**Capa**

**Histórico de Alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Descrição** | **Autor** |
|  | 0.0 | Criação do documento de requisitos, identificação dos requisitos | Rafael de Castro Gomes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sumário

[**1. INTRODUÇÃO** 3](#_Toc176355362)

[**1.1.** **Visão geral do documento** 4](#_Toc176355363)

[**1.2.** **Convenções, termos e abreviações** 4](#_Toc176355364)

[**2. DESCRIÇÃO GERAL DO SISTEMA** 4](#_Toc176355365)

[**3. REQUISITOS FUNCIONAIS (CASOS DE USO)** 4](#_Toc176355366)

[**4. REQUISITOS NÃO FUNCIONAIS** 8](#_Toc176355367)

[**5. ESPECIFICAÇÃO DE REQUISITOS DO SISTEMA** 9](#_Toc176355368)

[**5.1. Tabela Casos de Uso** 9](#_Toc176355369)

[**6. MODELOS DO SISTEMA** 34](#_Toc176355370)

[**7. EVOLUÇÃO DO SISTEMA** 35](#_Toc176355371)

[**8. GLOSSÁRIO** 35](#_Toc176355372)

[**9. FERRAMENTAS UTILIZADAS** 35](#_Toc176355373)

[**10. BOAS PRÁTICAS** 36](#_Toc176355374)

# 1. INTRODUÇÃO

Este documento detalha os requisitos do protótipo de uma rede social que funcionará em conjunto com uma inteligência artificial treinada em detecção de postagens tóxicas. O documento fornece as informações necessárias para o projeto e implementação do sistema, bem como para a realização dos testes e homologação dele.

## Visão geral do documento

Este documento está organizado da seguinte forma:

* **Seção 2 - Descrição Geral do Sistema:** Apresenta uma visão geral da rede social.
* **Seção 3 - Requisitos Funcionais (Casos de Uso):** Detalha brevemente os casos de uso do sistema.
* **Seção 4 - Requisitos Não-Funcionais:** Cita e explica os requisitos não funcionais do sistema.
* **Seção 5 – Especificação de Requisitos do Sistema:** Apresenta uma descrição detalhada dos requisitos funcionais**.**
* **Seção 6 - Modelos do Sistema:** Estabelece modelos que mostram as relações entre os componentes do sistema e seu ambiente.
* **Seção 7 - Evolução do Sistema:** Descreve as mudanças e melhorias previstas para o sistema.
* **Seção 8 - Glossário:** Define termos técnicos e abreviações usadas no documento.
* **Seção 9 –** **Ferramentas Utilizadas:** Descreve quais foram as ferramentas utilizadas no desenvolvimento, implementação e manutenção do protótipo da rede social Bem-te-vi.
* **Seção 10 – Boas Práticas:** Detalha as práticas adotadas para promover um código limpo, bem documentado e fácil de manter.

## Convenções, termos e abreviações

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

* **BERT:** Modelo de Transformador Bidirecional (Bidirectional Encoder Representations from Transformers), usado para análise de postagens
* **MFA:** Autenticação Multifator (Multifactor Authentication)
* **MVC:** Arquitetura Modelo-Visão-Controlador (Model-View-Controller)
* **RF:** Requisito Funcional
* **RNF:** Requisito Não Funcional
* **SQL:** Structured Query Language, utilizado para gerenciamento de bancos de dados relacionais

# 2. DESCRIÇÃO GERAL DO SISTEMA

O sistema é um protótipo de rede social que permitirá aos usuários registrados realizarem postagens, acessarem e gerenciarem seu próprio conteúdo. Além disso, usuários administradores terão a capacidade de monitorar as atividades e postagens dentro da rede. O protótipo também servirá como uma base para o funcionamento de uma inteligência artificial focada na detecção de postagens tóxicas ou ofensivas.

A ideia inicial da aplicação *web* é de um protótipo de rede social de microblogging com o diferencial visando um ambiente de interação social mais pacífico. Sendo assim, propõem-se uma forma de compartilhamento de mensagens de cunho mais leve, local onde os usuários se comunicam através de mensagens curtas de natureza amigável, positiva, motivacional e alegre.

Para a inspiração nesse contexto da plataforma, utiliza-se a representação do pássaro brasileiro Bem Te Vi como símbolo do protótipo de rede social, uma definição convidativa de desejar o bem ao próximo. Considera-se o uso deste pássaro como identidade e recurso visual para a aplicação.

# 3. REQUISITOS FUNCIONAIS (CASOS DE USO)

**RF001: Realizar Cadastro.**

* O sistema deve oferecer uma funcionalidade de cadastro que permita aos novos usuários criarem suas contas, fornecendo informações básicas e passando por processos de verificação de identidade quando necessário.

**RF002: Realizar Login.**

* O sistema deve oferecer uma funcionalidade de login que permita aos usuários registrados acessarem suas contas, utilizando credenciais seguras (endereço de e-mail e senha).

**RF003: Realizar Logout.**

* Usuários devem ter a capacidade de fazer logout de suas contas, garantindo que suas sessões sejam encerradas corretamente para proteger suas informações.

**RF004: Escrever Postagens.**

* Usuários devem ter a capacidade de criar conteúdo em formato de texto e publicá-los em seus perfis.

**RF005: Pesquisar Perfis de Outros Usuários.**

* Os usuários devem ter a capacidade de pesquisar, acessar e visualizar os perfis de outros usuários na rede social. Isso inclui ver todas as informações públicas, como nome de usuário, biografia e postagens. Como todos os perfis e postagens são públicos, os usuários podem visualizar o conteúdo de qualquer perfil sem a necessidade de seguir o usuário ou restrições de privacidade.

**RF006: Acessar Configurações.**

* O sistema deve disponibilizar uma seção de configurações onde os usuários podem acessar funcionalidades para editar perfil e visualizar log de acesso.

**RF007: Editar Perfil.**

* Os usuários devem poder alterar informações em seus perfis, como foto, nome, biografia e senha a fim de manter sua conta segura, a identidade digital atualizada e relevante.

**RF008: Visualizar Log de Acesso.**

* Usuários podem acessar um histórico de suas atividades e interações dentro da plataforma, incluindo datas e horários de acesso, para monitoramento pessoal de segurança e uso.

**RF009: Excluir Conta.**

* Usuários devem ter a capacidade de remover suas próprias contas, incluindo todos os dados associados, caso desejem deixar a plataforma.

**RF010: Acessar Interface Administrativa.**

* Administradores devem ter ferramentas para gerenciar contas de usuários, incluindo a habilidade de ativar e desativar o acesso dos usuários conforme necessário.

**RF011: Ativar/Desativar Acesso de Usuário.**

* Administradores devem ter a funcionalidade de suspender ou reativar contas de usuários conforme necessário, baseando-se em comportamentos suspeitos ou violações das regras da plataforma.

**RF012: Monitorar Logs de Acesso.**

* Administradores devem poder acessar e analisar registros de acesso detalhados dos usuários para monitorar atividades suspeitas e manter a segurança da plataforma.

**RF013: Gerenciar Conteúdo de Postagens.**

* Deve existir uma funcionalidade que permita aos administradores removerem qualquer conteúdo publicado na rede social para garantir a conformidade com as diretrizes da plataforma.

**RF014: Analisar Postagens de Usuários.**

* O sistema deve analisar as postagens de texto utilizando o modelo BERT para detectar conteúdo ofensivo.

**RF015: Notificar Usuários Sobre Conteúdo Ofensivo.**

* O sistema deve notificar os usuários quando suas postagens forem avaliadas como ofensivas.

**RF016: Permitir Criação de Novas Postagens após Notificação de Conteúdo Ofensivo.**

* O sistema deve permitir que os usuários criem uma nova postagem após serem notificados de que sua postagem anterior foi considerada ofensiva.

**RF017: Registrar Postagens Ofensivas.**

* O sistema deve registrar todas as postagens consideradas ofensivas pelo modelo BERT.

