GOVERNO DO ESTADO DE MATO GROSSO
SECRETARIA DE ESTADO DE PLANEJAMENTO E COORDENAÇÃO GERAL
CONSELHO SUPERIOR DO SISTEMA ESTADUAL DE INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

ANEXO I - RESOLUÇÃO Nº. 011/2011

GOVERNO DO ESTADO DE MATO GROSSO

Norma de Segurança Estadual para Gerenciamento de Senhas

SETEMBRO/2011

ANEXO I – RESOLUÇÃO 011/2011

Conselho Superior do Sistema Estadual de Informação e Tecnologia da informação – COSINT

FRANCISCO TARQUINIO DALTRO
Presidente do Conselho e
Vice Governador do Estado de Mato Grosso

JOSÉ GONÇALVES BOTELHO DO PRADO
Presidente do Conselho e
Secretário de Estado de Planejamento e Coordenação Geral

EDMILSON JOSÉ DOS SANTOS
Membro do Conselho
Secretário de Estado de Fazenda

JOSÉ ALVES PEREIRA FILHO
Membro do Conselho
Auditor Geral do Estado

CESAR ROBERTO ZILIO
Membro do Conselho
Secretário de Estado de Administração

WILSON CELSO TEIXEIRA
Membro do Conselho
Diretor Presidente do CEPROMAT

ÍNDICE

Introdução

Esta norma faz parte dos instrumentos normativos de Segurança da Informação das entidades governamentais do Poder Executivo do Estado de Mato Grosso e é especialmente complementar à ***Norma de Segurança Estadual para Acesso à Informação***.

Este documento contém princípios que devem ser observados por todos os Agentes Públicos e Prestadores de Serviço, de forma a preservar a segurança das informações da administração pública estadual no âmbito do Poder Executivo.

1. Objetivo

Estabelecer os procedimentos de segurança para gerenciamento de senhas para acesso aos diversos ativos de TI das entidades governamentais no âmbito do poder executivo estadual.

2. Referências

Norma ABNT NBR ISO/IEC 27001: 2005
Políticas e Diretrizes do SEITI
Norma de Segurança Estadual para Acesso a Informação

3. Definições e Convenções

Agente público - Toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja estagiário, ocupante de função, cargo ou de emprego público.

Confidencialidade - Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Criptografia - Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários, autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Ativo - É tudo aquilo que tem valor para a empresa; pode ser algo tangível ou intangível: instalações, máquinas, informações, etc.

Ativos de TI – São ativos de tecnologia da informação. Exemplos: softwares, dispositivos de rede, computadores, mídias de armazenamento de dados, impressoras, etc.

Ativos de TI Críticos- São ativos de tecnologia da informação que dão suporte, direta ou indiretamente, aos principais negócios da entidade governamental. A indisponibilidade ou o mal funcionamento desses ativos afetam os negócios da organização trazendo prejuízos à entidade governamental e/ou à sociedade.

Senha Complexidade Média – Possui letras e números não consecutivos.

Senha Complexidade Alta – Possui letras, números e símbolos especiais não consecutivos.

Usuário: Agente ou prestador de serviço que utiliza os recursos de TI.

4. Princípios

4.1. Gerenciamento de senhas dos usuários

4.1.1. Sempre que possível, o usuário deve manter suas próprias senhas. Neste caso, serão fornecidas senhas iniciais seguras, individualizadas e temporárias que deverão ser obrigatoriamente trocadas pelo usuário no primeiro acesso.

4.1.2. O fornecimento de senhas temporárias para o caso de o usuário esquecer sua senha, somente será efetuado por meio da conta de e-mail institucional (corporativo) de uso exclusivo do usuário, ou após a identificação mediante apresentação do documento de identificação pessoal e/ou confirmação dos dados cadastrais do solicitante, com um mínimo de três informações aleatórias deste.

4.1.3. Recomenda-se que os usuários acusem o recebimento das senhas e alteração destas.

4.2. Gerenciamento de senhas de administração de ativos

4.2.1. Os administradores devem possuir contas e senhas individualizadas com privilégios administrativos e somente deverão utilizar essas contas para o desempenho de suas atividades.

4.2.2. As contas e senhas padrões do fabricante de equipamentos e aplicações devem ser trocadas imediatamente após a instalação.

4.2.3. As contas e senhas de administração de ativos comuns e de altíssimos privilégios, como “root”, devem ser guardadas, com identificação do ativo, em envelope fechado e lacrado, em local seguro, com acesso apenas às pessoas autorizadas pelo responsável pelo recurso.

4.2.3.1. Esses envelopes somente devem ser abertos em caso de contingência, mediante autorização formal do responsável pelo recurso.

