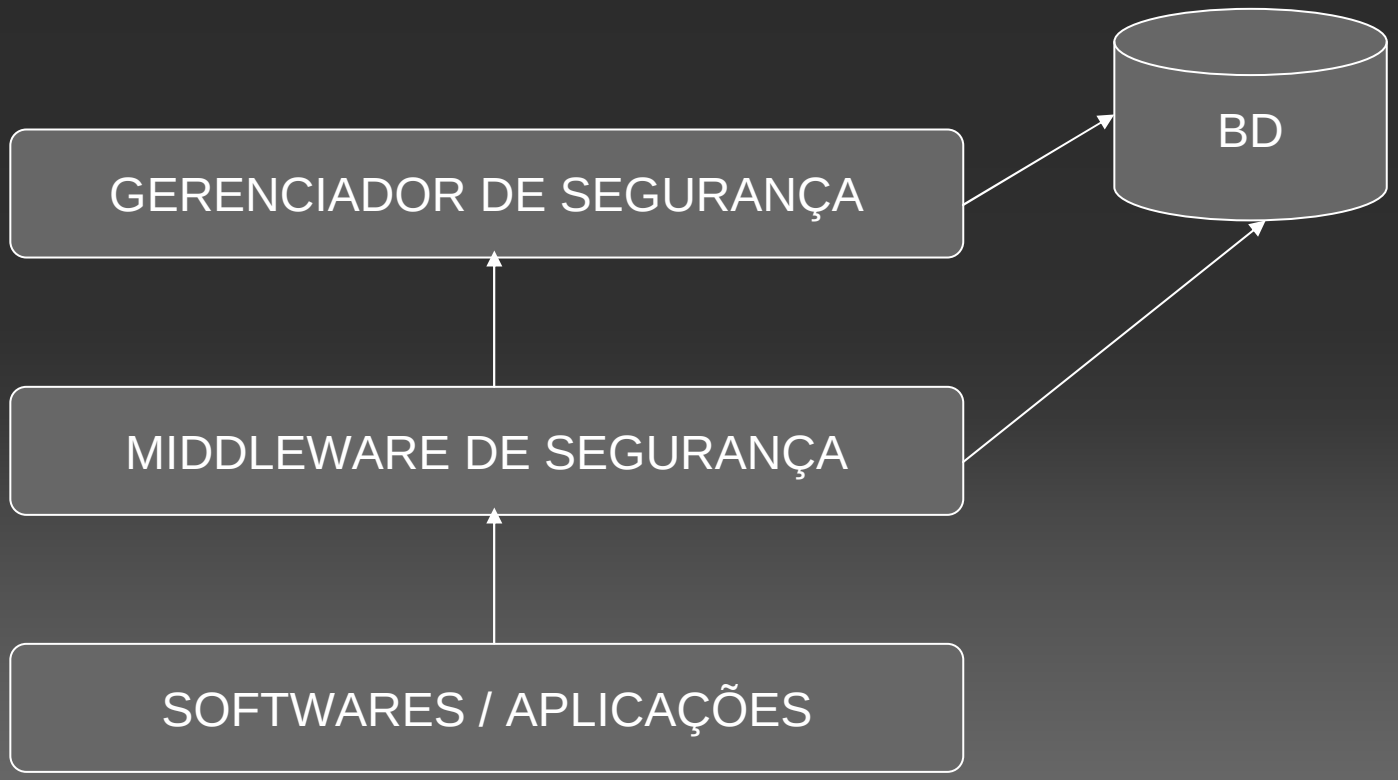
MIDDLEWARE

- **Definição**

  ✓ Uma camada de software que possibilita a comunicação entre aplicações distribuídas, tendo por objetivo diminuir a complexidade e heterogeneidade dos diversos sistemas existentes.

MIDDLEWARE

- **Estrutura**



Trabalhos correlatos

- Implementação de requisitos de segurança para o projeto de reastreabilidade bovina conforme ISO/IEC 15.408 (CARMISINI, 2010);
- Segurança no desenvolvimento de aplicações web (GOMES; SANTOS, 2006);
- PASS – Processo de Apoio a Segurança de Software (NUNES,2007).

