Documento de Requisitos do Sistema de Login e Cadastro

# 1. Introdução

Este documento apresenta os requisitos funcionais e não funcionais de um sistema web simples de autenticação, cadastro e controle de acesso baseado em papéis (roles). O sistema foi concebido com foco em segurança da informação e princípios da LGPD, garantindo confidencialidade, integridade e acesso restrito a dados pessoais.

# 2. Escopo do Sistema

O sistema possui as seguintes funcionalidades principais:

- Página de cadastro para administradores

- Página de cadastro para usuários comuns

- Página de login com autenticação via JSON Web Token (JWT)

- Acesso a telas específicas com base em papéis (admin ou usuário)

- Proteção dos dados pessoais com hash de senha

- Logs de ações do sistema visíveis apenas ao administrador

- Tela de perfil do usuário visível somente ao próprio usuário autenticado

# 3. Requisitos Funcionais (RF)

|  |  |  |
| --- | --- | --- |
| Código | Requisito Funcional | Descrição |
| RF01 | Cadastro de Administrador | O sistema deve permitir o cadastro de usuários com papel de "administrador". |
| RF02 | Cadastro de Usuário Comum | O sistema deve permitir o cadastro de usuários com papel de "usuário". |
| RF03 | Autenticação | O sistema deve autenticar usuários com login (e-mail) e senha. |
| RF04 | Geração de JWT | Após login, o sistema deve gerar um token JWT com as informações do usuário. |
| RF05 | Validação de Token | O sistema deve validar o token JWT antes de conceder acesso às páginas protegidas. |
| RF06 | Hash de Senha | O sistema deve armazenar senhas utilizando algoritmo de hash seguro (ex: bcrypt). |
| RF07 | Controle de Acesso por Role | O sistema deve restringir o acesso às páginas com base no papel do usuário. |
| RF08 | Acesso à Tela de Logs | Apenas administradores devem acessar a tela de logs do sistema. |
| RF09 | Acesso ao Perfil | Apenas o próprio usuário logado deve visualizar e editar seus dados. |
| RF10 | Registro de Logs | O sistema deve registrar ações dos usuários em um log de auditoria. |

# 4. Requisitos Não Funcionais (RNF)

|  |  |  |
| --- | --- | --- |
| Código | Requisito Não Funcional | Descrição |
| RNF01 | Segurança | O sistema deve garantir o uso de HTTPS para transmissão segura de dados. |
| RNF02 | LGPD | O sistema deve garantir que os dados pessoais sejam tratados com base nos princípios da LGPD, incluindo finalidade, necessidade e segurança. |
| RNF03 | Desempenho | O tempo de resposta das requisições autenticadas não deve exceder 1 segundo em 95% dos casos. |
| RNF04 | Escalabilidade | O sistema deve ser escalável horizontalmente com serviços stateless. |
| RNF05 | Portabilidade | O sistema deve ser compatível com os principais navegadores modernos. |
| RNF06 | Manutenibilidade | O código deve ser modular e bem documentado, facilitando futuras alterações. |
| RNF07 | Privacidade por Design | O sistema deve ser projetado com princípios de minimização de dados e acesso restrito desde o início. |
| RNF08 | Auditabilidade | O sistema deve manter um histórico de ações sensíveis para fins de auditoria. |
| RNF09 | Backup | O sistema deve realizar backups periódicos das informações críticas. |

# 5. Considerações Finais

Este documento foi elaborado com base na premissa de um sistema acadêmico com fins didáticos, respeitando os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) e as boas práticas de segurança da informação. Para uma implantação em ambiente real, recomenda-se a aplicação de técnicas adicionais de hardening, testes de invasão e validações legais específicas.