

# Dspace – Restringir acesso a coleções

## Objetivo

O objetivo deste documento é apresentar como é realizada a restrição de acesso de uma coleção e de seus itens no Dspace.

## Ambiente

O ambiente escolhido para realizar a demonstração será o ambiente de homologação (<https://basedeconhecimento-h.cgu.gov.br>) e será utilizada a coleção <https://basedeconhecimento-h.cgu.gov.br/handle/1/5455>.

Para realizar a restrição é necessário que o usuário esteja logado e tenha permissão de administrador para realizar a tarefa.

## Grupo padrão

Foi criado um grupo padrão chamado UsuarioCGU, o qual todos os usuários logados pertencerão a esse grupo, conforme imagem abaixo:

Editar grupo : UsuariosCGU (id: 48abbbbbe-327a-4612-9ace-352d248be760) 

Nome:

UsuariosCGU

Não é necessário adicionar usuários e nem grupos a esse grupo, pois a vinculação ao grupo é realizada automaticamente quando o usuário efetuar login no Dspace.

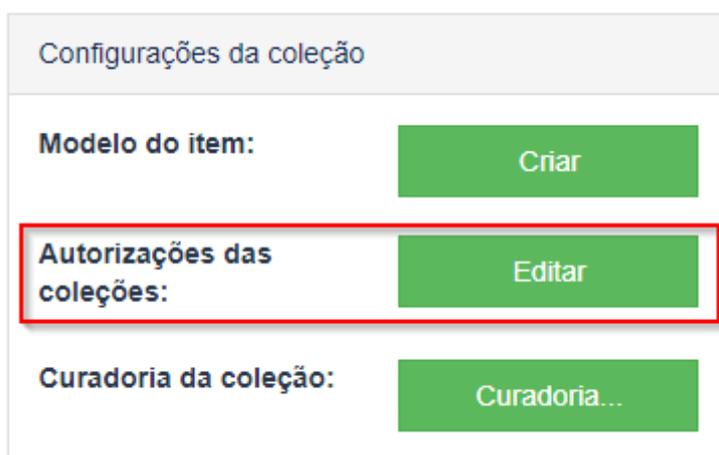
A configuração do grupo padrão para usuários logados é realizada em arquivo de configuração no servidor do Dspace, apenas a criação do grupo é possível ser realizada na interface do Dspace.

## Restrição de coleção

Na página da coleção, do lado direito, no menu **Ferramentas do administrador**, clique em **Editar**, conforme imagem abaixo:



Na página de edição da coleção, no lado direito, no menu **Configuração da coleção**, em **Autorizações das coleções**, clique em **Editar**, conforme imagem abaixo:



A próxima página é a página das políticas da coleção. Nela é listada todas as políticas atribuídas a determinada coleção.

Para restringir o acesso da coleção, é necessário alterar o grupo das políticas **DEFAULT\_ITEM\_READ**, **DEFAULT\_BITSTREAM\_READ** e **READ**, conforme imagem abaixo:

ID	Ação	Grupo		
292811	DEFAULT_ITEM_READ	Anonymous	<a href="#">Editar</a>	<a href="#">Excluir</a>
292812	DEFAULT_BITSTREAM_READ	Anonymous	<a href="#">Editar</a>	<a href="#">Excluir</a>
292813	ADD	Boas Práticas em Auditoria Interna_SUBMIT	<a href="#">Editar</a>	<a href="#">Excluir</a>
292814	WORKFLOW_STEP_2	Boas Práticas em Auditoria Interna_WORKFLOW_STEP_2	<a href="#">Editar</a>	<a href="#">Excluir</a>
292815	ADD	Boas Práticas em Auditoria Interna_WORKFLOW_STEP_2	<a href="#">Editar</a>	<a href="#">Excluir</a>
292810	READ	Anonymous	<a href="#">Editar</a>	<a href="#">Excluir</a>

Em cada política destacada acima, clique em **Editar** e altere o grupo **Anonymous** para o grupo padrão **UsuariosCGU** para restringir o acesso dela a somente usuários logados.

