

POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO (TI)

DATA	VERSÃO	ELABORAÇÃO	REVISÃO	APROVAÇÃO
02/05/2025	1	Gerência TI	Diretoria Administrativa	Responsável Legal

1. Objetivos

Esta Política de Tecnologia da Informação estabelece diretrizes para a gestão de Tecnologia da Informação (TI) no Hospital Vila Nova, garantindo a segurança, integridade, disponibilidade e confidencialidade das informações, além da conformidade legal e regulatória, alinhada às melhores práticas de governança.

Os principais objetivos são:

- Garantir a continuidade dos serviços hospitalares suportados por TI.
- Proteger dados sensíveis de pacientes, colaboradores e fornecedores.
- Assegurar conformidade com normas regulatórias, como LGPD, ANVISA e Resoluções do Conselho Federal de Medicina (CFM).
- Estabelecer responsabilidades para o uso adequado de ativos de TI.
- Prevenir incidentes de segurança e definir respostas eficazes a eventuais ameaças.

2. Abrangência

Esta Política se aplica a:

2.1 Todos os administradores, gestores e colaboradores do Hospital, incluindo médicos, enfermeiros, demais colaboradores e terceirizados.

2.2 Todos os dispositivos e sistemas utilizados no ambiente hospitalar, incluindo servidores, redes, computadores, dispositivos móveis e sistemas de gestão hospitalar (HIS, RIS, PACS etc.).

2.3 Dados coletados, processados e armazenados nos sistemas de TI do Hospital.

3. Definições

3.1 **Dados Sensíveis:** Informações pessoais ou clínicas dos pacientes e empregados, protegidas por regulamentações.

3.2 **Ativos de TI:** Equipamentos, softwares e infraestrutura de tecnologia da informação utilizados no hospital.

3.3 **Usuários:** Todos os profissionais que utilizam recursos de TI no ambiente hospitalar.

3.4 **Segurança da Informação:** Conjunto de práticas que garantem a confidencialidade, integridade e disponibilidade das informações.

3.5 **Gestão de Incidentes:** Processo para identificação, análise e resposta a eventos que comprometam a segurança ou disponibilidade dos sistemas.

4. Procedimentos

4.1. Gestão de Acesso

- O acesso aos sistemas será concedido com base no princípio do menor privilégio.
- Contas de usuários devem ser pessoais e intransferíveis, com autenticação multifator para acessos críticos.
- Logins de administradores e usuários serão monitorados e auditados regularmente.
-

4.2. Segurança da Informação

- O armazenamento e a transmissão de dados sensíveis devem utilizar criptografia.
- Dados de pacientes não devem ser armazenados em dispositivos pessoais ou compartilhados por meios não autorizados.
- Softwares e sistemas devem ser mantidos atualizados para minimizar vulnerabilidades.

4.3. Continuidade dos Serviços

- Devem existir planos de contingência para falhas em sistemas críticos, garantindo a continuidade da assistência hospitalar.
- Backups devem ser realizados regularmente e armazenados de forma segura.

4.4. Uso Adequado de Recursos de TI

- O uso dos sistemas deve ser exclusivamente para fins profissionais, respeitando normas institucionais.
- O acesso a sites e aplicativos não relacionados ao trabalho será restringido por políticas de firewall.

4.5. Gestão de Incidentes e Resposta a Ameaças

- Todos os incidentes de segurança devem ser reportados imediatamente à equipe de TI.
- A instituição deve manter um plano de resposta a incidentes para mitigar impactos e restaurar serviços rapidamente.

4.6. Conformidade e Auditoria

- A conformidade com esta política será auditada periodicamente.
- Serão realizados treinamentos regulares para conscientização dos usuários sobre boas práticas de segurança e uso de TI.

4.7 Disposições Finais

Esta Política entra em vigor na data de sua aprovação pela Diretoria e deve ser amplamente divulgada a todos os envolvidos no processo de contratação.

A Política deve ser revisada anualmente ou sempre que houver mudanças significativas nas operações ou na legislação.

5. Referências

- Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).
- Resolução CFM nº 2.314/2022 – Regras para o uso de tecnologia na prática médica.
- NIST Cybersecurity Framework.
- ITIL (Information Technology Infrastructure Library) para governança de TI.
- Norma ISO/IEC 27001 – Segurança da Informação.
- Agência Nacional de Vigilância Sanitária (ANVISA)

Esta Política entra em vigor na data de sua aprovação, pela Diretoria Executiva, em 02 de maio de 2025, e será revisado a cada dois anos ou sempre que necessário.