**RF018: Fornecer Relatórios Sobre Postagens Ofensivas.**

* O sistema deve fornecer relatórios detalhados sobre as postagens que foram filtradas pelo modelo BERT.

**RF019: Denunciar Postagens.**

* O sistema deve permitir que os usuários denunciem postagens que considerem inadequadas ou ofensivas. A denúncia deve ser encaminhada para a análise dos administradores para possíveis ações corretivas.

**RF020: Gerenciar Contas Administrativas**

* O sistema deve permitir a criação de uma conta inicial de administrador no banco de dados, que será utilizada para configurar e gerenciar outras contas administrativas.
* A conta inicial deve ter privilégios máximos e a capacidade de criar, modificar, suspender ou remover outras contas administrativas.
* Novas contas administrativas devem ser criadas a partir da interface de gerenciamento acessível apenas pela conta inicial ou por administradores com privilégios equivalentes.
* As credenciais das contas administrativas devem ser geradas com segurança, utilizando hashing para armazenar senhas, e devem incluir opções para autenticação multifator (MFA).
* O sistema deve registrar todas as ações realizadas pelas contas administrativas em logs de auditoria, incluindo a criação de novas contas, alterações de privilégios e suspensão de contas.
* Administradores devem ter a capacidade de redefinir suas senhas e ativar ou desativar a autenticação multifator para aumentar a segurança da conta.

# 4. REQUISITOS NÃO FUNCIONAIS

**RNF01: Segurança**

* O sistema deve implementar medidas de segurança robustas para proteger dados sensíveis e garantir a privacidade. Isso inclui a criptografia de dados, autenticação forte (incluindo autenticação multifator para contas administrativas), e políticas de controle de acesso rigorosas. Além disso, todas as atividades administrativas, como criação, modificação, ou remoção de contas, devem ser registradas em logs de auditoria para monitoramento e conformidade.

**RNF02: Escalabilidade**

* O sistema deve ser capaz de escalar horizontalmente ou verticalmente conforme necessário, mantendo a performance e a estabilidade à medida que a base de usuários cresce. Isso envolve a utilização de arquiteturas escaláveis, balanceamento de carga, e recursos de computação flexíveis para garantir que o sistema continue funcionando eficientemente sob diferentes cargas de trabalho.

**RNF03: Intuitividade**

* A interface do usuário deve ser clara, intuitiva e amigável, permitindo que usuários de todos os níveis técnicos interajam facilmente com a plataforma. Isso inclui uma navegação lógica, design responsivo e assistência ao usuário. Especial atenção deve ser dada à interface de administração, garantindo que os administradores possam gerenciar o sistema de maneira eficaz e sem complicações.

**RNF04: Desempenho**

* O sistema deve ser capaz de processar todas as requisições dentro de um tempo definido como aceitável, garantindo tempos de resposta rápidos mesmo sob carga pesada. Isso é essencial para proporcionar uma experiência de usuário fluida e responsiva, especialmente para operações críticas como o login de administradores e a análise de postagens pelo modelo BERT.

**RNF05: Disponibilidade**

* O sistema deve garantir uma disponibilidade contínua, com um tempo de operacionalidade de, pelo menos, 99%, minimizando interrupções e maximizando o acesso para os usuários e administradores. Isso é crucial para garantir que administradores possam intervir rapidamente em casos de necessidade, como ao lidar com conteúdo ofensivo ou gerenciamento de contas.

**RNF06: Compatibilidade**

* O sistema deve ser compatível com uma variedade de plataformas e dispositivos, incluindo computadores, smartphones e tablets, e deve funcionar eficientemente nos principais navegadores do mercado, como Chrome, Firefox, Safari e Edge. Isso garante que tanto usuários quanto administradores possam acessar e utilizar o sistema independentemente do dispositivo ou navegador utilizado.

**RNF07: Manutenibilidade**

* O sistema deve ser projetado para facilitar a manutenção e atualização, permitindo a fácil gestão de contas administrativas, ajustes de segurança, e implementação de novas funcionalidades. Isso inclui a utilização de código modular, documentação abrangente, e padrões de projeto que permitam futuras atualizações, correções de bugs e adições de novas funcionalidades sem interrupções significativas no serviço.

**RNF08: Desempenho do Modelo BERT**

* O modelo BERT utilizado no sistema deve operar de maneira eficiente, com baixo tempo de resposta para a análise de postagens. Isso garante que a moderação de conteúdo seja realizada de maneira oportuna e que as postagens sejam processadas sem atrasos perceptíveis.

**RNF09: Precisão do Modelo BERT**

* O sistema deve garantir uma alta precisão na detecção de conteúdo ofensivo utilizando o modelo BERT. Isso é fundamental para a confiabilidade do sistema, assegurando que o conteúdo seja moderado de acordo com as políticas da plataforma.

# 5. ESPECIFICAÇÃO DE REQUISITOS DO SISTEMA

## 5.1. Tabela Casos de Uso

|  |  |
| --- | --- |
| **Caso de uso 001 – Realizar Cadastro** | |
| Ator principal | Usuário |
| Resumo | Esse caso de uso, descreve a etapa em que o usuário faz seu cadastro em nosso banco de dados. |
| Pré-condições | O usuário possui um endereço de e-mail válido que ainda não está registrado no sistema; ter idade mínima de dezoito anos. |
|  |  |
| Pós-condições | O sistema confirma o sucesso do registro ao usuário, e ele pode fazer login no sistema usando os detalhes fornecidos. |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário clica no link descrito como Registre-se “Aqui”. | 1. Redireciona o usuário para a página de cadastro. |
| 1. O usuário pode preencher os campos solicitados e ou obrigatórios, como nome, e-mail, senha. Clica no link descrito “Cadastrar”. | 1. Um número de registro é criado para este usuário. O registro é único e exclusivo. |
|  | |
| **Restrições** | |
|  | **Ações do sistema** |
|  | Não podem existir dois ou mais registros iguais de usuários. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário entra com informações que já existem no sistema (como um e-mail já registrado). | 1. O sistema verifica a existência de duplicatas e exibe uma mensagem de erro indicando que o e-mail já foi registrado. |
| 1. O usuário pode corrigir as informações e tentar registrar novamente. |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta se registrar com informações inválidas (por exemplo, um formato de e-mail inválido). | 1. O sistema valida a entrada e exibe uma mensagem de erro solicitando que o usuário insira informações válidas. |
| **Regras de negócio** | |
| 1. O e-mail do usuário deve ser único. | |
| 1. O nome do usuário pode ser duplicado. | |
| 1. A senha do usuário deve atender aos requisitos mínimos de segurança (por exemplo, pelo menos 8 caracteres, incluindo números, letras maiúsculas e minúsculas, e símbolos especiais). | |

|  |  |
| --- | --- |
| **Caso de uso 002 – Realizar Login** | |
| Ator principal | Usuário |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário registrado faz login no sistema utilizando suas credenciais. |
| Pré-condições | O usuário deve ter uma conta registrada no sistema com um e-mail válido e uma senha. |
|  |  |
| Pós-condições | O sistema valida as credenciais do usuário e, se forem corretas, concede acesso à conta do usuário, permitindo que ele utilize as funcionalidades da plataforma. |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário acessa a página inicial do sistema. | 3. O sistema redireciona o usuário para a página de login. |
| 2. O usuário clica no link descrito como "Entrar". | 6. O sistema valida as credenciais fornecidas. |
| 4. O usuário preenche os campos de e-mail e senha com as credenciais registradas. | 7. Se as credenciais estiverem corretas, o sistema redireciona o usuário para a página inicial do seu perfil. |
| 5. O usuário clica no botão "Login". |  |
|  | |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema não deve permitir acesso a usuários com credenciais inválidas. |
|  | 2. O sistema deve bloquear a conta temporariamente após várias tentativas de login falhadas consecutivas (por exemplo, 5 tentativas). |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário esquece a senha e clica no link "Esqueci minha senha". | 1. O sistema redireciona o usuário para a página de recuperação de senha. |
| 1. O usuário insere o e-mail registrado e clica no botão "Enviar". | 4. O sistema envia um e-mail com instruções para redefinição de senha. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário insere um e-mail ou senha inválida. | 1. O sistema exibe uma mensagem de erro indicando que as credenciais são inválidas. |
| **Regras de negócio** | |
| 1. O e-mail do usuário deve estar registrado no sistema. | |
| 1. A senha deve corresponder à senha associada ao e-mail fornecido. | |
| 1. O sistema deve manter um registro de tentativas de login para evitar acessos não autorizados. | |
| 1. O sistema deve oferecer uma opção de recuperação de senha em caso de esquecimento. | |