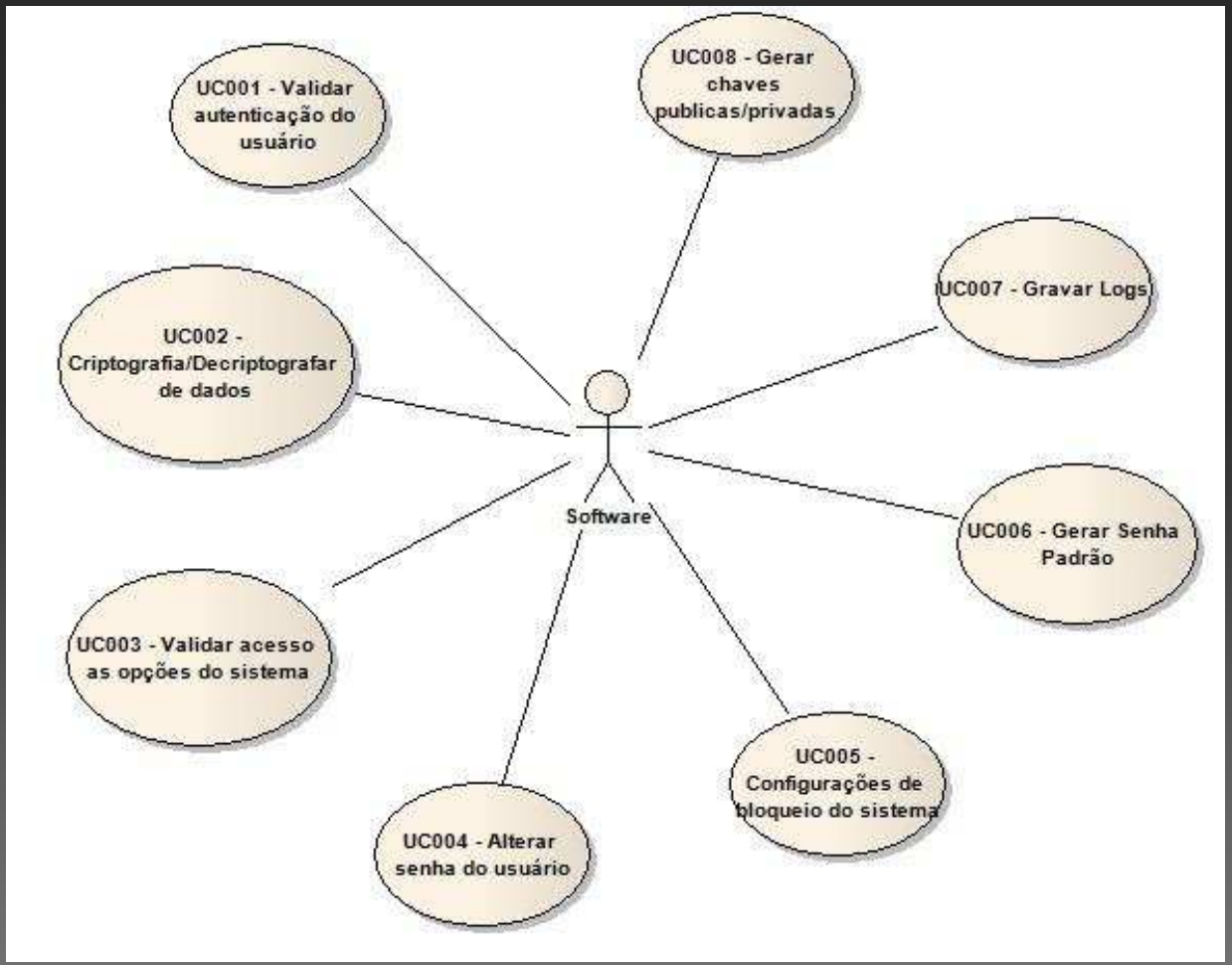
Desenvolvimento do middleware

Requisitos principais

Requisitos	UC
RF01: o *middleware* deve permitir realizar a validação do login	001
RF02: o *middleware* deve permitir criptografar dados de acesso	002
RF03: o *middleware* deve permitir validar acesso às opções do sistema	003
RF05: o *middleware* deve permitir realizar a verificação de tempo inativo	005
RF06: o *middleware* deve permitir gerar senha padrão	006
RF10: o *middleware* deve permitir gravar log de acesso ao sistema	007
RF22: o *middleware* deve permitir consultar os logs gerados	015

