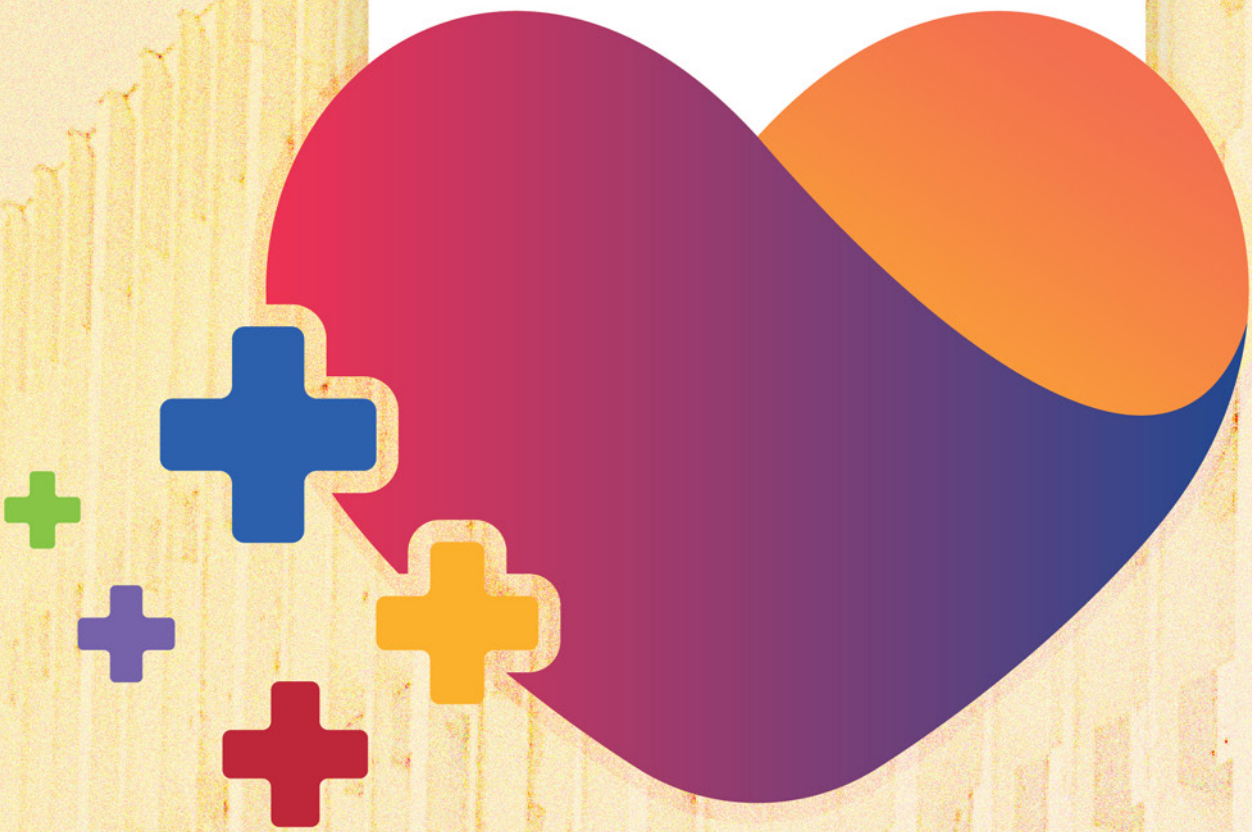
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



GRUPO SANTA CASA DE FRANCA

Experiência e inovação a serviço da vida.
Rumo aos 130 anos!

GRUPO
SANTA CASA
DE **FRANCA**

MISSÃO

Assistência e ensino voltado à saúde.

VISÃO

Ser uma instituição sustentável, com equilíbrio econômico financeiro, reconhecida pela excelência na assistência em saúde e na geração do conhecimento, através da melhoria contínua de processos, tecnologia inovadora e comprometimento de seus colaboradores.

VALORES

Empatia
Se colocar no lugar da outra pessoa entendendo seus sentimentos e emoções.
Transparência
Ter clareza nas ações e na prestação de contas.
Integridade
Honestidade e imparcialidade nas atitudes.
Comprometimento
Compromisso com o que faz
Acolhimento
Hospitalidade, ter afeto e acolher o outro.

