POLÍTICA - SEGURANÇA DA INFORMAÇÃO

Data de emissão e aprovação:	Data da revisão:	Versão:
08/09/2025	08/09/2027	1
Elaborado por:	**Aprovado por:**	
Luana Martins de Santana		
Este documento é classificado como: Público		

Sumário

Data de emissão e aprovação:	Data da revisão:	Versão:
08/09/2025	08/09/2027	1
Elaborado por:	**Aprovado por:**	
Luana Martins de Santana		
Este documento é classificado como: Público		

1. OBJETIVO

Definir as diretrizes de Segurança da Informação da Hapvida NotreDame Intermédica ("Companhia"), por meio do estabelecimento de regras para o manuseio, tratamento, controle e proteção das informações em qualquer meio de processamento, armazenamento e utilização, considerando as seguintes premissas:

a) Prevenir incidentes de segurança da informação;
b) Salvaguardar os ativos de informação;
c) Disseminar a importância da segurança da informação;
d) Garantir a continuidade do processamento das informações do negócio.

2. ABRANGÊNCIA

A Política de Segurança da Informação abrange todos os membros, conselheiros, diretores, administradores da Companhia e de suas controladas diretas ou indiretas, bem como, procuradores, responsáveis técnicos/administrativos, líderes, funcionários e prestadores de serviço, consultores, terceiros interpostos, dentre outros que mantenham relações e que tenham acesso a dados e informações de qualquer unidade, filial, sucursal etc. Para efeito da Política de Segurança da Informação, tais pessoas serão denominadas **usuários**.

3. REFERÊNCIAS

ISO/IEC 27001:2022
NIST Cybersecurity Framework V1.1
LGPD - Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018)
Código de Conduta da Companhia

4. DEFINIÇÕES E SIGLAS

Para os efeitos desta Política de Segurança da Informação aplicam-se os termos e definições abaixo:

- Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que possa resultar em dano para um sistema, órgão ou entidade da estrutura organizacional da empresa.
- Ativo de Informação: algo que tem valor para empresa, geralmente ativos que podem materialmente a entrega de um produto ou serviço, pela sua ausência ou deterioração, ou causar dano à empresa por meio da perda da disponibilidade, integridade ou confidencialidade.

- Incidente de segurança da informação: um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da empresa.
- PSI: Política de Segurança da Informação, documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na empresa.
- Sistemas de Informação: é um sistema cujo elemento principal é a informação. Seu objetivo é armazenar, tratar e fornecer informações de tal modo a apoiar as funções ou processos de uma organização.
- Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.
- N1: Executivo com reporte direto ao Presidente;
- N2: Executivo com reporte direto ao N1;
- N3: Executivo com reporte direto ao N2.

5. DESCRIÇÃO

5.1. CONTEÚDO GERAL

Os dados e informações dos beneficiários e pacientes consignados em cadastros, sistemas, prontuários, fichas clínicas etc., são protegidos por lei, revestidos de absoluto sigilo e confidencialidade e somente poderão ser divulgados mediante autorização do paciente e/ou seu responsável legal, observando os limites consignados no Código de Ética Médico publicado pelo Conselho Federal de Medicina, a Lei Geral de Proteção de dados (Lei Nº 13.709, de 14 de agosto de 2018), as políticas internas da empresa, as recomendações da área Jurídica e, se pertinente, da assessoria de imprensa no caso de envolvimento de mídias.

As informações da empresa e/ou consignadas são ativos essenciais no negócio, portanto elas deverão ser devidamente protegidas e utilizadas de modo ético e seguro, conforme preconiza o Código de Conduta da Companhia, garantindo confiabilidade através da proteção da:

a) **Confidencialidade**: Garantir que os dados e informações não sejam revelados ou estejam disponíveis para indivíduos, entidades e processos não autorizados;
b) **Integridade**: Garantir a salvaguarda da exatidão e totalidade dos dados e informações e dos métodos de processamento;

c) **Disponibilidade**: Garantir que dados e informações estejam sempre acessíveis e disponíveis quando necessário, considerando a Prontidão: Ser acessível sempre que necessária, a Continuidade: Manter-se disponível mesmo quando houver falhas nos sistemas, e a Robustez: Atender a todos os usuários do sistema sem que haja uma degradação que comprometa o resultado.