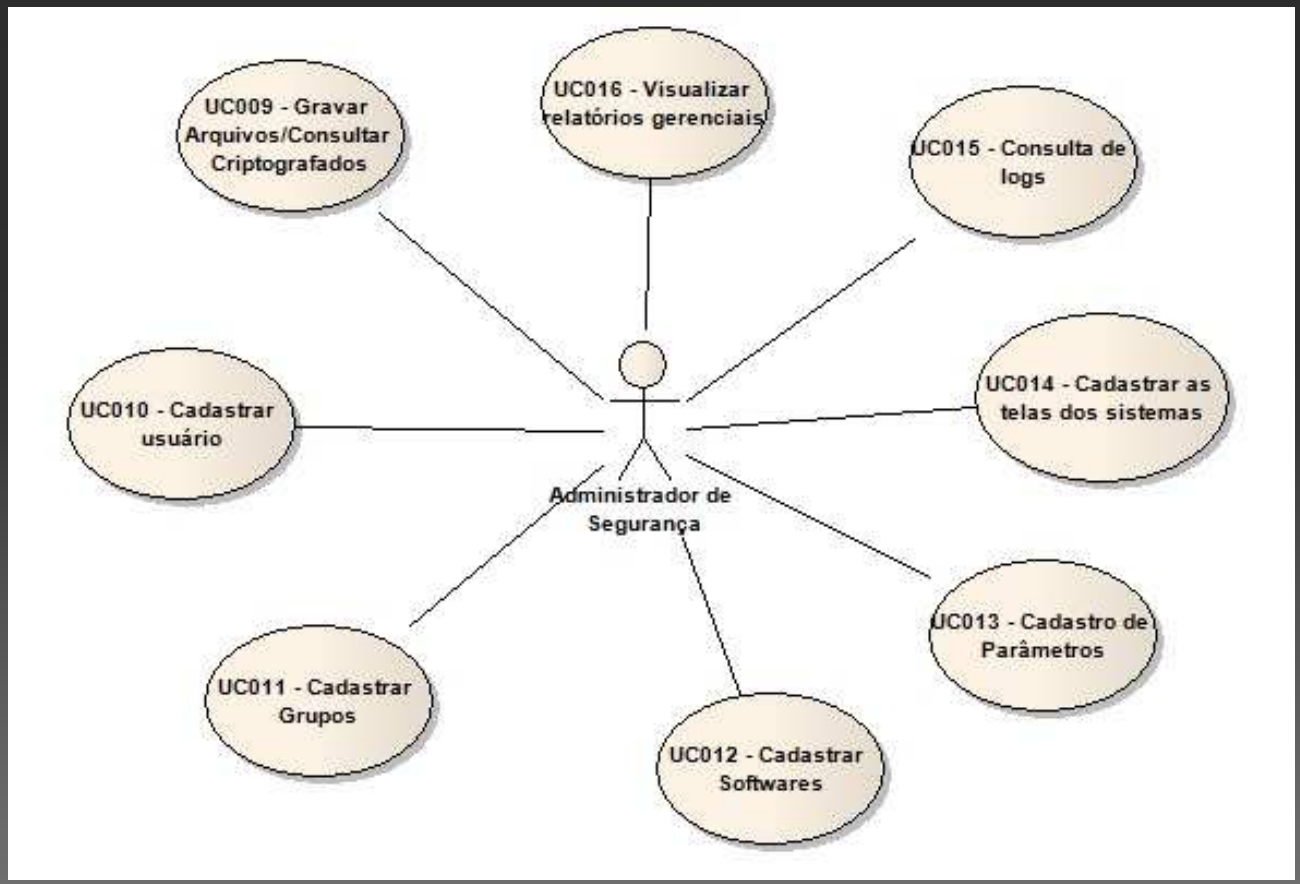
Especificação

- Caso de Uso – Ator Software

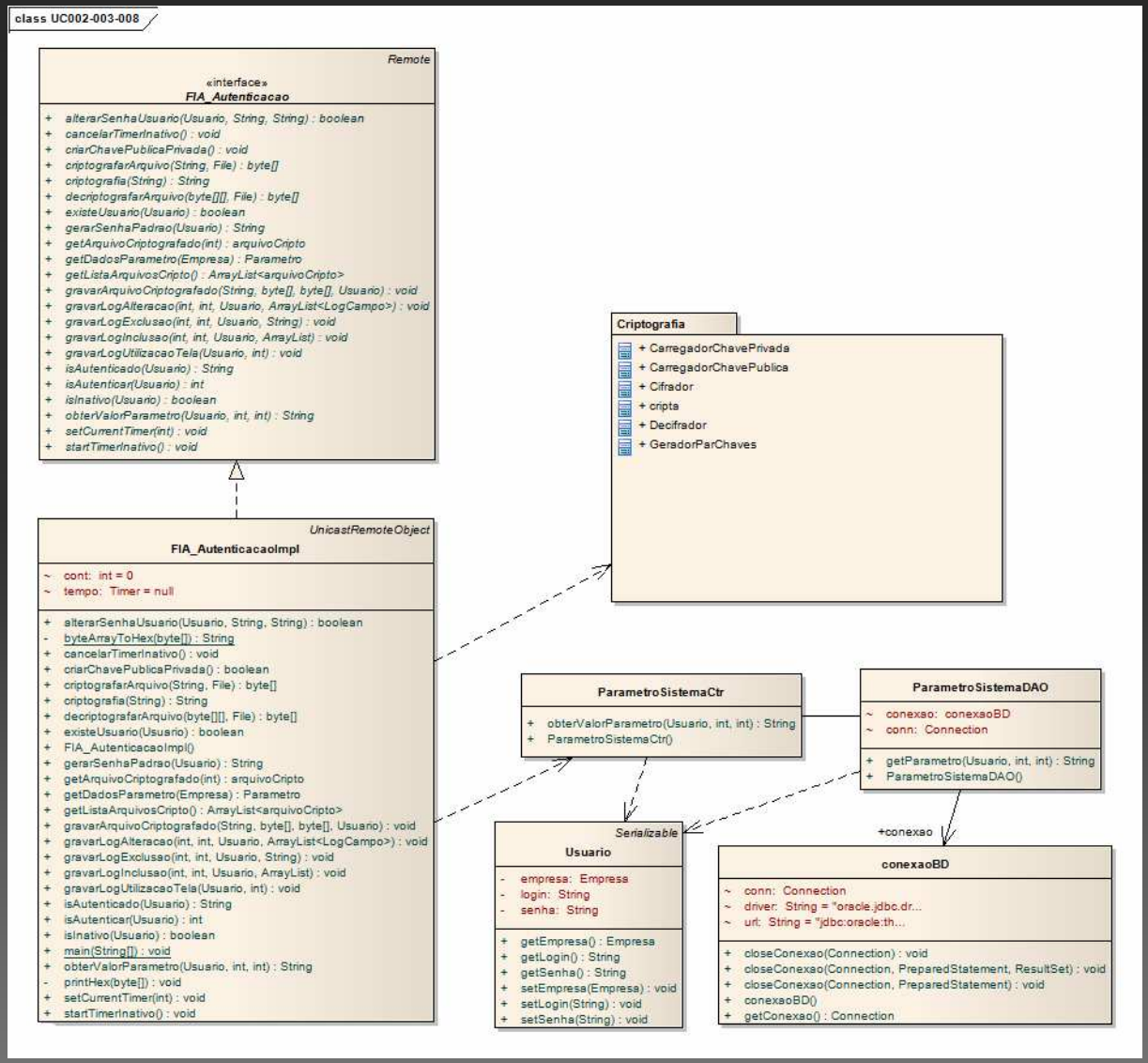


Especificação

- Caso de Uso – Ator Administrador de Segurança

