CESED – CENTRO DE ENSINO SUPERIOR E DESENVOLVIMENTO

PROJETAR SOFTWARE DE CRIPTOGRAFIA/COMPUTAÇÃO GRÁFICA

IMPLEMENTAÇÃO DE UMA BILHETERIA DE CINEMA

PROFESSOR(a): CARLOS DIEGO

ALEXANDRE FERNANDES DE OLIVEIRA BESSA

LUAN DOS SANTOS BARBOSA

LUIS VITOR GOMES ALVES DA SILVA

PEDRO HENRIQUE TEBERGES CAVALCANTI

RYANDRO DA SILVA TAVARES

BILHETERIA DE CINEMA

CAMPINA GRANDE – PB

SETEMBRO - 2025

1. Introdução

1.1 Objetivo

O objetivo deste documento é especificar os requisitos necessários para o desenvolvimento do Sistema de Bilheteria, que permitirá o cadastro e gerenciamento de filmes, o controle de ocupação de salas e a emissão de ingressos digitais com autenticação criptográfica.

Além disso, define os mecanismos de segurança que garantem a confidencialidade, integridade e autenticidade das informações processadas, servindo como base para o desenvolvimento, validação e testes do sistema.

1.2 Escopo do Sistema

O Sistema de Bilheteria tem como propósito gerenciar de forma segura e eficiente o catálogo de filmes e a emissão de ingressos digitais, permitindo a administração centralizada das salas de exibição.

O sistema será utilizado por administradores e operadores, que poderão cadastrar, atualizar e remover filmes, emitir bilhetes eletrônicos autenticados e monitorar a ocupação das salas.

Com foco em segurança, integridade e usabilidade, o sistema faz uso de técnicas criptográficas modernas para proteger as informações persistentes, assegurando a confidencialidade dos dados e a autenticidade dos ingressos emitidos.

As principais funcionalidades incluem:

- Adicionar filme a uma sala
- Atualizar ou remover filmes existentes
- Emitir ingressos (com assinatura digital RSA)
- Verificar tickets emitidos
- Listar todas as salas com status completo
- Filtrar filmes por nome ou data de saída
- Persistir dados criptografados usando AES-GCM com chave derivada por PBKDF2 (SHA-256)

1.3 Definições, Acrônimos e Abreviações

Sigla	Definição
RF	Requisito Funcional
RNF	Requisito Não Funcional
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman
HASH	Função de Dispersão (Hash Function)

2. Requisitos Funcionais

A tabela abaixo descreve as funcionalidades que o sistema deve oferecer.

ID	Descrição	Prioridade (Alta/Média/Baixa)
RF01	O sistema deve permitir adicionar um novo filme em uma das salas disponíveis.	Alta
RF02	O sistema deve permitir remover ou atualizar um filme existente em uma sala.	Alta
RF03	O sistema deve emitir um ingresso para o filme selecionado, gerando comprovante digital.	Alta
RF04	O sistema deve emitir o status de cada sala.	Média
RF05	O sistema deve permitir filtrar filmes por nome parcial e/ou intervalo de datas de lançamento.	Média
RF06	O sistema deve verificar a validade de um ticket emitido, garantindo que não seja reutilizado.	Alta
RF07	O sistema deve salvar o estado atual das salas e dos filmes para manter os dados após o fechamento da aplicação.	Alta

3. Requisitos Não Funcionais

A tabela abaixo apresenta os requisitos não funcionais que o sistema deve atender.

