# ANEXO III

## Documento de Padrões de Segurança de Acesso

| Histórico de Revisão | | | |
|---|---|---|---|
| Data | Versão | Descrição | Autor |
| 27/03/2014 | 1.0 | Criação do artefato. | Amélia Pessoa |
| 02/04/2014 | 1.1 | Inserção de novas regras | Amélia Pessoa |
| 27/08/2014 | 1.2 | Nova regra para contratos | Amélia Pessoa |
| 03/10/2014 | 1.3 | [RM1798] Novas regras para controle de acessos às funcionalidades | Mariana Victor |
| 05/06/2015 | 1.4 | [RM2374] Permitir que seja possível visualizar os itens de um pop up com todos os campos bloqueados | Amélia Pessoa |

## Introdução

Este documento tem como finalidade apresentar o padrão para o controle de acesso às funcionalidades do sistema **SIGANET**, bem como os padrões de segurança de acesso que estão presentes em todo o projeto, independente dos perfis de acesso do usuário. Os casos de uso das funcionalidades assim como os perfis podem restringir ainda mais a segurança de acesso do que as regras descritas nesse documento, porém não poderão excluir uma regra.

## Definições

Esta seção descreve as definições importantes para total entendimento do padrão para controle de acesso às funcionalidades e das regras de segurança descritas a seguir.

*Usuário da UGC*

A sigla UGC significa Unidade Gestora Central. Sabemos que o usuário faz parte da UGC quando a Unidade Gestora igual ao campo UNIDADEPROPRIETARIA da tabela PESSOA para o usuário em questão tem seu campo OWNER nulo.

*Operação*

Com exceção da operação "Consultar", todo registro na tabela OPERACAO representa um botão no sistema que possui controle de acesso (por exemplo: Cadastrar, Editar, Excluir). Botões que não possuem controle de acesso (por exemplo: Salvar, Limpar, Desfazer), ou seja, que por padrão devem ser exibidos para todos os usuários, não são representados por operações.

## Regras de Segurança

*RS01 - Unidade Gestora*

Quando a tela do sistema apresentar o campo **Unidade Gestora** para seleção do usuário, este campo deve listar:
Caso o usuário pertença a UGC: Todas as unidades disponíveis;
Caso contrário: Apenas a unidade a qual o usuário pertença. Neste caso o campo não deve sequer ser exibido na tela e para todas as consultas disponíveis na funcionalidade devem-se apresentar apenas os resultados relativos à unidade do usuário.

*RS02 - Estado*

Quando a tela do sistema apresentar o campo **Estado** e o mesmo se tratar do estado de localização da **Unidade Gestora**,



CNPJ: 05.080.329\0001-23
E-mail: asa@asabrasil.org.br – Fone/Fax: (81) 2121.7666
Rua Nicarágua, nº 111, Espinheiro, CEP: 52.020-190 - Recife/PE

semelhantemente ao que acontece na **RS01**, este campo deve listar:
Caso o usuário pertença a UGC: Todos os estados disponíveis;
Caso contrário: Apenas o estado da unidade a qual o usuário pertença. Neste caso o campo não deve sequer ser exibido na tela e para todas as consultas disponíveis na funcionalidade devem-se apresentar apenas os resultados relativos à unidade do usuário.

*RS03 - Botões*

Quando a tela do sistema contar com botões os quais o usuário logado não tem acesso, o mesmo não deve ser exibido na tela.

*RS04 - Contrato*

Quando a tela do sistema apresentar o campo **Contrato**, semelhantemente ao que acontece na **RS01**, este campo deve listar:
Caso o usuário pertença a UGC: Todos os contratos disponíveis;
Caso contrário: Apenas os contratos vinculados a unidade a qual o usuário pertença.

## Padrão para Controle de Acessos

Toda codificação e todo script para controle de acessos às **operações** e **funcionalidade**, deverão seguir as regras definidas nesta sessão. A explicação detalhada, definindo termo Funcionalidade, encontra-se no Documento de Padrões de Interface.