|  |  |
| --- | --- |
| **Caso de uso 003 – Realizar Logout** | |
| Ator principal | Usuário |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário registrado faz logout da plataforma, encerrando sua sessão para proteger suas informações pessoais. |
| Pré-condições | O usuário deve estar logado na plataforma. |
|  |  |
| Pós-condições | O sistema encerra a sessão do usuário, garantindo que todas as informações associadas à sessão sejam devidamente protegidas e que o usuário seja redirecionado para a página inicial ou de login. |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário clica no botão ou link descrito como "Sair" ou "Logout". | 3. O sistema redireciona o usuário para a página inicial ou de login, confirmando que ele foi desconectado. |
| 2. O usuário clica no link descrito como "Entrar". | 6. O sistema valida as credenciais fornecidas. |
| 4. O usuário preenche os campos de e-mail e senha com as credenciais registradas. | 7. Se as credenciais estiverem corretas, o sistema redireciona o usuário para a página inicial do seu perfil. |
| 5. O usuário clica no botão "Login". |  |
|  | |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema deve garantir que todas as sessões sejam encerradas corretamente. |
|  | 2. O sistema deve proteger qualquer informação sensível durante o processo de logout. |
| **Cenário alternativo** | |
| Nenhum cenário alternativo aplicável, pois a ação de sair é direta e sem etapas intermediárias. | |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário perde a conexão com a internet durante o processo de logout. | 1. O sistema deve manter o usuário logado até que a conexão seja restabelecida e o processo de logout possa ser concluído corretamente. |
| **Regras de negócio** | |
| 1. O sistema deve garantir que todas as sessões de usuários sejam encerradas de forma segura e que nenhum dado de sessão fique exposto. | |
| 1. O sistema deve proteger informações sensíveis do usuário durante o processo de logout. | |

|  |  |
| --- | --- |
| **Caso de uso 004 – Escrever Postagens** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o processo que um usuário registrado segue para criar e publicar um post em sua linha do tempo. |
|  |  |
| Pré-condições | O usuário deve estar autenticado e ter uma sessão ativa. |
|  |  |
| Pós-condições | O post do usuário é visível na linha do tempo do usuário e pode ser visto por outros usuários que o seguem. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário navega até a sua linha do tempo ou área de postagem. | 1. O sistema verifica o conteúdo do post contra o banco de dados de palavras proibidas. Se nenhuma palavra proibida for encontrada, o sistema publica o post na linha do tempo do usuário. |
| 1. O usuário clica no campo de entrada do post. |  |
| 1. O usuário insere o texto desejado no campo de entrada do post |  |
| 1. O usuário clica no botão "Postar". |  |
| **Restrições** | |
|  | **Ações do sistema** |
|  | O sistema deve monitorar e moderar o conteúdo postado para garantir que esteja em conformidade com as regras da comunidade e com as restrições de palavras específicas. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário insere o conteúdo do post, mas decide não postar. | 3. O sistema descarta o post não publicado. |
| 1. O usuário clica no botão "Cancelar" ou navega para outra parte do site. |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta postar conteúdo que contém palavras listadas no banco de dados de palavras proibidas. | 1. O sistema recusa a postagem e notifica o usuário sobre a restrição. |
| **Regras de negócio** | |
| 1. O conteúdo do post deve estar em conformidade com as regras da comunidade e não deve conter palavras proibidas. | |
| 1. O sistema deve limitar o conteúdo do post a um máximo de 250 caracteres. | |
| 1. As configurações de privacidade do usuário devem ser respeitadas em todas as postagens. | |

|  |  |
| --- | --- |
| **Caso de uso 005 – Pesquisar/Visualizar Perfis de Outros Usuários** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve a funcionalidade onde um usuário pesquisa, acessa e visualiza perfis de outros usuários na rede social. Isso inclui ver todas as informações públicas, como nome de usuário, biografia e postagens, sem a necessidade de seguir o usuário. |
|  |  |
| Pré-condições | O usuário está logado na plataforma. |
|  |  |
| Pós-condições | O usuário visualizou as informações públicas e postagens de outro perfil na rede social. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário utiliza a barra de pesquisa para procurar perfis na rede social. | 1. O sistema exibe os resultados de pesquisa com perfis correspondentes. |
| 1. O usuário seleciona um perfil nos resultados de pesquisa. | 1. O sistema exibe o perfil selecionado, incluindo todas as informações públicas e postagens associadas. |
| **Restrições** | |
| Não há restrições específicas, já que todos os perfis e postagens são públicos. | |
| **Cenário alternativo** | |
| Nenhum cenário alternativo relevante. | |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário pesquisa por um perfil inexistente. | 1. O sistema exibe uma mensagem indicando que nenhum perfil foi encontrado. |
| **Regras de negócio** | |
| 1. Um usuário deve poder acessar e visualizar qualquer perfil público sem restrições ou necessidade de seguir o usuário. | |
| 1. Todas as postagens e informações no perfil devem ser públicas e acessíveis a qualquer usuário registrado. | |

|  |  |
| --- | --- |
| **Caso de uso 006 – Acessar Configurações** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o acesso e uso da área de configurações onde os usuários podem editar seu perfil e visualizar o log de acesso. |
|  |  |
| Pré-condições | O usuário deve estar logado na plataforma. |
|  |  |
| Pós-condições | O usuário pode acessar a área de configurações e realizar ações como editar seu perfil e visualizar o log de acesso. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário clica no link ou ícone de configurações no menu de navegação. | 1. O sistema redireciona o usuário para a página de configurações. |
| 1. O usuário seleciona a opção para editar o perfil ou visualizar o log de acesso. | 4. O sistema exibe a interface correspondente à opção selecionada (editar perfil ou visualizar log de acesso). |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema deve garantir que apenas usuários autenticados acessem a área de configurações. |
|  | 2. O sistema deve proteger qualquer informação sensível durante o acesso à área de configurações. |
|  | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta acessar a área de configurações sem estar logado. | 2. O sistema redireciona o usuário para a página de login. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta acessar a área de configurações durante uma manutenção do sistema. | 1. O sistema exibe uma mensagem de manutenção e impede o acesso temporário à área de configurações. |
| **Regras de negócio** | |
| 1. O sistema deve garantir que somente usuários autenticados possam acessar e modificar suas configurações. | |
| 1. O sistema deve oferecer opções claras para editar o perfil e visualizar o log de acesso. | |
| 1. As informações pessoais e de atividades devem ser protegidas conforme as políticas de privacidade e segurança da plataforma. | |

