# POLÍTICA INSTITUCIONAL

| *TÍTULO* | *CONTROLE* | *REVISÃO* |
|---|---|---|
| ***POLÍTICA DE SEGURANÇA DA INFORMAÇÃO*** | *PI-INSGQ-011* | *003* |
| *ÁREA RESPONSÁVEL* | | *VIGÊNCIA* |
| *TECNOLOGIA DA INFORMAÇÃO* | | *2026* |



## *ABRANGÊNCIA*

Hospital Infantil Francisco de Assis

## *TERMOS E DEFINIÇÕES*

- PEP - Prontuário Eletrônico do Paciente;
- SI - Sistemas de Informação;
- TI - Tecnologia da Informação;
- PSI - Política de Segurança da Informação;
- GTI - Gerência de Tecnologia da Informação;
- PSI - Política de Segurança da Informação;
- DPO - Data Protection Officer.

## *1. OBJETIVO*

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio e local em que ela esteja contida, com base na legislação vigente, órgãos reguladores, autorreguladores e nas boas práticas de segurança da informação.

## *2. DIRETRIZES*

**1. DEFINIÇÃO — Versão Revisada e Melhorada**

Segurança da Informação é o conjunto de práticas, processos, políticas, tecnologias e responsabilidades organizacionais destinados a proteger as informações contra ameaças internas e externas, assegurando sua **confidencialidade, integridade, disponibilidade e autenticidade**. Seu objetivo central é garantir a continuidade das operações da instituição, reduzir riscos e preservar o valor dos ativos de informação.
A proteção das informações é alcançada por meio da implementação e melhoria contínua de controles administrativos, físicos, tecnológicos e organizacionais, que devem ser **estabelecidos, monitorados, avaliados criticamente e aprimorados de forma sistemática**.
Para fins desta Política, considera-se **informação** toda forma de dado, conhecimento, documento, conteúdo, mensagem, processo, critério, diretriz ou registro — em meio físico ou eletrônico — pertencente, sob responsabilidade ou sob custódia da instituição. Incluem-se, também, dados de clientes, colaboradores, fornecedores e demais partes relacionadas.

A seguir, apresentam-se os termos utilizados nesta Política:
**A**

- **Acesso:** Ato de ingressar, consultar ou utilizar informações ou ativos de informação.
- **Ameaça:** Qualquer fator interno ou externo que possa explorar vulnerabilidades e causar impacto negativo.
- **Análise de riscos:** Processo para identificar ameaças, vulnerabilidades e estimar os riscos associados.
- **Atividade:** Conjunto de processos que produzem ou suportam produtos, informações ou serviços institucionais.
- **Ativo:** Qualquer recurso (humano, tecnológico, físico, lógico ou processual) com valor para a organização.
- **Ativos de Informação:** Informações, sistemas, meios de armazenamento, transmissão, processamento, instalações e pessoas que interagem com esses elementos.
- **Autenticidade:** Garantia de que a informação foi criada, enviada ou alterada por fonte legítima.
- **Avaliação de riscos:** Comparação entre riscos identificados e critérios predefinidos para determinar sua relevância.

**C**

- **Celeridade:** Prontidão na resposta a incidentes, falhas e eventos de segurança.
- **Classificação da informação:** Processo de categorização conforme sensibilidade, criticidade e necessidade de proteção.
- **Confidencialidade:** Garantia de que a informação somente é acessível a pessoas e sistemas autorizados.
- **Controle de acesso:** Conjunto de mecanismos para conceder, restringir ou revogar acessos.
- **Custodiante do ativo de informação:** Pessoa ou área responsável pela guarda, preservação, operação ou manutenção de um ativo de informação.

**D**

- **Disponibilidade:** Garantia de acesso à informação e aos sistemas sempre que necessário.

**E**

- **Ética:** Observância dos direitos, responsabilidades e condutas esperadas, sem prejuízo à segurança da informação.
- **Evento de segurança da informação:** Qualquer ocorrência que indique possível violação, falha de controle ou situação anômala.

**G**

- **Gerenciamento de ativos:** Atividades de identificação, documentação, controle e manutenção dos ativos de informação.
- **Gerenciamento de riscos de Segurança da Informação e Comunicações (SIC):** Conjunto de processos para identificar, tratar e monitorar riscos sobre os ativos de informação.
- **Gestão de Segurança da Informação e Comunicações:** Conjunto integrado de práticas que abarcam gestão de riscos, continuidade, tratamento de incidentes, conformidade, segurança lógica, física e organizacional.

**I**

- **Incidente de SIC:** Ocorrência que cause danos, interrupção ou coloque em risco ativos críticos de informação.
- **Informação:** Dados, textos, imagens, registros, processos ou quaisquer representações com significado e valor organizacional.
- **Integridade:** Garantia de que a informação não foi alterada de forma não autorizada ou acidental.

**P**

- **Política de Segurança da Informação e Comunicações:** Documento formal que estabelece diretrizes, responsabilidades e princípios para a proteção das informações.
- **Proprietário de ativos de informação:** Unidade administrativa que detém responsabilidade sobre um conjunto de informações e seus respectivos ativos.

**Q**

- **Quebra de segurança:** Ação ou omissão acidental ou intencional que comprometa a segurança da informação.

**R**

- **Resiliência:** Capacidade da instituição de resistir, responder e recuperar-se de incidentes e desastres.
- **Responsabilidade:** Obrigação dos usuários, gestores e colaboradores de cumprir esta Política e os controles de segurança.
- **Risco de SIC:** Probabilidade de exploração de vulnerabilidades por ameaças, causando impacto negativo ao negócio.

**T**

- **Terceiros:** Pessoas ou organizações externas à instituição que tenham interação com seus ativos de informação.
- **Tratamento de incidentes:** Processo de recepção, análise, classificação, resposta, correção, registro e comunicação de incidentes de segurança.

**U**

- **Usuário:** Qualquer pessoa autorizada a acessar ativos de informação.

**V**

- **Vulnerabilidade:** Fraqueza ou condição que pode ser explorada por uma ameaça.

| TÍTULO | CONTROLE | REVISÃO |
|---|---|---|
| **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** | PI-INSGQ-011 | 003 |
| ÁREA RESPONSÁVEL | | VIGÊNCIA |
| TECNOLOGIA DA INFORMAÇÃO | | 2026 |



## 2. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política de Segurança da Informação (PSI) está em conformidade com as principais leis, normas e diretrizes que regem a proteção da informação, privacidade de dados pessoais e governança institucional, aplicando-se integralmente ao HIFA e às suas unidades.

As referências legais e normativas consideradas para elaboração e aplicação desta PSI incluem, mas não se limitam a:

- **ISO/IEC 27000 e família ISO/IEC 27001/27002**, que estabelecem fundamentos, diretrizes e controles para a Gestão de Segurança da Informação;
- **Lei nº 12.965/2014 — Marco Civil da Internet**, que disciplina o uso da internet no Brasil e assegura direitos e garantias fundamentais;
- **Lei nº 13.709/2018 — Lei Geral de Proteção de Dados (LGPD)**, que estabelece princípios, direitos e obrigações relacionadas ao tratamento de dados pessoais;
- **Código de Conduta e Ética do HIFA**, que orienta comportamentos e responsabilidades individuais;
- **Contrato de Trabalho**, contendo obrigações legais e condutas esperadas de colaboradores;
- **Contratos de Prestação de Serviços**, que estabelecem responsabilidades e requisitos aplicáveis a terceiros;
- **Política de Tratamento de Dados Pessoais do HIFA**, que define diretrizes específicas para proteção e uso adequado de dados pessoais e sensíveis.