*Funcionalidade*

Os atributos da funcionalidade deverão seguir as seguintes regras:

- **Nome** - deverá conter o nome da funcionalidade que será exibido para o usuário;
- **Página** - deverá conter o caminho do xhtml que representa a funcionalidade;
- **Descrição** - deverá conter a Descrição da Funcionalidade presente no caso de uso correspondente;
- **Ícone** - por padrão deverá conter o valor "ui-icon-bullet";
- **Grupo** - deverá conter o Grupo presente no caso de uso correspondente;

*Operação*

A operação deverá ter exatamente o mesmo nome do botão que a mesma representa.

**Toda funcionalidade sempre deverá possuir a operação Consultar**, pois esta operação representa que o usuário tem permissão básica para a funcionalidade, independente das demais operações. Quando o usuário tiver acesso apenas a essa operação o sistema deve permitir filtragem e abertura de registros porém ser deixar que nada seja alterado.

No código do componente que a operação representa, deverá ser adicionado um atributo como o exemplo a seguir:

```
rendered="#{usuarioMB.possuiPermissao(msg.alterarPerfis)}"
```

*Permissões de Acesso*

Por padrão, todas as funcionalidades e operações deverão ser incluídas nos acessos do perfil ADMINISTRADOR WEB. Opcionalmente, as funcionalidades e operações poderão ser atribuídas aos acessos de determinado(s) perfil(is) e/ou como permissões de acesso de determinado(s) usuário(s).

*Script*

O script relativo ao controle de acesso, deverá ser incluído no arquivo "**scripts_funcionalidades.sql**" presente no diretório raiz do projeto SigaNet e deverá seguir o seguinte exemplo:



CNPJ: 05.080.329/0001-23
E-mail: asa@asabrasil.org.br – Fone/Fax: (81) 2121.7666
Rua Nicarágua, nº 111, Espinheiro, CEP: 52.020-190 - Recife/PE

```
-- Remover os novos dados para caso o script já tenha sido rodado
DELETE ASASIGA1.USUARIO_PERMISSAO WHERE func_operacao in (SELECT FO.ID FROM ASASIGA1.FUNC_OPERACAO FO
                 INNER JOIN ASASIGA1.FUNCIONALIDADE FN ON fn.id = fo.funcionalidade
                WHERE fn.nome like 'Nome da Funcionalidade');
DELETE ASASIGA1.PERFIL_ACESSO WHERE func_operacao in (SELECT FO.ID FROM ASASIGA1.FUNC_OPERACAO FO
                          INNER JOIN ASASIGA1.FUNCIONALIDADE FN ON fn.id = fo.funcionalidade
                         WHERE fn.nome like 'Nome da Funcionalidade');
DELETE ASASIGA1.FUNC_OPERACAO WHERE funcionalidade in
      (SELECT FN.ID FROM ASASIGA1.FUNCIONALIDADE FN WHERE fn.nome like 'Nome da Funcionalidade');
DELETE ASASIGA1.FUNCIONALIDADE WHERE nome = 'Nome da Funcionalidade';
DELETE ASASIGA1.OPERACAO WHERE nome in ('Operação 1');
DELETE ASASIGA1.GRUPO_FUNCIONALIDADE WHERE nome = 'Grupo X'
      and modulo in (SELECT modu.id FROM ASASIGA1.MODULO modu WHERE modu.nome like 'Financeiro');

-- Criar a nova operação
INSERT INTO ASASIGA1.OPERACAO (ID, NOME, SYS_USER, SYS_INACTIVE) VALUES (ASASIGA1.SEQ_OPERACAO.NEXTVAL,
'Operação 1', 433443, 0);

-- Criar o novo grupo
INSERT INTO ASASIGA1.GRUPO_FUNCIONALIDADE (ID, NOME, MODULO, SYS_USER, SYS_INACTIVE)
VALUES (ASASIGA1.SEQ_GRUPO_FUNCIONALIDADE.NEXTVAL, 'Grupo X',
 (SELECT modu.id FROM ASASIGA1.MODULO modu WHERE modu.nome like 'Financeiro'), 433443, 0);

-- Criar a nova funcionalidade
INSERT INTO ASASIGA1.FUNCIONALIDADE (ID, NOME, PAGINA, DESCRICAO, ICONE,
     GRUPO_FUNCIONALIDADE,SYS_USER,SYS_INACTIVE)
VALUES (ASASIGA1.SEQ_FUNCIONALIDADE.NEXTVAL, 'Nome da Funcionalidade',
'/configuracoes/seguranca/exemploFuncionalidade.xhtml', 'Descrição da funcionalidade.', 'ui-icon-bullet',
 (SELECT gr.id FROM ASASIGA1.GRUPO_FUNCIONALIDADE gr
              INNER JOIN ASASIGA1.MODULO modu ON modu.id = gr.modulo
              WHERE gr.nome like 'Grupo X' and modu.nome like 'Financeiro'),
  433443, 0);

-- Atribuir as operações para a nova funcionalidade (SEMPRE ATRIBUIR A OPERAÇÃO "Consultar")
INSERT INTO ASASIGA1.FUNC_OPERACAO (ID, OPERACAO, SYS_USER, FUNCIONALIDADE)
  SELECT ASASIGA1.SEQ_FUNC_OPERACAO.NEXTVAL, op.id, 433443,
    (SELECT func.id FROM ASASIGA1.FUNCIONALIDADE func WHERE func.nome like 'Nome da Funcionalidade')
  FROM ASASIGA1.OPERACAO op
  WHERE op.nome in ('Consultar', 'Editar', 'Operação 1');

-- Atribuir o acesso de todas as operações da funcionalidade ao perfil 'ADMINISTRADOR WEB'
INSERT INTO ASASIGA1.PERFIL_ACESSO (ID, FUNC_OPERACAO, SYS_USER, SYS_INACTIVE, PERFIL)
  SELECT ASASIGA1.SEQ_PERFIL_ACESSO.NEXTVAL, fo.id,433443, 0,
    (SELECT PF.ID FROM ASASIGA1.PERFILUSUARIOS PF
       WHERE PF.NOME LIKE 'ADMINISTRADOR WEB' AND ORIGEM_SIGANET = 2)
  FROM ASASIGA1.FUNC_OPERACAO fo
  WHERE funcionalidade in (SELECT FN.ID FROM ASASIGA1.FUNCIONALIDADE FN WHERE FN.NOME like 'Nome da
Funcionalidade');

-- Atribuir apenas a operação 'Operação 1' da funcionalidade aos perfis 'UNIDADE GESTORA' e 'UGC - TESOURARIA'
INSERT INTO ASASIGA1.PERFIL_ACESSO (ID, FUNC_OPERACAO, SYS_USER, SYS_INACTIVE, PERFIL)
  SELECT ASASIGA1.SEQ_PERFIL_ACESSO.NEXTVAL, fo.id, 433443, 0, PF.ID
  FROM ASASIGA1.FUNC_OPERACAO fo, ASASIGA1.PERFILUSUARIOS PF
  WHERE PF.NOME in ('UGC - TESOURARIA', 'UGC - CONCILIACAO') AND PF.ORIGEM_SIGANET = 2
       and operacao in (SELECT op.ID FROM ASASIGA1.OPERACAO op WHERE op.NOME in ('Consular','Operação 1'))
       and funcionalidade in (SELECT FN.ID FROM ASASIGA1.FUNCIONALIDADE FN WHERE FN.NOME like 'Nome da
Funcionalidade');

-- Exemplo de permissão especial para determinado usuário
INSERT INTO ASASIGA1.USUARIO_PERMISSAO (ID, FUNC_OPERACAO, SYS_INACTIVE, SYS_USER, USUARIO)
  SELECT ASASIGA1.SEQ_USUARIO_PERMISSAO.NEXTVAL, fo.id, 0, 433443,
     (SELECT U.ID FROM ASASIGA1.USUARIO U WHERE U.PESSOA = 1657) -- UZIEL BUARQUE WANDERLEY
  FROM ASASIGA1.FUNC_OPERACAO fo
  WHERE funcionalidade in (SELECT FN.ID FROM ASASIGA1.FUNCIONALIDADE FN WHERE FN.NOME in ('Nome da
Funcionalidade'));
```



CNPJ: 05.080.329/0001-23
E-mail. asa@asabrasil.org.br – Fone/Fax: (81) 2121.7666
Rua Nicarágua, nº 111, Espinheiro, CEP: 52.020-190 - Recife/PE