MINISTÉRIO DA EDUCAÇÃO
Universidade Tecnológica Federal do Paraná
Campus Santa Helena

CURSO SUPERIOR DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Erick Bonruque

PLANO DE DESENVOLVIMENTO DE SOFTWARE - SHIELDPASS: GERENCIADOR INTELIGENTE DE ACESSOS E SENHAS

ORIENTAÇÃO:

PROFESSOR: GIUVANE CONTI

SANTA HELENA – PR

2024

1 IDENTIFICAÇÃO

1.1 SHIELDPASS: GERENCIADOR INTELIGENTE DE ACESSOS E SENHAS

1.2 ERICK BONRUQUE

1.2.1 Professor Orientador

Giuvane Conti

1.2.2 Desenvolvedor

Erick Bonruque

2 POSICIONAMENTO

A aplicação desktop é projetada para atender qualquer pessoa que utiliza frequentemente a internet, redes sociais, websites ou aplicações que exigem segurança no gerenciamento de senhas. O projeto tem como objetivo não apenas facilitar a organização e o armazenamento de senhas, mas também fortalecer a segurança do usuário no ambiente online.

2.1 DESCRIÇÃO DO PROBLEMA

Pessoas que utilizam aplicações e websites com muita frequência enfrentam problemas comuns, como a falta de um gerenciamento eficaz de senhas. Muitas vezes, isso resulta no uso da mesma senha para diferentes sistemas, o que pode se tornar um grande risco em caso de vazamento de dados. Além disso, a dificuldade em lembrar diversas senhas é uma dor de cabeça recorrente. Pensando nesses desafios, o projeto propõe o desenvolvimento de um sistema desktop open-source para gerenciamento de senhas, com recursos como geração de senhas fortes e criptografia de ponta a ponta, garantindo máxima segurança para o usuário.

3 Descrição dos Envolvidos e dos Usuários

3.1 Resumo dos Envolvidos

Nome	Função	Responsabilidades
Erick Bonruque	Tech Lead	Liderar a equipe técnica e garantir qualidade.
Erico ruque	Desenvolvedor Front-end	Criar interfaces e experiências do usuário.
Eric hulk	Desenvolvedor Back-end	Gerenciar lógica do servidor e banco de dados.

Erique Hulk do bem	QA	Testar e garantir qualidade do produto.

3.2 Resumo dos Usuários

Nome	Descrição	Responsabilidades	Envolvido
Maria Oliveira	Administradora	Especificar os requisitos para o sistema de login e cadastro de usuários.	Erick Bonruque
Lucas Fernandes	Usuário Comum	Detalhar como deve funcionar a interface de registro e visualização de logins.	Erico ruque
Julia Andrade	Cliente	Definir os critérios de segurança para geração de senhas fortes e criptografia.	Eric hulk
Ricardo Menezes	Funcionário	Explicar como o sistema deve permitir a edição e exclusão de dados cadastrados.	Erique Hulk do bem

3.3 Ambiente do Usuário

O ambiente em que o usuário irá operar é um sistema digital acessível, com uma interface mais intuitiva possível, projetada para atender tanto usuários casuais quanto os com mais registros de senhas. A aplicação será utilizada localmente em computadores pessoais e funcionará como um sistema desktop.

O sistema oferece funcionalidades voltadas para o gerenciamento seguro de senhas, permitindo que os usuários acessem suas informações de forma prática e organizada.

Usuários terão acesso a:

- Tela de login e cadastro com campos básicos (e-mail e senha).
- Tela principal (dashboard) com opções para registrar novos logins, visualizar os logins já cadastrados, editar ou excluir dados, e adicionar notas relacionadas aos sistemas registrados.

O ambiente foi projetado com foco em simplicidade, segurança e eficiência, promovendo uma experiência fluida e garantindo a proteção das informações dos usuários.

3.4 Principais Necessidades dos Usuários e dos Envolvidos

Necessidade	Preocupações	Solução Atual	Soluções Propostas
Facilidade de Gerenciamento de Senhas	Usuários enfrentam dificuldades em organizar e lembrar diversas senhas, resultando no uso inseguro de senhas repetidas.	Gerenciamento manual ou uso de blocos de notas.	Implementação de um sistema desktop com painel centralizado para armazenar e organizar senhas.
Segurança no Armazenamento	Há risco de vazamento de dados sensíveis devido ao armazenamento desprotegido de senhas.	Armazenamento sem criptografia ou não centralizado.	Criptografia de ponta a ponta para garantir segurança no armazenamento e acesso aos dados.
Facilidade de Edição e Consulta	Usuários podem se perder ao consultar e atualizar informações já registradas.	Depende de anotações manuais ou sistemas confusos.	Criação de uma interface intuitiva com opções claras para editar, excluir e visualizar logins cadastrados.
Geração de Senhas Fortes	Muitos usuários não sabem como criar senhas fortes e seguras para seus logins.	Uso de senhas fracas ou geradas de forma repetitiva.	Implementação de um gerador automático de senhas fortes no sistema, seguindo padrões de segurança atualizados.