Na página de edição da política, em **Grupo** selecione o grupo **UsuariosCGU** e clique em **Salvar**, conforme imagem abaixo:

1 UsuariosCGU

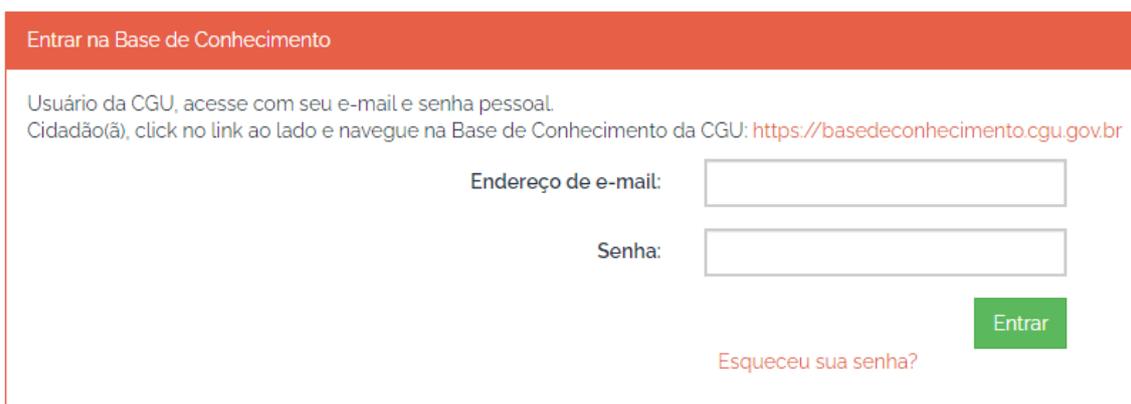
2 Salvar Cancelar

Ao final da edição das três políticas, o resultado deve estar conforme imagem abaixo:

Ação	Grupo
DEFAULT_BITSTREAM_READ	UsuariosCGU
DEFAULT_ITEM_READ	UsuariosCGU
READ	UsuariosCGU
ADD	Boas Práticas em Auditoria Interna_SUBMIT
WORKFLOW_STEP_2	Boas Práticas em Auditoria Interna_WORKFLOW_STEP_2
ADD	Boas Práticas em Auditoria Interna_WORKFLOW_STEP_2

## Acessando a coleção restrita

Após a configuração das políticas da coleção, ao tentar acessá-la, sem efetuar login, será apresentada a tela de login e será necessário efetuar login para visualizar o seu conteúdo, conforme imagem abaixo:



Entrar na Base de Conhecimento

Usuário da CGU, acesse com seu e-mail e senha pessoal.  
Cidadão(ã), click no link ao lado e navegue na Base de Conhecimento da CGU: <https://basedeconhecimento.cgu.gov.br>

Endereço de e-mail:

Senha:

[Esqueceu sua senha?](#)

## Ponto de atenção ao se restringir apenas a coleção

Os itens aceitos em uma coleção herdam as políticas de autorização associadas **DEFAULT\_ITEM\_READ** e **DEFAULT\_BITSTREAM\_READ**, que se tornam políticas **READ** para o item e seus anexos.

No entanto, ao alterar as políticas padrão de uma coleção, depois que os itens forem aceitos, as políticas dos itens existentes não serão alteradas automaticamente.

Logo, um usuário, sem efetuar login e de posse do link de um dos itens da coleção, terá acesso ao item e seu conteúdo.

Para contornar esse ponto, será preciso alterar as permissões dos itens da coleção usando a **Ferramenta de administração de política** para torná-los acessíveis somente aos usuários logados.

## Ferramenta de administração de política

Essa ferramenta possibilita editar as políticas de todos os itens de uma coleção de uma só vez, evitando que a alteração seja realizada item a item.

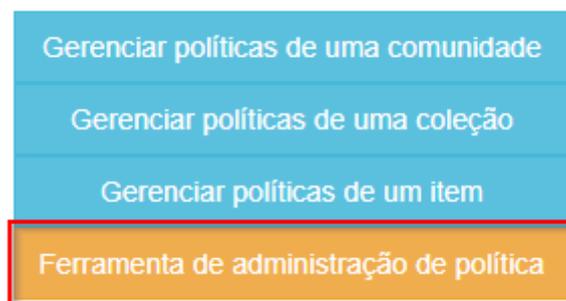
Para acessar a ferramenta, clique no ícone do usuário, no lado direito, e em **Administrador**, conforme imagem abaixo:



Na página das **Ferramentas de administração**, clique no menu **Controle de acesso** e em **Autorização**, conforme imagem abaixo:



Na página **Administrar políticas de autorização**, clique em **Ferramenta de administração de política**, conforme imagem abaixo:



Na página **Gerenciar políticas avançadas**, será possível editar a política de todos os itens de uma coleção, selecionando a coleção, o tipo de conteúdo (item ou anexo), o grupo e finalmente a ação (política) a ser editada, conforme imagem abaixo:

<b>Coleção:</b>	1ª Conferência Internacional de Promoção da Integridade Acordos de Leniência Administração Direta Agências Reguladoras Análise – Gestão de Pessoas Análise – Tomada de Contas Especial Apresentações Apresentações Institucionais Apresentações - LGPD Apresentações PGD Anexos - Evidências
<b>Tipo de conteúdo:</b>	item
<b>Grupo:</b>	1ª Conferência Internacional de Promoção da Integridade_SUBMIT 1ª Conferência Internacional de Promoção da Integridade_WORKFLOW_STEP_2 Acordos de Cooperação Técnica 2004 a 2010_WORKFLOW_STEP_2 Acordos de Cooperação Técnica 2011 a 2015_WORKFLOW_STEP_2 Acordos de Cooperação Técnica 2016 a 2020_WORKFLOW_STEP_2 Acordos de Leniência_SUBMIT Acordos de Leniência_WORKFLOW_STEP_2 Administração Direta_SUBMIT Administração Direta_WORKFLOW_STEP_2 Administrador Agências Reguladoras_SUBMIT
<b>Ação:</b>	READ

Para cada item de uma coleção, há apenas uma política **READ** configurada para o grupo **Anonymous**.

No entanto, a ferramenta não possui a opção de editar as políticas, possuindo apenas as opções de adicionar e deletar políticas.

Logo, será preciso primeiramente deletar as políticas dos itens e dos arquivos binários (anexos) e em seguida criar novas políticas **READ** vinculadas ao grupo **UsuariosCGU** para eles.

## Restrição de itens usando a Ferramenta de administração de política

Como dito anteriormente, o primeiro passo é deletar a política **READ** dos itens e dos anexos da coleção.

Na página **Gerenciar políticas avançadas**, realize os passos seguintes, conforme imagem abaixo:

- Em **Coleção**, selecione a coleção deseje, nesse caso a coleção **Boas Práticas em Auditoria Interna**;
- Em **Tipo de conteúdo**, selecione **item**;
- Em **Ação**, selecione **READ**;
- Clique no botão **Deletar políticas**

<b>Coleção:</b>	<ul style="list-style-type: none"> <li>Boas Práticas de Corregedorias</li> <li><b>Boas Práticas em Auditoria Interna</b></li> <li>Boas Práticas em Combate à Corrupção</li> <li>Boas Práticas em Correição</li> <li>Boas Práticas em Gestão Interna</li> <li>Boas Práticas em Governança Interna</li> <li>Boas Práticas em Ouvidoria e Controle Social</li> <li>Boas Práticas em Prevenção à Corrupção</li> <li>Boas Práticas em Tecnologia da Informação</li> <li>Boas Práticas em Transparência Pública</li> <li>Boletins Base de Conhecimento</li> </ul>
<b>Tipo de conteúdo:</b>	item
<b>Grupo:</b>	<ul style="list-style-type: none"> <li>1ª Conferência Internacional de Promoção da Integridade_SUBMIT</li> <li>1ª Conferência Internacional de Promoção da Integridade_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2004 a 2010_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2011 a 2015_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2016 a 2020_WORKFLOW_STEP_2</li> <li>Acordos de Leniência_SUBMIT</li> <li>Acordos de Leniência_WORKFLOW_STEP_2</li> <li>Administração Direta_SUBMIT</li> <li>Administração Direta_WORKFLOW_STEP_2</li> <li>Administrator</li> <li>Aplicativos Desempenho_SUBMIT</li> </ul>
<b>Ação:</b>	READ

(aviso: ao deletar o sistema apagará todas as políticas de um determinado c

Volte para a página **Gerenciar políticas avançadas**, clicando em **Ferramenta de administração de política**, e repita os passos anteriores, alterando apenas o **Tipo de conteúdo** para **arquivo binário**, conforme imagem abaixo:

<b>Coleção:</b>	<ul style="list-style-type: none"> <li>Base de Conhecimento da CGU</li> <li>Benefícios Financeiros e Não Financeiros - Ouvidoria</li> <li>Boas Práticas de Corregedorias</li> <li><b>Boas Práticas em Auditoria Interna</b></li> <li>Boas Práticas em Combate à Corrupção</li> <li>Boas Práticas em Correição</li> <li>Boas Práticas em Gestão Interna</li> <li>Boas Práticas em Governança Interna</li> <li>Boas Práticas em Ouvidoria e Controle Social</li> <li>Boas Práticas em Prevenção à Corrupção</li> <li>Boas Práticas em Tecnologia da Informação</li> </ul>
<b>Tipo de conteúdo:</b>	arquivo binário
<b>Grupo:</b>	<ul style="list-style-type: none"> <li>1ª Conferência Internacional de Promoção da Integridade_SUBMIT</li> <li>1ª Conferência Internacional de Promoção da Integridade_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2004 a 2010_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2011 a 2015_WORKFLOW_STEP_2</li> <li>Acordos de Cooperação Técnica 2016 a 2020_WORKFLOW_STEP_2</li> <li>Acordos de Leniência_SUBMIT</li> <li>Acordos de Leniência_WORKFLOW_STEP_2</li> <li>Administração Direta_SUBMIT</li> <li>Administração Direta_WORKFLOW_STEP_2</li> <li>Administrator</li> <li>Aplicativos Desempenho_SUBMIT</li> </ul>
<b>Ação:</b>	READ

