Sistema de Gerenciamento de Acesso Seguro

Versão 1.3

Documento de Especificação de Requisitos

Equipe Responsável pela Elaboração
Arthur da Conceição Ferreira
Bruno Felipe Silva
Leonardo Serpa Nicoletti

Público Alvo
Este documento destina-se à equipe de desenvolvimento do projeto Sistema de Gerenciamento de Acesso Seguro, como analistas, desenvolvedores e testes, assim como para o cliente ou usuários para obtenção, apresentação e aprovação.

Documento de Especificação de Requisitos
Versão 1.3

Histórico da Revisão

Data	Versão	Descrição	Autor
02/10/2018	1.1	Início da documentação de requisitos	Leonardo Serpa Nicoletti
03/10/2018	1.2	Escrita da seção 2.1 até a 2.4, ajuste e escrita dos requisitos funcionais, requisitos não funcionais e regras de negócio	Bruno Felipe Silva
03/10/2018	1.3	Alteração e levantamento de novos requisitos faltantes; rastreabilidade de requisitos	Arthur da Conceição Ferreira

Sumário

1. Introdução

1.1 Objetivo do Documento

Este documento especifica o **Sistema de Gerenciamento de Acesso Seguro**, o qual tem como objetivo permitir que usuários se autentiquem de forma segura, realizem o cadastro de suas contas e redefinam senhas por meio de um código enviado ao e-mail. O sistema visa garantir a segurança dos dados dos usuários e assegurar que apenas pessoas autorizadas tenham acesso à aplicação.

1.2 Convenções, termos e abreviações

1.2.1 Identificação dos Requisitos

- Requisitos Funcionais são identificados como **RF** seguido por um número (por exemplo, RF01).
- Requisitos Não Funcionais são identificados como **RNF** seguido por um número (por exemplo, RNF01).
- Regras de Negócio são identificadas como **RN** seguido por um número (por exemplo, RN01).

1.2.2 Prioridades dos Requisitos

- **Essencial**: Requisito sem o qual o sistema não pode funcionar.
- **Importante**: Requisito que deve ser implementado, mas não impede o funcionamento inicial do sistema.
- **Desejável**: Requisito que pode ser implementado em versões futuras sem comprometer as funcionalidades principais.

1.3 Abreviações

Sigla	Definição
SGBD	Sistema Gerenciador de Banco de Dados
BD	Banco de Dados
PHP	Hypertext Preprocessor
MFA	Autenticação Multifator
RNF	Requisitos Não Funcionais
RN	Regras de Negócio
RF	Requisitos Funcionais

1.4 Referências

- DOC01 - Documento de Requisitos; Data; Instituição, divisão ou equipe responsável pelo documento.

2. Descrição Geral do Sistema

Visão Geral:
Este sistema foi desenvolvido para garantir o acesso seguro de usuários através de login e senha, possibilitando a criação de contas, recuperação de senhas e confirmação de identidade por e-mail. O sistema visa fornecer uma plataforma confiável e segura, evitando acessos não autorizados.

Descrição dos Stakeholders:

- **Usuário Final**: Responsável por utilizar o sistema, realizando ações como criar conta, fazer login e recuperar senha.
- **Administrador do Sistema**: Responsável pela manutenção do sistema e gerenciamento dos usuários, incluindo a exclusão de contas e redefinição de senhas, além de monitorar atividades suspeitas.

Descrição dos Usuários:

Nome	Perfil	Responsabilidades	Envolvido
Administrador	Usuário com acesso total ao sistema, responsável pela gestão de contas de usuários	Possui a funcionalidade de realizar manutenção no cadastro de usuários, podendo incluir, alterar a senha ou excluir um usuário.	O responsável por este perfil é o administrador do sistema.
Usuário Final	Usuário que acessa o sistema para realizar suas atividades	Usuário responsável por criar uma conta, fazer login, alterar dados da conta e solicitar recuperação de senha.	Qualquer pessoa que necessite utilizar o sistema de forma segura.

