

Especificação de Requisitos do Sistema (ERS)

Módulo de Login – Portal da Intranet

1. Introdução

Este documento apresenta a Especificação de Requisitos do Sistema (ERS) para o módulo de Login da Intranet, definindo os processos de autenticação, validações de entrada, comunicação entre frontend e backend, regras de armazenamento seguro e comportamento do sistema diante de novos registros. O escopo contempla apenas as operações essenciais de login, excluindo funcionalidades como recuperação de senha, permissões e gerenciamento de contas. A especificação detalha requisitos funcionais, regras de negócio, fluxo de operação e restrições tecnológicas, servindo como referência para desenvolvimento, testes e manutenção do módulo.

1.1 Objetivo

Este documento descreve a especificação do módulo de Login do Portal da Intranet da empresa.

O objetivo é definir o funcionamento do processo de autenticação, garantindo segurança, integridade das informações e controle de acesso ao ambiente interno.

2. Escopo - O módulo de Login contempla:

- Exibição da interface de autenticação (formulário de e-mail e senha).
- Validações de entrada no frontend.
- Validações e autenticação no backend.
- Armazenamento seguro das credenciais no banco de dados.
- Registro automático da data e hora de criação do login.
- Registro de status inicial do usuário no banco de dados.

O acesso à Intranet depende da autenticação bem-sucedida.

3. Fora do Escopo

As seguintes funcionalidades não fazem parte deste módulo:

- Recuperação de senha (“Esqueci minha senha”).
- Edição, alteração ou exclusão de contas.
- Criação de contas pela interface (cadastro aberto).
- Sistema de permissões ou perfis de usuário.
- Autenticação em duas etapas (MFA).

- Envio de e-mails ou notificações.
- Telas internas da Intranet após o login.

Este documento abrange exclusivamente o módulo de login.

4. Requisitos Funcionais

RF01 – Exibir formulário de login: O sistema deve apresentar um formulário composto pelos campos: E-mail, Senha, Botão de envio (Login)

RF02 – Validar e-mail no frontend: O sistema deve impedir o envio do formulário caso: O campo esteja vazio. O e-mail possua menos de 6 caracteres.

Mensagem esperada:

"Preencha um email válido."

RF03 – Validar senha no frontend: O sistema deve bloquear o envio se:

- A senha possuir menos de 6 caracteres.

Mensagem esperada: "A senha tem que conter no mínimo 6 caracteres."

RF04 – Enviar dados para o backend: Ao clicar em "Login", o frontend deve enviar uma requisição POST para: <http://localhost:3000/login>

Conteúdo enviado:

- email
- senha

RF05 – Verificar existência do e-mail (backend): O backend deve consultar a tabela "login" para verificar se o e-mail já está cadastrado. Se o e-mail existir, retornar: "Email já cadastrado."

RF06 – Criptografar a senha: Antes de armazenar a senha, o servidor deve gerar um hash utilizando bcrypt com 10 rounds.

RF07 – Registrar novo usuário no banco

O backend deve inserir:

- email

- senha (hash)
- criado_em (timestamp automático)
- status_lei = "Aguardando resposta"

RF08 – Mensagem de sucesso: Se o cadastro for concluído, o backend deve retornar: "Cadastro realizado com sucesso."

RF09 – Exibir o retorno do servidor: O frontend deve exibir ao usuário a resposta fornecida pelo backend.

5. Regras de Negócio

RN01 – Armazenamento seguro de senha: Nenhuma senha poderá ser armazenada em texto puro.

RN02 – E-mail único: O e-mail é um identificador único; não podem existir registros duplicados.

RN03 – Status padrão: Todo novo registro deve conter o status: "Aguardando resposta".

RN04 – Registro de data/hora: A criação do login deve ser registrada automaticamente no campo criado_em.

6. Modelo de Dados

Atributo	Tipo	Chave
id_login	INT	PK
email	VARCHAR(150)	
senha	TEXT	
criado_em	TIMESTAMP	
status_lei	VARCHAR(50)	

7. Restrições do Sistema

1. O backend deve ser implementado em Node.js com Express.
2. O banco de dados deve ser MySQL/MariaDB.
3. O frontend deve ser desenvolvido em HTML, CSS e JavaScript.
4. As requisições devem ser feitas no formato JSON.
5. O sistema deve rodar localmente na porta 3000.
6. O hashing deve ser feito com bcrypt.

8. Fluxo Principal

1. O usuário acessa a página de login.
2. Preenche o e-mail e a senha.
3. O frontend valida os campos.
4. A requisição é enviada ao backend.
5. O backend valida novamente os dados.
6. O sistema verifica se o e-mail já existe.
7. O sistema gera o hash da senha.
8. O novo registro é salvo no banco de dados.
9. O backend retorna a resposta.
10. O frontend exibe a mensagem ao usuário.

9. Considerações Finais: O presente documento descreve todas as especificações necessárias para o funcionamento do módulo de Login da Intranet.

Ele serve como referência para desenvolvimento, testes, homologação e futuras manutenções.