## 3. PRINCÍPIOS DA INSTITUIÇÃO

A presente PSI está fundamentada nos princípios institucionais que orientam a atuação responsável, transparente e segura no tratamento das informações. São eles:

- **Celeridade:** As ações de Segurança da Informação e Comunicações (SIC) devem assegurar respostas rápidas a incidentes, falhas, vulnerabilidades e demais situações que possam comprometer ativos de informação.
- **Ética:** A proteção dos direitos, interesses e da privacidade de usuários, agentes públicos, colaboradores e demais partes devem ser garantida, sem prejuízo às medidas de segurança.
- **Clareza:** As regras, diretrizes e controles de segurança devem ser apresentadas de forma objetiva, precisa e de fácil compreensão, facilitando sua aplicação e fiscalização.
- **Legalidade:** Todas as ações relativas à segurança da informação devem observar rigorosamente a legislação vigente, normas internas, políticas institucionais e atribuições estatutárias.
- **Publicidade:** O tratamento da informação deve observar o princípio da transparência, exceto nos casos em que o sigilo seja necessário para proteção legal, regulatória, estratégica ou operacional.

## 4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios fundamentais da Segurança da Informação que orientam esta PSI são:

**• Confidencialidade**

Garantir que a informação seja acessível exclusivamente a pessoas, sistemas ou entidades devidamente autorizados. Informações confidenciais devem ser protegidas contra divulgação não autorizada, assegurando sigilo e acesso restrito conforme necessidade institucional.

**• Integridade**

Assegurar que a informação permaneça exata, completa e não modificada de forma indevida, acidental ou não autorizada. Esse princípio garante que os dados preservem seu formato, conteúdo e finalidade original, sustentando a confiabilidade dos processos institucionais.

**• Disponibilidade**

Garantir que a informação, os sistemas e os serviços estejam acessíveis sempre que necessários para o desempenho das atividades institucionais. A disponibilidade depende de infraestrutura adequada, continuidade operacional, eficiência dos sistemas e resiliência tecnológica.

**• Autenticidade**

Assegurar que a informação seja produzida, modificada ou consultada por indivíduos ou sistemas legítimos,

permitindo identificar sua origem e autoria. Para garantir esse princípio, é indispensável o uso de credenciais seguras, a proteção de senhas, o não compartilhamento de acessos e a prevenção de uso indevido de contas institucionais.

## 5. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) Lei nº 13.709/2018 estabelece princípios, direitos e obrigações voltados à proteção dos direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural.

O HIFA adota as diretrizes da LGPD e aplica controles que asseguram:

- O tratamento legítimo, ético e transparente de dados pessoais e dados pessoais sensíveis;
- O respeito aos direitos dos titulares;
- A adoção de medidas técnicas e administrativas adequadas para prevenir, detectar e responder a incidentes envolvendo dados pessoais;
- A promoção da cultura de privacidade e de responsabilidade institucional.

## 6. DIRETRIZES GERAIS

As diretrizes desta POSIC constituem pilares para a Gestão de Segurança da Informação no HIFA, orientando a criação, revisão e manutenção dos seguintes documentos institucionais:

- **Norma Geral de Segurança da Informação (PSI) do HIFA**, destinada aos usuários;
- **Plano de Gerenciamento de Riscos (PGR)**;
- **Plano de Gerenciamento de Incidentes (PGI)**;
- **Plano de Continuidade de Negócios (PCN)**;
- **Política de Backup e Restauração**;
- **Política de Tratamento de Dados Pessoais e Dados Sensíveis**;
- **Política de Privacidade de Dados**.

Casos omissos, dúvidas de interpretação ou necessidades de atualização decorrentes da aplicação desta PSI devem ser submetidos ao **Grupo Gestor de Segurança da Informação (GGSI)** para análise e deliberação.

## 7. TRATAMENTO DA INFORMAÇÃO

A informação sob custódia do HIFA independentemente de pertencer à instituição, pacientes, colaboradores, corpo clínico, fornecedores ou terceiros deve ser protegida contra acessos não autorizados, uso indevido, perda, alteração ou destruição.

O tratamento das informações deve observar os seguintes requisitos:

**• Proteção Contra Acessos Indevidos**

Informações devem ser acessadas somente por usuários autorizados, conforme perfil de acesso e necessidade de atuação profissional.

**• Ciclo de Vida da Informação**

As etapas de **acesso, geração, utilização, classificação, modificação, armazenamento, transferência, distribuição e eliminação** devem seguir procedimentos documentados, refletindo os requisitos legais e operacionais aplicáveis.

**• Direito de Auditoria**

O HIFA reserva-se o direito de consultar, analisar e auditar informações armazenadas em suas dependências, dispositivos, sistemas, malotes, envelopes, arquivos físicos e eletrônicos produzidos ou recebidos mediante uso de recursos institucionais.

**• Recursos Autorizados**

Somente recursos e ferramentas previamente autorizados pela área responsável devem ser utilizados para o compartilhamento, processamento ou armazenamento de informações institucionais, garantindo sua segurança e rastreabilidade.

**Armazenamento da Informação**

A informação deve ser armazenada pelo período definido pela instituição, pela legislação ou pela regulação vigente aplicando-se sempre o maior prazo entre eles. Durante todo o período de retenção, as informações devem permanecer **íntegras, disponíveis e recuperáveis** sempre que necessário.

Os locais de armazenamento, sejam físicos ou digitais, devem ser **adequados ao tipo de informação**, dotados de controles que assegurem **proteção contra sinistros** (como incêndio, umidade, falhas elétricas e outros eventos) e **prevenção contra acessos não autorizados**, preservando sua confidencialidade, integridade e disponibilidade.

## 8. ACESSO À INFORMAÇÃO

O uso de redes externas de comunicação (Internet, redes privadas, VPNs e conexões de terceiros) deve ser rigorosamente controlado por meio de **Firewalls**, **Servidores de Acesso à Internet**, **Soluções AntiSpam**, **Ferramentas Antivírus/EDR**, além de políticas e configurações de sistemas operacionais que assegurem que **apenas os recursos necessários ao trabalho** estejam disponíveis, evitando riscos ao ambiente operacional.

O acesso externo aos sistemas institucionais, por colaboradores da Área de Suporte Técnico ou por prestadores de serviço, deve ser **previamente autorizado, formalizado e documentado**, restringindo-se estritamente ao mínimo necessário. Esse tipo de acesso deve manter **trilhas de auditoria**, possuir **controle de duração** e ser revogado imediatamente após o término da necessidade operacional.

A transmissão ou remessa de dados da organização — seja para atender requisitos de negócio, suporte técnico ou resolução de problemas — deve ser precedida de avaliação de riscos e seguir procedimentos formais que garantam:

- **Integridade e confidencialidade** dos dados;
- **Legitimidade e identificação clara do receptor**;
- **Finalidade autorizada**;
- **Registro e aprovação** pelos gestores responsáveis.

É expressamente proibido aos usuários do HIFA utilizar os recursos de TIC para:

- fins pessoais ou de terceiros;
- atividades de entretenimento;
- manifestação ou disseminação de conteúdo político-partidário ou religioso;
- práticas ilícitas, ofensivas, discriminatórias, assediadoras, difamatórias ou que violem direitos autorais;
- qualquer ação que prejudique pessoas, comprometa ativos informacionais, ou coloque em risco a imagem e a segurança da instituição.

Tais condutas comprometem diretamente os pilares de **integridade, confidencialidade, autenticidade, confiabilidade e disponibilidade** das informações, sendo vedadas em qualquer circunstância.

## 9. GRUPO GESTOR DE SEGURANÇA DA INFORMAÇÃO (GGSI)

O Grupo Gestor de Segurança da Informação (GGSI) desempenhará atividade **cooperativa, colaborativa e contínua**, atuando como instância de governança e deliberação estratégica para segurança da informação no HIFA.

**Composição mínima do GGSI:**

- Gerente de Tecnologia da Informação, Coordenação de Sustentação e Automação e Coordenação Geral de Tecnologia da Informação;
- Jurídico e Compliance;
- DPO (Encarregado de Proteção de Dados).

**Atribuições específicas do GGSI:**

- Elaborar, revisar e manter atualizada a Política de Segurança da Informação do HIFA, atuando também como referência para iniciativas de educação, capacitação e disseminação da cultura de segurança;
- Reavaliar periodicamente as ações educacionais existentes, incluindo treinamentos obrigatórios de Segurança da Informação para novos colaboradores e programas de atualização contínua para todo o corpo funcional;
- Revisar, propor e supervisionar procedimentos de continuidade dos negócios, incluindo o Plano de Contingência e documentos correlatos, assegurando a capacidade operacional do HIFA frente aos riscos identificados pelo Grupo Gestor de Riscos;
- Apoiar tecnicamente a elaboração de novos procedimentos relativos à proteção da informação, gestão de riscos, resposta a incidentes, privacidade e conformidade;
- Monitorar e revisar eventos críticos, incidentes de segurança, recomendações de auditorias e demais

indicadores que possam impactar a postura de segurança da instituição.