2.4 Necessidades

Necessidade	Prioridade	Preocupações	Solução Atual	Soluções Propostas
NEC01: Garantir a segurança no acesso ao sistema	Alta	Prevenir acessos não autorizados e proteger dados sensíveis	O sistema permite login e senha básicos	Implementar autenticação multifator (MFA) e criptografia de senhas.
NEC02: Facilitar a recuperação de contas	Média	Ajudar usuários a recuperar acesso rapidamente e com segurança	Envio de e-mail para redefinição de senha	Enviar um código temporário via e-mail que expira em 15 minutos.
NEC03: Evitar acessos não autorizados	Alta	Garantir que apenas usuários legítimos utilizem o sistema	Nenhum mecanismo adicional	Implementar verificação por e-mail e bloqueio temporário após várias tentativas falhas.

2.5 Benefícios

- Garante uma forma segura de acesso, utilizando confirmação por e-mail para assegurar a identidade do usuário.
- Evita que usuários não autorizados acessem informações sensíveis, garantindo que cada conta seja única e protegida.
- Proporciona uma experiência de recuperação de senha mais eficiente e segura, garantindo rapidez e confiança aos usuários.

2.6 Escopo do Produto

- **Módulo de Cadastro**: Permite criar contas de usuário e realizar validação via e-mail.
- **Módulo de Login**: Permite que usuários acessem o sistema com segurança.
- **Módulo de Recuperação de Senha**: Facilita a recuperação de senha através do envio de código de verificação.
- **Módulo de Segurança**: Implementa autenticação multifator (MFA) e bloqueio temporário para tentativas de login mal sucedidas.

2.7 Limitações e Restrições

- O sistema não enviará SMS para confirmação devido a custos adicionais e ao foco na confirmação via e-mail.

- O sistema não enviará e-mail para pessoas interessadas sem cadastro, pois é necessário garantir que apenas usuários autorizados interajam com a plataforma.
- O sistema não importará planilhas com dados de usuários inicialmente, focando apenas em cadastros autônomos por questões de segurança.
- O sistema não gerará relatórios de usuários. Essa funcionalidade poderá ser incluída em futuras versões.
- O sistema deve rodar em um Sistema Operacional 64 bits com 10 GB de RAM e processador com 2.4 GHz.
- O sistema será desenvolvido com a linguagem de programação PHP, utilizando frameworks como Bootstrap e Jquery.

3. Requisitos

3.1 Requisitos Funcionais

- **RF01**: O sistema deve permitir aos usuários acessarem a área interna através de código de usuário e senha (login).
  - Prioridade: Essencial
- **RF02**: O sistema deve permitir que o usuário se cadastre de maneira autônoma.
  - Prioridade: Essencial
- **RF03**: O sistema deve cadastrar o status do usuário como "ativo", "bloqueado" ou "bloqueado definitivamente".
  - Prioridade: Essencial
- **RF04**: O sistema deve enviar um token de acesso para confirmação de cadastro do usuário.
  - Prioridade: Essencial
- **RF05**: O sistema deve enviar um token de acesso para quando o usuário esquecer a senha e quiser cadastrar uma nova.
  - Prioridade: Essencial
- **RF06**: O sistema deve bloquear o usuário quando ele errar a senha atual mais de 2 vezes.
  - Prioridade: Essencial
- **RF07**: O sistema deve bloquear o usuário definitivamente quando ele errar o token de desbloqueio de senha mais de 1 vez.
  - Prioridade: Essencial

3.2 Requisitos Não Funcionais

- **RNF01**: O sistema deverá criptografar a senha ao ser gravada no banco de dados.
  - Prioridade: Essencial

- **RNF02**: O sistema deve possuir planos de assinatura vinculados a cada usuário, sendo o plano "básico" o padrão no momento do cadastro.
    - Prioridade: Importante
- **RNF03**: O servidor de banco de dados deve ter disco rígido de no mínimo 500 GB livres.
    - Prioridade: Importante
- **RNF04**: O sistema será desenvolvido com a linguagem de programação PHP puro, usando apenas frameworks front-end como Bootstrap e Jquery.
    - Prioridade: Importante