4.2.3.2. Ao serem utilizadas as contas de contingência, estas devem ser alteradas e guardadas novamente, seguindo os mesmos procedimentos de proteção.

4.2.3.3. Esses procedimentos devem ser controlados e documentados com a justificativa, data e demais informações necessárias para uma possível auditoria.

4.2.4. A admissão ao grupo de administração deve ser controlada, registrada e mediante autorização do setor responsável conforme regimento interno do órgão.

4.3. Sistema de Gerenciamento de Senhas

4.3.1. O gerenciamento de senhas de sistemas corporativos e finalísticos, ativos de redes, servidores em geral e demais recursos de TI atualmente em operação (legado) deve, sempre que possível e o sistema permitir, ser modificado, ou configurado de maneira a:

- permitir que o usuário selecione e modifique suas próprias senhas;
- possuir um procedimento de confirmação na criação/modificação de senhas para evitar erros de digitação;
- obrigar a escolha de senhas de qualidade (senhas fortes) atendendo os requisitos mínimos aceitáveis, conforme descrito no Anexo I deste documento;
- obrigar a troca de senhas iniciais e temporárias no primeiro acesso;
- manter o registro das últimas senhas utilizadas, conforme regras estabelecidas no anexo I deste documento;
- não mostrar as senhas na tela quando forem digitadas; melhor ainda se não mostrar a quantidade de caracteres digitados;
- armazenar o arquivo de senhas separadamente dos dados de sistemas e de aplicação;
- armazenar as senhas na forma cifrada, preferencialmente usando algoritmo de criptografia unidirecional (HASH);
- Permitir inclusão e edição de dicionários para garantir a qualidade das senhas;
- Permitir que o administrador customize a complexidade das senhas a serem criadas pelo usuário, conforme descrito no Anexo I deste documento.

4.3.2. Os sistemas corporativos e finalísticos, ativos de redes, servidores em geral e demais recursos de TI a serem desenvolvidos ou adquiridos a partir

da data de publicação desta norma devem obrigatoriamente atender os requisitos do Anexo I da presente norma.

4.4. Regras para aceitação de senhas através de sistemas de gerenciamento

4.4.1. No anexo I são apresentadas as regras a serem configuradas nos diversos sistemas de gerenciamento e a definição dos níveis de complexidade requeridos para as senhas.

4.5. Monitoração e Auditoria

4.5.1. Periodicamente deverá haver auditorias internas ou externas nos diversos ambientes operacionais para confirmar a aplicação das normas descritas neste documento.

4.5.2. Nos casos de auditoria externa o órgão deve designar um responsável para acompanhar a execução dos trabalhos.

5. Disposições Finais

Casos omissos a este documento devem ser tratados pelo setor responsável pela segurança da informação no Órgão ou pelo Grupo Temático de Segurança da Informação.

Não é dado aos agentes públicos e prestadores de serviço, responsáveis pela administração de senhas de acesso aos recursos de TI, o direito de alegar desconhecimento da presente norma.

O não cumprimento da presente norma acarretará ao Agente Público e Prestador de Serviço as penalidades cabíveis, previstas no âmbito administrativo, cível e criminal.

Os acessos que o órgão concede a pessoas não classificados nas categorias de agentes públicos e nem de usuários serão de responsabilidade do órgão.

ANEXO I – Requisitos Mínimos para Gerenciamento de Senhas

ATIVO	**PERFIS**	**Regras Criação / Bloqueio**	**Regras Histórico**	**Logs**
Recursos para usuários finais, como: sistemas aplicativos, redes corporativas, Intranet, estações de trabalho, Internet, correio eletrônico, dentre outros	**Usuário final**	**Tamanho** – 8 caracteres **Complexidade** - média **Bloqueio -** na 3ª tentativa consecutiva inválida; ou após 30 dias de inatividade.	**Idade (*aging*)**: Trocar a senha após um período de 90 dias. **Reutilização**: permitida após ***5*** trocas.	Opcional, conforme a criticidade do recurso acessado
	Usuário Administrador de Estação de Trabalho	**Tamanho** – 16 caracteres **Complexidade** - alta	**Idade (*aging*)**: Trocar a senha quando se fizer necessário. **Reutilização**: permitida após ***5*** trocas	Opcional, conforme a criticidade do recurso acessado
Servidores de serviços e ativos de rede como: servidor de aplicação, servidor Web, servidor de e-mail, servidor de banco de dados, DNS, Firewall, Roteador, Switch, dentre outros	**Usuário Administrador**	**Tamanho** – 16 caracteres **Complexidade** - alta	**Idade (*aging*)**: Trocar a senha no máximo a cada 90 dias, ou antes, se fizer necessário. **Reutilização**: permitida após ***5*** trocas	Ativar