**Responsabilidades dos Demais Usuários**

Todos os demais usuários, independentemente do vínculo, são responsáveis por:

- **Conhecer, compreender e cumprir integralmente** a Política de Segurança da Informação do HIFA e toda a documentação correlata, incluindo normas, procedimentos, diretrizes e instruções complementares;
- **Reportar imediatamente** qualquer prática, comportamento, evento ou situação que se configure como não conformidade com a Política de Segurança da Informação, colaborando com a correção e reeducação de práticas inadequadas;
- **Comunicar ao Grupo Gestor de Segurança da Informação (GGSI)** ou aos canais oficiais disponibilizados toda suspeita, tentativa ou confirmação de descumprimento da PSI, de seus controles, diretrizes e objetivos.

**Incidentes de Segurança**

São considerados incidentes de Segurança da Informação, entre outros:

- Acesso não autorizado a recursos de TI, sistemas, redes, estações de trabalho ou bancos de dados, próprios ou de terceiros;
- Infecção por vírus, malware, ransomware, spyware ou qualquer software malicioso;
- Ataques de negação de serviço (DoS ou DDoS) e tentativas de exploração de vulnerabilidades;
- Violação desta Política ou de procedimentos correlatos de Segurança da Informação;
- Acesso indevido, perda, exposição ou **vazamento de dados**, incluindo dados pessoais e dados pessoais sensíveis sob custódia do HIFA;
- Uso inadequado, impróprio ou indevido de informações;
- Atos de pirataria, uso de softwares não licenciados ou violação de direitos autorais;
- Falhas, danos, defeitos ou mau funcionamento em equipamentos, sistemas ou ativos tecnológicos do HIFA que comprometam a segurança ou a disponibilidade de informações.

**CLASSIFICAÇÃO DA INFORMAÇÃO**

Toda informação criada, manuseada, armazenada, transportada ou descartada pelo HIFA deve ser classificada conforme critérios estabelecidos pela **Lei nº 12.527/2011 (Lei de Acesso à Informação)**, bem como pelas diretrizes internas de Segurança da Informação.

Cada usuário deve ser capaz de **identificar a classificação** atribuída a uma informação sob sua responsabilidade e respeitar rigorosamente suas **restrições de uso, acesso, divulgação, transmissão e armazenamento**.

Para fins desta PSI, aplicam-se as seguintes classes:

**• PÚBLICA**

Informação cujo acesso é irrestrito e sua divulgação ao público interno e externo **não causa impacto ao negócio**. Ainda que seja pública, **não deve ser acessada sem necessidade**, respeitando-se princípios de uso responsável e minimização.

**• INTERNA**

Informação destinada exclusivamente ao ambiente institucional.

Caso seja divulgada externamente, **não acarreta danos significativos**, porém requer salvaguardas principalmente quanto à **integridade**, evitando adulterações.

**• CONFIDENCIAL**

Informação cuja divulgação não autorizada pode gerar **danos financeiros, operacionais, legais, estratégicos ou de imagem** ao HIFA.

Requer controles formais de acesso, mecanismos de criptografia e procedimentos rigorosos de armazenamento e descarte seguro.

**Informações confidenciais nunca devem ser transmitidas pela Internet sem criptografia apropriada.**

• **RESTRITA**

Informação de altíssima criticidade, cuja exposição indevida inclusive para usuários internos sem necessidade operacional pode causar **danos severos ou irreversíveis** ao negócio.

Requer controles reforçados:

- acesso altamente limitado;
- monitoramento contínuo;
- registros de auditoria detalhados.

O acesso é permitido **somente** a usuários que necessitem dessa informação para execução de suas atividades.

**ARMAZENAMENTO E TRANSMISSÃO DE INFORMAÇÕES CONFIDENCIAIS**

Em conformidade com requisitos legais, regulatórios e contratuais de sigilo, devem ser utilizados **somente meios de armazenamento devidamente aprovados** pelo HIFA, tais como:

- Discos, diretórios ou volumes **criptografados**;
- Transmissão via rede utilizando protocolos seguros, como **TLS 1.2+**
- Utilização de **SSH ou SFTP** (FTP sobre SSH) para transferência de arquivos.

Para transmissão de informações confidenciais por e-mail entre servidores ou domínios diferentes, deve-se utilizar **camadas adicionais de criptografia**. Recomenda-se:

- compactação criptografada ou criptografia em nível de arquivo usando **AES-256**;
- aplicação obrigatória de **senha forte** em arquivos protegidos;
- proteção por senha de chaves privadas, certificados e credenciais sensíveis.

Devem ser classificadas como **CONFIDENCIAIS** todas as informações cuja natureza, origem ou criticidade indiquem que **não devem ser acessadas, compartilhadas ou divulgadas** sem autorização expressa.

Exemplos incluem (não limitado a):

- dados de clientes;
- senhas, chaves criptográficas, tokens ou credenciais de acesso;
- informações financeiras e de salários;
- código-fonte;
- registros clínicos, quando aplicável;
- dados pessoais e dados pessoais sensíveis;
- documentos estratégicos ou contratuais.

**DEVERES E RESPONSABILIDADES**

**Atribuição Inicial da Classificação da Informação**

Cabe ao **colaborador AUTOR da informação** entendido como aquele que primeiro produz, registra ou manipula a informação no ambiente do HIFA atribuir sua classificação inicial, bem como definir os **acessos, permissões, níveis de confidencialidade e formas de proteção**, quando se tratar de informação **RESTRITA, CONFIDENCIAL ou SENSÍVEL**.

Todo colaborador é responsável por:

- Classificar adequadamente a informação produzida ou manipulada;
- Armazenar e tratar os dados conforme esta PSI e seus procedimentos complementares;
- Utilizar exclusivamente os meios autorizados pela TI para armazenamento e compartilhamento;
- Garantir que informações institucionais **não sejam armazenadas localmente** em computadores pessoais ou corporativos (HD local), pois **não há backup** desses dispositivos;
- Realizar o armazenamento **somente** nos servidores institucionais, pastas de rede ou soluções corporativas autorizadas.

À **Área de Segurança da Informação** compete:

- Orientar e prestar suporte técnico aos autores quanto à classificação, armazenamento seguro e proteção das informações;
- Promover treinamentos periódicos e ações educativas sobre segurança da informação e privacidade.

À **Tecnologia da Informação (TI)** compete:

- Disponibilizar e manter os recursos tecnológicos seguros de armazenamento;
- Ofertar ferramentas de acesso, criptografia, backup, controle de permissões e proteção de dados;
- Garantir que os ambientes corporativos estejam em conformidade com as políticas técnicas de segurança.

**DADOS PESSOAIS COLETADOS**

A instituição coleta e trata dados pessoais exclusivamente para fins legítimos, específicos e compatíveis com suas atividades assistenciais, administrativas, legais e regulatórias, nos termos da LGPD.

