Política de Acesso Remoto para Segurança Cibernética Hospitalar

Baseada no Framework NIST 800-53

2. Propósito

Estabelecer requisitos para o acesso remoto aos recursos de informação e tecnologia do hospital, visando garantir a segurança da informação e a proteção dos dados.

3. Escopo

Aplica-se a todos os usuários que necessitem acessar os recursos de informação e tecnologia do hospital remotamente, incluindo:

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

4. Política

4.1. Permissão de Acesso

O acesso remoto aos recursos de informação e tecnologia do hospital só será permitido mediante autorização expressa da equipe de TI.

4.2. Requisitos de Segurança

Para acessar os recursos de informação e tecnologia do hospital remotamente, os usuários devem:

- Utilizar uma VPN (Virtual Private Network) configurada pelo hospital;

- Utilizar um dispositivo com sistema operacional atualizado e software de segurança instalado;
- Utilizar uma senha forte para autenticação;
- Não compartilhar suas credenciais de acesso com ninguém;
- Notificar a equipe de TI imediatamente em caso de qualquer suspeita de atividade maliciosa.

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

- **Acesso remoto:** acesso a um sistema de informação a partir de uma localização externa à rede local do hospital.

- **VPN:** rede privada virtual que criptografa o tráfego de dados e garante a segurança da comunicação.
- **Software de segurança:** software antivírus, antispyware e firewall que protege o dispositivo contra ataques cibernéticos.
- **Credenciais de acesso:** nome de usuário e senha utilizados para autenticação em um sistema de informação.

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.