Política de Identificação de Ativos de Segurança Cibernética Hospitalar

Baseado no Framework NIST Cybersecurity

2. Propósito

Estabelecer um processo formal para a identificação e classificação de ativos de informação e tecnologia no ambiente hospitalar, visando a proteção contra ameaças cibernéticas.

3. Escopo

Aplica-se a todos os ativos de informação e tecnologia utilizados no hospital, incluindo:

- **Hardware:** computadores, servidores, dispositivos móveis, impressoras, etc.
- **Software:** sistemas operacionais, aplicativos, bancos de dados, etc.
- **Rede:** infraestrutura de rede, incluindo roteadores, switches, firewalls, etc.
- **Dados:** prontuários eletrônicos, informações financeiras, dados de pesquisa, etc.

4. Política

4.1. Responsabilidades

- **Diretor de TI:** responsável pela implementação e monitoramento da política.

- **Gerente de Segurança da Informação:** responsável pela criação e atualização do inventário de ativos.
- **Proprietários de ativos:** responsáveis por fornecer informações precisas sobre seus ativos.
- **Usuários de ativos:** responsáveis por usar os ativos de forma segura e responsável.

4.2. Processo de Identificação

- Todos os ativos de informação e tecnologia devem ser identificados e classificados de acordo com sua criticidade para o negócio.
- A classificação deve ser baseada em critérios como confidencialidade, integridade e disponibilidade dos dados.
- O inventário de ativos deve ser atualizado periodicamente para refletir mudanças no ambiente do hospital.

4.3. Ferramentas e Recursos

- Ferramentas de varredura de rede e software de gerenciamento de ativos podem ser utilizados para auxiliar na identificação de ativos.
- O inventário de ativos deve ser armazenado em um local seguro e acessível aos responsáveis pela segurança da informação.

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 ativos
- 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 ativos de informação e tecnologia.

8. Cronograma de Revisão

Esta política será revisada anualmente ou quando necessário.

9. Definições

- **Ativo de informação:** qualquer informação que tenha valor para o hospital.
- **Ativo de tecnologia:** qualquer componente de hardware, software ou rede que seja utilizado para processar, armazenar ou transmitir informações.
- **Criticidade:** importância de um ativo para o negócio.
- **Confidencialidade:** garantia de que apenas pessoas autorizadas tenham acesso a um ativo.
- **Integridade:** garantia de que um ativo é preciso e completo.
- **Disponibilidade:** garantia de que um ativo está disponível para uso quando necessário.