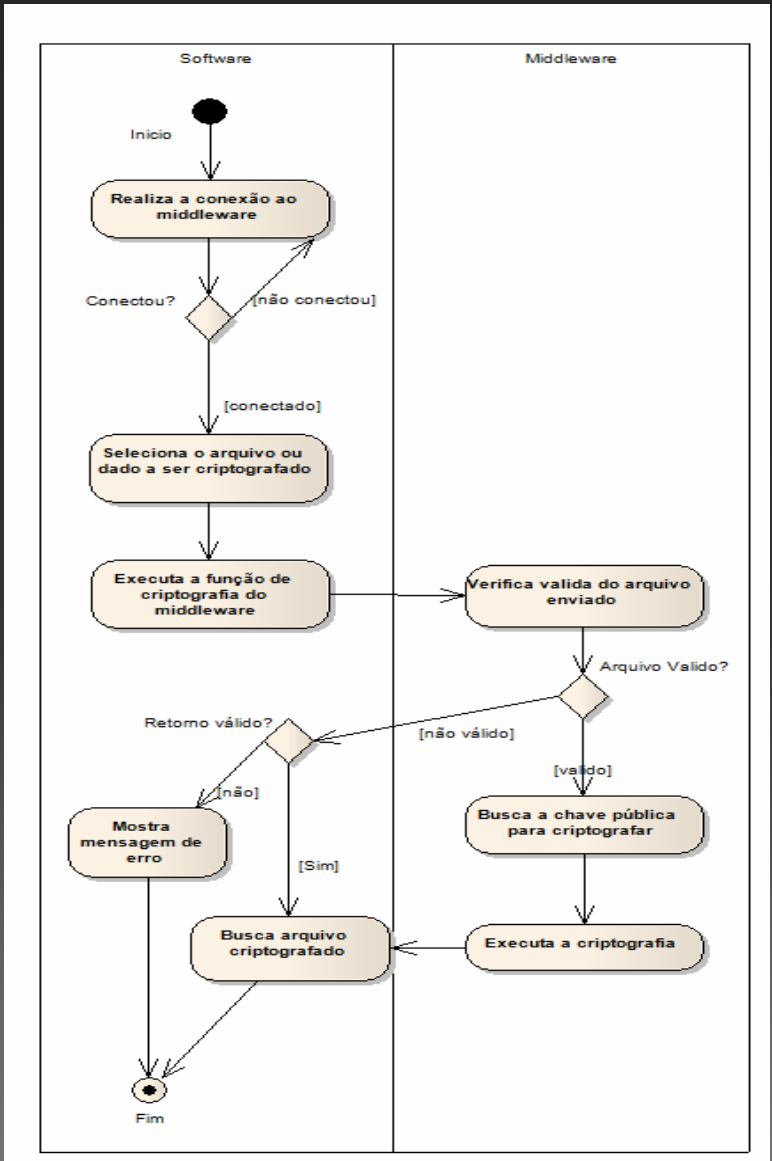


Especificação



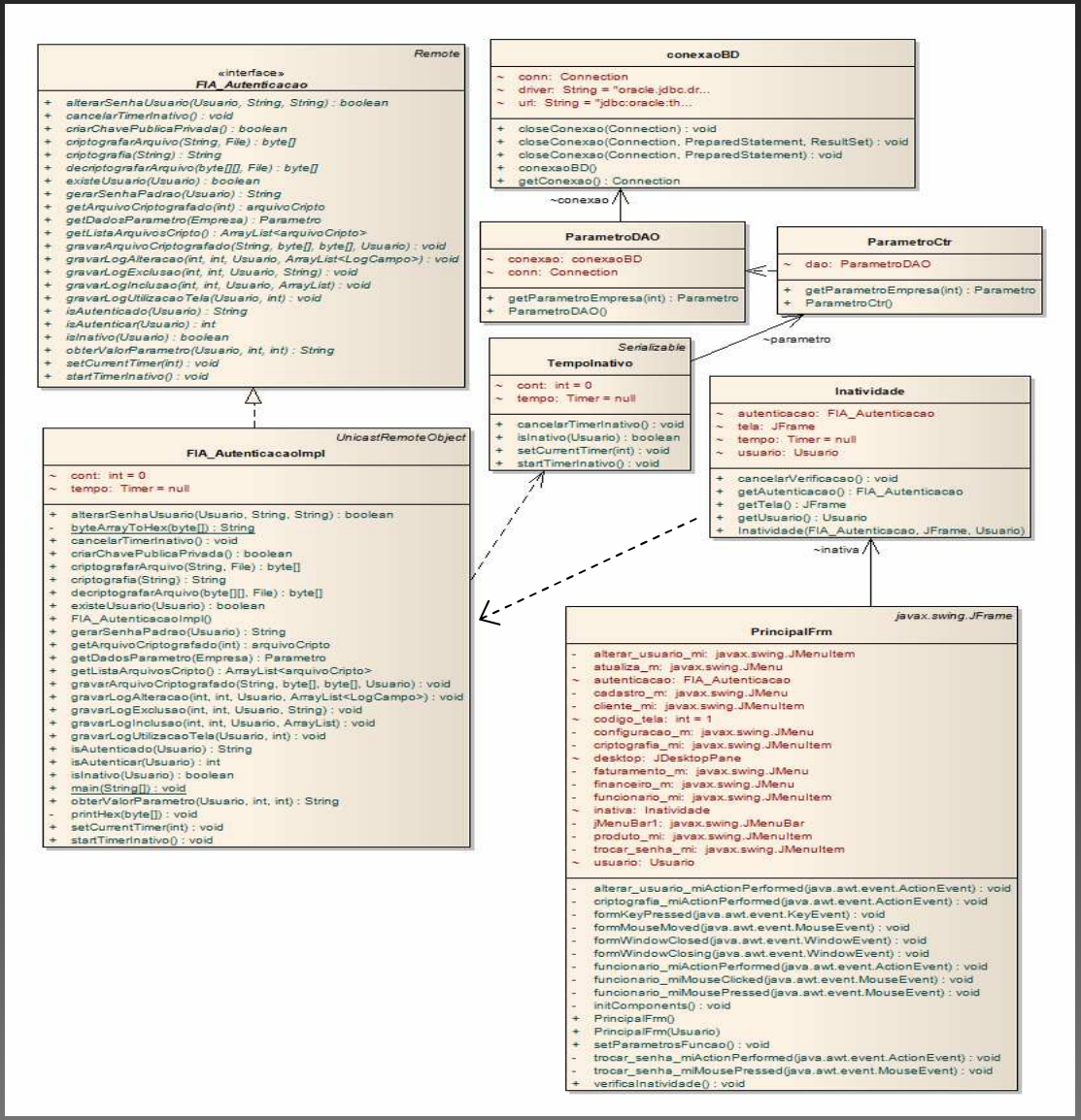
- Diagrama de classe dos casos de uso UC002 e UC003