**2.13.1. Dados pessoais de pacientes internos e externos**

**Dados pessoais (não sensíveis):**

- Nome
- Dados de contato (telefone, e-mail, endereço)
- Empresa em que trabalha e profissão
- Filiação
- Responsável financeiro
- Nacionalidade / Naturalidade
- Documentos de Identificação (CPF, RG, número de carteira do plano de saúde, Cartão SUS, passaporte)
- Estado civil
- Nome social
- Dados cadastrais gerais

**Dados pessoais sensíveis:**

- Raça/cor
- Gênero
- Dados biométricos (foto/ biometria)
- Histórico clínico, diagnósticos, exames, prescrições e informações de saúde

**Dados pessoais de colaboradores (funcionários e corpo clínico)**

**Dados pessoais (não sensíveis):**

- Nome
- Nome social
- Dados de contato (telefone, e-mail, endereço)
- Filiação
- Estado civil
- Nacionalidade
- Grau de instrução
- Documentos de identificação (CPF, RG, CTPS, Título de Eleitor, Cartão SUS, Certificado de Reservista, PIS/PASEP, CNH, Passaporte, registro de conselho profissional)

**Dados pessoais sensíveis:**

- Gênero
- Cor/raça
- Dados biométricos (foto, biometria)

**Dados pessoais de terceiros (prestadores, visitantes, fornecedores)**

- Nome
- Dados de contato (telefone, e-mail, endereço)
- Documentos de identificação (CPF, RG, título de eleitor, CNH, entre outros necessários à finalidade)

**Dados Pessoais Não Sensíveis (Classificação LGPD)**

- Identificação civil (nome, CPF, RG, data de nascimento)
- Identificação hospitalar (número de prontuário, código do paciente)

- Dados financeiros (convênio, número de carteirinha, dados de faturamento)

**Dados Pessoais Sensíveis (Classificação LGPD)**

- **Dados de saúde**: diagnósticos, resultados de exames, histórico clínico, evolução, prescrições
- **Dados sociais**: religião, etnia, orientação sexual (quando coletados)
- **Dados biométricos**: digitais, reconhecimento facial, QR code identificador em pulseiras

**DIREITOS DOS TITULARES DE DADOS**

Conforme a LGPD (arts. 6º, 18 e 20), o titular dos dados pessoais possui os seguintes direitos, assegurados pelo HIFA ao longo de todo o ciclo de tratamento:

- Confirmação da existência de tratamento
- Acesso aos dados
- Correção de dados incompletos, inexatos ou desatualizados
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade
- Portabilidade, mediante solicitação expressa e conforme regulamentação
- Eliminação dos dados tratados com base no consentimento
- Informação sobre compartilhamento com terceiros
- Informação sobre a possibilidade e consequências da não concessão do consentimento
- Revogação do consentimento a qualquer momento
- Oposição ao tratamento, quando aplicável
- Não discriminação pelo uso dos dados
- Revisão de decisões tomadas unicamente com base em tratamento automatizado

**ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO**

Para garantir anonimização e pseudonimização eficazes, devem ser observados:

- Levantamento dos processos de trabalho que tratam dados pessoais
- Identificação clara dos dados sujeitos à anonimização ou pseudonimização
- Avaliação do ciclo de vida dos dados, priorizando eliminação de dados desnecessários
- Análise do risco de reidentificação
- Definição de plano de comunicação de incidentes relacionados a dados tratados anonimamente
- Documentação de processos, incidentes e violações
- Registro e rastreabilidade das operações quando pseudonimização for utilizada

**PROTEÇÃO DOS DADOS**

O HIFA estabelece diretrizes de segurança e confidencialidade que visam proteger os dados e impedir vazamentos, acessos indevidos e perdas operacionais.

Incluem-se entre essas diretrizes:

- **Backup diário às 20h**
- Armazenamento de backups em **Storage**, conforme política interna
- Execução de **procedimentos de restauração periódicos** para garantir integridade e recuperabilidade dos dados
- Utilização de **criptografia forte** em repouso e em trânsito (AES-256, TLS 1.2+)
- Adoção de práticas de minimização, segregação de acesso, registros de auditoria e controles de acesso baseados no menor privilégio.
- A **restauração (restore)** é realizada mediante demanda, garantindo a integridade, a disponibilidade e a recuperabilidade das informações armazenadas.

**GESTÃO DE IDENTIDADE E ACESSOS**

O HIFA estabelece diretrizes para o controle de identidade e acesso a ativos, sistemas e informações, garantindo que

todo acesso seja **necessário, proporcional, rastreável e autorizado**. A concessão, alteração e revogação de acessos são de responsabilidade da área de Tecnologia da Informação, baseada no **princípio do menor privilégio** e na **necessidade de acesso**.

As atividades de gestão de identidade e acesso incluem:

- Criação e ativação de logins;
- Gestão de privilégios e perfis de acesso;
- Concessão ou negação de acesso a sistemas, redes e aplicações;
- Aplicação e fiscalização da Política de Senhas;
- Controle de acesso remoto;
- Controles de acesso físico a ambientes restritos.

**Assinatura de Sigilo**

No ato de admissão, todo colaborador e corpo clínico deve assinar termo contendo cláusula de **sigilo e confidencialidade**, assumindo responsabilidade pela proteção das informações acessadas no exercício profissional.

**Credenciais de Acesso**

Cada colaborador recebe credenciais individuais (login e senha), que são **pessoais, intransferíveis** e vinculadas ao seu perfil de acesso.

O acesso ao prontuário eletrônico deve ocorrer **exclusivamente** por meio de credencial individual, obedecendo ao perfil e às permissões atribuídas.

**Boas Práticas de Senhas**

Os usuários devem observar obrigatoriamente as seguintes condutas:

- Senhas **não podem ser compartilhadas** em hipótese alguma;
- Senhas **não devem ser anotadas** em locais visíveis ou acessíveis a terceiros;
- Senhas inicializadas devem ser alteradas no primeiro acesso;
- A reutilização de senhas pessoais em sistemas externos é proibida.

**Responsabilidade do Usuário**

Todo usuário é responsável por **todas as ações realizadas** com o uso de seu login, inclusive se executadas por terceiros por negligência na guarda da credencial.

**Perfis de Acesso**

Os perfis de usuários são definidos conforme a necessidade operacional de cada setor. Cada funcionário deve utilizar seus acessos de forma adequada e compatível com suas atribuições.

**Tabela de Perfis (exemplo estrutural)**

| PERFIL | DESCRIÇÃO DAS PERMISSÕES |
|---|---|
| (preencher) | (ex.: acesso a módulos administrativos, clínicos, financeiros, etc.) |

**Fluxo de Tratamento das Informações por Documento**

**Prontuário Médico**

- **Coleta:** informações inseridas por médicos, enfermeiros e equipe multiprofissional.
- **Armazenamento:** SAME (Serviço de Arquivo Médico e Estatística).
- **Movimentação:** restrita ao setor de faturamento mediante solicitação formal.
- **Acesso:** apenas profissionais autorizados, com trilhas de auditoria (logs).
- **Dados contidos:**
  - Não sensíveis: identificação do paciente.
  - Sensíveis: histórico clínico, exames, evolução médica, prescrições.
- **Medidas de segurança:**
  - Controle de acesso físico (chaves, crachás).
  - Controle de acesso digital (senhas, perfis, logs, autenticação).

**Termos de Consentimento**

- **Coleta:** assinatura física ou digital do paciente/responsável.

- **Armazenamento:** SAME físico ou módulo eletrônico específico.
- **Movimentação:** acessados em auditorias, inspeções, avaliações jurídicas ou regulatórias.
- **Dados contidos:**
  - Não sensíveis: nome, CPF, assinatura.
  - Sensíveis: informações de saúde relacionadas ao procedimento.
- **Base legal:** consentimento explícito do titular.
- **Medidas de segurança:**
  - Guarda segura em prontuário físico ou digital.
  - Acesso controlado conforme perfil.

**Espelho de Exame**

- **Coleta:** gerado pelo laboratório ou serviço de diagnóstico.
- **Armazenamento:** SAME e prontuário digital.
- **Movimentação:** acesso por médicos assistentes e setor de faturamento.
- **Dados contidos:**
  - Não sensíveis: identificação do paciente.
  - Sensíveis: resultados de exames laboratoriais ou de imagem.
- **Medidas de segurança:**
  - Armazenamento seguro no SAME e no sistema eletrônico.
  - Controle de acesso digital e registro de logs.

**REQUISITOS DE SEGURANÇA DO AMBIENTE**

**AMBIENTE FÍSICO**

As máquinas e servidores que armazenam sistemas e informações do HIFA encontram-se instalados em **Data Center próprio**, localizado na unidade Hospital Maternidade, estruturado com medidas físicas de proteção adequadas.
O Data Center possui:

- **Acesso controlado e monitorado**, restrito apenas à equipe de Tecnologia da Informação;
- Entradas autorizadas somente mediante **autenticação (senha, controle de acesso ou outro mecanismo equivalente)**;
- Acesso de terceiros **somente quando previamente autorizados**, devidamente identificados e **obrigatoriamente acompanhados** por profissionais da TI;
- Restrição de entrada a quaisquer colaboradores, visitantes ou prestadores que não possuam autorização formal.