(aviso: ao deletar o sistema apagará todas as políticas de um determinado c

Realizados os procedimentos anteriores, agora podem ser criadas as políticas **READ** associadas ao grupo **UsuariosCGU**.

Na página **Gerenciar políticas avançadas**, realize os passos seguintes, conforme imagem abaixo:

- Em **Coleção**, selecione a coleção deseja, nesse caso a coleção **Boas Práticas em Auditoria Interna**;
- Em **Tipo de conteúdo**, selecione **item**;
- Em **Grupo**, selecione o grupo **UsuariosCGU**;
- Em **Ação**, selecione **READ**;
- Clique no botão **Adicionar política**

<b>Coleção:</b>	Base de Conhecimento da CGU Benefícios Financeiros e Não Financeiros - Ouvidoria Boas Práticas de Corregedorias <b>Boas Práticas em Auditoria Interna</b> Boas Práticas em Combate à Corrupção Boas Práticas em Correição Boas Práticas em Gestão Interna Boas Práticas em Governança Interna Boas Práticas em Ouvidoria e Controle Social Boas Práticas em Prevenção à Corrupção Boas Práticas em Tecnologia da Informação
<b>Tipo de conteúdo:</b>	<input type="text" value="item"/>
<b>Grupo:</b>	Teses – Governança_WORKFLOW_STEP_2 Teses – Ouvidoria_SUBMIT Teses – Ouvidoria_WORKFLOW_STEP_2 Teses – Prevenção da Corrupção, Integridade e Transparência Pública_SUBMIT Teses – Prevenção da Corrupção, Integridade e Transparência Pública_WORKFLOW_STEP_2 Teses – Tecnologia da Informação_SUBMIT Teses – Tecnologia da Informação_WORKFLOW_STEP_2 Teses Transparência_WORKFLOW_STEP_2 <b>UsuariosCGU</b> Visita Columbia University_SUBMIT Visita Columbia University_WORKFLOW_STEP_2
<b>Ação:</b>	<input type="text" value="READ"/>

(aviso: ao deletar o sistema apagará todas as políticas de um determinado conjunto de c

Volte para a página **Gerenciar políticas avançadas**, clicando em **Ferramenta de administração de política**, e repita os passos anteriores, alterando apenas o **Tipo de conteúdo** para **arquivo binário**, conforme imagem abaixo:

<b>Coleção:</b>	Base de Conhecimento da CGU Benefícios Financeiros e Não Financeiros - Ouvidoria Boas Práticas de Corregedorias <b>Boas Práticas em Auditoria Interna</b> Boas Práticas em Combate à Corrupção Boas Práticas em Correição Boas Práticas em Gestão Interna Boas Práticas em Governança Interna Boas Práticas em Ouvidoria e Controle Social Boas Práticas em Prevenção à Corrupção Boas Práticas em Tecnologia da Informação
<b>Tipo de conteúdo:</b>	<input type="text" value="arquivo binário"/>
<b>Grupo:</b>	Teses – Governança_WORKFLOW_STEP_2 Teses – Ouvidoria_SUBMIT Teses – Ouvidoria_WORKFLOW_STEP_2 Teses – Prevenção da Corrupção, Integridade e Transparência Pública_SUBMIT Teses – Prevenção da Corrupção, Integridade e Transparência Pública_WORKFLOW_STEP_2 Teses – Tecnologia da Informação_SUBMIT Teses – Tecnologia da Informação_WORKFLOW_STEP_2 Teses Transparência_WORKFLOW_STEP_2 <b>UsuariosCGU</b> Visita Columbia University_SUBMIT Visita Columbia University_WORKFLOW_STEP_2
<b>Ação:</b>	<input type="text" value="READ"/>

(aviso: ao deletar o sistema apagará todas as políticas de um determinado conjunto de c

A partir desse momento, todos os itens dessa coleção estão com os seus acessos restritos a somente usuários que efetuarem login no Dspace, mesmo que um usuário tenha acesso ao link direto do item e nem será possível realizar uma busca pelo item restrito.