**ANÁLISE DE REQUISITOS**

A análise de requisitos nos permite identificar às reais necessidades de um sistema proposto, bem como suas regras de negócio. Dessa forma fica claro à equipe de desenvolvimento qual o propósito do desenvolvimento.

**Requisitos Funcionais:**

Os requisitos estão relacionados ao Gerenciamento do Modelo de Segurança existente no contexto onde a solução será instalada.

|  |
| --- |
| Necessidade |
| Gerenciar Modelo de Segurança |
| Descrição |
| O sistema deverá permitir o gerenciamento do modelo de segurança, no âmbito de grupos de usuários e permissões. |
| Requisitos Funcionais |
| RF01: Gerenciar Grupo;  RF02: Gerenciar Permissão;  RF03: Visualizar Modelo de Segurança; |

**Requisitos Não-Funcionais**

* O sistema deverá ser construído como uma Web Part da plataforma web do Sharepoint;
* Apenas usuários autenticados e membros do grupo Administrativo poderão acessar a Web Part;
* A visualização dos dados do Modelo de Segurança deverá apresentar um tempo de resposta de, preferencialmente, até 3 segundos;

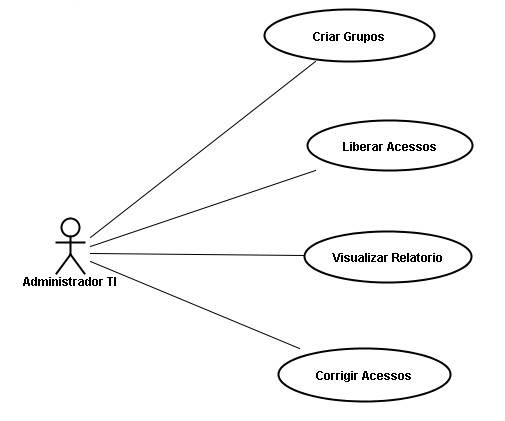
**Regras de Negócio:**

1. Não deverá ser permitido criação de grupos com duplicação de nome.
2. Na configuração da webpart deverá ser informado os seguintes dados abaixo:
   1. String de conexão: dados de conexão do banco de dados de conteúdo da aplicação web que se deseja gerenciar;
   2. Login: login do usuário administrador do ambiente SharePoint; e
   3. Senha: senha do usuário informado no campo Login.
3. Edição da tela de Permissão deverá exibir campos <campos> bloqueados e apenas o campo Nível de Permissão liberado para seleção.

**MODELAGEM DE REQUISITOS**

**Casos de Usos:**

Casos de uso são narrativas em texto que descrevem uma unidade funcional. Elas são utilizadas, principalmente para encontrar e registrar requisitos funcionais nos sistemas.



**RF01. GERENCIAR GRUPO**

**Caso de Uso – Gerenciar Grupo**

**Descrição**

Esse caso de uso permite ao usuário gerenciar grupos, e seus membros, presentes o modelo de segurança do ambiente SharePoint.

**Atores**

* Administrador TI

**Pré-Condições**

* Web Part implantada numa página no ambiente SharePoint;
* Usuário autenticado.

**Fluxo Básico: Adicionar Grupo de Segurança**

Esse caso de uso é iniciado após o Administrador indicar a intenção de adicionar um novo grupo de segurança:

1. Usuário seleciona a aba *Administração* e expande a seção *Grupos*;
2. Sistema exibe a relação de grupos existente no modelo de segurança; **[A1]**
3. Usuário aciona o botão *Adicionar Novo Grupo*;
4. Sistema exibe tela de cadastro com os campos Nome, Descrição, Proprietário do Grupo e Permissão (a ser concedida no site raiz); **[RN01]**
5. Usuário preenche informações e aciona o botão *Criar*;
6. Sistema cria o novo grupo e adiciona a permissão no site raiz;
7. Caso de uso se encerra;

**Fluxo Alternativo A1: Visualizar Membros**

No passo 2 do fluxo básico, o usuário seleciona um dos grupos exibidos:

1. Sistema exibe a relação de usuários pertencentes ao grupo; **[A2][A3]**
2. Caso de uso se encerra;

**Fluxo Alternativo A2: Adicionar Membros**

No passo 1 do fluxo alternativo A1, usuário aciona o botão *Adicionar Novo Usuário*:

1. Sistema exibe a relação de usuários pertencentes ao grupo;
2. Sistema exibe tela de cadastro com o campo Usuário;
3. Usuário preenche informações e aciona o botão *Criar*;
4. Sistema associa o usuário ao grupo selecionado;
5. Caso de uso se encerra;

**Fluxo Alternativo A3: Remover Membro**

No passo 1 do fluxo alternativo A1, usuário aciona o botão *Remover Usuário* do usuário que deseja remover:

1. Sistema exibe uma pop-up que confirmação de exclusão;
2. Usuário confirma a ação;
3. Sistema remove o usuário do grupo selecionado;
4. Caso de uso se encerra;

**Pós-Condições**

Não é relevante.

**Requisitos Não-Funcionais**

Interface web.

**RF02. GERENCIAR PERMISSÃO**

**Caso de Uso – Gerenciar Permissão**

**Descrição**

Esse caso de uso permite ao usuário gerenciar as permissões concedidas à sites no ambiente SharePoint.

**Atores**

* Administrador TI

**Pré-Condições**

* Web Part implantada numa página no ambiente SharePoint;
* Usuário autenticado.

**Fluxo Básico: Visualizar Permissões**

Esse caso de uso é iniciado após o Administrador indicar a intenção de visualizar as permissões de um determinado site:

1. Usuário seleciona a aba *Administração* e expande a seção *Permissões*;
2. Sistema exibe a hierarquia de sites existente no modelo de segurança;
3. Usuário seleciona um site;
4. Sistema exibe os grupos que possuem permissão no site selecionado, bem como qual permissão possui; **[A1][A2]**
5. Caso de uso se encerra.

**Fluxo Alternativo A1: Adicionar Permissão**

No passo 4 do fluxo básico, usuário aciona o botão *Adicionar Permissão*:

1. Sistema exibe tela de cadastro com os campos *Grupo* e *Permissão*;
2. Usuário preenche informações e aciona o botão *Salvar*;
3. Sistema associa o grupo ao site selecionado;
4. Caso de uso se encerra;

**Fluxo Alternativo A2: Editar Permissão**

No passo 4 do fluxo básico, usuário aciona o botão *Remover Permissão* do grupo que deseja remover:

1. Sistema exibe uma pop-up que confirmação de exclusão;
2. Usuário confirma a ação;
3. Sistema remove o grupo do site selecionado;
4. Caso de uso se encerra;

**Pós-Condições**

Não é relevante.

**Requisitos Não-Funcionais**

Interface web.

**RF03. GERENCIAR MODELO DE SEGURANÇA**

**Caso de Uso – Visualizar Modelo de Segurança**

**Descrição**

Esse caso de uso permite ao usuário consultar o modelo de segurança (permissões atribuídas à usuários e grupos) aos sites de uma aplicação web, existentes no ambiente SharePoint.

**Atores**

* Administrador TI

**Pré-Condições**

* Web Part implantada numa página no ambiente SharePoint;
* Usuário autenticado.

**Fluxo Básico: Visualizar Permissões**

Esse caso de uso é iniciado após o Administrador indicar a intenção de visualizar permissões:

1. Usuário acessa a aba *Relatório* da página onde a Web Part foi implantada;
2. Sistema exibe uma tabela com todas as permissões de usuários e grupos em sites presentes numa aplicação web (web application); **[A1]**
3. Caso de uso se encerra;

**Fluxo Alternativo A1: Filtrar Permissões**

No passo 2 do fluxo básico, o usuário indica a intenção de Filtrar Permissões:

1. Usuário marca os itens que deseja filtrar de cada filtro (*Grupos, Usuários, Permissões e Sites*);
2. Sistema atualiza a tabela de permissões filtrando com as informações marcadas;
3. Caso de uso se encerra;

**Pós-Condições**

Não é relevante.