3.3 Regras de Negócios

- **RN01**: Um usuário deve estar registrado e ter confirmado sua identidade através do código enviado por e-mail antes de acessar o sistema.
- **RN02**: O sistema deve bloquear temporariamente o acesso do usuário após 3 tentativas de login falhas. O bloqueio terá duração de 15 minutos.
- **RN03**: Caso o usuário erre o token de desbloqueio de senha mais de uma vez, sua conta deve ser marcada como "bloqueada definitivamente" e ser necessária a intervenção do administrador para desbloqueá-la.
- **RN04**: Senhas devem ter no mínimo 8 caracteres e incluir pelo menos um número e um caractere especial para serem consideradas válidas.
- **RN05**: O administrador tem permissão para criar, editar ou remover contas de usuários, bem como desbloquear contas bloqueadas definitivamente.
- **RN06**: A redefinição de senha deve ser realizada através de um link válido por apenas 15 minutos, enviado ao e-mail do usuário.

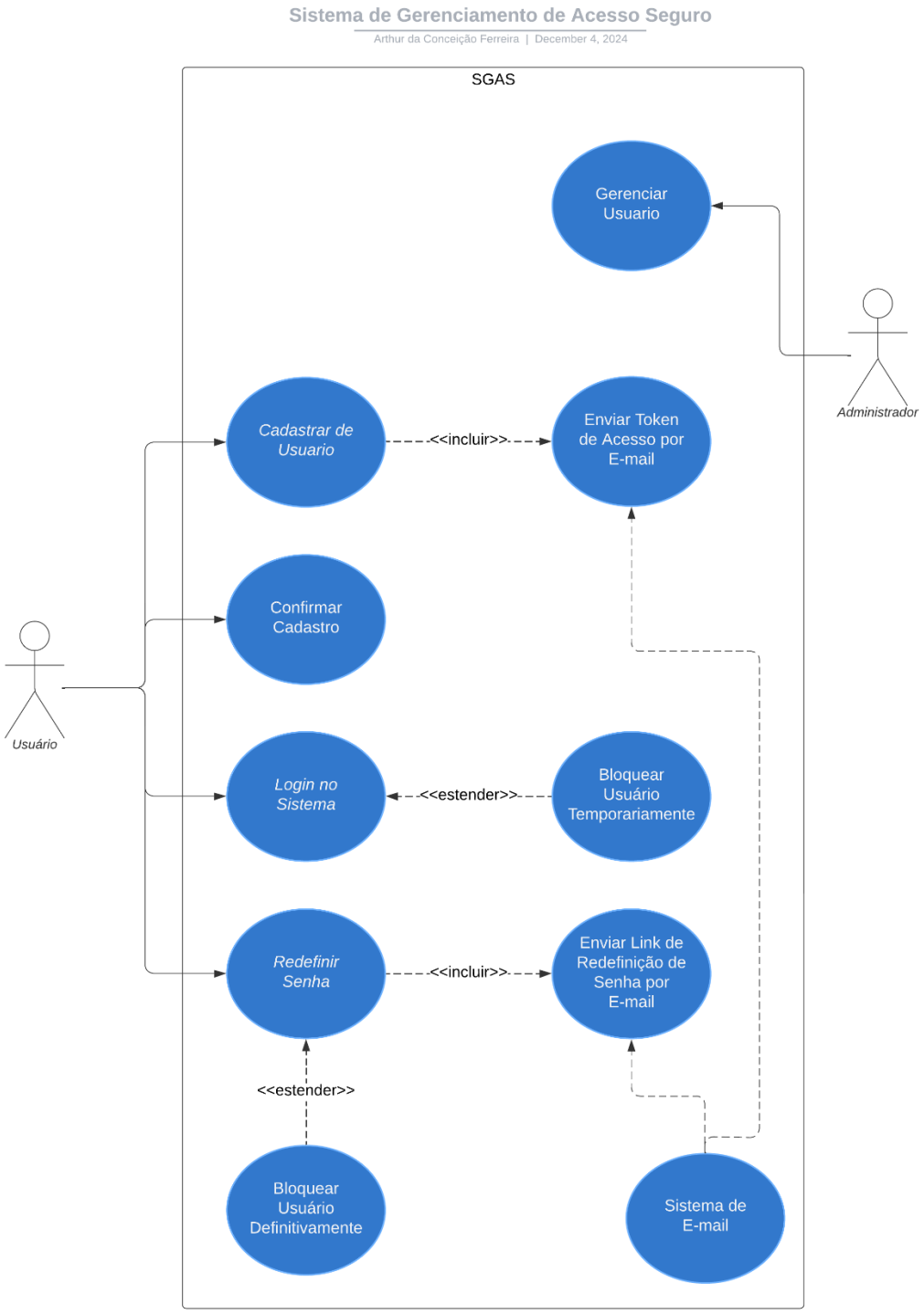
4. Glossário

Termos e Definições:

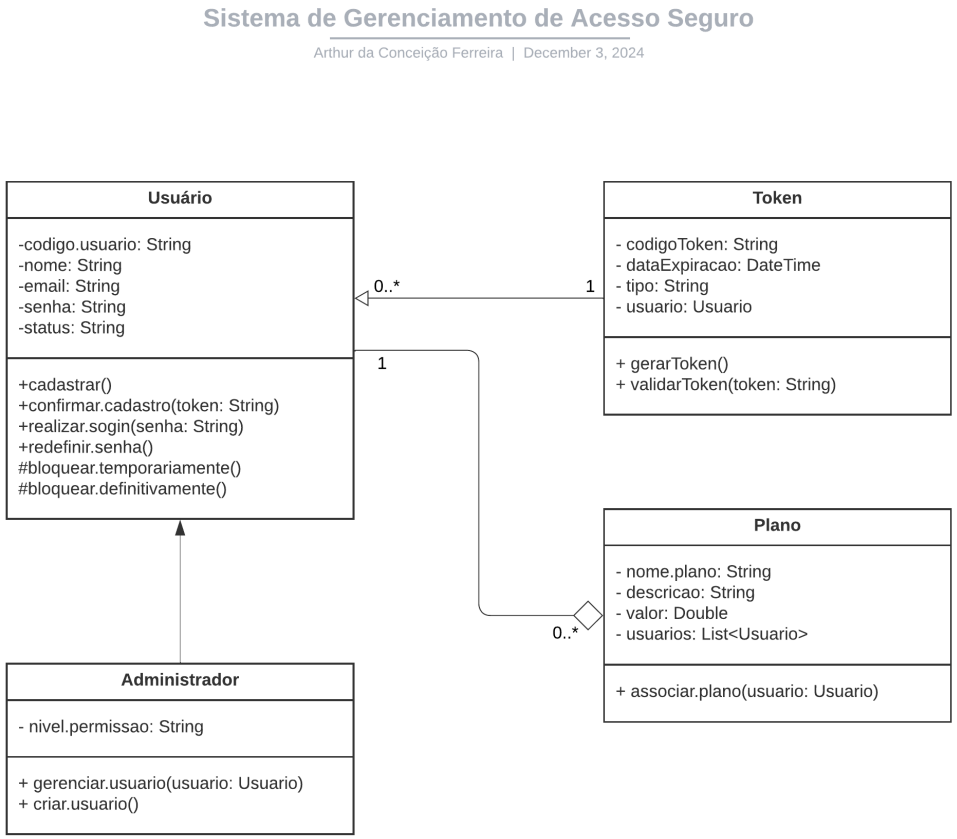
- **Usuário Final**: Pessoa que acessa o sistema para utilizar os serviços disponíveis.
- **Administrador**: Pessoa responsável por gerenciar o sistema e os usuários.
- **Código de Verificação**: Código enviado ao e-mail do usuário para validar sua identidade.
- **Token de Acesso**: Código temporário enviado ao usuário para verificar sua identidade durante o cadastro ou recuperação de senha.
- **Autenticação Multifator (MFA)**: Um método de autenticação que exige múltiplas formas de verificação para aumentar a segurança.
- **Usuário Bloqueado**: Status de um usuário que teve seu acesso temporariamente suspenso devido a tentativas incorretas de senha.

5. Modelagem do Sistema

5.1 Diagrama de Casos de Uso



5.2 Diagrama de Classe



Visibilidade

+ (Público): Pode ser acessado por qualquer classe.
- (Privado): Pode ser acessado apenas pela própria classe.
 # (Protegido): Pode ser acessado pela própria classe e por classes herdeiras.