Especificação



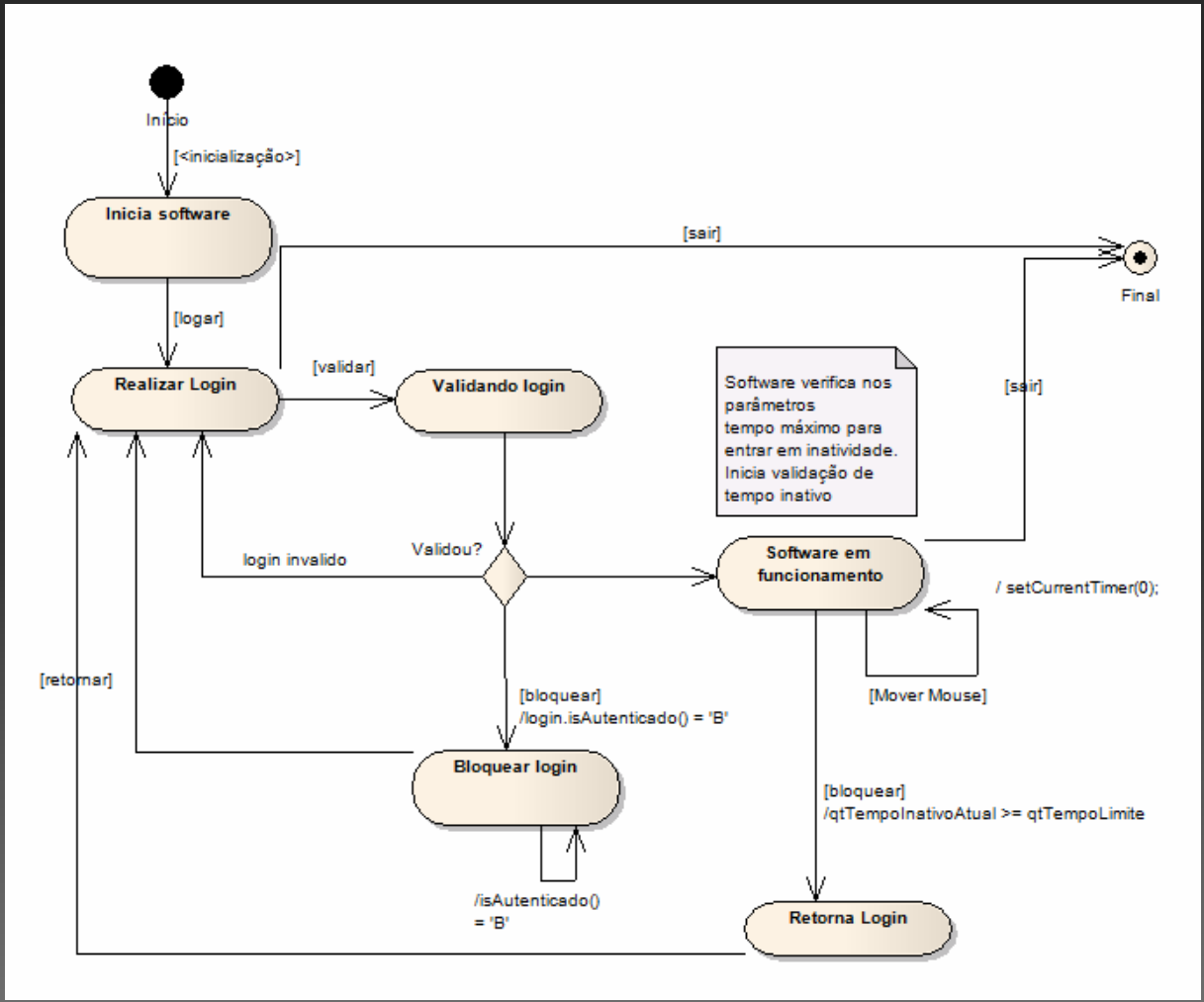
- Diagrama de atividade do caso de uso UC002 – Criptografia / Decriptografia de dados

Especificação



- Diagrama de classe do caso de uso UC005 – Configuração de bloqueio do sistema (inatividade)

Especificação



- Diagrama de estado do caso de uso UC005 – Configuração de bloqueio do sistema (inatividade)

Implementação

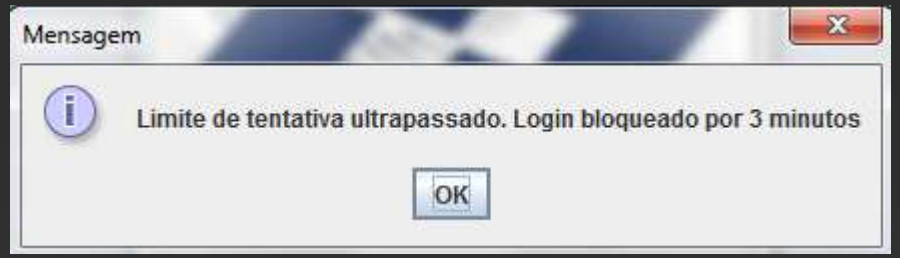
Tecnologias e ferramentas utilizadas

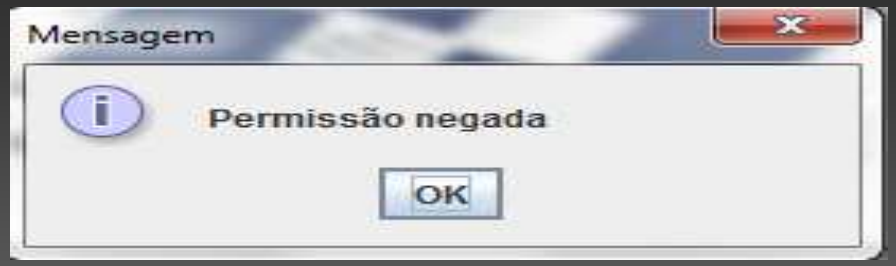
- Linguagem de programação Java.
  - Desenvolvimento do *middleware.*
- Linguagem de programação Delphi 7 (Pascal).
  - Desenvolvimento do gerenciador de segurança.
- Remote Method Invocation (RMI).
  - Comunicação entre o software e o *middleware*
- Algoritmo RSA e AES.
  - Criptografia dos dados.
- Banco de dados Oracle 10g.

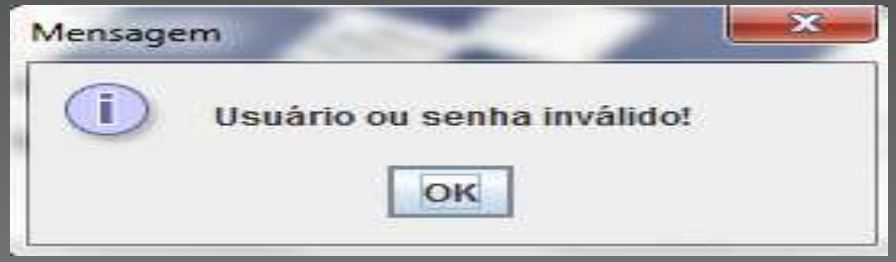
Operacionalidade

Operacionalidade da classe FTA

- Validação dos dados de acesso ao sistema.