O objetivo desses controles é garantir a proteção física dos equipamentos, evitar acessos indevidos e reduzir riscos de interrupção, danos ou exposição indevida de informações.

**AMBIENTE LÓGICO**

O acesso aos ambientes lógicos, sistemas, redes e bases de dados do HIFA deve ser **controlado e autorizado**, de modo a garantir que somente pessoas devidamente habilitadas possam acessar informações institucionais.
O ambiente lógico deve assegurar:

- Proteção contra ações não autorizadas, acidentais ou maliciosas;
- Controles que preservem a **integridade, confidencialidade, autenticidade e disponibilidade** das informações;
- Medidas preventivas para redução de riscos relacionados à perda, modificação indevida ou indisponibilidade dos ativos.

**SISTEMAS E SOFTWARES**

É expressamente proibido:

- Executar programas destinados a decodificação de senhas, monitoramento de rede, captura de dados de terceiros, propagação de malware, destruição de arquivos ou indisponibilização de serviços;

- Instalar softwares, dispositivos ou qualquer recurso que facilite acessos indevidos à rede corporativa do HIFA;
- Enviar **informações confidenciais** para e-mails externos sem proteção adequada arquivos devem possuir, no mínimo, **criptografia** ou **senha forte**;
- Utilizar sistemas sem as devidas permissões previamente validadas.

Todos os sistemas devem possuir mecanismos de **controle de acesso**, garantindo que apenas usuários autorizados consigam utilizá-los.

A autorização deve ser concedida somente após validação do gestor da área e registrada nos meios formais da instituição.

**USO DE INTELIGÊNCIA ARTIFICIAL (IA) NA SAUDE — DIREITOS E DEVERES**

**Princípios e Finalidade**

As soluções de IA devem ser empregadas **exclusivamente como apoio** à decisão clínica, à gestão e à pesquisa, **sem substituir a autonomia e o juízo crítico do profissional de saúde**. A decisão final diagnóstica, terapêutica e prognóstica é **sempre do médico e equipe multidisciplinar**, com comunicação clínica mantida pelo profissional e **não delegada** ao sistema de IA. O paciente tem direito à **informação clara** sobre o uso de IA no seu cuidado.

A adoção de IA deverá observar os **princípios da LGPD** (finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas) e as políticas institucionais de segurança da informação e privacidade.

A SBIS promove a **saúde digital confiável**, com ênfase em qualidade de dados, prontuário eletrônico e interoperabilidade pilares essenciais para sistemas de apoio à decisão baseados em IA.

**Governança, Risco e Auditoria**

- **Classificação de risco e supervisão humana:** sistemas de IA devem ser **avaliados, auditados e monitorados** de forma contínua, com **supervisão clínica obrigatória** e documentação das limitações do modelo; quando houver papel relevante da IA no atendimento, esse uso deve ser **registrado no prontuário**.
- **Gestão de riscos e DPIA/RIPD:** antes da implementação, realizar **avaliação de impacto** (risco clínico, risco à privacidade, vieses algorítmicos), com plano de mitigação, métricas de desempenho/segurança e ciclos de revisão.
- **Transparência e explicabilidade:** garantir **rastreabilidade**, logs, versão do modelo e de dados de treino (quando aplicável), e **explicabilidade proporcional ao risco**.
- **Programa SUS Digital (contexto público):** fomentar uso **ético** de tecnologias digitais, letramento em saúde digital e proteção de dados; quando aplicável a parcerias com o SUS, observar diretrizes do Programa.

**Conformidade Regulatório-Sanitária (Anvisa)**

- **Enquadramento SaMD:** softwares de IA com **finalidade médica** (diagnóstico, monitoramento, suporte terapêutico) são **Software as a Medical Device (SaMD)** e **devem ser regularizados** junto à Anvisa (RDC 657/2022, RDC 751/2022 e RDC 848/2024), seguindo requisitos de **segurança e desempenho**.
- **Manual Anvisa 2025:** a versão atualizada do **Manual para Regularização de Equipamento Médico e SaMD** traz **orientações operacionais** (classificação de risco, dossiê técnico, rotulagem, evidências clínicas/técnicas).
- **Tendências em revisão da RDC 657/2022:** atenção a propostas que tratam de **IA adaptativa** e exigências adicionais (dados representativos, performance e controlabilidade), fortalecendo **equidade e segurança**.

**Obrigação institucional:** Apenas soluções de IA **regularizadas** (quando enquadradas como SaMD) e **homologadas internamente** poderão ser utilizadas. É vedado empregar IA com finalidade clínica **sem registro** (ou notificação, quando cabível) na Anvisa.

**Proteção de Dados e Privacidade (LGPD/ANPD)**

- **Bases legais e princípios:** todo tratamento de dados pessoais/sensíveis em IA deve observar **bases legais** compatíveis com a finalidade assistencial ou regulatória e os **princípios do art. 6º** da LGPD.
- **Minimização e anonimização:** privilegiar **minimização de dados**, anonimização/pseudonimização quando possível, além de controle de acesso (menor privilégio) e retenção conforme a lei e a política interna.

- **Incidentes com dados pessoais:** incidentes que possam causar **risco ou dano relevante** devem ser comunicados à **ANPD e aos titulares em até 3 dias úteis** (complementação em até 20 dias), mantendo-se **registros por 5 anos**.

**Direitos dos Pacientes e Usuários**

- **Informação e consentimento informado (quando aplicável):** o paciente deve ser **informado de forma clara** quando a IA tiver papel relevante em seu atendimento e pode **recusar o uso da tecnologia**; a instituição deve assegurar **alternativas** compatíveis com a segurança do cuidado.
- **Acesso e transparência (LGPD):** os titulares têm direito de **acesso, correção, informação sobre compartilhamentos** e **revisão de decisões automatizadas**; a instituição deve prover canais e prazos para exercício desses direitos.

**Deveres de Profissionais, Fornecedores e Instituição**

**Profissionais de saúde (médicos e equipe):**

- Manter **juízo clínico independente**, validar as **recomendações da IA** e registrar o uso quando relevante; é lícito **recusar tecnologia não validada** ou sem certificação/regulação pertinente.
- Reportar **falhas**, vieses percebidos e eventos adversos relacionados à IA.

**Fornecedores e parceiros:**

- Comprovar **conformidade regulatória** (Anvisa, quando SaMD), segurança, desempenho, **cibersegurança** e governança de dados; fornecer **informações técnicas** (versões, dataset(s), validação clínica) e colaborar com auditorias internas.

**Instituição de saúde:**

- Estabelecer **comitê de IA/saúde digital** alinhado à governança clínica e de dados; definir políticas de **aquisição, validação, monitoramento** e **descontinuação**; promover **capacitação contínua** e **campanhas de letramento digital**.
- Manter **SoP/POPs**: (i) avaliação de risco/impacto; (ii) validação clínica/tecnológica; (iii) gestão de mudança do modelo; (iv) segurança da informação e **resposta a incidentes** (ANPD); (v) ciclo de vida e descarte de dados/modelos.

**Qualidade de Dados, Interoperabilidade e Equidade**

A qualidade e a interoperabilidade de dados clínicos (PEP/RES) são condições para **IA confiável**; recomenda-se aderência a padrões e práticas de saúde digital reconhecidos por entidades como a **SBIS**. Além disso, bases de treino e validação devem considerar **representatividade e equidade**, mitigando vieses e impactos discriminatórios.

**Cibersegurança e Continuidade**

Soluções de IA devem seguir políticas de **cibersegurança** (hardening, gestão de vulnerabilidades, criptografia em repouso e trânsito, MFA), com **planos de contingência e continuidade** para indisponibilidades do modelo/serviço e **testes periódicos** de restauração/retorno ao serviço.