ID	Nome	Descrição	Tipo

RNF01	Derivação de Chave para Criptografia do Estado	O sistema deve derivar uma chave criptográfica segura usando PBKDF2-HMAC-SHA256 com salt aleatório e iterações altas para criptografar o estado	Segurança
RNF02	Verificação de Senha para Descriptografar	O sistema deve validar a senha informada pelo usuário tentando descriptografar o estado criptografado (`state.enc`). A senha será considerada incorreta caso o processo de derivação + descriptografia AES-GCM falhe.	Segurança
RNF03	Criptografia do Estado do Sistema	O estado contendo salas e filmes deve ser criptografado utilizando **AES-256-GCM**, garantindo confidencialidade, integridade e autenticação dos dados persistentes.	Segurança
RNF04	Assinatura Digital de Tickets	Cada ticket emitido deve ser assinado digitalmente usando uma chave privada RSA, permitindo sua verificação posterior através da chave pública.	Integridade
RNF05	Geração de Chaves Públicas/Privadas	Na primeira execução, o sistema deve gerar um par de chaves RSA (privada + pública) utilizado exclusivamente para assinatura e verificação de tickets.	Segurança
RNF06	Estado Persistente Criptografado	O arquivo que contém o estado (`state.enc`) deve permanecer sempre criptografado, protegendo-o contra leitura e adulteração.	Segurança
RNF07	Validação de Data ISO	O sistema deve validar datas no formato `YYYY-MM-DD` antes de armazená-las ou utilizá-las em filtros.	Usabilidade
RNF08	Validação Interativa de Entradas	Para entradas fornecidas via CLI, caso o usuário forneça dados inválidos, o sistema deve permanecer no fluxo até que uma opção válida seja fornecida ou até que o usuário cancele.	Usabilidade
RNF09	Conversão de Datas (BR → ISO)	Datas inseridas no formato brasileiro `DD/MM/AAAA` devem ser convertidas automaticamente para o formato ISO `YYYY-MM-DD` antes de serem salvas.	Integridade

4. Algoritmos Criptográficos

Para assegurar a proteção de dados sensíveis, serão utilizados **três algoritmos criptográficos**, um de cada classe, conforme as orientações do projeto.

Classe Criptográfica	Algoritmo Escolhido	Descrição Técnica / Justificativa de Uso
Criptografia Simétrica	AES-GCM (AES-256-GCM)	Algoritmo usado para criptografar e descriptografar o arquivo `state.enc`. AES-GCM fornece **confidencialidade**, **integridade** e **autenticação** dos dados através de *nonce* + *tag*.
Derivação de Chave (KDF)	PBKDF2-HMAC-SHA256	Responsável por **gerar a chave criptográfica** usada pelo AES-GCM a partir da senha informada pelo usuário. Emprega *salt* aleatório e número elevado de iterações para aumentar a segurança contra ataques de força bruta.
Criptografia Assimétrica	RSA (assinatura digital com chave privada/pública)	A chave privada é usada para **assinar tickets**; a chave pública é usada para **verificá-los**. Garante autenticidade, não-repúdio e integridade dos tickets emitidos.

5. Requisitos de Segurança

O sistema deverá atender aos seguintes requisitos de segurança:

ID	Descrição
RS01	O sistema deve derivar uma chave criptográfica segura a partir da senha informada pelo usuário utilizando **PBKDF2-HMAC-SHA256** com *salt* aleatório e iterações elevadas, garantindo proteção contra ataques de força bruta.
RS02	O arquivo de estado do sistema (`state.enc`) deve ser protegido com criptografia simétrica **AES-256-GCM**, assegurando **confidencialidade**, **integridade** e **autenticação** dos dados armazenados.
RS03	Cada ingresso digital emitido deve conter uma **assinatura digital RSA** utilizando a chave privada, permitindo que sua autenticidade e integridade sejam verificadas com a **chave pública** correspondente.
RS04	As chaves criptográficas RSA devem ser armazenadas em arquivos separados (`private_key.pem` e `public_key.pem`) e mantidas de forma segura, evitando acesso não autorizado e prevenindo exposição ao usuário final.

6. Conclusão

Este documento serve como base para o desenvolvimento do Sistema de Bilheteria, explicando de forma clara as partes técnicas, funcionais e de segurança do sistema.

Com as informações descritas aqui, as equipes de desenvolvimento e teste terão um guia prático para criar, testar e garantir que tudo funcione da maneira certa.

O uso correto dos algoritmos de criptografia e das assinaturas digitais vai garantir que os dados do sistema sejam sempre protegidos, íntegros e autênticos.

No futuro, este documento pode ser complementado com:

- Um Plano de Testes, para confirmar se os requisitos estão sendo cumpridos;
- Um Manual do Usuário, explicando como usar o sistema;
- É um Plano de Implantação, que vai ajudar na instalação e funcionamento em ambiente real.

Assim, o Sistema de Bilheteria vai conseguir funcionar de forma segura, confiável e eficiente, atendendo bem tanto as necessidades do projeto quanto dos usuários.