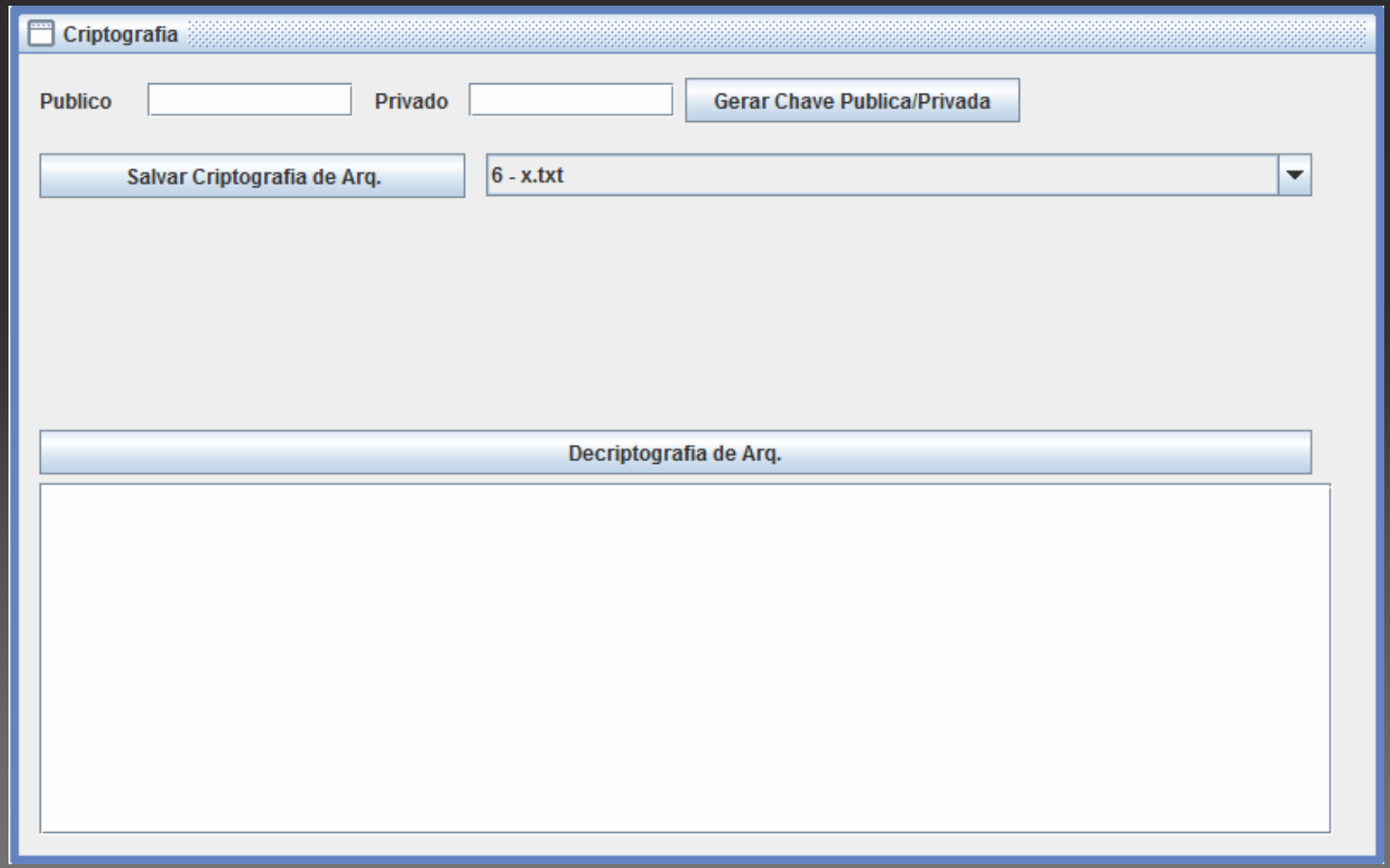




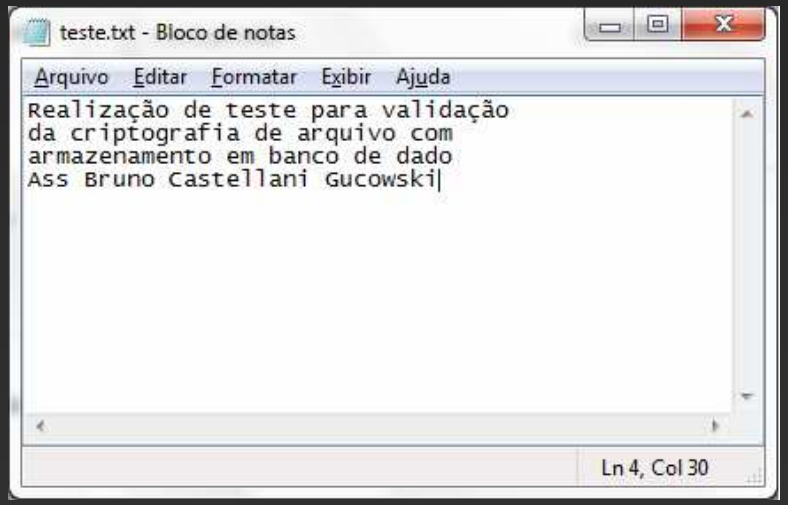


Operacionalidade da classe FCS

- Garantir a segurança dos principais dados.

