	POLÍTICA		POL-DIR-01.00
	Política de Segurança da informação		
Origem	**Data de Emissão**	**Versão**	**Aprovadores**
NTI	28/12/2024	00	Diretoria: Diretor Geral

Introdução

A segurança da informação visa proteger as informações, sistemas, recursos e outros ativos contra desastres, problemas e manipulação indevida, para reduzir as chances e impactos de incidentes de segurança.

Objetivo

Definir diretrizes e regras para a proteção das informações da organização, visando:

- Proteger os dados de acessos não autorizados.
- Preservar a integridade e a precisão das informações.
- Assegurar a disponibilidade dos sistemas e dados para os usuários autorizados.
- Promover o cumprimento das normas regulamentares aplicáveis, incluindo a LGPD (Lei Geral de Proteção de Dados).

Aplicação

Esta política aplica-se a:

- Todos os colaboradores, prestadores de serviço, parceiros e terceiros que tenham acesso às informações da organização.
- Todos os sistemas, equipamentos e recursos tecnológicos utilizados para o armazenamento, processamento ou transmissão de informações institucionais.
- Todas as informações, independentemente do formato (físico ou digital), relacionadas às atividades da instituição.

Responsabilidades

Este documento é de responsabilidade do setor NTI

Descrição

1. Atribuições
   - 1.1. Diretoria
     - 1.1.1. Garantir o apoio e o comprometimento com a implementação das diretrizes de segurança da informação.
     - 1.1.2. Aprovar os recursos necessários para a execução desta política.
   - 1.2. Gestão de TI
     - 1.2.1. Desenvolver e implementar controles para proteger os sistemas e as informações institucionais.
     - 1.2.2. Monitorar e revisar regularmente os controles de segurança da informação.
     - 1.2.3. Assegurar que os colaboradores recebam treinamento periódico em segurança da informação.
   - 1.3. Colaboradores e Terceiros
     - 1.3.1. Cumprir as diretrizes estabelecidas nesta política.
     - 1.3.2. Relatar imediatamente quaisquer incidentes de segurança da informação.
     - 1.3.3. Comitê de Segurança da Informação
     - 1.3.4. Supervisionar a implementação e conformidade com esta política.
     - 1.3.5. Avaliar riscos e propor medidas corretivas

2. Diretrizes Gerais
   2.1. Confidencialidade: Todas as informações sensíveis devem ser acessadas apenas por pessoas devidamente autorizadas.
   2.2. Integridade: As informações devem ser protegidas contra alterações não autorizadas.
   2.3. Disponibilidade: Os sistemas e as informações devem estar acessíveis sempre que necessário para os usuários autorizados.
3. Controles Técnicos
   3.1. Controle de Acesso
      3.1.1. Implementar controles para garantir que somente usuários autorizados tenham acesso a sistemas e dados.
      3.1.2. Restringir o acesso a sistemas, documentos e dados sensíveis apenas para usuários autorizados.
      3.1.3. Rever periodicamente as permissões de acesso concedidas aos colaboradores e terceiros.
   3.2. Firewall e Monitoramento de Rede
      3.2.1. Implantar firewalls para proteger a rede hospitalar contra acessos não autorizados.
      3.2.2. Utilizar sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar atividades suspeitas.
   3.3. Gestão de Vulnerabilidades e Atualizações
      3.3.1. Realizar atualizações regulares de software e sistemas para corrigir vulnerabilidades conhecidas.
   3.4. Backup e Recuperação de Dados
      3.4.1. Implementar backups regulares e automatizados de todos os sistemas importantes.
      3.4.2. Certificar de que os backups sejam armazenados em locais seguros, incluindo locais remotos, e testados regularmente para recuperação.
   3.5. Antivírus e Antimalware
      3.5.1. Manter soluções de segurança atualizadas em todos os dispositivos conectados à rede.
      3.5.2. Realizar varreduras regulares para identificar e eliminar ameaças.
4. Controles Organizacionais
   4.1. Políticas e Procedimentos
      4.1.1. Desenvolver políticas de segurança da informação específicas para o hospital, incluindo:
         4.1.1.1. Política de controle de acessos.
         4.1.1.2. Política de uso de dispositivos pessoais (BYOD).
         4.1.1.3. Política de resposta a incidentes de segurança.
   4.2. Treinamento e Conscientização
      4.2.1. Promover treinamentos regulares para colaboradores sobre boas práticas de segurança, incluindo:
      4.2.2. Identificação de phishing e golpes digitais.
      4.2.3. Uso adequado de senhas.
      4.2.4. Manuseio seguro de informações confidenciais.
   4.3. Gestão de Riscos
      4.3.1. Conduzir avaliações regulares de riscos para identificar ameaças e vulnerabilidades em sistemas hospitalares.

4.3.2. Desenvolver um plano de mitigação de riscos alinhado às melhores práticas.

5. Controles Processuais
   5.1. Gerenciamento de Incidentes de Segurança
      5.1.1. Estabelecer um procedimento claro para identificar, registrar, responder e resolver incidentes de segurança da informação
   5.2. Auditorias e Monitoramento
      5.2.1. Realizar auditorias periódicas para verificar a conformidade com políticas de segurança e regulamentações, como a LGPD.
      5.2.2. Utilizar ferramentas de monitoramento de logs para rastrear acessos e atividades suspeitas
   5.3. Proteção de Dados Pessoais (LGPD)
      5.3.1. Promover que o tratamento de dados pessoais sensíveis (como prontuários) esteja em conformidade com a LGPD.
      5.3.2. Obter consentimento explícito dos pacientes para coleta e uso de dados, quando necessário.
      5.3.3. Encarregar o (DPO - Data Protection Officer) para supervisionar a conformidade com a legislação.
   5.4. Segurança Física
      5.4.1. Controle o acesso físico a áreas sensíveis, como servidores e arquivos de prontuários, com uso de crachás ou biometria.
      5.4.2. Instale câmeras de segurança e implemente políticas para visitantes.
   5.5. Requisitos de Conformidade
      5.5.1. LGPD (Lei Geral de Proteção de Dados): Proteja os dados pessoais dos pacientes, incluindo informações sensíveis.
      5.5.2. ISO 27001: Implemente e certifique um Sistema de Gestão de Segurança da Informação (SGSI) alinhado ao padrão internacional.

Controle de Revisão

Data	Revisão	Motivo	Responsável
28/12/2024	00	Primeira Elaboração	NTI

Aprovadores

Nome	Cargo	Assinatura	Data
Nome	**Cargo**	**Assinatura**	**Data**

	POLÍTICA		POL-DIR-01.00
	Política de Segurança da informação		
Origem	**Data de Emissão**	**Versão**	**Aprovadores**
NTI	28/12/2024	00	Diretoria: Diretor Geral