5.2. DIRETRIZES

Para endereçar todo o esforço e manutenção necessária para a Gestão de Segurança da Informação, a empresa estabelece as seguintes diretrizes:

a) Uma estrutura de Gestão da Segurança da Informação está estabelecida e mantida com apoio da Alta Administração;
b) A informação deverá ser utilizada com senso de responsabilidade e de modo ético, de forma clara, completa e segura por todos os usuários, em benefício exclusivo dos negócios corporativos;
c) Todos os ativos de informação deverão ser devidamente identificados, classificados e monitorados;
d) A identificação de cada usuário da empresa deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
e) Controles tecnológicos e/ou processuais devem ser definidos e incorporados no desenho da solução, para todo desenvolvimento interno ou externo, na contratação de soluções como serviço e que envolvam o uso de novas tecnologias, com objetivo de proteger as informações e os ativos de tecnologia e minimizar os riscos associados. As diretrizes de segurança especificadas neste documento e nas Normativas Administrativas devem ser obrigatoriamente respeitadas;
f) Medidas de segurança física devem ser adotadas para garantir a proteção das informações e dos ativos de tecnologia da empresa contra acessos não autorizados, eventos que acarretem danos aos ativos, incluindo desastres ambientais como incêndio, terremotos, enchentes ou explosão;
g) Um programa de conscientização, educação e treinamento em Segurança da Informação deve ser implementado para garantia dos objetivos, princípios e diretrizes definidas neste documento e nas Normativas Administrativas;
h) Todas as pessoas físicas ou jurídicas que prestam serviços internos ou externos devem utilizar os ativos de acordo com as cláusulas contratuais firmadas com fornecedores, parceiros e clientes. A utilização de ativos da informação deve respeitar a legislação vigente,

esta PSI e demais documentos internos que versem sobre o tema Segurança da Informação da Companhia;

i) Avaliações de riscos de Segurança da Informação serão realizadas, para identificar os riscos associados ao comprometimento da confidencialidade, integridade e disponibilidade da informação;

j) Todos os riscos relativos à segurança da informação deverão ser analisados, classificados e apresentados à área de Riscos e Controles Internos, que deliberará sobre o tratamento adequado para tais juntamente com a área técnica especializada;

k) Todos os incidentes de segurança devem ser reportados a área de Segurança da Informação, para que sejam analisados, avaliados, tratados e comunicados a Alta Administração da Companhia. Quando houver impacto em dados pessoais e sensíveis, estes devem ser reportados também à área de Diretoria de Riscos, Proteção de Dados e Responsabilidade Social.

5.3. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Para manter um nível satisfatório de segurança da informação foi constituído um conjunto de documentações para sustentar as diretrizes apresentadas. Essas documentações se encontram publicadas na intranet da empresa.

Situações específicas não contempladas ou que estejam conflitantes com esta PSI, devem ser analisadas pela área de Governança de Segurança da Informação e formalmente documentadas. As áreas de Compliance e de Auditoria Interna poderão ser envolvidas sempre que se fizer necessário.

5.4. MONITORAMENTO E AUDITORIA

A empresa deve monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto, a organização deve manter controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgar necessários para reduzir os riscos, e reservar-se o direito de:

a) Implantar sistemas de monitoramento de acesso aos ativos de informação da empresa. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

b) Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;

c) Instalar câmeras nas instalações físicas.

5.5. PAPÉIS E RESPONSABILIDADES

5.5.1. Usuários

Os usuários da empresa, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis em cumprir, fazer cumprir e zelar pela materialização e realização eficaz da PSI, no compromisso com os critérios legais e éticos que envolvem a empresa.

É de inteira responsabilidade de cada usuário qualquer prejuízo ou dano que vierem a sofrer ou causarem a empresa e/ou a terceiros, em decorrência de não atendimento às diretrizes dessa PSI.

Cabe a todos os usuários:

a) Cumprir fielmente as diretrizes descritas nessa PSI;
b) Buscar orientação do superior hierárquico, quando houver dúvidas relacionadas à segurança da informação;
c) Assinar o Termo de Responsabilidade ou ciência eletrônica, formalizando a ciência da PSI bem como assumindo a responsabilidade pelo seu cumprimento;
d) Proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela empresa;
e) Os logins e senhas utilizados para acesso aos sistemas e aplicações são pessoais, confidenciais e intransferíveis;
f) Utilizar senha segura, devendo alterar a mesma, conforme periodicidade determinada pela empresa;
g) Assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse da empresa;
h) Comunicar imediatamente através dos canais formais, à área de Segurança da Informação, a ocorrência de um incidente de segurança da informação, bem como qualquer descumprimento ou violação desta PSI;
i) Classificar e proteger as informações da empresa.

5.5.2. Gestores

É responsabilidade de cada gestor levantar, atribuir valor e analisar as informações quanto aos riscos de segurança da informação, todos os ativos de informação necessários à sua área.