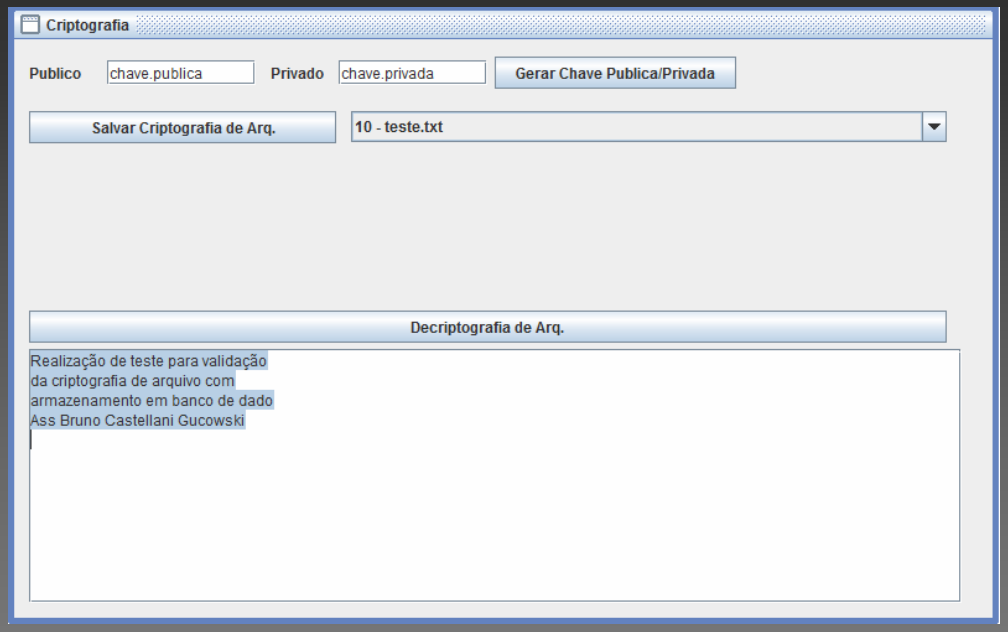


Operacionalidade da classe FCS



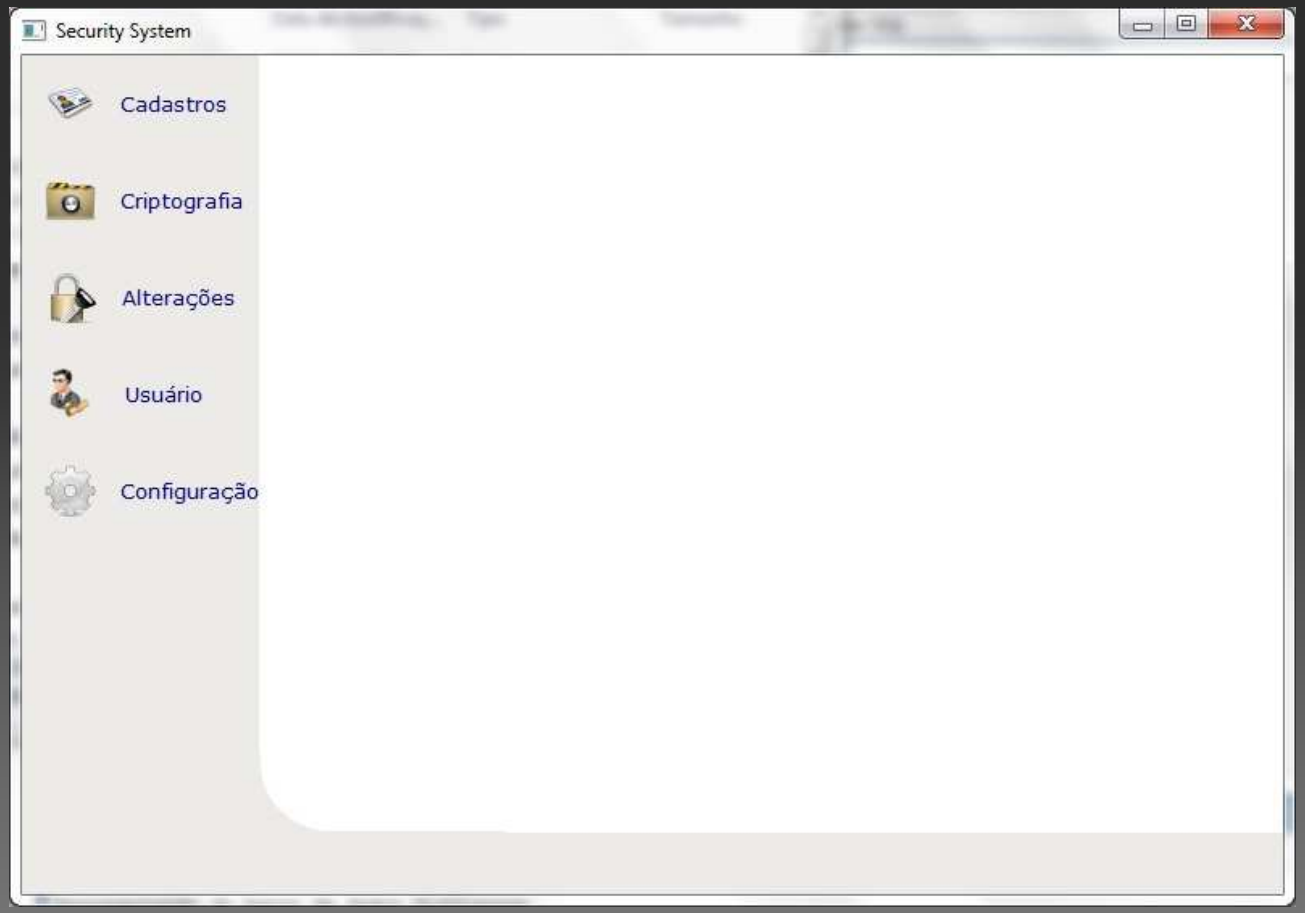
- Arquivo a ser gravado em banco de dado
- Utilização de chave pública e privada