|  |  |
| --- | --- |
| **Caso de uso 007 – Editar Perfil** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário registrado pode editar e atualizar informações em seu perfil, incluindo foto, nome, biografia e senha. |
|  |  |
| Pré-condições | O usuário deve estar logado na plataforma. |
|  |  |
| Pós-condições | As informações do perfil do usuário são atualizadas no sistema, refletindo as mudanças feitas pelo usuário. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário acessa a área de configurações do perfil. | 3. O sistema exibe um formulário com os campos editáveis do perfil do usuário, como foto, nome, biografia e senha. |
| 2. O usuário seleciona a opção para editar o perfil. | 6. O sistema valida as informações inseridas. |
| 4. O usuário altera as informações desejadas nos campos fornecidos. | 7. O sistema atualiza as informações do perfil do usuário e exibe uma mensagem de confirmação de sucesso. |
| 5. O usuário clica no botão "Salvar" para aplicar as mudanças. |  |
| **Restrições** | |
|  | **Ações do sistema** |
|  | O sistema deve garantir que as novas informações atendam aos requisitos de segurança e formato (por exemplo, senha forte, e-mail válido, etc.). |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta salvar alterações sem preencher todos os campos obrigatórios. | 1. O sistema exibe uma mensagem de erro indicando quais campos precisam ser preenchidos. |
| 1. O usuário seleciona uma nova imagem e confirma. | 1. O sistema atualiza a imagem de perfil. |
| **Editar senha:** |  |
| 1. O usuário clica para alterar a senha. | 1. O sistema pede a senha atual e a nova senha. |
| 1. O usuário insere as informações requeridas. | 1. O sistema valida e atualiza a senha. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário insere informações inválidas (por exemplo, uma senha fraca). | 1. O sistema exibe uma mensagem de erro solicitando que o usuário insira informações válidas (por exemplo, uma senha que atenda aos critérios de segurança). |
| **Regras de negócio** | |
| 1. A senha do usuário deve atender aos requisitos mínimos de segurança (por exemplo, pelo menos 8 caracteres, incluindo números, letras maiúsculas e minúsculas, e símbolos especiais). | |
| 1. O nome do usuário pode ser duplicado, mas o e-mail deve ser único. | |
| 1. As informações do perfil devem ser válidas e seguir as políticas de uso da plataforma. | |

|  |  |
| --- | --- |
| **Caso de uso 008 – Visualizar log de acesso** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário registrado pode visualizar seu próprio log de acessos, mostrando os horários e talvez até locais de login anteriores. |
|  |  |
| Pré-condições | O usuário deve estar autenticado e ter uma sessão ativa. |
|  |  |
| Pós-condições | O usuário tem mais informações sobre suas atividades de login, o que pode ser útil para monitorar a segurança de sua conta. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário navega até a seção de segurança ou configurações de sua conta. | 1. O sistema exibe as opções disponíveis relacionadas à segurança e configurações. |
| 1. O usuário seleciona a opção para visualizar o log de acesso. | 1. O sistema recupera os dados do log de acesso do banco de dados e os exibe ao usuário, mostrando os horários de login anteriores. |
| **Restrições** | |
|  | **Ações do sistema** |
|  | Apenas o próprio usuário pode visualizar seu log de acesso; terceiros ou usuários não autenticados não têm essa permissão. |
| **Cenário alternativo** | |
|  | **Ações do sistema** |
|  | Se não houver dados de log disponíveis, o sistema informa ao usuário que não existem logs de acesso para serem visualizados no momento. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta acessar o log de acesso de outro usuário. | 1. O sistema nega o acesso e exibe uma mensagem de erro, informando que o usuário não tem permissão para acessar esses dados. |
| **Regras de negócio** | |
| 1. O sistema deve garantir que apenas o proprietário da conta possa acessar o log de acesso. | |
| 1. O log de acesso deve ser mantido de forma segura para garantir que informações sensíveis não sejam expostas. | |

|  |  |
| --- | --- |
| **Caso de uso 009 – Excluir Conta** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário registrado pode apagar sua própria conta, incluindo todos os dados associados, caso deseje deixar a plataforma. |
|  |  |
| Pré-condições | O usuário deve estar logado na plataforma. |
|  |  |
| Pós-condições | A conta do usuário e todos os dados associados são permanentemente removidos do sistema. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário acessa a área de configurações do perfil. | 3. O sistema exibe um aviso de confirmação, informando o usuário sobre as consequências de apagar a conta (por exemplo, perda de dados, irreversibilidade da ação). |
| 2. O usuário seleciona a opção para apagar a conta. | 5. O sistema valida a solicitação e apaga a conta do usuário, incluindo todos os dados associados. |
| 4. O usuário confirma a intenção de apagar a conta. | 6. O sistema exibe uma mensagem confirmando que a conta foi apagada com sucesso e redireciona o usuário para a página inicial. |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema deve garantir que a exclusão da conta seja um processo irreversível. |
|  | 2. O sistema deve proteger qualquer informação sensível durante o processo de exclusão. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário decide não apagar a conta após visualizar o aviso de confirmação. | 2. O sistema cancela a solicitação de exclusão e retorna o usuário à área de configurações. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário perde a conexão com a internet durante o processo de exclusão da conta. | 1. O sistema deve reverter a ação e manter a conta ativa até que o processo possa ser concluído corretamente. |
| **Regras de negócio** | |
| 1. A exclusão da conta deve ser irreversível e remover todos os dados associados ao usuário do sistema. | |
| 1. O sistema deve garantir que a ação de apagar a conta seja realizada apenas após a confirmação explícita do usuário. | |
| 1. O sistema deve proteger as informações do usuário durante todo o processo de exclusão. | |

|  |  |
| --- | --- |
| **Caso de uso 010 – Acessar Interface Administrativa** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um administrador acessa a interface administrativa para gerenciar contas de usuários, incluindo a ativação e desativação de acessos conforme necessário. |
|  |  |
| Pré-condições | O administrador deve estar logado na plataforma com permissões de acesso à interface administrativa. |
|  |  |
| Pós-condições | As contas de usuários são gerenciadas conforme as ações do administrador, e todas as alterações são registradas no sistema para auditoria e rastreamento. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador faz login na plataforma com suas credenciais de administrador. | 1. O sistema autentica o administrador e verifica suas permissões de acesso. |
| 1. O administrador navega até a área de interface administrativa. | 1. O sistema exibe a interface administrativa, incluindo uma lista de usuários com suas informações básicas e status de conta. |
| 1. O administrador seleciona um usuário específico para gerenciar. | 1. O sistema exibe as opções disponíveis para gerenciar a conta do usuário (ativar, desativar, editar informações, etc.). |
| 1. O administrador escolhe a ação desejada (por exemplo, desativar a conta do usuário) e confirma a ação. | 1. O sistema aplica a mudança na conta do usuário conforme a ação do administrador. |
|  | 1. O sistema registra a ação no log de atividades para auditoria. |
|  | 1. O sistema notifica o usuário sobre a mudança de status de sua conta, se aplicável. |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema deve garantir que apenas administradores autorizados possam acessar e gerenciar contas de usuários. |
|  | 2. O sistema deve manter um registro de todas as ações de gerenciamento realizadas pelos administradores para fins de auditoria e rastreamento. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador tenta acessar a interface administrativa sem ter as permissões necessárias. | 2. O sistema exibe uma mensagem de erro indicando que o administrador não possui as permissões necessárias para realizar a ação. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador perde a conexão com a internet durante o processo de gerenciamento. | 1. O sistema deve garantir que a ação não seja aplicada parcialmente, mantendo a conta do usuário no estado anterior até que a conexão seja restabelecida e o processo possa ser concluído corretamente. |
| **Regras de negócio** | |
| 1. Apenas administradores com as permissões adequadas podem acessar a interface administrativa e gerenciar contas de usuários. | |
| 1. Todas as ações de gerenciamento realizadas por administradores devem ser registradas em logs para auditoria e rastreamento. | |
| 1. Os usuários devem ser notificados imediatamente sobre qualquer mudança no status de suas contas, se aplicável. | |