Cabe a todo gestor de área:

a) Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores internos sob a sua gestão;
b) Garantir que os colaboradores acessem os conteúdos obrigatórios na plataforma educacional para a formalização da PSI e Normativas Administrativas;
c) Cumprir e fazer cumprir esta PSI;
d) Assegurar que suas equipes possuam acesso e conheçam esta PSI;
e) Conscientizar sobre a PSI na fase de contratação de terceirizados e parceiros, quando este necessitar ter contato com informações da empresa;
f) Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para prestadores de serviços em geral que não sejam contratados;
g) Requisitar o acesso aos ativos de informação, somente no nível necessário, para a execução da atividade de seu funcionário ou colaborador;
h) Solicitar o imediato cancelamento do acesso aos ativos de informação de todo o funcionário e/ou prestador de serviço, sob a sua gestão, que seja desligado da empresa ou que tenha seu contrato finalizado;
i) Adaptar as documentações, processos, e Sistemas sob sua responsabilidade para atender a esta PSI.

5.5.3. Proprietários da Informação

O Proprietário da informação é o N2 dono do processo, e na sua ausência sendo o N3. Tem como responsabilidade à determinada informação ou conjunto de informações pertencentes à empresa ou sob sua guarda.

Cabe ao proprietário da informação:

a) Implementar e zelar pelo cumprimento dos controles de segurança a serem aplicados aos ativos de informação sob sua responsabilidade;
b) Definir a finalidade para o tratamento das informações e o período de retenção das informações sob sua responsabilidade;

c) Autorizar e avaliar periodicamente os acessos as informações sob sua responsabilidade junto a área de Segurança da Informação e identificar aqueles que não são mais necessários;
d) Classificar as informações sob sua responsabilidade e reclassificá-las sempre que necessário;
e) Adotar medidas para mitigar riscos associados aos ativos de informação sob sua responsabilidade e, aceitar os riscos em caso de não cumprimento das diretrizes de Segurança da informação em conjunto com a Diretoria das áreas envolvidas;
f) Participar sempre que convocado dos fóruns de Segurança da Informação, prestando os esclarecimentos quando solicitado;
g) Classificar o dado compartilhado e designá-lo apenas para o grupo específico de pessoas de acordo com a finalidade determinada, a fim de evitar possíveis riscos de exposição de informações

5.5.4. Segurança da Informação

A área será responsável por:

a) Estabelecer e manter atualizada a PSI e respectivas documentações;
b) Verificar o cumprimento das regras definidas na PSI juntamente com a Auditoria;
c) Identificar e documentar as violações e suas consequentes ações disciplinares juntamente com os gerentes locais e a área de Recursos Humanos, tendo como base o processo de gestão de incidentes de Segurança da Informação;
d) Propor as metodologias e processos específicos para a Segurança da Informação, como por exemplo, Análises, Avaliações e Tratamento de Riscos;
e) Promover, junto às demais áreas de apoio, conscientização dos colaboradores internos, externos e parceiros em relação à relevância da Segurança da Informação para o negócio da empresa;
f) Avaliar e adequar controles específicos de Segurança da Informação para sistemas ou serviços;
g) Analisar criticamente incidentes e reportar para a Alta Administração;
h) Manter a empresa informada sobre novas tendências e ameaças, além de propor medidas, arquiteturas e processos para elevar o nível de segurança da informação.

5.5.5. Tecnologia da Informação

A área será responsável por:

a) Manter atualizado o inventário de todos os ativos tecnológicos (Infraestrutura e Sistemas);
b) Atualizar sempre que possível os ativos tecnológicos de acordo com a liberação dos fabricantes;
c) Adotar as diretrizes de Segurança da Informação para o desenvolvimento ou aquisição de sistemas de informação;
d) Adotar as diretrizes de Segurança da Informação para configuração de ativos tecnológicos;
e) Gerir o uso de tecnologias necessárias e garantia do bom andamento dos negócios da empresa, incluindo ações preventivas e tratamento de incidentes a fim de promover maior nível de Segurança da Informação;
f) Avaliar e tratar vulnerabilidades relacionados a riscos identificados pelas áreas de Segurança da Informação, Auditoria, Compliance e Controles Internos;
g) Propor e apoiar iniciativas que visem à segurança dos ativos de informação da empresa.

