

Política de Senhas para Segurança Cibernética Hospitalar

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer requisitos para a criação e utilização de senhas fortes, visando proteger os recursos de informação e tecnologia do hospital contra acesso não autorizado.

3. Escopo

Aplica-se a todos os usuários dos recursos de informação e tecnologia do hospital, incluindo:

- **Funcionários:** colaboradores, médicos, enfermeiros, etc.
- **Estagiários:** estudantes que realizam atividades no hospital.
- **Prestadores de serviço:** empresas e profissionais que prestam serviços ao hospital.
- **Pacientes:** pessoas que utilizam os serviços do hospital.

4. Política

4.1. Requisitos de Senhas

Todas as senhas utilizadas no hospital devem:

- Ter no mínimo 12 caracteres;
- Conter letras maiúsculas e minúsculas, números e símbolos;
- Não conter informações pessoais, como nome completo, data de nascimento ou CPF;
- Ser alteradas a cada 90 dias;
- Ser únicas para cada conta de usuário.

4.2. Gerenciamento de Senhas

Os usuários são responsáveis por:

- Manter suas senhas confidenciais;
- Não compartilhar suas senhas com ninguém;
- Memorizar suas senhas;
- Não anotar suas senhas em locais óbvios;
- Reportar qualquer suspeita de acesso não autorizado à equipe de TI.

5. Procedimentos Relacionados

- Política de Segurança da Informação
- Política de Controle de Acesso
- Política de Gerenciamento de Vulnerabilidades

6. Não Conformidade

O não cumprimento desta política pode resultar em sanções disciplinares, incluindo:

- Advertência verbal
- Advertência por escrito
- Suspensão do acesso aos recursos de informação e tecnologia
- Rescisão do contrato de trabalho

7. Compromisso/Autoridade da Gestão

A alta administração do hospital está comprometida com a segurança da informação e com a proteção dos dados. A equipe de TI é responsável pela implementação e monitoramento desta política.

8. Cronograma de Revisão

Esta política será revisada anualmente ou quando necessário.

9. Definições

- **Senha:** sequência de caracteres utilizada para autenticar um usuário em um sistema de informação.
- **Senha forte:** senha que é difícil de adivinhar ou decifrar.
- **Acesso não autorizado:** acesso a um sistema de informação sem a devida autorização.

Observações:

- Esta política é um exemplo e pode ser adaptada às necessidades específicas do hospital.
- É importante consultar especialistas em segurança da informação para auxiliar na implementação da política.