1. FINALIDADE

1.1. Estabelecer os regulamentos para a utilização de senhas de acessos à rede corporativa da SEPLAG.

2. APLICABILIDADE

2.1. Todos os usuários da SEPLAG.

3. CONCEITOS

3.1. **ASI** – Área responsável pela Segurança da Informação na SEPLAG.

3.2. **Incidente de Segurança da Informação** – É uma indicação de eventos, indesejados ou inesperados, que podem ameaçar a Segurança da Informação.

3.3. ***Logon*** – Processo de entrada de um usuário no sistema.

3.4. **Rede Corporativa** – São computadores e outros dispositivos interligados que compartilham informações ou recursos da SEPLAG.

3.5. **Senha** – Validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço.

3.6. **Servidor** - Computador responsável pelo compartilhamento de recursos com os demais computadores a ele conectados.

3.7. **Usuário** – É todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em Órgão ou Entidade da Administração Pública Direta e Indireta do Estado de Minas Gerais.

4. GERENCIAMENTO DE SENHAS

4.1. As identificações e as senhas para acesso à rede corporativa são de uso pessoal e intransferível.

4.2. Na liberação da identificação para o usuário é fornecida uma senha temporária, que deve ser alterada no primeiro acesso.

4.3. A senha de acesso do usuário tem, no mínimo, 5 (cinco) e, no máximo, 8 (oito) caracteres.

4.4. É solicitada a troca de senha a cada 4 (quatro) meses.

4.5. O usuário deve trocar sua senha sempre que existir qualquer indicação de possível comprometimento da rede corporativa ou da própria senha.

4.6. Recomenda-se fortemente que o usuário selecione senhas que:

4.6.1. Sejam fáceis de lembrar.

4.6.2. Sejam isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos.

4.6.3. Não sejam baseadas em coisas que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, tais como nome, sobrenome, números de documentos, placas de carros, números de telefones, datas importantes, entre outras.

5. NÃO É PERMITIDO

5.1. Registrar senha em papel ou em qualquer outro meio que coloque em risco a descoberta da senha por outro usuário.

5.2. Fornecer a senha de acesso à rede corporativa da SEPLAG para outro usuário.

5.3. Acessar qualquer rede da SEPLAG por meio da identificação de outro usuário.

5.4. Tentar obter acesso não autorizado, tais como tentativa de fraudar autenticação de usuário ou segurança de qualquer servidor da rede corporativa da SEPLAG.

5.5. Incluir senhas em processos automáticos, como por exemplo, em macros ou teclas de função.

6. RESPONSABILIDADES

6.1. Usuários

6.1.1. Manter o sigilo da senha.

6.1.2. Responder pelo acesso à rede corporativa, por meio de sua identificação.

6.1.3. Reportar incidentes de segurança da informação à ASI.

6.2. Direção

6.2.1. Orientar os usuários sob sua coordenação sobre a utilização de senhas.

6.3. Área de Informática

6.3.1. Padronizar e configurar os critérios das senhas de acesso à rede.

6.4. ASI

6.4.1. Analisar os incidentes de segurança da informação e recomendar ações corretivas e preventivas.

6.5. Auditoria Setorial

6.5.1. Verificar a conformidade com o estabelecido nesta norma e recomendar as ações necessárias.

7. PENALIDADES

7.1. O não cumprimento desta norma está sujeito às penalidades previstas em Lei.