5.5.6. Jurídico

Cabe ao Departamento Jurídico:

a) Promover apoio, respaldo e embasamento legal para as ações voltadas à Segurança da Informação, incluindo exposição na mídia, uso dos recursos tecnológicos, entre outros;
b) Acompanhar incidentes que violem a PSI e as Normativas de Segurança da Informação;
c) Orientar para a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário;
d) Elaborar e revisar documentos jurídicos relacionados à Segurança da Informação;
e) Acompanhar o processo disciplinar interno, validando as penalidades e exceções, quando houver;
f) Informar a Segurança da Informação sobre eventuais alterações legais e/ou regulatórias, que impliquem responsabilidade e/ou ações envolvendo proteção da informação;
g) Assessorar a área de Segurança da Informação, quando solicitada, na adoção de medidas em função do descumprimento da Política de Segurança da Informação, e também na revisão do conteúdo da PSI.

5.5.7. Recursos Humanos

Cabe ao Departamento de Recursos Humanos:

a) Garantir a disponibilização dos conteúdos da PSI na plataforma digital homologada, garantindo a transmissão das informações;
b) Fornecer para a área de Tecnologia da Informação, informações sobre admissões, desligamentos, afastamentos ou férias, movimentações de áreas dos funcionários;

c) Apoiar a área de Segurança da Informação no programa de treinamento e conscientização em Segurança da Informação dos funcionários, bem como, na realização de avaliações periódicas do grau conscientização em Segurança da Informação;
d) Colaborar com a área de Segurança da Informação na avaliação da infração e na determinação da penalidade quando observada alguma violação à Política de Segurança da Informação.

5.6. VIOLAÇÕES E SANÇÕES

São consideradas violações a esta PSI e as Normativas Administrativas de Segurança da Informação as seguintes situações, não se limitando às mesmas:

a) Não cumprimento das diretrizes e requisitos estabelecidos na PSI da empresa;
b) Uso indevido, divulgação não autorizada de informações, segredos comerciais ou outras informações sem autorização formal do gestor responsável;
c) Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis, regulamentos internos e externos e Código de Ética da empresa;
d) Qualquer situação que exponha a empresa à perda financeira ou comprometimento de imagem, em decorrência violação da confidencialidade, integridade ou disponibilidade das suas informações ou das quais que detenham custódia;
e) Não é permitido que funcionários e prestadores de serviço se manifestem sobre qualquer assunto de interesse da empresa pela imprensa, meio de comunicação externa, redes sociais, sem prévia e formal autorização do gestor competente.

Toda e qualquer infração ou suspeita de descumprimento à PSI e às Normativas Administrativas de Segurança da Informação deverá ser informada à área de Segurança da Informação por meio dos canais disponíveis, inclusive o Canal de Denúncias, amplamente divulgado nos sites e intranet da Companhia. Por conseguinte, apurada por meio de procedimentos internos com ciência e/ou suporte da Diretoria de Auditoria e Compliance da Companhia.

Qualquer descumprimento desta PSI por parte do usuário estará sujeito as sanções estabelecidas na Política de Consequências e no Código de Conduta Ética da Companhia.

Em caso de incidentes de segurança decorrente do uso indevido, negligente ou imprudente dos recursos e serviços, a empresa reserva-se do direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais

cabíveis. Essa análise não requer comunicação prévia ao portador do recurso (telefone, e-mail etc.).

5.7. DIVULGAÇÃO E DECLARAÇÃO DE RESPONSABILIDADE

A PSI deve ser de conhecimento de todos os usuários. Sua divulgação e educação são de suma importância para a empresa, e poderá ser divulgada ou publicada das seguintes formas:

a) Impressa;
b) Digital; e
c) Áudio visual.

Cabe as unidades de negócios juntamente com a equipe de Segurança da Informação e equipe de Comunicação Interna e Marketing, analisar e definir a melhor forma de divulgação, considerando e respeitando a cultura e costumes, leis e regulamentos vigentes, e evitando qualquer tipo de discriminação.

Todos os usuários devem aderir formalmente ao "**Termo de Ciência e Responsabilidade da PSI**" físico ou eletrônico, confirmando a ciência e comprometendo-se a respeitar esta PSI e suas Normativas Administrativas de forma integral.

6. DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação entrará em vigor a partir de sua aprovação e publicação.

7. HISTÓRICO DE ALTERAÇÕES

Data	Versão	Área	Descrição da Atividade
29.06.2023	1.0	Conselho de administração - CA	Aprovação da emissão
14.01.2025	2.0	Segurança da Informação	Retirada a referência ao documento: Manual - Classificação e Manuseio de Informação
08.09.2025	3.0	Segurança da Informação	Retirada a referência ao documento: Manual – Gestão de Documentos