3.1 Norma de Gestão de Senhas

1. Objetivo

Estabelecer requisitos e diretrizes para criação, manutenção, armazenamento e auditoria de senhas, garantindo acesso seguro aos sistemas e conformidade com o CIS Controls v8 IG1 (C5).

2. Escopo

Aplica-se a todas as contas de usuários, de serviço e administrativas em todos os sistemas, aplicações, dispositivos de rede e serviços em nuvem gerenciados pela empresa.

3. Responsabilidades

- **Equipe de TI / Administradores de Sistemas**: Configurar políticas de senha nos sistemas, implementar controles técnicos e monitorar conformidade.
- **Gestor de Segurança da Informação**: Revisar políticas periodicamente, aprovar exceções e gerar relatórios de auditoria.
- **Todos os Colaboradores**: Criar e manter senhas conforme esta norma e usar gerenciador de senhas quando aplicável.

4. Definições

- **Senha**: Segredo utilizado para autenticar identidade de usuários em sistemas.
- **Autenticação Multifator (MFA)**: Processo de validação que exige dois ou mais fatores distintos.
- **Gerenciador de Senhas**: Ferramenta segura para armazenamento e preenchimento automático de credenciais.

5. Requisitos de Senha

- **Regras de complexidade (ex.: mínimo 12 caracteres) e expiração** (CIS C5)
- **Uso de gerenciador de senhas para contas privilegiadas** (CIS C5)

1. **Complexidade Mínima**: 12 caracteres contendo pelo menos três dos quatro grupos: maiúsculas, minúsculas, números e símbolos.
2. **Expiração**: Senhas de usuário devem expirar a cada 90 dias; senhas de serviço e administrativas, somente se exigido por compliance.
3. **Histórico**: Manter histórico dos últimos 10 usos para evitar reutilização imediata.
4. **Bloqueio de Conta**: Bloqueio automático após 5 tentativas de acesso inválidas, com desbloqueio manual pela TI.
5. **Desabilitação de Contas Inativas**: Contas sem uso por 60 dias devem ser desabilitadas.
6. **Complexidade Mínima**: 12 caracteres contendo pelo menos três dos quatro grupos: maiúsculas, minúsculas, números e símbolos.

7. **Expiração**: Senhas de usuário devem expirar a cada 90 dias; senhas de serviço e administrativas, somente se exigido por compliance.
8. **Histórico**: Manter histórico dos últimos 10 usos para evitar reutilização imediata.
9. **Bloqueio de Conta**: Bloqueio automático após 5 tentativas de acesso inválidas, com desbloqueio manual pela TI.
10. **Desabilitação de Contas Inativas**: Contas sem uso por 60 dias devem ser desabilitadas.

6. Autenticação Multifator

- **Obrigatório** para todas as contas com privilégios administrativos, acesso remoto e sistemas críticos.
- **Recomendada** para todas as demais contas de usuários.

7. Uso de Gerenciador de Senhas

- Usuários devem adotar o gerenciador corporativo homologado.
- Senhas devem ser geradas aleatoriamente pelo gerenciador, evitando padrões previsíveis.
- Compartilhamento de senhas via e-mail, chat ou documentos não é permitido.

8. Monitoramento e Auditoria

- Gerar relatórios mensais de conformidade de políticas de senha.
- Alertas em tempo real para tentativas de login suspeitas e bloqueios de conta.
- Revisão semestral de políticas e ajustes conforme novas ameaças ou tecnologias.

9. Revisão da Norma

Este documento será revisado anualmente ou sempre que houver mudanças significativas em requisitos de segurança ou tecnologia.