|  |  |
| --- | --- |
| **Caso de uso 011 – Ativar/Desativar Acesso de Usuário** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um administrador pode ativar ou desativar o acesso a contas de usuários com base em comportamentos suspeitos ou violações das regras da plataforma. |
|  |  |
| Pré-condições | O administrador deve estar logado na plataforma com as permissões necessárias para gerenciar contas de usuários. |
|  |  |
| Pós-condições | O acesso à conta do usuário é ativado ou desativado conforme a ação do administrador, e o usuário é notificado sobre a mudança de status de sua conta. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador acessa a área de gerenciamento de usuários. | 3. O sistema exibe as opções para ativar ou desativar a conta do usuário. |
| 2. O administrador seleciona a conta do usuário que deseja ativar ou desativar. | 6. O sistema aplica a mudança de status à conta do usuário. |
| 4. O administrador escolhe a opção de ativar ou desativar a conta do usuário. | 7. O sistema notifica o usuário sobre a ativação ou desativação de sua conta. |
| 5. O administrador confirma a ação. | 8. O sistema registra a ação realizada pelo administrador no log de atividades. |
| **Restrições** | |
|  | **Ações do sistema** |
|  | 1. O sistema deve garantir que apenas administradores autorizados possam realizar essas ações. |
|  | 2. O sistema deve manter um registro de todas as ativações e desativações de contas para auditoria. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador tenta ativar ou desativar uma conta sem as permissões necessárias. | 2. O sistema exibe uma mensagem de erro indicando que o administrador não possui as permissões necessárias para realizar a ação. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador perde a conexão com a internet durante o processo de ativação ou desativação. | 1. O sistema deve garantir que a ação não seja aplicada parcialmente e manter a conta do usuário no estado anterior até que a conexão seja restabelecida e o processo possa ser concluído corretamente. |
| **Regras de negócio** | |
| 1. Somente administradores com as permissões adequadas podem ativar ou desativar contas de usuários. | |
| 1. O sistema deve registrar todas as ações de ativação e desativação para auditoria e rastreamento. | |
| 1. Os usuários devem ser notificados imediatamente sobre qualquer mudança no status de suas contas. | |

|  |  |
| --- | --- |
| **Caso de uso 012 – Monitorar Logs de Acesso** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso permite ao usuário administrador monitorar os logs de acesso de todos os usuários registrados. Isso inclui informações como data, hora. |
|  |  |
| Pré-condições | O usuário administrador deve estar autenticado. |
|  |  |
| Pós-condições | O sistema deve registrar a atividade do administrador para fins de auditoria. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário administrador acessa a página de monitoramento de logs de acesso. | 1. O sistema exibe uma lista dos logs de acesso mais recentes para todos os usuários registrados. |
| 1. O administrador analisa os registros para identificar qualquer atividade suspeita ou não autorizada. | 1. N/A (Neste cenário, assumimos que o administrador apenas visualiza os dados). |
| **Restrições** | |
|  | **Ações do sistema** |
|  | Todas as atividades de monitoramento realizadas pelo administrador devem ser registradas em um log de auditoria. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| **Filtrar registros:** |  |
| 1. O administrador usa filtros para restringir os registros exibidos. | 1. O sistema atualiza a lista de registros de acordo com os critérios selecionados. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador tenta acessar logs de acesso que ele não tem permissão para ver. | 1. O sistema nega o acesso e informa ao administrador que ele não tem permissão para visualizar esses registros. |
| **Regras de negócio** | |
| 1. Somente usuários com privilégios de administrador podem acessar a página de monitoramento de logs de acesso. | |
| 1. O acesso a logs sensíveis deve ser restrito e estar em conformidade com políticas de privacidade e regulamentações aplicáveis. | |

|  |  |
| --- | --- |
| **Caso de uso 013 – Gerenciar Conteúdo de Postagens** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso permite ao administrador gerenciar o conteúdo postado na rede social. O administrador pode visualizar e, ou remover postagens para garantir que todas estejam em conformidade com as diretrizes da plataforma. |
|  |  |
| Pré-condições | O administrador deve estar autenticado na plataforma com permissões de gerenciamento de conteúdo. |
|  |  |
| Pós-condições | O administrador recebe um feedback sobre o sucesso ou falha das ações realizadas, e as alterações nas postagens são registradas para auditoria. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador acessa a página de gerenciamento de conteúdo. | 1. O sistema exibe uma lista de postagens recentes ou sinalizadas para revisão. |
| 1. O administrador seleciona uma postagem para gerenciar. | 1. O sistema exibe as opções disponíveis: qualificar ou remover a postagem. |
| 1. O administrador realiza a ação desejada (qualificada ou remover). | 1. O sistema atualiza o status da postagem conforme a ação realizada pelo administrador. |
| **Restrições** | |
|  | **Ações do sistema** |
|  | Todas as alterações devem ser registradas em logs para futura auditoria e rastreamento. |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| **Pesquisa avançada:** |  |
| 1. O administrador utiliza filtros avançados de pesquisa para encontrar postagens específicas (por exemplo, por data, autor, ou palavras-chave). | 1. O sistema atualiza a lista de postagens de acordo com os critérios de pesquisa selecionados. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador tenta qualificar ou remover uma postagem que ele não tem permissão para modificar. | 1. O sistema nega a ação e informa ao administrador que ele não possui as permissões necessárias para realizar a modificação. |
| **Regras de negócio** | |
| 1. Somente administradores autenticados e autorizados podem acessar a página de gerenciamento de conteúdo e realizar ações de edição ou remoção de postagens. | |
| 1. O administrador deve seguir as diretrizes e políticas da plataforma ao tomar decisões de moderação de conteúdo. | |
| 1. Todas as ações de gerenciamento de conteúdo devem ser registradas em logs de auditoria para garantir transparência e responsabilidade. | |

|  |  |
| --- | --- |
| **Caso de uso 014 – Analisar Postagens com Modelo BERT** | |
| Ator principal | BERT |
|  |  |
| Resumo | Este caso de uso permite que o modelo BERT analise as postagens de texto enviadas pelos usuários para detectar conteúdo ofensivo. |
|  |  |
| Pré-condições | 1. O usuário deve estar autenticado. |
| 2. O sistema deve estar configurado com o modelo BERT treinado. |
|  |  |
| Pós-condições | 1. A postagem é classificada como aceitável ou ofensiva. |
| 2. A postagem ofensiva é registrada e o usuário é notificado. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário cria e envia uma nova postagem. | 1. O sistema recebe a postagem e a submete ao modelo BERT para análise. |
|  | 1. O BERT analisa a postagem para detectar conteúdo ofensivo. |
|  | 1. O sistema registra a classificação da postagem. |
|  | 1. Se a postagem for aceitável, o sistema publica a postagem. |
|  | 1. Se a postagem for ofensiva, o sistema registra a postagem como ofensiva e notifica o usuário. |
| **Restrições** | |
| Todas as análises e classificações realizadas pelo BERT devem ser registradas para auditoria futura. | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário escreve uma nova postagem. | 1. O sistema submete a nova postagem ao BERT para análise. |
|  | 1. Se a postagem for aceitável, o sistema publica a postagem. |
|  | 1. Se a postagem continuar ofensiva, o sistema registra novamente e notifica o usuário. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O BERT falha ao analisar a postagem devido a problemas técnicos. | 1. O sistema informa ao usuário que houve um erro e que a postagem não pôde ser analisada no momento. |
|  | 1. O sistema registra o erro e notifica o administrador do sistema. |
|  | 1. O sistema não publica a postagem. |
| **Regras de negócio** | |
| 1. O sistema deve submeter todas as postagens de texto ao BERT para análise antes de publicação. | |
| 1. Postagens classificadas como ofensivas não devem ser publicadas e devem ser registradas para revisão. | |
| 1. O usuário deve ser notificado imediatamente se a postagem for considerada ofensiva, com uma mensagem clara e opções para submeter uma nova postagem. | |
| 1. As ações do BERT devem ser registradas para auditoria e monitoramento contínuo da eficácia do modelo. | |