4 Visão Geral do Produto

O sistema irá facilitar o gerenciamento seguro e eficiente de senhas para os usuários. Ele proporcionará um ambiente centralizado e intuitivo para armazenar, organizar e consultar logins, reduzindo a dificuldade em lembrar diversas senhas e promovendo maior segurança online.

Com recursos como geração de senhas fortes, criptografia de ponta a ponta e uma interface amigável, o sistema garantirá praticidade e proteção das informações do usuário. Além disso, permitirá a edição e exclusão de dados cadastrados de forma simples, oferecendo relatórios detalhados de uso e possibilitando o registro de feedback para melhorias contínuas.

Essa solução visa atender tanto usuários casuais quanto avançados, fortalecendo a segurança no ambiente digital e otimizando a gestão de credenciais de acesso.

4.1 Levantamento de requisitos

Requisitos Funcionais

1. **Cadastro e Login de Usuários**
    - O sistema deve permitir que usuários se registrem informando e-mail e senha.
    - O sistema deve autenticar usuários com validação de e-mail e senha no login.
2. **Gerenciamento de Logins e Senhas**
    - O sistema deve permitir que o usuário registre novos logins, incluindo nome do sistema, e-mail, senha, link e notas adicionais.
    - O sistema deve listar todos os logins cadastrados na dashboard principal.
    - O sistema deve permitir a edição e exclusão de logins existentes.

3. **Geração de Senhas Fortes**
    - O sistema deve oferecer uma funcionalidade para gerar senhas fortes, seguindo padrões de segurança (caracteres especiais, números, letras maiúsculas e minúsculas).
4. **Visualização de Perfil**
    - O sistema deve permitir que o usuário visualize e edite seus dados cadastrados.
    - Deve ser possível deslogar da conta no sistema.
5. **Segurança**
    - Todas as senhas cadastradas devem ser criptografadas antes de serem armazenadas no banco de dados.

Requisitos Não Funcionais

1. **Segurança**
    - O sistema deve implementar criptografia de ponta a ponta para armazenamento e transmissão de dados sensíveis.
    - O acesso ao sistema deve ser protegido contra ataques de força bruta com bloqueio após múltiplas tentativas de login.
2. **Usabilidade**
    - A interface do sistema deve ser amigável e intuitiva, com opções bem definidas e fáceis de acessar.
    - Deve ser responsiva em diferentes resoluções de tela de desktop.
3. **Performance**
    - O tempo de carregamento da dashboard deve ser inferior a 2 segundos em condições normais.
4. **Portabilidade**
    - O sistema deve ser compatível com os sistemas operacionais Windows, macOS e Linux.
5. **Manutenibilidade**
    - O código deve ser modular e seguir padrões de boas práticas, facilitando a adição de novas funcionalidades no futuro.
6. **Disponibilidade**
    - O sistema deve garantir estabilidade em funcionamento offline, já que é uma aplicação desktop.

4.2 Casos de Uso

Caso de Uso 1: Cadastro de Usuário

Ator: Usuário comum

Descrição: O usuário acessa a tela de cadastro, informa seu e-mail e cria uma senha para registrar sua conta no sistema.

Fluxo Principal:

1. O usuário abre o sistema e seleciona a opção "Cadastrar".
2. O sistema solicita o preenchimento do e-mail, senha e confirmar senha.
3. O usuário preenche os campos e clica em "Cadastrar-se".
4. O sistema valida os dados e cria a conta do usuário.
5. O usuário é redirecionado para a tela de login.

Caso de Uso 2: Login no Sistema

Ator: Usuário comum

Descrição: O usuário acessa a tela de login e autentica sua conta usando o e-mail e senha cadastrados.

Fluxo Principal:

1. O usuário abre o sistema e vai para a tela de login.
2. O sistema solicita o e-mail e senha.
3. O usuário preenche os campos e clica em "Login".
4. O sistema valida as credenciais. Se corretas, o usuário é redirecionado para o dashboard.

Caso de Uso 3: Registro de Novo Login

Ator: Usuário comum

Descrição: O usuário registra um novo login, incluindo as informações do site, e-mail, senha, link (se houver) e uma nota adicional.

Fluxo Principal:

1. O usuário acessa o dashboard e seleciona a opção "Adicionar Senha".

2. O sistema solicita que o usuário preencha as informações necessárias: nome do site, e-mail, senha, link e nota.
3. O usuário preenche os campos e clica em "Cadastrar Login".
4. O sistema armazena os dados e exibe a nova entrada na lista de logins cadastrados.

Caso de Uso 4: Visualizar Logins Cadastrados

Ator: Usuário comum

Descrição: O usuário acessa a lista de logins cadastrados no sistema, visualizando os detalhes de cada um.

