**Documento de Requisitos do Sistema**

***Cofre Cryptos***

**Versão 1.1**

**Equipe:**

**Rogério Peixoto**

**Luan Andrade**

**André Melo**

# Histórico de Alterações

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Descrição** | **Autor** |
| 28/03/2013 | 1.0 | Versão inicial. | Rogério Peixoto |
| 01/03/2013 | 1.1 | Correções e Acréscimos | Rogério Peixoto/ Luan Andrade |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Conteúdo**

[**Histórico de Alterações**](#h.8ih6s577efes)

[**- Introdução**](#h.eramf3tkwvzl)

[**1. Visão geral do documento**](#h.wpdalg6qchvk)

[**2. Convenções, termos e abreviações**](#h.uu90785lxj8r)

[**3. Identificação dos requisitos**](#h.cx6n9okzj86)

[**4. Prioridades dos requisitos**](#h.cx73iaif7pej)

[**- Descrição geral do sistema**](#h.m35owqmfjly9)

[**1. Abrangência e sistemas relacionados**](#h.ghgchy7el4ro)

[**- Requisitos funcionais (casos de uso)**](#h.ysm68qm9cgl0)

[**1. Controle de Acesso**](#h.vttrml2ody5y)

[**- [RF001] Cadastrar Usuário**](#h.hvjka94f92i)

[**- [RF002] Login**](#h.w86wadrgf2he)

[**- [RF003] Recuperar Senha**](#h.j96hmgubaw1o)

[**- [RF004] Visualizar Arquivos**](#h.6tgsi6ea7u84)

[**- [RF005] Criptografar Arquivo**](#h.gfs1lmv8zwvm)

**-** [**[RF006] Descriptografar Arquivo**](#h.50hi4gnlgn9k)

[**- Requisitos não-funcionais**](#h.dzwvk4mrhztb)

[**- [NF001] Usabilidade**](#h.xd9wcobvs011)

[**- [NF002] Desempenho**](#h.7cwxz28pjoe3)

[**- [NF003] Hardware e Software**](#h.xeg0erp43sww)

[**- [NF004] Segurança**](#h.krg2314ut3zb)

[**- Referências**](#h.wkbc3b5pzaz3)

# Introdução

Este documento especifica os requisitos do sistema *Cofre Cryptos*, fornecendo aos desenvolvedores as informações necessárias para o projeto e implementação, assim como para a realização dos testes e homologação do sistema.

## 1. Visão geral do documento

Além desta seção introdutória, as seções seguintes estão organizadas como descrito abaixo.

1. **Seção 2 – Descrição geral do sistema**: apresenta uma visão geral do sistema, caracterizando qual é o seu escopo e descrevendo seus usuários.
2. **Seção 3 – Requisitos funcionais (casos de uso)**: especifica todos os casos de uso do sistema, descrevendo os fluxos de eventos, prioridades, atores, entradas e saídas de cada caso de uso a ser implementado.
3. **Seção 4 – Requisitos não-funcionais**: especifica todos os requisitos não funcionais do sistema, divididos em requisitos de usabilidade, confiabilidade, desempenho, segurança, distribuição, adequação a padrões e requisitos de hardware e software.
4. **Seção 5 – Referências:** apresenta referências para outros documentos utilizados para a confecção deste documento.

## 2. Convenções, termos e abreviações

A correta interpretação deste documento exige o conhecimento de algumas convenções e termos específicos, que são descritos a seguir.

## 3. Identificação dos requisitos

Por convenção, a referência a requisitos é feita através do nome da subseção onde eles estão descritos, seguidos do identificador do requisito, de acordo com a especificação a seguir:

[*nome da subseção. identificador do requisito*]

Por exemplo, o requisito funcional [Cadastro de Usuário.RF001] deve estar descrito em uma subseção chamada “Cadastro de Usuário”, em um bloco identificado pelo número [RF001]. Já o requisito não-funcional [Segurança. NF004] deve estar descrito na seção de requisitos não-funcionais de “Segurança”, em um bloco identificado por [NF004].

Os requisitos devem ser identificados com um identificador único. A numeração inicia com o identificador [RF001] ou [NF001] e prossegue sendo incrementada à medida que forem surgindo novos requisitos.

## 4. Prioridades dos requisitos

Para estabelecer a prioridade dos requisitos, nas seções 4 e 5, foram adotadas as denominações “essencial”, “importante” e “desejável”.

1. **Essencial** é o requisito sem o qual o sistema não entra em funcionamento. Requisitos essenciais são requisitos imprescindíveis, que têm que ser implementados impreterivelmente.
2. **Importante** é o requisito sem o qual o sistema entra em funcionamento, mas de forma não satisfatória. Requisitos importantes devem ser implementados, mas, se não forem, o sistema poderá ser implantado e usado mesmo assim.
3. **Desejável** é o requisito que não compromete as funcionalidades básicas do sistema, isto é, o sistema pode funcionar de forma satisfatória sem ele. Requisitos desejáveis podem ser deixados para versões posteriores do sistema, caso não haja tempo hábil para implementá-los na versão que está sendo especificada.

# **Descrição geral do sistema**

## 1. Abrangência e sistemas relacionados

O sistema *Cofre Cryptos* é uma ferramenta para plataforma Android que criptografa arquivos. Fornece uma listagem dos arquivos da memória e do Sdcard do Android e criptografa os arquivos que forem selecionados e esconde em outra pasta.

