



MANGUE SECO 2
ENERGIA EÓLICA

POLÍTICA DE GESTÃO DE ACESSOS LÓGICOS.

ATA DE APROVAÇÃO – RCA de 31/08/2018

1. OBJETIVO

Estabelecer requisitos e orientações para a efetiva gestão de acessos lógicos na Eólica Mangue Seco 2.

2. ABRANGÊNCIA

Aplica-se à Eólica Mangue Seco 2, respeitando-se os devidos trâmites societários, conforme disposto em seu Estatuto Social.

3. DESCRIÇÃO

A gestão dos acessos lógicos é atividade fundamental na preservação da segurança das informações e se constitui de controle indispensável na mitigação de riscos como acesso indevido, roubo, vazamento de informações, perda de integridade e alteração não autorizada de informações.

Neste sentido é fundamental que os processos de concessão, revogação, revisão de acessos, bem como a gestão de perfis e a correta definição das ações críticas e as que devem ser segregadas por conta de conflitos que levem a riscos estejam corretamente definidos, sejam seguidos e monitorados.

3.1 Autoridade e responsabilidade

Caberá à Diretoria Executiva conceder, revogar e revisar os acessos dos seus colaboradores ao Servidor de Arquivos da Eólica Mangue Seco 2, quando o mesmo for instalado e utilizado.

Para tanto, a Diretoria Executiva poderá:

- a) Analisar as solicitações de concessão, revogação e revisão de acesso;
- b) Restringir o acesso dos colaboradores a determinados arquivos e conteúdos, quando for necessário, a seu critério, ou por determinação do Conselho de Administração e/ou pela Assembleia de Acionistas;



- c) Promover as revogações por desligamento;
- d) Avaliar as matrizes de riscos;
- e) Garantir que os colaboradores da companhia só tenham acesso ao Servidor de Arquivos com login e senha pessoais, bem como mediante termo de sigilo e confidencialidade;

3.2 Concessão de acessos

- a) todo acesso deve ser autorizado formalmente pela Diretoria Executiva, mediante termo de sigilo e confidencialidade firmado pelo colaborador da Eólica Mangue Seco 2, após a instalação do servidor de arquivos;
- b) Em razão da estrutura operacional pequena, com apenas 04 (quatro) colaboradores cedidos pelos acionistas, bem como, os 2 (dois) membros da Diretoria Executiva, todos os colaboradores e membros da Diretoria terão completo acesso ao Servidor de Arquivos da Eólica Mangue Seco 2, quando o mesmo for instalado, salvo se identificada a possibilidade de restrição, prevista no item 3.1 "b" *supra*.

3.4. Análise de riscos

- a) a análise dos riscos da matriz deve ser documentada mesmo que não existam riscos mapeados para o Servidor de Arquivos da Companhia, assim que o servidor de arquivos for instalado na Companhia;
- b) a matriz de riscos deverá ser revista e atualizada sempre que surjam novos riscos inerentes do negócio ou sistema ou de forma anual. A revisão deve ser documentada, mesmo que não haja alterações, bem como os critérios utilizados na revisão;
- c) alguns eventos exemplificativos utilizados na revisão da matriz de riscos podem ser encontrados abaixo:
 - alteração de perfis;
 - criação de novos perfis;
 - criação de novas funcionalidades no sistema;
 - alteração de funcionalidades do sistema.
- d) as concessões devem ser precedidas de análise de riscos que levem em conta a necessidade de conhecimento, os impactos e controles para proteção das informações, as ações conflitantes e críticas;

- e) a análise dos riscos das concessões de acesso, pelos gestores de risco, deverá ser documentada preferencialmente em sistema previsto para esta finalidade;
- f) a análise deve ser feita no momento da construção e alteração do perfil e não é necessária que seja feita a cada caso.

3.5 Revogação de acessos

A Diretoria Executiva pode a qualquer tempo suspender, revogar ou restringir o acesso aos dados e informações sob sua responsabilidade.

3.6 Revisão dos acessos dos usuários

- a) os acessos e perfis devem ser revisados e revalidados pela Diretoria Executiva, se necessário;

3.7 Definição de ações críticas

- a) devem ser definidas, caso existam, as ações em sistemas que são críticas devido a sua relevância para a execução do processo, que possam pôr em risco o sigilo, disponibilidade, integridade dos dados e informações e aquelas que possam gerar impactos operacionais, legais, financeiros ou de reputação;
- b) os critérios que levaram à definição de ações críticas devem ser definidos e documentados;
- c) é de responsabilidade da Diretoria Executiva revisar a totalidade dos usuários que incorram em tais acessos críticos visando manter ou revogar tais acessos pelo menos uma (01) vez por ano.

3.8 Gestão de perfis

- a) perfis de acesso só poderão ser modificados, criados ou removidos dos ambientes de produção após a autorização e validação da Diretoria Executiva da Companhia;
- b) as ações críticas só poderão existir em perfis cujas ações sejam rastreáveis (*log de ações*);
- c) perfis descontinuados não devem ser mapeados para nenhum usuário.

3.9 Monitoramento

- a) a qualquer tempo o Conselho de Administração da Companhia poder avaliar a totalidade dos acessos e perfis de acesso sob sua responsabilidade;
- b) a qualquer tempo o Conselho de Administração da Companhia poderá avaliar a totalidade do histórico de concessões de acesso e perfis sob sua responsabilidade;
- c) dever haver por parte da Diretoria Executiva, bem como do Conselho de Administração, o monitoramento periódico das ações críticas realizadas;
- d) as ações de usuários de serviço ou com acesso a sistemas por meio de perfis temporários ou de emergência devem ser rastreáveis e monitoradas pela Diretoria Executiva.

3.10 Usuários externos

- a) quando houver necessidade de uso de sistemas por parte de usuários externos (estrangeiros, usuários de fora da Eólica Mangue Seco 2, ou outros casos), incluindo os cadastros em bases ou serviços/servidores locais, os mesmos cuidados já descritos neste padrão devem ser tomados pelos gestores de tais sistemas;
- b) os usuários Externos devem ser identificados de forma inequívoca através de número de CPF. Quando se tratar de estrangeiro, poderá ser utilizado CPF, passaporte ou número do documento de identificação de estrangeiro do seu país de origem;
- c) o responsável pelo cadastro deverá providenciar formulários e cópias da documentação de forma a identificar os usuários que são externos à Eólica Mangue Seco 2 ou estrangeiros;
- d) os controles de concessão, revisão, revogação, monitoramento, gestão de perfis, e definição de ações críticas devem ser observados, conforme descrito neste padrão. Não sendo possível a automatização em sistema específico, deve ser criado e mantido um processo que garanta os controles citados neste padrão.



3.11 Prazo para implantação

Os prazos para implantação nos sistemas e aplicações já existentes dos controles definidos neste padrão, a partir da data de sua aprovação pelo Conselho de Administração é de 180 dias, após a instalação do servidor de arquivos.

Caso a Eólica Mangue Seco 2 venha adquirir ou utilizar novos sistemas ou aplicações desenvolvidas, sob qualquer forma de comercialização, deverá rever a presente diretriz de modo a adequá-la à Diretriz PE-1PBR-00029 Versão: F "GESTÃO DE ACESSOS LÓGICOS" da sua acionista Petróleo Brasileiro S.A. ("Petrobras").