**Responsabilização e Prestação de Contas**

A instituição e os agentes envolvidos devem comprovar **conformidade e eficácia** das medidas de governança, segurança e privacidade aplicáveis às soluções de IA, observando **princípios de accountability (LGPD)** e **exigências regulatórias (CFM/Anvisa).**

**MÁQUINAS ESTAÇÃO DE TRABALHO**

As estações de trabalho incluindo computadores de mesa, notebooks corporativos e demais dispositivos devem ser protegidos contra danos, perdas, furtos e acessos indevidos.

Diretrizes:

- Cada estação possui um **identificador interno**, para rastreabilidade de atividades;
- O colaborador é **responsável** por todas as ações realizadas em sua estação e com seu login;

- Ao final do expediente, o dispositivo deve ser **desligado**, exceto em casos de equipamentos que devem permanecer ligados 24h;
- Ao se ausentar da mesa, o usuário deve **bloquear a estação** de trabalho, garantindo privacidade e segurança;
- Apenas a equipe autorizada da TI pode realizar **instalação de softwares**, sempre utilizando versões licenciadas;
- A TI é responsável por definir controles, padronização, distribuição e instalação de softwares corporativos;
- Em caso de dúvidas, o usuário deve contatar a TI pelos canais formais de suporte.

**UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES / TERCEIROS**

- Notebooks pessoais **não têm acesso** à rede interna do HIFA; nesses casos, é disponibilizado apenas o acesso ao **Wi-Fi para visitantes**, totalmente isolado da rede corporativa;
- Equipamentos de terceiros (como consultores, fornecedores, auditores) **não** possuem acesso à rede de arquivos da instituição;
- O acesso de equipamentos externos à rede interna somente será permitido por **VPN corporativa**, mediante solicitação oficial à Central de Serviços e **apenas quando houver autorização prévia**.

Estas regras impedem que dispositivos não gerenciados representem risco ao ambiente interno e aos dados institucionais.

**PUBLICAÇÃO DE INFORMAÇÕES ABERTAS**

Somente os **gestores do HIFA**, com o apoio e validação da **área de Comunicação**, podem classificar informações como públicas e autorizar sua divulgação externa.
Todos os demais colaboradores devem abster-se de divulgar informações institucionais sem autorização formal.

**DESCARTE DE INFORMAÇÃO CLASSIFICADA**

As informações classificadas como **RESTRITA, CONFIDENCIAL ou SENSÍVEL** devem receber **tratamento especial no momento do descarte**, garantindo que não possam ser recuperadas ou acessadas por pessoas não autorizadas.
Os métodos de descarte seguro podem incluir:

- Trituração física (quando em papel);
- Eliminação segura conforme técnicas adequadas (mídias digitais);
- Formatação segura e/ou sanitização;
- Exclusão definitiva de dispositivos e sistemas, seguindo procedimentos internos.

**DESCARTE DE INFORMAÇÃO — Versão Revisada e Melhorada**

O descarte de Informações, sejam armazenadas em meio físico ou eletrônico, deve ser realizado conforme os procedimentos definidos pela área de Segurança da Informação, assegurando que a informação descartada **não possa ser recuperada por nenhum meio**.
Além dos procedimentos específicos:

1. **Informações impressas** devem ser **trituradas** antes do descarte, impedindo leitura, reconstrução ou reutilização indevida;
2. **Aparelhos eletrônicos** devem ser **resetados**, com remoção total de dados e configurações;
3. **Informações eletrônicas** devem ser eliminadas por meio de ferramentas adequadas de descarte seguro, seguindo métodos reconhecidos, como os definidos no **NIST 800-88 – Data Sanitization**, disponibilizados pela área de TI/SI.

**EXTRAVIO DE INFORMAÇÃO**

Qualquer evento de **perda, extravio, roubo, destruição acidental ou acesso indevido** a informações deve ser comunicado **IMEDIATAMENTE** ao Grupo de Segurança da Informação, por meio do e-mail: **ggsi@hifa.org.br**
A comunicação imediata é obrigatória, pois possibilita iniciar rapidamente procedimentos de contenção, investigação e mitigação de danos.

| TÍTULO | CONTROLE | REVISÃO |
|---|---|---|
| **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** | PI-INSGQ-011 | 003 |
| ÁREA RESPONSÁVEL | | VIGÊNCIA |
| TECNOLOGIA DA INFORMAÇÃO | | 2026 |



**USO DOS ATIVOS DE TI (FERRAMENTAS CORPORATIVAS) — Versão Revisada**

O HIFA poderá fornecer aos colaboradores ferramentas corporativas, como:

- conta de e-mail institucional;
- acesso à internet e sistemas;
- dispositivos físicos (computadores, celulares corporativos, armários, gavetas);
- ferramentas de comunicação e produtividade.

O uso dessas ferramentas está condicionado:

- ao **cumprimento integral desta Política**;
- às autorizações e perfis de acesso concedidos;
- às deliberações do GGSI.

**Princípio do Menor Privilégio**

O acesso concedido ao colaborador é limitado ao **mínimo necessário** para o desempenho de suas atividades, não sendo permitidos acessos adicionais sem justificativa e autorização formal.

**Condutas Proibidas**

É estritamente proibido:

- utilizar recursos corporativos para **fins pessoais**, próprios ou de terceiros;
- praticar **atos ilícitos**, ofensivos, discriminatórios ou que possam comprometer a imagem institucional;
- utilizar computadores, redes, sistemas ou canais corporativos para qualquer finalidade contrária às leis, políticas internas ou normas éticas.

O colaborador é responsável:

- pela **guarda, zelo e uso adequado** dos ativos de TI que lhe forem disponibilizados;
- pelas **informações que inserir, manipular ou armazenar** nesses ativos.

**ACESSO E USO DA INTERNET — Versão Revisada**

O HIFA poderá permitir acesso à Internet e navegação conforme critérios definidos pela Política de Segurança da Informação, sujeita a:

- bloqueios automáticos de sites inseguros, maliciosos ou inadequados;
- filtros de navegação baseados em categorias;
- monitoramento para garantir conformidade e segurança.

É **estritamente proibido**:

- realizar transferência de arquivos utilizando ferramentas, aplicativos, protocolos (FTP, torrent, compartilhadores, mensageiros não autorizados etc.) ou plataformas **não aprovadas previamente** pela área de Segurança da Informação.

**Aprovação de Ferramentas**

A adoção de qualquer ferramenta externa deve ser precedida de:

- análise de segurança da solução;
- verificação da maturidade do fornecedor em SI e proteção de dados;
- avaliação das políticas de privacidade e práticas de compliance;
- liberação formal pela Segurança da Informação.

Essa prática impede:

- herança de vulnerabilidades vindas de softwares inseguros;
- uso de ferramentas sem controle;
- exposição desnecessária de dados a fornecedores sem maturidade em segurança;
- riscos de vazamento, sequestro de dados ou comprometimento da infraestrutura.

**Regras sobre Downloads e Softwares**

É proibido realizar download de materiais protegidos por direitos autorais sem autorização ou instalar softwares que não tenham sido previamente homologados pela área de Segurança da Informação.

O colaborador deve sempre consultar o departamento de TI **antes** de realizar o download de qualquer software de terceiros, pago ou gratuito.

| TÍTULO | CONTROLE | REVISÃO |
|---|---|---|
| **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** | PI-INSGQ-011 | 003 |
| ÁREA RESPONSÁVEL | | VIGÊNCIA |
| TECNOLOGIA DA INFORMAÇÃO | | 2026 |



**E-MAIL / CORREIO ELETRÔNICO**

O e-mail corporativo do HIFA, assim como todas as ferramentas de comunicação disponibilizadas pela instituição, é destinado **exclusivamente ao uso profissional**.

As informações contidas nas mensagens eletrônicas são **propriedade do HIFA**, podendo ser **monitoradas** a qualquer momento, sem aviso prévio, para fins de auditoria, conformidade e segurança, conforme previsto na seção de Monitoração desta Política.

**Envio de Informações Classificadas**

- É **proibido** enviar informações classificadas como **INTERNAS** ou **CONFIDENCIAIS** para endereços externos que não pertençam aos domínios **hifa.org.br** ou **hifaci.org.br**.
- O envio poderá ocorrer **somente** para terceiros envolvidos diretamente no assunto e mediante proteção adequada da informação.
- Informações classificadas como **SECRETAS não podem ser transmitidas por e-mail simples**. Nesses casos, é **obrigatório** o uso de **criptografia forte** aplicada ao conteúdo e anexos, com aprovação da área de Segurança da Informação e validação do superior imediato.