Utilizando o aplicativo, o usuário vai pode após um simples cadastro logar-se atraves de uma senha e ter acesso ao painel que exibe a árvore de diretórios do dispositivo em questão, nesta o usuário poderá selecionar arquivos para adicionar em seu cofre criptografado. Além disso, remover e consultar arquivos criptografados. Por meio de um algoritmo a aplicação utiliza como base a senha digitada pelo usuário para proteger os arquivos.

A proteção oferecida pela aplicação é de nível leve, por tanto direcionada para o usuário doméstico que deseja proteger seus arquivos pessoais de acessos não autorizados ao seu dispositivo. Diante da interface intuitiva e facilidade de adicionar uma proteção extra aos seus arquivos, o *Cofre Crypto* contribui de modo decisivo na segurança de seus arquivos pessoais em seu dispositivo.

# **Requisitos funcionais (casos de uso)**

## 1. Controle de Acesso

### [RF001] Cadastrar Usuário

**Descrição do caso de uso:** Este caso de uso permite que o usuário se cadastre no sistema.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: O usuário entra com o seu email e a senha para cadastro.

**Saídas e pós-condição**: um usuário é cadastrado no sistema.

### [RF002] Login

**Descrição do caso de uso:** Este caso de uso permite que o usuário entre com sua senha para abertura da sessão do aplicativo que dá acesso a arquivos previamente armazenados no cofre.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: O usuário precisa estar previamente cadastrado, recebe como entrada a senha do usuário.

**Saídas e pós-condição**: o usuário consegue entrar no sistema e visualizar os arquivos armazenados previamente.

### **[RF003] Recuperar Senha**

**Descrição do caso de uso:** Este caso de uso permite que o usuário envie através da aplicação um email para recuperação da senha cadastrada.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: O usuário precisa estar previamente cadastrado.

**Saídas e pós-condição**: um componente é alterado no sistema.

**2. Gerenciamento de Arquivos.**

### [RF004] Visualizar Arquivos

**Descrição do caso de uso:** Este caso de uso permite que o usuário visualize os arquivos que se encontram atualmente no sistema de arquivos do aparelho (tanto SDCard quando memória interna) e também os arquivos que já estão criptografados.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: o usuário necessita estar logado no sistema.

**Saídas e pós-condição**: o usuário visualiza a árvore de diretórios.

### **[RF005] Criptografar Arquivo**

**Descrição do caso de uso:** Este caso de uso permite que o usuário selecione o arquivo a ser criptografado e mova o mesmo para o cofre criptografado.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: O usuário precisa estar cadastrado no sistema. Recebe como entrada o arquivo que o usuário deseja criptografar.

**Saídas e pós-condição**: o usuário consegue mover o arquivo para o diretório do cofre de maneira criptografada.

### [RF006] Descriptografar Arquivo

**Descrição do caso de uso:** Este caso de uso permite que o usuário selecione um arquivo previamente criptografado no cofre, descriptografe este e devolva este ao diretório atual exibido na árvore de diretórios.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

**Entradas e pré-condições**: O usuário precisa estar cadastrado no sistema [RF001]. O usuário precisa ter criptografado algum arquivo previamente [RF006].

**Saídas e pós-condição**: o usuário consegue descriptografar o arquivo e mover para o local desejado.

# **Requisitos não-funcionais**

### [NF001]Usabilidade

A interface com o usuário é de vital importância para o sucesso do sistema. Como a aplicação não tem como público alvo o usuário corporativo e sim o usuário doméstico esporádico, o usuário não possui tempo disponível para aprender como utilizar o sistema.

O sistema terá uma interface amigável e intuitiva ao usuário primário sem se tornar cansativa aos usuários mais experientes.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

### **[NF002] Desempenho**

Embora não seja um requisito essencial ao sistema, deve ser considerada importante por corresponder a um fator de qualidade de software e pelo processo de criptografia de arquivos ser custoso em termos de uso de CPU do dispositivo móvel.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

### **[NF003] Hardware e Software**

Visando criar um produto com maior abrangência e facilidade de desenvolvimento o produto deverá ser inicialmente desenvolvido na plataforma Android. A aplicação só deverá funcionar em aparelhos que utilizem versão 2.3.3 ou posteior do Android (nível de API 10). O dispositivo deve possuir memória interna ou um SDCard com sistema de arquivos compatível a API do Android.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

### 

### **[NF004] Segurança**

A aplicação é feita para usuários não corporativos que desejam proteger arquivos pessoais de serem roubados em caso de acesso não autorizado do aparelho. Para garantir uma segurança de nível leve dos arquivos, utilizaremos um algorítmo de criptografia baseado na senha digitada pelo usuário (PBE ou Password Based Cryptography), o algorítmo utilizado será o DES juntamente com o MD5 para checksum. Tais algorítmos já são suportados pela API nativa do Android.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prioridade**: |  | Essencial |  | Importante |  | Desejável |

# **Referências**

1. Furlan, J. D. **Modelagem de Objetos através da UML**. São Paulo, Makron Books, 1998.
2. Kruchten, P. **The Rational Unified Process – An introduction**. Addison-Wesley, 1998.
3. Wikipedia.org EN - Artigo - Data Encryption Standard   
   <http://en.wikipedia.org/wiki/Data_Encryption_Standard>
4. Wikipedia.org EN - Artigo - Password-based Cryptography  
   <http://en.wikipedia.org/wiki/Password-based_cryptography>
5. Wikipedia.org EN - Artigo - Message-Digest Algorithm 5  
   <http://en.wikipedia.org/wiki/MD5>
6. Código de aplicação protótipo desenvolvido em outra disciplina. - Source -   
   https://github.com/rcbpeixoto/android\_projs.git/CryptosVault/