Fluxo Principal:

1. O usuário acessa o dashboard e vê a lista de logins registrados.
2. O usuário clica em qualquer login na lista.
3. O sistema exibe os detalhes do login selecionado, incluindo e-mail, senha, link e notas.

Caso de Uso 5: Editar Login Cadastrado

Ator: Usuário comum

Descrição: O usuário edita um login previamente cadastrado, alterando informações como senha, e-mail ou nota.

Fluxo Principal:

1. O usuário acessa o dashboard e visualiza a lista de logins.
2. O usuário clica no login que deseja editar.
3. O sistema exibe os detalhes do login selecionado e oferece a opção de edição.
4. O usuário altera as informações desejadas e clica em "Atualizar".
5. O sistema atualiza o login no banco de dados e exibe a versão editada na lista.

Caso de Uso 6: Excluir Login Cadastrado

Ator: Usuário comum

Descrição: O usuário exclui um login registrado no sistema.

Fluxo Principal:

1. O usuário acessa o dashboard e visualiza a lista de logins.
2. O usuário clica no login que deseja excluir.
3. O sistema exibe um pop up pedindo a confirmação da exclusão.
4. O usuário confirma a exclusão.
5. O sistema remove o login do banco de dados e atualiza a lista de logins cadastrados.

Caso de Uso 7: Geração de Senha Forte

Ator: Usuário comum

Descrição: O usuário gera uma senha forte para um login, utilizando a funcionalidade do sistema.

Fluxo Principal:

1. Ao criar uma nova senha/ novo login o sistema sugere uma senha forte.
2. O sistema gera uma senha aleatória seguindo critérios de segurança (números, letras maiúsculas e minúsculas, caracteres especiais).
3. O usuário pode usar a senha forte sugerida ou criar uma senha própria.

Caso de Uso 8: Visualizar e Editar Perfil

Ator: Usuário comum

Descrição: O usuário visualiza e edita suas informações de perfil, como e-mail e senha.

Fluxo Principal:

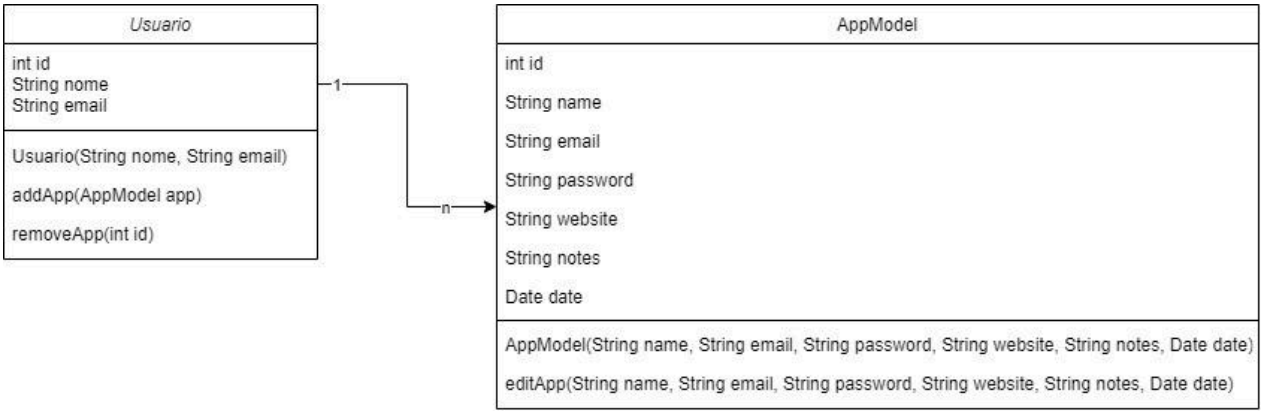
5 O usuário acessa a tela de perfil a partir do dashboard.

6 O sistema exibe as informações atuais do perfil.

7 O usuário pode editar o e-mail ou a senha e clicar em "Salvar".

8 O sistema valida os dados e atualiza o perfil do usuário.

8.1 Diagrama de classe



9 Cronograma

Atividades Desenvolvidas	Dezembro	Janeiro	Fevereiro
Levantamento de requisitos/objetivos gerais e específicos	x		
Plano de Desenvolvimento	x		
Modelagem de Requisitos	x	x	
Modelagem do banco de dados	x		
Implementação de classes (AppModel, Usuario)	x	x	
Desenvolvimento de funcionalidades principais (Login, Cadastro, Dashboard)	x	x	x
Implementação de navegação entre páginas (Login, Dashboard, etc.)	x	x	
Desenvolvimento de telas de interface (Cadastro, Login, etc.)	x	x	x
Testes de funcionalidade (Login, Cadastro, Dados do perfil)		x	x
Testes de segurança (criptografia, armazenamento de senhas)			x
Testes de usabilidade			x
Implementação de melhorias e ajustes finais			x
Documentação do sistema			x
Entrega final do sistema			x