**Requisitos Não-Funcionais**

* Interface web;
* Tempo de Resposta em torno de 7 segundos.

**RF03. GERENCIAR MODELO DE SEGURANÇA**

**Caso de Uso – Exportar Modelo de Segurança**

**Descrição**

Esse caso de uso permite ao usuário exportar o modelo de segurança (permissões atribuídas à usuários e grupos) aos sites de uma aplicação web, existentes no ambiente SharePoint.

**Atores**

* Administrador TI

**Pré-Condições**

* Web Part implantada numa página no ambiente SharePoint;
* Usuário autenticado.

**Fluxo Básico: Exportar Modelo**

Esse caso de uso é iniciado após o Administrador indicar a intenção de Exportar o Modelo de Segurança:

1. Usuário acessa a aba *Relatório* da página o site onde a Web Part foi implantada;
2. Sistema exibe todas as permissões de usuários e grupos em sites presentes numa aplicação web (web application);
3. Usuário aciona o botão de exportar dados;
4. Sistema efetua o download de um arquivo excel com os dados exibidos na tela;
5. Caso de uso se encerra;

**Pós-Condições**

Não é relevante.

**Requisitos Não-Funcionais**

* Interface web;

**Prototipação:**

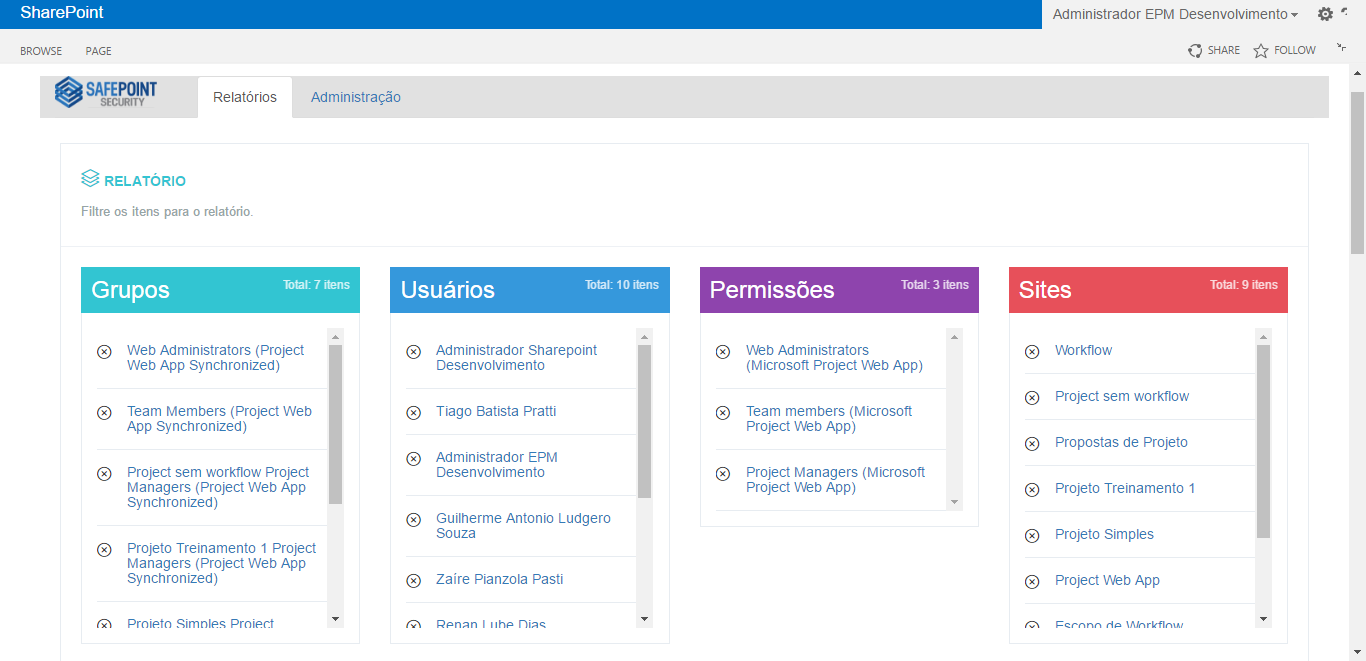


Figura 1: Aba Relatório - Filtros

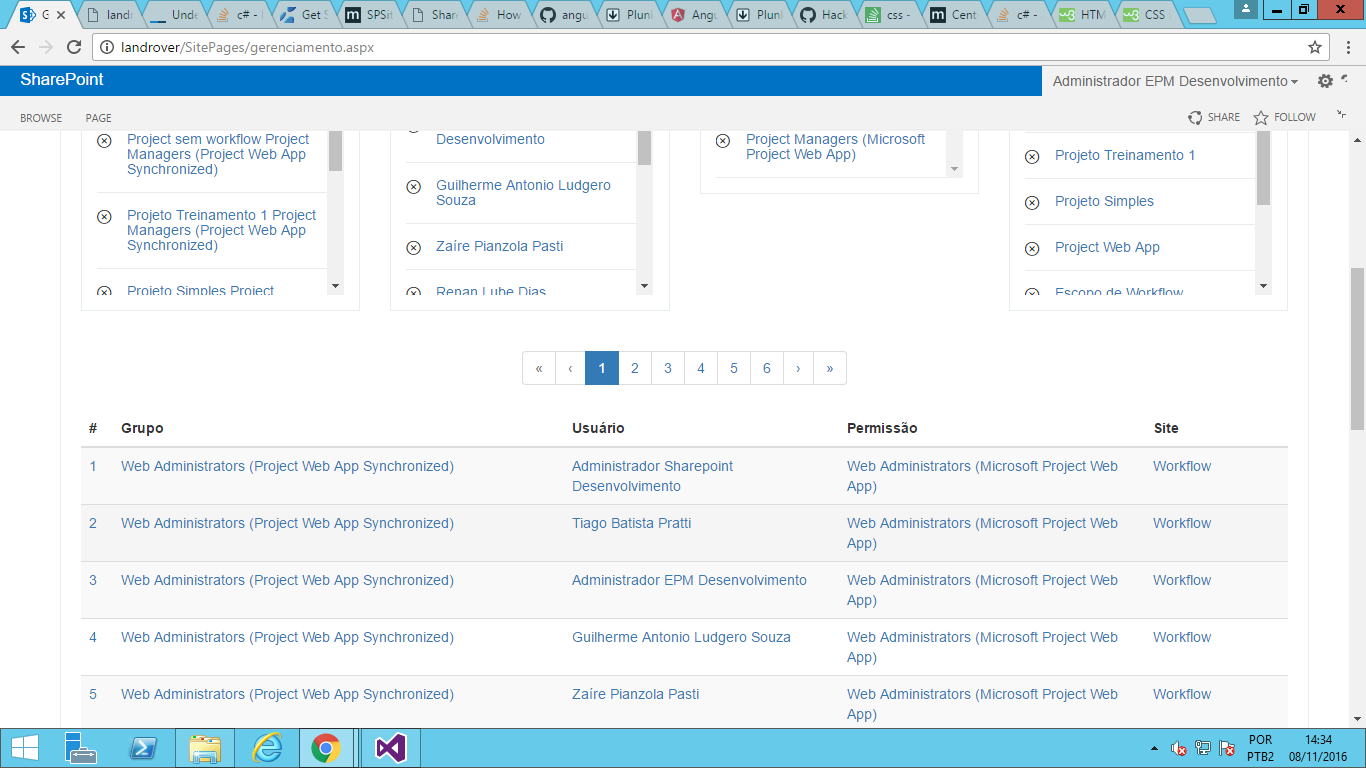


Figura 2: Aba Relatório: Tabela com modelo de segurança

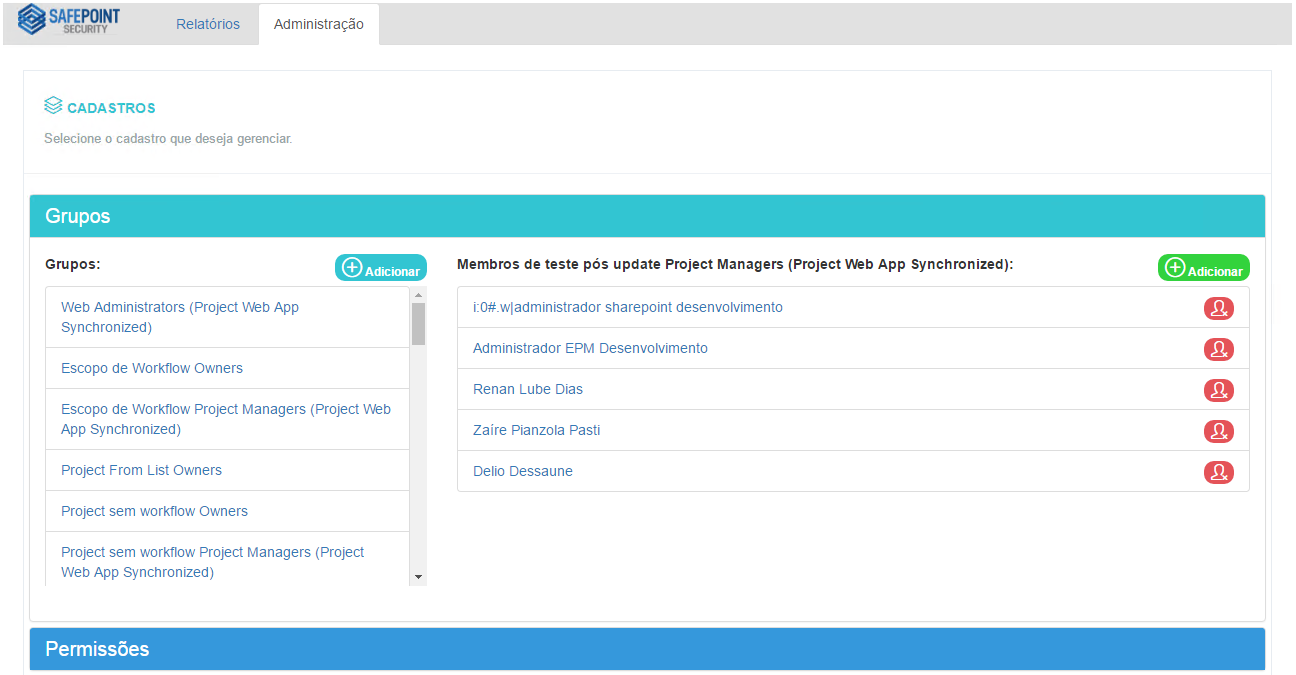