**Procedimentos em caso de desligamento**

- O colaborador deverá ser informado da **suspensão** de sua conta de e-mail.
- O colaborador poderá, acompanhado de outro funcionário designado, retirar mensagens pessoais que, de forma excepcional, constem na caixa de e-mail corporativa.
- O e-mail suspenso deve emitir **resposta automática** informando o desligamento e indicando outro canal de contato.
- A conta permanecerá ativa por até **30 dias**, após o que será **excluída definitivamente**, incluindo todos os dados pessoais nela armazenados.

**SENHAS DE ACESSO**

A senha de acesso aos sistemas e recursos computacionais é de **inteira responsabilidade** do colaborador. É proibido:

- compartilhar senhas com colegas ou terceiros;
- armazená-las de forma visível ou insegura;
- utilizar senhas fracas.

**Requisitos de Senhas**

- Senhas devem conter **no mínimo 9 caracteres**, combinando letras e números (preferencialmente incluindo caracteres especiais).
- Informações classificadas como **SECRETAS** devem ser protegidas por senhas de **no mínimo 16 caracteres**, ou por **chaves criptográficas** de alta robustez, sempre protegidas por senha adicional.

Toda ação realizada com o uso da credencial do colaborador será atribuída ao mesmo — dentro ou fora do ambiente computacional do HIFA.

**CONTAS INATIVAS**

Qualquer credencial de acesso que permanecer **30 dias sem uso** deve ser automaticamente **bloqueada** em todos os sistemas corporativos.

**AUTENTICAÇÃO DE MÚLTIPLOS FATORES (MFA)**

O uso de autenticação multifator (MFA/2FA) é **obrigatório** para **todos os serviços** em que a funcionalidade estiver disponível, reforçando a segurança das credenciais.

**DIRETRIZES QUANTO AO USO DE MÍDIAS REMOVÍVEIS**

O uso de mídias removíveis deve ser encarado como **exceção**.

Regras:

- Seu uso deve ser **previamente autorizado pela TI**.
- A transmissão de informações deve ocorrer prioritariamente pelas **ferramentas corporativas**.

- É proibido utilizar modem 3G/4G enquanto conectado à rede corporativa.
- Usuários serão responsabilizados por danos decorrentes do uso inadequado (vazamentos, vírus, malware).
- Caso seja necessário transportar arquivos em mídia removível, recomenda-se:
    - **criptografar** os arquivos;
    - **apagar** os dados da mídia após o uso.

**ACESSO REMOTO**

O acesso remoto ao ambiente computacional do HIFA será permitido apenas mediante:

1. **Aprovação prévia do gestor**;
2. **Abertura de chamado** na Central de Serviços;
3. Utilização **exclusiva** de equipamentos corporativos fornecidos pelo HIFA;
4. Conexão realizada unicamente por meio de **VPN corporativa**.

Todos os controles de segurança vigentes se aplicam integralmente.

**MESA LIMPA**

Todos os colaboradores devem manter o ambiente de trabalho limpo e organizado, evitando exposição indevida de informações.

Regras:

- Documentos devem permanecer nas mesas **somente de forma temporária**.
- Devem ser guardados em **compartimentos fechados** quando não estiverem sendo utilizados.
- Qualquer informação deixada sobre mesas pode ser **destruída** pelo responsável ou por outro colaborador que identificar o risco.
- Documentos "órfãos" importantes (com assinaturas, por exemplo) devem ser depositados no **armário tipo boca-de-lobo**, localizado ao lado das impressoras.

A política se aplica a mesas, estações de trabalho, gavetas, arquivos e lixeiras.

**BLOQUEIO DE DISPOSITIVO POR INATIVIDADE**

Todos os dispositivos corporativos devem ser configurados para **bloqueio automático após 10 minutos** de inatividade.

Aplicável a:

- computadores;
- notebooks;
- smartphones;
- tablets;
- quaisquer dispositivos móveis ou fixos conectados aos sistemas do HIFA.

**CAPTURA DE TRÁFEGO NA REDE**

É proibida a **captura, inspeção ou interceptação** de tráfego de rede da infraestrutura do HIFA, salvo quando:

- houver autorização **expressa** do GGSI;
- a finalidade for **diagnóstico, auditoria ou monitoração autorizada**.

**DISPOSITIVOS PESSOAIS**

- Dispositivos pessoais devem acessar **somente a rede de convidados**.
- É proibido conectar dispositivos não corporativos às redes internas, cabeadas ou Wi-Fi.
- Colaboradores que necessitem de dispositivos móveis corporativos receberão equipamentos fornecidos pelo HIFA, configurados com os controles de segurança adequados.

**REDES SOCIAIS**

- É proibido publicar, comentar, responder ou emitir comunicados **em nome do HIFA** sem autorização formal das áreas de Marketing/Comunicação.
- Apenas equipes autorizadas podem interagir institucionalmente em redes sociais.

- Colaboradores devem evitar publicar fotos em áreas internas, pois podem conter informações restritas.
- A divulgação só poderá ocorrer mediante **autorização da Comunicação**.

**SOFTWARE, APPS E PLUGINS**

É proibida a instalação de softwares, aplicativos ou plugins gratuitos ou pagos que **não tenham sido previamente aprovados** pela TI e pela área de Segurança da Informação.

Observações:

- A TI mantém um **portfólio oficial** de ferramentas aprovadas.
- A maioria desses softwares já vem pré-instalada nos equipamentos corporativos.
- Qualquer necessidade adicional deve ser formalmente solicitada pelos canais de suporte.

**POSTURA GERAL DE PRIVACIDADE**

A privacidade das informações é um princípio fundamental no HIFA. Todos os acessos aos sistemas internos devem possuir **justificativa legítima**, vinculada a um **propósito real de negócio** e compatível com as atribuições do colaborador.

É **expressamente proibido** acessar informações de pacientes, colaboradores, fornecedores ou quaisquer registros institucionais **por curiosidade**, interesse pessoal ou qualquer finalidade não relacionada ao exercício das funções profissionais.

São exemplos de violações:

- Acessar dados de celebridades, pessoas públicas, amigos, parentes ou quaisquer terceiros **sem necessidade operacional assistencial, administrativa ou jurídica**;
- Alterar informações cadastrais próprias: se necessário, o colaborador deve **abrir chamado** e solicitar que outro profissional autorizado realize a ação;
- Acessar Prontuário Eletrônico de Pacientes **sem necessidade assistencial**, ou sem solicitação jurídica formalizada, e apenas por colaboradores que tenham **permissão específica** para manejo de prontuário.

Todo acesso indevido constitui **violação de privacidade**, podendo gerar responsabilização administrativa, civil e penal.

**MONITORAÇÃO**

O HIFA se reserva o direito de **monitorar todas as atividades** realizadas nos seus sistemas de informação, equipamentos corporativos e rede interna, com finalidade de:

- Garantir conformidade com esta PSI e demais políticas internas;
- Proteger a instituição contra incidentes de segurança;
- Atender obrigações legais, regulatórias e contratuais.

Ambientes internos do HIFA podem ser monitorados por **gravação audiovisual**, exclusivamente para fins de **segurança patrimonial, física e operacional**.

A monitoração será realizada de forma proporcional, respeitando a legislação vigente e as diretrizes internas de privacidade e proteção de dados.

**MODIFICAÇÃO / ROOT / JAILBREAKING**

Para garantir a segurança das informações corporativas e reduzir vulnerabilidades, é **proibido** acessar ferramentas, sistemas ou dados corporativos a partir de dispositivos que tenham sofrido **modificações no sistema operacional**, tais como:

- **Root** em dispositivos Android;
- **Jailbreak** em dispositivos iOS (iPhone ou iPad).

A utilização de dispositivos pessoais com tais modificações também é **expressamente proibida**, mesmo que o acesso ocorra por meio de VPN ou aplicativos institucionais.

Essas práticas comprometem mecanismos nativos de segurança, expondo sistemas e dados sensíveis a riscos elevados.