- Salvar
- Visualizar
- Descriptografar



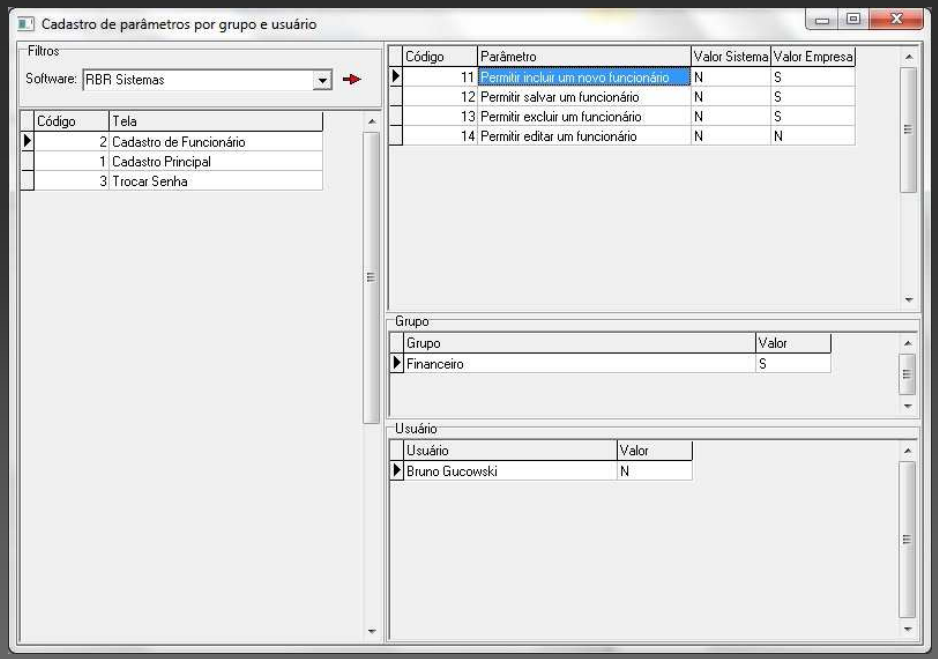
Operacionalidade da classe FMT e FAU

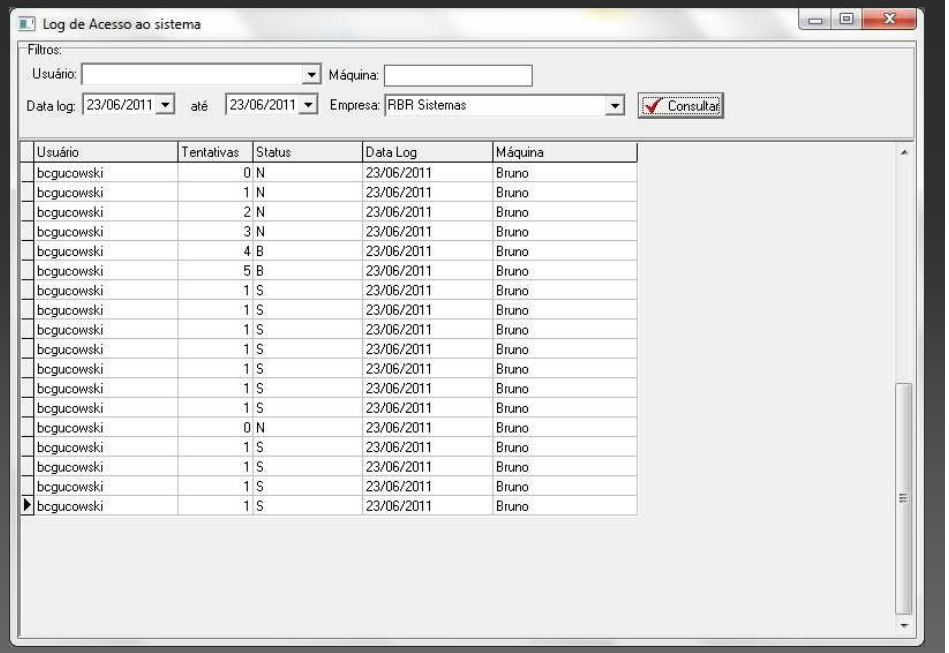
- Gerenciamento e auditoria de segurança.



Operacionalidade da classe FMT e FAU

- Permissão de consulta e configuração do sistema de segurança.





Resultados e discussão

Resultados e discussão

Classe	Sigla	Item atendido
Proteção de dados do usuário	FDP	◉ FDP_ACF.1 – controle de acesso com base de atributos de segurança; ◉ FDP_ACC.1 – controle de acesso de subconjuntos; ◉FDP_DAU.2 – autenticidade dos dados com identidade do gerador; ◉FDP_ROL.1 – Retorno básico.
Auditoria	FAU	◉FAU_GEN.1 – geração de dados para auditoria; ◉FAU_GEN.2 – associação do usuário ao evento da auditoria; ◉FAU_SAA.1 – análise de violação potencial; ◉FAU_SAR.1 – revisão da auditoria; ◉FAU_SEL.1 – auditoria seletiva; ◉FAU_STG.1 – armazenamento protegido da trilha de auditoria; ◉FAU_STG.2 – garantia da disponibilidade dos dados para auditoria.
Criptografia	FCS	◉FCS_COP.1 - operação de criptografia.

Resultados e discussão

Classe	Sigla	Item atendido
Autenticação	FIA	◉FIA_AFL.1 – tratamentos de falhas de autenticação; ◉FIA_ATD.1 – definição de atributos do usuário para autenticação; ◉FIA_SOS.1 – métrica mínima das senhas; ◉FIA_SOS.2 – capacidade de gerar senhas; ◉FIA_UAU.1 – ações anteriores a autenticação; ◉FIA_UAU.2 – autenticação do usuário antes de qualquer coisa; ◉FIA_UAU.6 – re-autenticação; ◉FIA_UAU.7 – resposta restrita da autenticação; ◉FIA_USB.1 – ligação do usuário com o sistema.
Acesso ao sistema	FTA	◉ FTA_LSA.1 – Limitações de escopo no acesso ao sistema; ◉FTA_SSL.1 – Travamento automático de sessão; ◉FTA_SSL.2 – Travamento de sessão por requisição do usuário.
Gerenciamento de segurança	FMT	◉FMT_MOF.1 – Gerenciamento de funções de segurança; ◉FMT_MSA.1 – Gerenciamento de atributos de segurança; ◉FMT_MTD.1 – Gerenciamento de dados de segurança.

Conclusão

- Os objetivos do trabalho foram atingidos;
- Foram implementados os principais itens de segurança;
- Middleware implementado para softwares desenvolvidos em Java;
- Melhor segurança e mais agilidade no desenvolvimento de softwares.

Extensões

- Análise e implementação de outros itens de segurança segundo a norma ISO/IEC 15.408;
- Desenvolvimento do middleware em modo webservice;
- Disponibilizar o middleware para aplicações feitas em outras linguagens.

OBRIGADO!