Figura 3: Aba Administração: Gerenciamento de Grupos

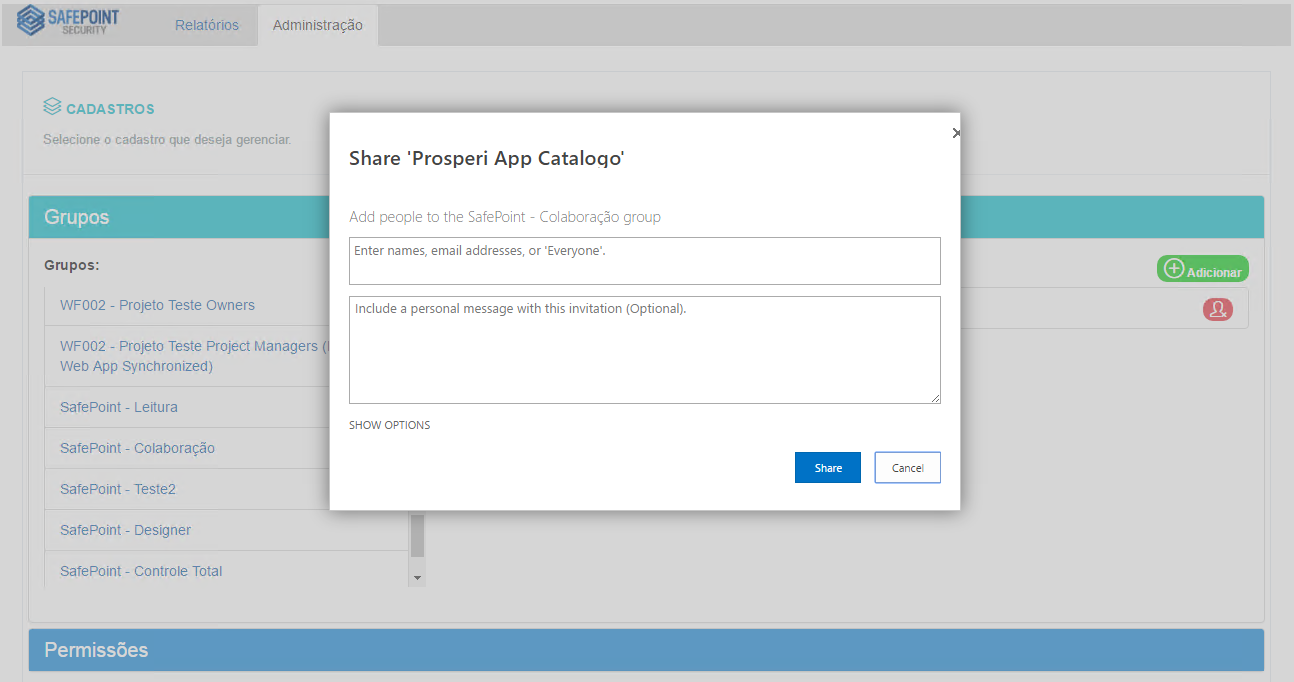


Figura 4: Aba Administração: Adicionar Membros

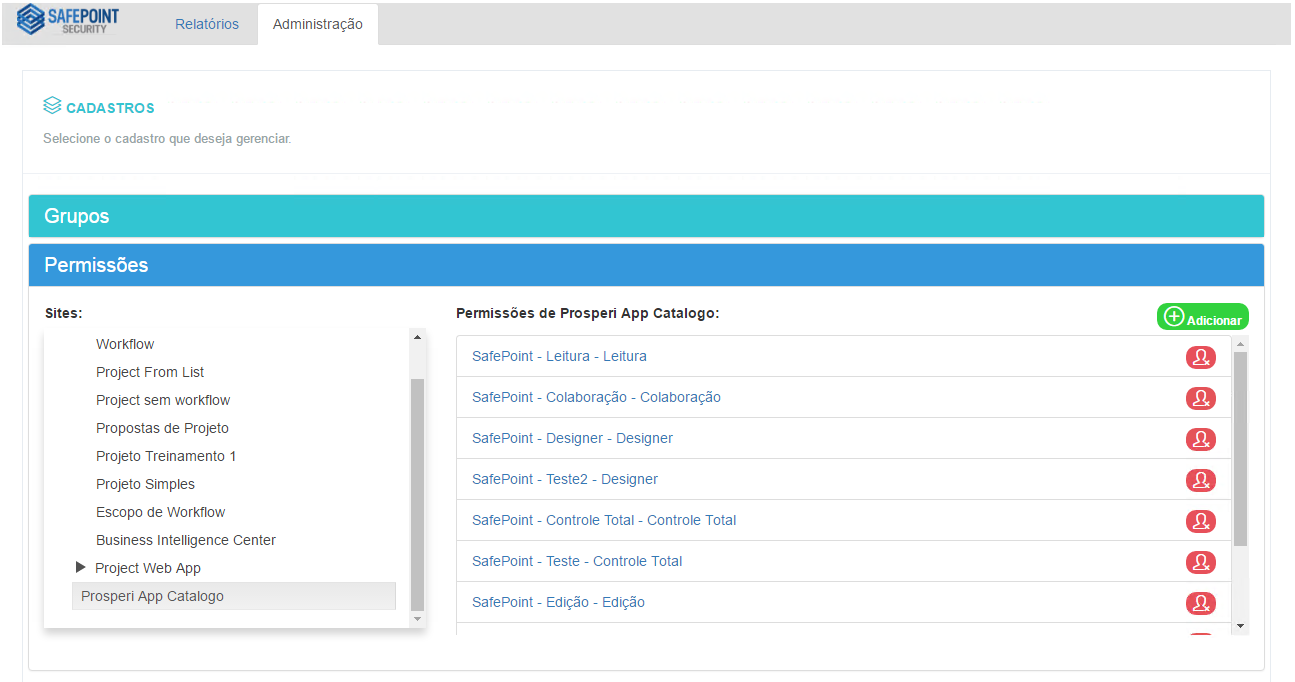


Figura 5: Aba Administração: Gerenciamento de Permissões

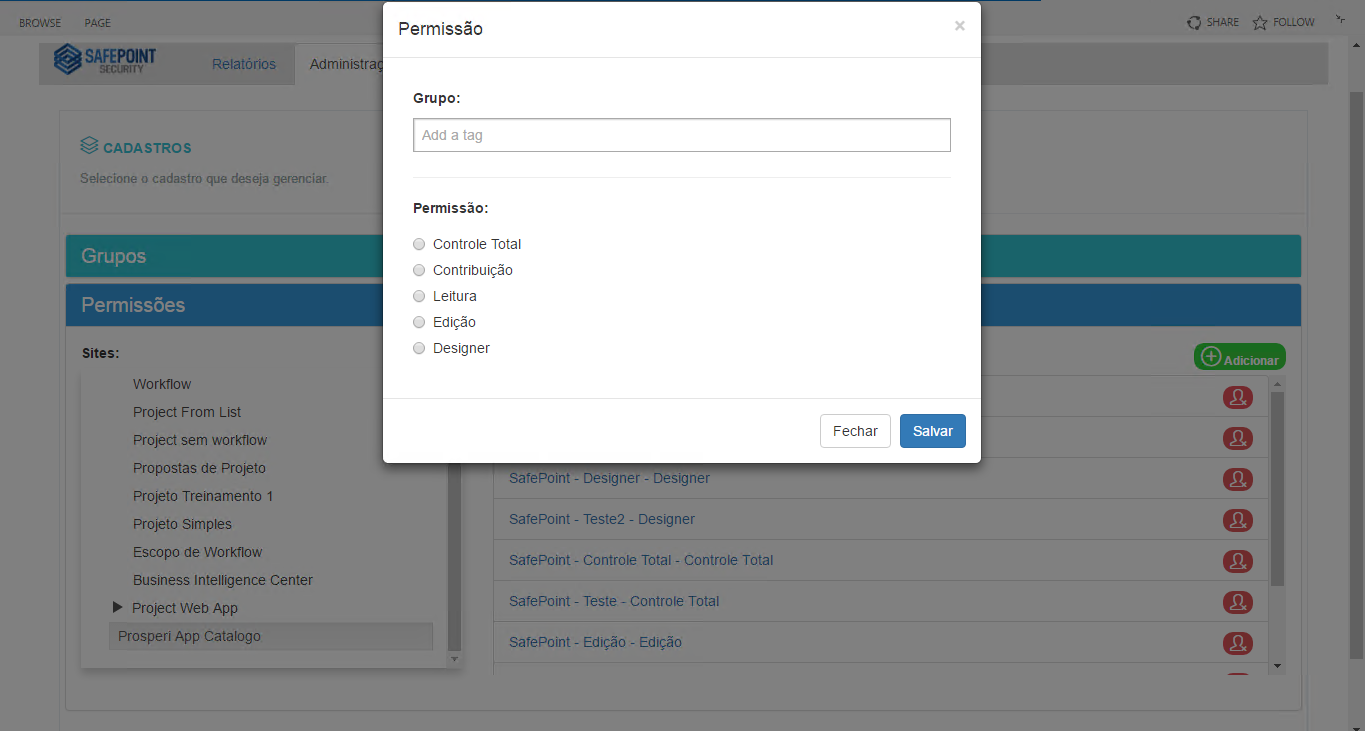
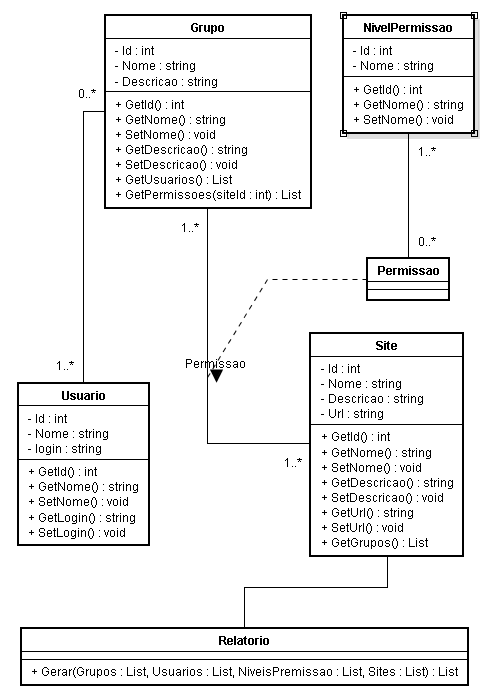