|  |  |
| --- | --- |
| **Caso de uso 015 – Notificar Usuários Sobre Conteúdo Ofensivo** | |
| Ator principal | BERT |
|  |  |
| Resumo | Este caso de uso permite que o sistema notifique os usuários quando suas postagens forem avaliadas como ofensivas pelo modelo BERT. |
|  |  |
| Pré-condições | 1. O usuário deve estar autenticado. |
| 2. O modelo BERT deve ter analisado a postagem e classificado-a como ofensiva. |
|  |  |
| Pós-condições | 1. O usuário é notificado sobre o conteúdo ofensivo de sua postagem. |
| 2. O usuário é redirecionado para a página de criação de nova postagem. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O BERT classifica a postagem do usuário como ofensiva. | 1. O sistema exibe uma mensagem de notificação ao usuário indicando que a postagem é ofensiva e não será publicada. |
|  | 1. A mensagem inclui um aviso em vermelho: "Este conteúdo não se adequa às políticas da rede social, por favor edite sua postagem." |
|  | 1. O sistema mantém a mensagem na tela por 10 segundos. |
|  | 1. Após 10 segundos, o sistema redireciona o usuário para a página de criação de nova postagem. |
| **Restrições** | |
| 1. A mensagem de notificação deve ser exibida de forma clara e destacada. | |
| 2. O redirecionamento deve ocorrer automaticamente após 10 segundos. | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta criar outra postagem enquanto a notificação está sendo exibida. | 1. O sistema bloqueia a criação de novas postagens até que o redirecionamento ocorra. |
|  | 1. O sistema exibe uma mensagem adicional informando que o usuário deve esperar até ser redirecionado. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
|  | 1. O sistema falha ao exibir a mensagem de notificação. |
|  | 2. O sistema registra o erro e notifica o administrador do sistema. |
| 3. O usuário é redirecionado diretamente para a página de criação de nova postagem sem ver a mensagem de notificação. |  |
| **Regras de negócio** | |
| 1. A notificação deve ser clara e compreensível para garantir que o usuário entenda por que a postagem foi rejeitada. | |
| 1. O redirecionamento automático após 10 segundos deve garantir que o usuário tenha tempo suficiente para ler a mensagem. | |
| 1. Todas as notificações e ações relacionadas a postagens ofensivas devem ser registradas para auditoria e revisão administrativa. | |
| 1. A interface de notificação deve ser responsiva e funcionar de maneira consistente em todos os dispositivos e navegadores suportados. | |

|  |  |
| --- | --- |
| **Caso de uso 016 – Permitir Criação de Novas Postagens após Notificação de Conteúdo Ofensivo** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso permite que os usuários criem uma nova postagem após serem notificados de que sua postagem anterior foi considerada ofensiva pelo modelo BERT. |
|  |  |
| Pré-condições | 1. O usuário deve estar autenticado. |
| 2. O usuário deve ter sido notificado de que sua postagem anterior foi considerada ofensiva. |
|  |  |
| Pós-condições | 1. O usuário cria e envia uma nova postagem. |
| 2. A nova postagem é submetida ao modelo BERT para análise. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário é notificado de que sua postagem foi considerada ofensiva. | 1. O sistema exibe a notificação com a mensagem: "Este conteúdo não se adequa às políticas da rede social, por favor faça outra postagem." |
|  | 3. O sistema mantém a mensagem na tela por 10 segundos e redireciona o usuário para a página de criação de nova postagem. |
|  |  |
| 4. O usuário acessa a página de criação de nova postagem. | 5. O sistema exibe o editor de postagens para o usuário. |
| 6. O usuário cria uma nova postagem. | 7. O sistema recebe a nova postagem e a submete ao modelo BERT para análise. |
|  | 8. O BERT analisa a nova postagem e classifica o conteúdo. |
|  | 9. O sistema publica a postagem se ela for aceitável ou notifica o usuário novamente se for considerada ofensiva. |
| **Restrições** | |
| O sistema deve garantir que a nova postagem seja submetida ao BERT para análise antes de ser publicada. | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário opta por não criar uma nova postagem imediatamente após ser redirecionado. | 1. O sistema mantém o estado do redirecionamento até que o usuário decida criar uma nova postagem ou saia da página. |
| 3. O usuário retorna posteriormente para criar uma nova postagem. | 4. O sistema exibe o editor de postagens quando o usuário retorna à página. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
|  | 1. O sistema falha ao redirecionar o usuário para a página de criação de nova postagem. |
|  | 2. O sistema exibe uma mensagem de erro e solicita ao usuário que tente acessar a página de criação de nova postagem manualmente. |
|  | 3. O sistema registra o erro e notifica o administrador do sistema. |
| **Regras de negócio** | |
| 1. O usuário deve ser notificado de maneira clara e compreensível sobre a necessidade de criar uma nova postagem após a rejeição da postagem anterior. | |
| 1. O sistema deve garantir que toda nova postagem criada após uma notificação de conteúdo ofensivo seja analisada pelo BERT antes de ser publicada. | |
| 1. Todas as ações relacionadas à criação de novas postagens após notificações de conteúdo ofensivo devem ser registradas para auditoria e revisão administrativa. | |
| 1. A interface de criação de postagens deve ser responsiva e funcionar de maneira consistente em todos os dispositivos e navegadores suportados. | |

|  |  |
| --- | --- |
| **Caso de uso 017 – Registrar Postagens Ofensivas** | |
| Ator principal | BERT |
|  |  |
| Resumo | Este caso de uso permite que o sistema registre todas as postagens consideradas ofensivas pelo modelo BERT. |
|  |  |
| Pré-condições | 1. O usuário deve estar autenticado. |
| 2. O modelo BERT deve ter analisado a postagem e classificado-a como ofensiva. |
|  |  |
| Pós-condições | 1. A postagem ofensiva é registrada no sistema para revisão futura. |
| 2. O administrador pode acessar os registros das postagens ofensivas para revisão. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário cria e envia uma nova postagem. | 1. O sistema recebe a postagem e a submete ao modelo BERT para análise. |
|  | 3. O BERT analisa a postagem e a classifica como ofensiva. |
|  | 4. O sistema registra a postagem ofensiva no log de postagens ofensivas, incluindo detalhes como o conteúdo da postagem, o autor e a data/hora. |
|  | 5. O sistema notifica o usuário que a postagem foi considerada ofensiva e não será publicada. |
| **Restrições** | |
| O sistema deve registrar todas as postagens consideradas ofensivas de maneira detalhada e segura. | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário edita e reenvia uma postagem previamente rejeitada. | 1. O sistema submete a postagem editada ao BERT para uma nova análise. |
|  | 3. O BERT reanalisa a postagem e, se ainda for considerada ofensiva, o sistema registra novamente a postagem editada no log de postagens ofensivas. |
|  | 4. O sistema notifica o usuário novamente que a postagem continua ofensiva e não será publicada. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
|  | 1. O sistema falha ao registrar a postagem ofensiva. |
|  | 2. O sistema exibe uma mensagem de erro para o administrador e registra o erro no log do sistema. |
|  | 3. O administrador do sistema é notificado sobre a falha no registro da postagem ofensiva. |
| **Regras de negócio** | |
| 1. Todas as postagens consideradas ofensivas pelo modelo BERT devem ser registradas no sistema para auditoria e revisão futura. | |
| 1. O registro das postagens ofensivas deve incluir detalhes como o conteúdo da postagem, o autor, a data/hora e a razão da classificação como ofensiva. | |
| 1. O sistema deve garantir a segurança e a integridade dos dados registrados, utilizando criptografia e políticas de controle de acesso. | |
| 1. O administrador deve ter acesso aos registros de postagens ofensivas para monitorar e tomar ações corretivas conforme necessário. | |

