Política de perfil de usuário

Plone 4.3

1. Justificativa para a Restrição de Acesso Administrativo no Plone

O Princípio do Mínimo Privilégio (ou Princípio do Menor Privilégio) é uma prática de segurança que se baseia na ideia de conceder a um usuário, programa ou processo apenas os privilégios (permissões) necessários para realizar suas funções específicas, nada mais. Aqui estão os pontos principais:

1. Redução de Risco: Ao limitar os privilégios, reduz-se o risco de danos acidentais ou intencionais, como a exclusão de dados ou a modificação de configurações críticas.

2. Mitigação de Vulnerabilidades: Se um usuário ou processo com privilégios limitados for comprometido, o alcance dos danos será menor em comparação com um usuário ou processo com privilégios amplos.

3. Isolamento de Funções: Ao segregar tarefas e atribuir apenas os privilégios necessários para cada função, minimiza-se o impacto de um possível ataque ou erro.

4. Melhoria na Auditoria e Controle: Facilita a monitoração e auditoria das ações dos usuários, uma vez que suas atividades são limitadas e bem definidas.

5. Boa Prática de Governança: Alinha-se com as melhores práticas de governança e conformidade, sendo frequentemente um requisito em normas e regulamentos de segurança da informação.

2. Exemplos de Aplicação

1. Contas de Usuários: Funcionários devem ter acesso apenas aos dados e sistemas necessários para seu trabalho, evitando acesso desnecessário a informações sensíveis ou sistemas críticos.

2. Aplicações e Serviços: Programas ou serviços devem operar com privilégios mínimos necessários. Por exemplo, um servidor web não precisa de acesso de escrita em diretórios de sistema críticos.

3. Sessões de Administração: Administradores de sistema devem usar contas com privilégios elevados apenas quando necessário, operando normalmente com contas de privilégios reduzidos.

3. Benefícios

- Segurança Aprimorada: Limita a superfície de ataque e reduz o potencial de exploração de vulnerabilidades.
- Redução de Impacto de Incidentes: Qualquer incidente terá um impacto mais contido, facilitando a recuperação e minimizando danos.
- Compliance: Auxilia no cumprimento de regulamentações e padrões de segurança da informação.

4. Política Nacional de Segurança da Informação (PNSI)

A PNSI, estabelecida pelo Decreto nº 9.637/2018, tem como objetivo garantir a segurança dos dados custodiados por entidades públicas e a segurança da informação das infraestruturas críticas. O Art. 4º, VI, d, da PNSI orienta ações relacionadas ao tratamento das informações com restrição de acesso, justificando a necessidade do Princípio do Mínimo Privilégio. Este princípio minimiza riscos ao limitar privilégios desnecessários, prevenindo acessos indevidos e potenciais vulnerabilidades.

Fonte: Decreto nº 9.637/2018

5. Perfil de usuário Plone

O grupo UNIRIO foi criado para unificar o acesso de todos os usuários de sites Plone da Universidade Federal do Estado do Rio de Janeiro. Esse grupo combina as funcionalidades dos perfis de **Editor, Colaborador e Revisor**, padrão no Plone, que disponibilizam as seguintes permissões:

- **Adicionar Conteúdo**: Pode criar, editar e excluir conteúdo em todo o site.
- **Publicar Conteúdo**: Pode publicar ou retirar a publicação de conteúdo, tornando-o visível ou invisível para o público.
- **Gerenciar Configurações de Conteúdo**: Pode configurar opções de exibição e propriedades do conteúdo.
- **Revisar Conteúdo**: Pode revisar o conteúdo enviado por colaboradores e aprová-lo para publicação.
- **Gerenciamento de Pastas**: Pode criar e organizar pastas e outros contêineres de conteúdo.

Além disso, foram adicionadas quatro permissões consideradas essenciais para o gerenciamento de conteúdo nos sites, que antes só estavam disponíveis para administradores do site, garantindo ao mesmo tempo a integridade e segurança das estruturas:

- Portlets: Gerenciar seus próprios portlets
- Portlets: Gerenciar portlets
- plone.app.collection: Adicionar coleção
- plone.portlet.static: Adicionar portlet estático

Usuários interessados em solicitar outras alterações podem fazê-lo abrindo um chamado na ferramenta GLPI. As solicitações serão revisadas e, se aprovadas, implementadas pela DTIC.

Para mais detalhes sobre as permissões dos perfis padrão do Plone, consulte o manual disponível em: Working with Content — Plone Documentation v4.3.