Política de **Gestão de Informação**

HOSPITAL SÃO FRANCISCO
NA PROVIDÊNCIA DE DEUS

1. INTRODUÇÃO

A Política de Segurança de Informação do Hospital São Francisco na Providência de Deus estabelece diretrizes para assegurar o uso seguro e responsável das informações, visando proteger a integridade e confidencialidade dos dados e evitar riscos à organização.

2. JUSTIFICATIVA

A necessidade de uma Política de Segurança de Informação no Hospital São Francisco na Providência de Deus surge do crescente volume de dados gerenciados e do avanço das ameaças cibernéticas. Informações hospitalares, por sua natureza, são altamente sensíveis e requerem proteção rigorosa para evitar acesso não autorizado, manipulação indevida e possíveis interrupções nos serviços.

Estabelecer uma política clara é fundamental para criar uma cultura de segurança, onde todos os colaboradores entendam a importância da proteção de dados e as melhores práticas a serem seguidas. Além disso, essa política contribui para a conformidade com normas legais e regulatórias, garantindo que a organização esteja preparada para responder a incidentes e preservar a confiança de pacientes e parceiros.

3. OBJETIVOS

Esta política tem como objetivo fornecer uma estrutura para a gestão das informações, protegendo-as contra uso inadequado, vazamentos, e outros riscos que possam comprometer a operação da organização. A política se aplica a todos os funcionários, parceiros, prestadores de serviço e outros que possam ter acesso as informações da instituição.

4. TERMOS E DEFINIÇÕES

MFA - Autenticações de Múltiplos Fatores

VPN - Virtual Private Network

5. DESCRIÇÃO

Os princípios norteadores incluem confidencialidade, integridade e disponibilidade das informações. Estes princípios garantem que os dados:

- Estejam acessíveis apenas para aqueles com permissão (confidencialidade).
- Mantenham-se completos e inalterados sem autorização (integridade).
- Sejam acessíveis sempre que necessário (disponibilidade).

Classificação da Informação

As informações são classificadas para definir os níveis de segurança e controle:

- **Confidencial**
- **Restrita**
- **Interna**
- **Pública**

Cada categoria terá medidas específicas de segurança para proteger contra acesso não autorizado.

Controle de Acesso e Privilégios

Controle de Acesso

O acesso às informações é concedido com base no cargo e nas responsabilidades de cada colaborador, usando o Princípio do Menor Privilégio.

Privilégios e Responsabilidades

- **Autenticação:** Senhas e autenticações de múltiplos fatores (MFA) são exigidas para sistemas sensíveis.
- **Autorização:** O acesso é revisado regularmente para garantir que privilégios obsoletos sejam removidos.

Manuseio, Armazenamento e Proteção de Informações

Manuseio de Informações

A informação sensível deve ser manipulada com cuidados específicos, como:
- **Documentação física:** Armazenada em locais seguros e de acesso controlado.
- **Documentação digital:** Protegida com criptografia e senhas fortes.

Armazenamento Seguro

- **Digital:** Armazenamento em servidores seguros, com backup regular.
- **Físico:** Setor especifica com acesso restrito e locais seguros para armazenamento de documentos físicos.

Proteção de Informações em Trânsito

Uso de VPNs e criptografia para proteger dados transferidos via rede e entre dispositivos.

Retenção, Descarte e Conformidade

Retenção de Informações

A informação deve ser mantida apenas pelo período necessário para cumprir suas finalidades operacionais, legais ou regulamentares.

Descarte Seguro

Descarte eletrônico: Limpeza segura de dispositivos antes do descarte ou reciclagem.
Descarte físico: Fragmentação de documentos impressos confidenciais.

Conformidade

Todos os membros da organização devem seguir esta política. Qualquer violação poderá levar a ações disciplinares, incluindo demissão e possíveis sanções legais.

Monitoramento, Treinamento e Revisão

Monitoramento

A organização se compromete a monitorar o cumprimento da política, usando ferramentas e auditorias regulares para identificar possíveis incidentes de segurança.

Treinamento

Todo o colaborador recebeu treinamento sobre a política de segurança e manuseio da informação ao serem admitidos e em intervalos regulares.

Gestão de Documentos e Padronização de Processos

Documentação e Padronização de Processos

As informações necessárias para a padronização de processos e procedimentos devem estar centralizadas em sistemas dedicados, como o sistema Tasy, por meio da aplicação "Gestão da Qualidade". Cada setor é responsável por criar e manter documentos que orientem a execução correta das suas rotinas, em conformidade com a Política da Qualidade estabelecida.

Responsabilidade pelo Controle e Inserção de Documentos

O controle e a inserção de documentos no sistema são de responsabilidade do setor da Qualidade. Esse setor deve garantir que todos os documentos sejam atualizados e reflitam as práticas atuais da organização.

Distribuição e Obtenção de Cópias Controladas

A obtenção de cópias controladas é permitida mediante solicitação formal por e-mail ao setor da Qualidade, com uma justificativa apropriada para o pedido. Essa medida assegura o controle adequado de documentos e a sua distribuição.

Documentos Válidos para Auditoria

Para fins de auditoria, apenas os documentos institucionais disponíveis no sistema Tasy são considerados válidos, com exceção de formulários setoriais obtidos por meio do almoxarifado central ou instrumentos utilizados para coleta de dados

Revisão da Política

A política será revisada periodicamente para garantir sua adequação e atualização conforme novas regulamentações e mudanças tecnológicas.

6. RESPONSÁVEIS

Setor de Tecnologia da Informação, Qualidade e o SAME.

7. ANEXOS

Não se aplica.

8. REFERÊNCIAS BIBLIOGRÁFICAS

Não se aplica.