Figura 6: Aba Administração: Adicionar Permissão

**Diagrama de Classes:**

Um diagrama de classe UML descreve, sem referência de implementação específica, um objeto e as informações do sistema.

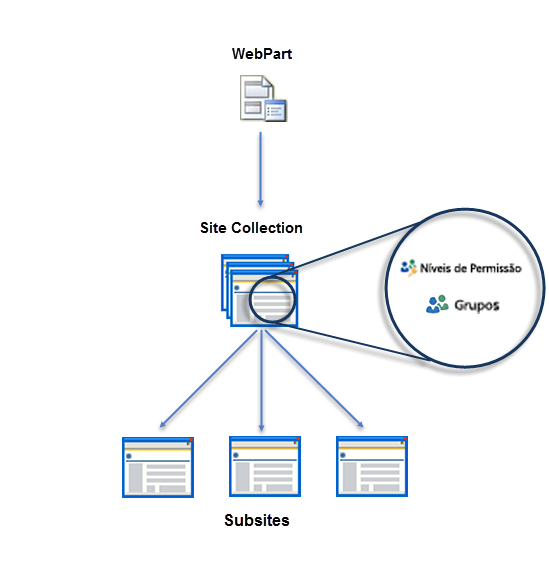
O diagrama desenvolvido abaixo, tem por objetivo trazer uma compreensão melhor de como os objetos do sistema irão se relacionar.



**PROJETO DE SISTEMA**

**Arquitetura do Sistema:**

Para a arquitetura da solução foi desenvolvido uma Web Part, com possibilidade de implantação em qualquer site dentro de uma coleção de sites. Nessa coleção de sites que o Sharepoint possui, existe toda a relação de grupos, usuários e níveis de permissão, além dos subsites existentes no mesmo.



**Padrões de Projetos utilizados:**

Para o back-end, além de levar em consideração a separação de camadas da arquitetura MVC, também foi utilizado os padrões de projetos Singleton e Facade, respectivamente, nos seguintes casos:

* Garantir uma instância única para o objeto da classe Connection, que armazena as informações de acesso como a string de conexão e o usuário do banco de dados;
* "Fachada" de acesso às classes da camada que realiza o gerenciamento dos dados no sistema