|  |  |
| --- | --- |
| **Caso de uso 018 – Fornecer Relatórios Sobre Postagens Filtradas** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso permite que o sistema forneça relatórios detalhados sobre as postagens que foram filtradas pelo modelo BERT, classificadas como ofensivas. |
|  |  |
| Pré-condições | 1. O usuário deve estar autenticado. |
| 2. O sistema deve ter registros de postagens filtradas pelo modelo BERT. |
|  |  |
| Pós-condições | 1. O administrador recebe um relatório detalhado das postagens filtradas. |
| 2. O administrador pode tomar ações baseadas nas informações fornecidas nos relatórios. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador acessa a seção de relatórios de postagens filtradas. | 2. O sistema exibe opções de filtro para gerar relatórios detalhados. |
| 3. O administrador seleciona os critérios de filtragem desejados (por exemplo, período de tempo, tipo de conteúdo ofensivo). | 4. O sistema gera um relatório baseado nos critérios selecionados. |
| 5. O administrador solicita a visualização do relatório. | 6. O sistema exibe o relatório detalhado, incluindo informações como o conteúdo das postagens, o autor, a data/hora e a razão da classificação como ofensiva. |
| 7. O administrador revisa o relatório e toma ações corretivas se necessário. | 8. O sistema registra as ações tomadas pelo administrador para auditoria futura. |
| **Restrições** | |
| O sistema deve garantir que apenas administradores autenticados possam acessar os relatórios detalhados. | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador exporta o relatório para análise offline. | 2. O sistema gera um arquivo (por exemplo, CSV, PDF) com o relatório detalhado. |
| 3. O administrador faz download do arquivo gerado. | 4. O sistema registra a exportação do relatório para auditoria futura. |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
|  | 1. O sistema falha ao gerar o relatório solicitado pelo administrador. |
|  | 2. O sistema exibe uma mensagem de erro e solicita ao administrador que tente novamente. |
|  | 3. O sistema registra o erro e notifica o administrador do sistema. |
| **Regras de negócio** | |
| 1. O sistema deve permitir que administradores filtrem e gerem relatórios detalhados sobre postagens filtradas pelo modelo BERT. | |
| 1. Os relatórios devem incluir informações completas e precisas, como conteúdo das postagens, autores, datas/horas e razões para a classificação como ofensiva. | |
| 1. O acesso aos relatórios deve ser restrito a administradores autenticados para garantir a segurança e a privacidade dos dados. | |
| 1. Todas as ações relacionadas à geração, visualização e exportação de relatórios devem ser registradas para auditoria e monitoramento. | |

|  |  |
| --- | --- |
| **Caso de uso 019 – Denunciar Postagens** | |
| Ator principal | Usuário |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual um usuário pode denunciar postagens que considere inadequadas ou ofensivas. A denúncia é então encaminhada para análise dos administradores, que tomarão as ações corretivas necessárias. |
|  |  |
| Pré-condições | O usuário deve estar logado na plataforma. |
|  |  |
| Pós-condições | A denúncia é registrada no sistema e encaminhada para a análise dos administradores. O usuário que fez a denúncia pode receber um feedback confirmando que a denúncia foi enviada. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário navega pela rede social e encontra uma postagem que considera inadequada ou ofensiva. | 2. O sistema exibe as opções de interação com a postagem, incluindo a opção de "Denunciar". |
| 3. O usuário clica na opção "Denunciar". | 4. O sistema solicita ao usuário que selecione um motivo para a denúncia a partir de uma lista de opções (por exemplo, conteúdo ofensivo, spam etc.). |
| 5. O usuário seleciona o motivo da denúncia e confirma a ação. | 6. O sistema registra a denúncia e encaminha a informação para a análise dos administradores. |
|  | 7. O sistema exibe uma mensagem de confirmação ao usuário, informando que a denúncia foi recebida e está sendo analisada. |
| **Restrições** | |
|  | **Ações do Sistema** |
|  | 1. O sistema deve permitir apenas que usuários logados denunciem postagens. |
|  | 1. O sistema deve registrar todas as denúncias em um log para auditoria e rastreamento. |
|  | 1. A denúncia deve ser encaminhada automaticamente para a fila de análise dos administradores. |
|  | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário acidentalmente seleciona a opção "Denunciar" mas decide não prosseguir. | 2. O sistema permite que o usuário cancele a ação de denúncia antes de confirmá-la, sem registrar a denúncia. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O usuário tenta denunciar uma postagem mas não consegue completar a ação devido a problemas de conexão. | 2. O sistema informa ao usuário que a denúncia não pôde ser registrada devido a um problema técnico e sugere tentar novamente mais tarde. |
|  |  |
| **Regras de negócio** | |
| 1. Somente usuários logados podem denunciar postagens. | |
| 1. Todas as denúncias devem ser analisadas por administradores, que tomarão as ações corretivas necessárias conforme as políticas da plataforma. | |
| 1. O sistema deve garantir que cada denúncia seja única para evitar múltiplas denúncias desnecessárias sobre a mesma postagem. | |
| 1. A denúncia não deve resultar em ação imediata (como a remoção automática da postagem), mas deve ser submetida à revisão dos administradores. | |

|  |  |
| --- | --- |
| **Caso de uso 019 – Gerenciar Contas Administrativas** | |
| Ator principal | Administrador |
|  |  |
| Resumo | Este caso de uso descreve o processo pelo qual a conta inicial de administrador ou um administrador com privilégios equivalentes pode criar, modificar, suspender ou remover outras contas administrativas. O caso de uso também abrange a segurança no armazenamento de credenciais e a auditoria de todas as ações realizadas. |
|  |  |
| Pré-condições | O administrador deve estar logado na plataforma com privilégios máximos. |
|  |  |
| Pós-condições | As contas administrativas são gerenciadas conforme as ações do administrador, e todas as atividades são registradas em logs de auditoria para rastreamento e conformidade. |
|  |  |
| **Cenário principal** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador acessa a interface de gerenciamento de contas administrativas. | 2. O sistema exibe uma lista de contas administrativas existentes e opções para gerenciar essas contas. |
| 3. O administrador seleciona a opção para criar uma nova conta administrativa. | 4. O sistema solicita ao administrador que insira as informações necessárias para a nova conta (nome, email, privilégios, etc.). |
| 5. O administrador insere as informações e define as credenciais iniciais. | 6. O sistema aplica o hashing à senha e armazena as credenciais com segurança. |
| 7. O administrador finaliza a criação da conta e configura a autenticação multifator (MFA) se necessário. | 8. O sistema cria a nova conta, registra a ação no log de auditoria e confirma a criação ao administrador. |
| 9. O administrador decide modificar uma conta administrativa existente. | 10. O sistema exibe as opções de modificação (alterar privilégios, redefinir senha, ativar/desativar MFA, suspender conta, etc.). |
| 1. O administrador realiza as modificações necessárias. | 1. O sistema aplica as modificações, registra a ação no log de auditoria e notifica o administrador da conclusão. |
| **Restrições** | |
|  | **Ações do Sistema** |
|  | 1. Somente a conta inicial de administrador ou administradores com privilégios máximos podem acessar e gerenciar contas administrativas. |
|  | 1. Todas as ações de gerenciamento de contas devem ser registradas em logs de auditoria para futura revisão e conformidade. |
|  | 1. O sistema deve garantir que as senhas sejam armazenadas de maneira segura, utilizando hashing, e que MFA possa ser configurado para todas as contas administrativas. |
|  | |
| **Cenário alternativo** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador utiliza a interface para redefinir sua própria senha. | 2. O sistema solicita a confirmação de identidade através de MFA antes de permitir a redefinição da senha. |
| 3. O administrador confirma sua identidade e redefine a senha. | 4. O sistema aplica o hashing à nova senha, atualiza as credenciais e registra a ação no log de auditoria. |
|  |  |
| **Cenário de exceção** | |
| **Ações do ator** | **Ações do sistema** |
| 1. O administrador tenta criar ou modificar uma conta administrativa, mas não possui privilégios máximos. | 2. O sistema impede a ação e exibe uma mensagem de erro, indicando que o administrador não possui as permissões necessárias. |
|  |  |
| **Regras de negócio** | |
| 1. Apenas a conta inicial de administrador ou administradores com privilégios máximos podem criar, modificar, suspender ou remover outras contas administrativas. | |
| 1. As credenciais de todas as contas administrativas devem ser armazenadas de maneira segura, utilizando técnicas de hashing, e devem oferecer suporte à autenticação multifator (MFA). | |
| 1. Todas as ações realizadas por administradores na interface de gerenciamento de contas administrativas devem ser registradas em logs de auditoria para garantir a transparência e conformidade com as políticas da plataforma. | |
| 1. Administradores devem ter a capacidade de redefinir suas senhas e ativar ou desativar a autenticação multifator (MFA) para aumentar a segurança da conta. | |

# 6. MODELOS DO SISTEMA

## 6.1. Diagrama de Casos de Uso

Diagrama

Descrição gerada automaticamente

## 6.2. Diagrama de Classes

Diagrama, Desenho técnico, Esquemático

Descrição gerada automaticamente

## 6.3. Entidades de Relacionamento

Imagem

# 7. EVOLUÇÃO DO SISTEMA

... (possíveis atualizações, adições de novas funcionalidades, etc.)