GRUPO SANTA CASA DE FRANCA

INFORMAÇÕES **Documentais**

Documento: nº 01

Código: POL - 07

Data Revisão: -

Revisão: -

Vigência: 2 ANOS

Elaborado por: Willian Sartorio, Rosilaine Pessoni e Thales

Aprovado por: Thiago Silva, Tony Graciano, Alan Riboli e Willian Sartorio

Emissão: 05/2024

DECLARAÇÃO

A Política de segurança da informação tem por finalidade assegurar as diretrizes e regras estabelecidas para orientar o uso eficiente, seguro e estratégico de recursos da tecnologia da informação, desempenhando um papel crucial na gestão da infraestrutura tecnológica e na garantia da conformidade com regulamentos. Ainda, têm como base a proteção de dados, o gerenciamento de riscos e a otimização dos recursos.

PRINCÍPIOS

Confidencialidade;
Integridade;
Disponibilidade;
Autenticidade;
Legalidade.

DIRETRIZES

Segurança da Informação;
Lei Geral de Proteção de Dados (LGPD);
Inovação;
Parque tecnológico;
Sistemas de Informação;
Gestão de Riscos;
Gestão de Dados;
Gestão de Contratos.

OBJETIVOS

Estabelecer as responsabilidades, obrigações e comportamentos esperados dos usuários da informação, com o uso adequado dos recursos tecnológicos, fortalecendo a proteção contra ameaças internas e externas.

AÇÕES

São processos que visam, com ações planejadas e coordenadas, a concretizar as diretrizes da Política de segurança da informação:

1. *Segurança da Informação*

Gerenciar o controle de acesso dos usuários da informação, definindo critérios de senhas, perfis de permissões e restrições, utilização de softwares e navegação de internet;
Definir regras de segurança para uso de dispositivos (computadores, tablets, smartphone, etc) pessoais e da organização;
Definir regras de conectividade dos equipamentos de segurança da organização (Firewall);
Definir regras de segurança para conectividade WI-FI para colaboradores, visitantes e pacientes;
Manter atualizados os sistemas computacionais, assegurando as aplicações de patchs de segurança;
Realizar os backups dos arquivos de trabalho e banco de dados das aplicações através das ferramentas padronizadas e automatizadas, com garantia de retenções.

2. *Lei Geral de Proteção de Dados (LGPD)*

Os dados pessoais só serão coletados com consentimento explícito dos titulares.
Os dados devem ser limitados ao mínimo necessário para a finalidade específica e devem ser mantidos atualizados e precisos;
O compartilhamento de dados pessoais com terceiros só é permitido quando estritamente necessário e com base em contratos que garantam a segurança e conformidade com a LGPD;
É vedada a divulgação de informações pertinentes a dados pessoais, sensíveis, documentos físicos e digitais e de cunho institucional entre setores ou de forma externa ao ambiente de necessidade de uso da informação a fim de preservar a informação e inibir que estas sejam utilizadas para práticas ilícitas, como fraudes e crimes – no mundo digital ou não, divulgação inapropriada e/ou pejorativa e sem autorização do detentor dos dados.

3. *Inovação*

Informatizar os processos executados de forma manual;
Utilizar as várias potencialidades da inteligência artificial, em uma convivência saudável e ética com a atividade humana, para reduzir o tempo e o custo dos processos e aumentar a eficiência.
Telemedicina para o cuidado dos pacientes.

4. Parque Tecnológico

Promover a renovação dos equipamentos de informática;
Realizar o descarte ecologicamente correto dos equipamentos de informática.

5. Sistemas de Informação

Promover a utilização dos sistemas de Gestão para todos os registros hospitalar, pessoas e rotinas administrativas;
Interoperabilidade entre sistemas.

6. Gestão de Riscos

Links de conectividade, assegurando estabilidade junto aos fornecedores;
Servidores de aplicações, permitindo segurança na disponibilidade dos sistemas aos usuários;
Rotinas de backups, assegurando integridade dos dados para possível restore em casos de desastres;
Atualizações de sistemas em ambientes de homologação, permitindo a validação de patchs de correção e atualização.

7. Gestão de Dados

Fomentar a análise de Indicadores para tomada de decisão;
Promover a utilização de relatórios padronizados como fonte de informações;
Construir painéis visuais acessível para monitoramento e tomadas de decisão.

FORMA DE MONITORAMENTO

Monitoramento de links de conectividade;
Monitoramento de servidores de aplicações;
Conferência de backups;
Consulta de logs;
Relatório mensal de diagnóstico de ambiente.

GRUPO
SANTA CASA
DE FRANCA

gruposantacasadefranca.com.br