# 8. GLOSSÁRIO

* **Autenticação Multifator (MFA):** Método de segurança que exige mais de uma forma de verificação antes de conceder acesso a uma conta.
* **Denúncia:** Ação realizada por um usuário para reportar uma postagem como inadequada ou ofensiva, para ser analisada por administradores.
* **Inteligência Artificial:** Mecanismos automatizados, como o modelo BERT, usados para analisar e detectar postagens ofensivas no sistema.
* **Log de Acesso:** Histórico de acessos de um usuário, registrando datas e horas de login na plataforma.
* **Perfil:** Conjunto de informações visíveis publicamente sobre um usuário, incluindo biografia e postagens.
* **Postagem:** Conteúdo publicado por um usuário em seu perfil, visível por todos na rede social.
* **Postagem Ofensiva:** Postagem identificada pelo modelo BERT ou denunciada pelos usuários por violar as políticas da plataforma.
* **Usuário:** Indivíduo registrado na plataforma que pode postar e interagir com outros perfis.
* **Usuário Administrador:** Usuário com permissões elevadas para gerenciar contas e conteúdo dentro do sistema.

# 9. FERRAMENTAS UTILIZADAS

Este capítulo descreve as ferramentas escolhidas para o desenvolvimento, implementação e manutenção do protótipo da rede social Bem-te-vi, delineando como cada uma contribui para a realização dos objetivos específicos do projeto. A seleção dessas ferramentas visa estabelecer um ambiente de desenvolvimento robusto, eficiente e adaptado às necessidades específicas do sistema.

***Laravel*:** é um *Framework* PHP para desenvolvimento *web* que segue o padrão arquitetural MVC (*Model-View-Controller*). Ele será utilizado para construir a estrutura básica da rede social, oferecendo uma rica biblioteca de funcionalidades que facilitam tarefas comuns como autenticação de usuários, roteamento, sessões e *caching*. A escolha do *Laravel* permite um desenvolvimento ágil e uma manutenção simplificada do código, o que é crucial para a adaptação rápida às necessidades de moderação de conteúdo e segurança.

***Laragon*:** é um ambiente de desenvolvimento portátil e isolado que facilita a gestão de serviços como *Apache*, *My*SQL e PHP no desenvolvimento local. Será utilizado para configurar rapidamente um ambiente de desenvolvimento consistente entre todos os membros da equipe, minimizando possíveis inconsistências entre diferentes ambientes de desenvolvimento.

***Maria*DB e *Heidi*SQL:** *Maria*DB, um sistema de gerenciamento de banco de dados derivado do *MySQL*, será usado para armazenar e gerenciar todas as informações da rede social. *Heidi*SQL, uma interface gráfica para gestão de bases de dados, será usada para facilitar a visualização e manipulação dos dados. Esta combinação permite um gerenciamento eficiente dos dados com alta performance, segurança e escalabilidade.

***Visual Studio Code*:** é um editor de código fonte leve, mas poderoso, que suporta uma variedade de linguagens de programação e *Frameworks*, incluindo PHP e *Laravel*. Ele é usado por programadores para escrever e revisar o código de forma eficiente, com suporte a extensões que melhoram a produtividade e a colaboração, como correção de código e controle de versão integrado.

***Bulma* *Framework*:** é um *Framework* CSS baseado em *Flexbox* que será utilizado para a construção das interfaces do usuário. Com sua abordagem modular e fácil de usar, o *Bulma* permite um desenvolvimento rápido e responsivo do *front-end*, assegurando que a rede social seja acessível em diversos dispositivos e tamanhos de tela.

***Visual Paradigm Online*:** é uma ferramenta utilizada para a criação de diagramas de casos de uso e classes, facilitando a visualização das estruturas de dados e fluxos de trabalho do sistema. *Visual Paradigm Online* ajuda a manter a documentação do projeto clara e atualizada, essencial para o alinhamento da equipe e para futuras revisões do projeto.

***Trello*:** é uma ferramenta de gerenciamento de projetos baseada em *Kanban*, será usada para organizar as tarefas de desenvolvimento, monitorar o progresso e priorizar atividades. Facilita a comunicação e colaboração entre os membros da equipe, garantindo que todos estejam alinhados com os objetivos do projeto.

***Git* e *GitHub*:** esteserá usado para controle de versão, permitindo que múltiplos desenvolvedores trabalhem simultaneamente no código sem conflitos. *GitHub*, uma plataforma de hospedagem de código-fonte, será usada para armazenar o repositório do projeto, facilitar revisões de código, rastrear problemas e gerenciar atualizações. Essas ferramentas são essenciais para a colaboração efetiva e para manter um histórico detalhado das mudanças no código.

Estas ferramentas foram selecionadas não apenas por suas capacidades individuais, mas também pela forma como se integram para criar um ambiente de desenvolvimento coeso e eficaz, diretamente alinhado com os objetivos específicos do projeto Bem-te-vi, especialmente no que tange à criação de um ambiente virtual seguro e amigável para compartilhamento de mensagens.

# 10. BOAS PRÁTICAS

A adoção de boas práticas de desenvolvimento é crucial para garantir a qualidade, a manutenção e a escalabilidade do código no projeto da rede social Bem-te-vi. Este capítulo detalha as práticas adotadas pelos autores para promover um código limpo, bem documentado e fácil de manter.

**Guia de Estilo de Codificação (PSR-1/PSR-2 para PHP):** a adesão aos padrões PSR-1 e PSR-2 é fundamental para garantir a uniformidade e legibilidade do código PHP utilizado no projeto. O PSR-1 estabelece normas básicas de codificação, como o uso de *tags* de fechamento PHP, a codificação de caracteres UTF-8 sem BOM para arquivos PHP, e nomes de classes em *StudlyCaps*. Por sua vez, o PSR-2 trata de aspectos de formatação, como a indentação por quatro espaços (sem uso de tabulações), linhas com no máximo 120 caracteres, e colocação de chaves seguindo o estilo K&R.A implementação desses guias de estilo ajuda a manter o código organizado e consistente, facilitando a revisão por outros desenvolvedores e contribuindo para um ambiente de trabalho colaborativo mais eficiente. Além disso, a consistência promovida pelos padrões PSR facilita a detecção e correção de erros, melhorando a qualidade geral do *software*.

***DocBlock* para PHP:** O uso de *DocBlock* é essencial para a documentação no código PHP. *DocBlock* é um formato de comentário de múltiplas linhas que é colocado antes das declarações de classes, métodos e funções para descrever o comportamento, os parâmetros, os retornos e as exceções desses componentes de *software*. A prática de utilizar *DocBlock* permite que ferramentas de geração de documentação automática, como phpDocumentor, criem uma documentação de API detalhada e acessível. A documentação de código com *DocBlock* é especialmente importante em um projeto colaborativo como o Bem-te-vi, onde os desenvolvedores podem trabalhar em diferentes partes do sistema. Com uma documentação clara e acessível, os membros da equipe podem entender rapidamente a funcionalidade e o propósito do código existente, facilitando a integração e a continuidade do desenvolvimento. Além disso, uma boa documentação é crucial para a manutenção a longo prazo do sistema, permitindo que alterações e expansões sejam realizadas com segurança e eficácia.

Adotar essas práticas de desenvolvimento não apenas melhora a qualidade do código, mas também fomenta uma cultura de desenvolvimento disciplinado e comprometido com a qualidade entre os programadores, elementos essenciais para o sucesso do projeto da rede social Bem-te-vi.