**ACESSO A UNIDADES INTERNAS E DE VISITANTES**

| TÍTULO | CONTROLE | REVISÃO |
|---|---|---|
| **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** | PI-INSGQ-011 | 003 |
| ÁREA RESPONSÁVEL | | VIGÊNCIA |
| TECNOLOGIA DA INFORMAÇÃO | | 2026 |



O acesso às unidades internas do HIFA **não pode ser realizado de forma desacompanhada** por visitantes ou prestadores de serviço.
Regras obrigatórias:

1. Visitantes devem ser **acompanhados desde a recepção** até o local autorizado, seguindo os protocolos institucionais.
2. O acesso deve ser registrado em sistema de portaria, com **biometria ou crachá**.
3. Prestadores externos devem possuir **cadastro obrigatório** e ser acompanhados por colaborador responsável.
4. As portas das unidades internas **devem permanecer fechadas**. A presença de pessoas não identificadas deve ser imediatamente comunicada à segurança.
5. É proibido atender fornecedores fora da área designada para recepção de fornecedores.
6. Estranhos ou pessoas sem identificação **não podem permanecer nos corredores**, devendo ser escoltados à recepção para identificação.

Essas medidas garantem proteção dos pacientes, dos profissionais e da infraestrutura assistencial.

**CONFIDENCIALIDADE E INTEGRIDADE**

Os gestores devem assegurar que colaboradores, clientes, fornecedores e usuários compreendam que todas as informações tratadas nos sistemas e processos do HIFA são:

- de **propriedade da instituição** (ou de seus clientes);
- sujeitas a requisitos legais e contratuais;
- protegidas por políticas de confidencialidade e segurança.

Regras essenciais:

- Informações confidenciais devem ser protegidas contra acessos não autorizados, independentemente da mídia (cloud, impressos, mídias físicas, dispositivos móveis, arquivos digitais etc.).
- Colaboradores devem **bloquear a estação de trabalho** ao se ausentarem do ambiente, especialmente fora do horário de trabalho.
- Informações manuseadas em notebooks corporativos devem seguir os requisitos de proteção definidos pela TI.
- Informações classificadas como **RESTRITAS ou CONFIDENCIAIS** devem ser **destruídas de forma segura** após o período de retenção previsto em lei, regulamento ou contrato.
- Gestores devem garantir que terceiros que armazenem, processem ou acessem informações do HIFA adotem medidas compatíveis com esta política.
- A instituição deve monitorar fornecedores que tratam informações críticas, com especial atenção ao cumprimento de controles de segurança.
- Para terceiros, acordos formais de confidencialidade (NDA – "Non Disclosure Agreement") devem ser estabelecidos antes do acesso às informações.

**ADOÇÃO DE COMPORTAMENTO SEGURO**

A informação, independentemente de sua forma, meio ou finalidade, está presente em praticamente todas as atividades executadas pelos profissionais do HIFA. Sendo assim, a adoção de **comportamentos seguros** é essencial para garantir a proteção, confidencialidade, integridade e disponibilidade das informações institucionais.
Todos os colaboradores, prestadores de serviços e demais agentes envolvidos devem:

- Adotar postura **proativa e engajada** na proteção das informações;
- Conhecer e compreender ameaças externas, como vírus, malware, ataques de engenharia social, interceptação de mensagens e tentativas de roubo de credenciais;
- Respeitar a premissa de que **todo acesso não autorizado é proibido**, independentemente da intenção;
- Evitar discutir assuntos confidenciais em locais públicos ou expostos (ônibus, Uber, aviões, restaurantes, filas, coworking, elevadores, redes sociais etc.);
- Manter senhas **pessoais, intransferíveis e protegidas**, sem anotação em papel, agendas, pastas digitais visíveis ou compartilhamento com terceiros;
- Utilizar **apenas softwares homologados** pela equipe de TI, instalados exclusivamente pelos responsáveis;

- Cumprir rigorosamente a política de uso da Internet, e-mail e demais ferramentas corporativas;
- Nunca abrir anexos, arquivos ou links de origem desconhecida;
- Guardar documentos impressos e arquivos confidenciais em locais protegidos e adequados;
- Procurar a área de TI imediatamente em caso de dúvidas ou suspeitas relacionadas à Segurança da Informação;
- Obedecer a todas as normas de segurança, submetendo exceções para análise e validação prévia da TI.

**AVALIAÇÃO DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO — Versão Revisada**

A área de Tecnologia da Informação deve realizar avaliações periódicas de riscos relacionados à Segurança da Informação, com o objetivo de:

- Identificar vulnerabilidades, ameaças e riscos que possam comprometer os ativos do HIFA;
- Priorizar ações de mitigação, incluindo novos controles, revisão de processos, ajustes de permissões, reformulação de sistemas e políticas;
- Planejar e executar, no mínimo trimestralmente, ciclos de avaliação e revisão de riscos, ajustando a periodicidade conforme necessário;
- Utilizar ferramentas de gestão de risco, compliance e análise de vulnerabilidades como suporte ao processo decisório.

A avaliação pode contemplar toda a organização ou áreas específicas, sistemas, aplicações, componentes de rede, fluxos de dados e processos críticos.

**GESTÃO DE ACESSO A SISTEMAS E AMBIENTES — Versão Revisada**

Todo acesso lógico ou físico aos ambientes e informações do HIFA deve seguir controles formais, baseados nos princípios de **necessidade**, **menor privilégio** e **responsabilidade individual**.

A política de controle de acesso deve prever:

- Procedimento formal de concessão e cancelamento de acessos;
- Aprovação expressa do proprietário da informação;
- Identificadores individuais (IDs) para todos os usuários;
- Revisão periódica das permissões;
- Cancelamento automático de acessos após desligamento — com integração entre RH e TI;
- Ajuste imediato do perfil quando houver mudança de função;
- Política formal de criação, manutenção e uso de senhas.

**SEGURANÇA EM REDES — Versão Revisada**

O HIFA mantém infraestrutura de rede protegida por dispositivos empresariais de segurança, incluindo **Appliances NFGW**, capazes de detectar, bloquear e responder tentativas de intrusão ou atividades suspeitas.

Controles de rede incluem:

- Firewalls corporativos;
- Antivírus/EDR;
- Monitoramento contínuo;
- Segmentação de rede;
- Políticas de acesso baseado em perfil.

**RESPOSTA A INCIDENTES DE SEGURANÇA — Versão Revisada**

A área de TI deve assegurar que todos os sistemas que armazenam informações confidenciais mantenham trilhas de auditoria capazes de registrar:

- Tentativas de violação de segurança;
- Eventos significativos relativos à administração e transações;
- Ações suspeitas ou fora do padrão operacional.

Diretrizes:

- Atividades suspeitas devem ser verificadas imediatamente;

- Problemas classificados como **alto risco** nos testes de vulnerabilidade deve ser corrigidos antes da entrada em produção;
- Cada área deve garantir que produtos e aplicativos conectados à Internet passem por avaliação técnica de vulnerabilidade aprovada pela TI;
- Testes de vulnerabilidade devem ser realizados **após mudanças significativas** e **anualmente**.

**TREINAMENTO E CONSCIENTIZAÇÃO — Versão Revisada**
Todos os colaboradores, prestadores e fornecedores devem receber treinamento obrigatório sobre Segurança da Informação:

- Na admissão;
- Em mudança de função;
- Periodicamente, conforme necessidade institucional.

O objetivo é reforçar o conhecimento, reduzir riscos e promover cultura de proteção contínua.

**PRODUTOS E SERVIÇOS DE GERENCIAMENTO DE SEGURANÇA — Versão Revisada**
A contratação de sistemas e serviços de segurança somente poderá ocorrer com **aprovação da TI**.
Diretrizes:

- Todos os alarmes, logs e eventos de segurança devem ser registrados e arquivados diariamente;
- Eventos de segurança devem ser reportados e tratados conforme procedimentos definidos pela área de Segurança da Informação;
- Conexões IP com terceiros devem ser protegidas por firewalls e controles de acesso adequados.

**GESTÃO DE TERCEIROS — Versão Revisada**
O HIFA poderá contratar terceiros para serviços tecnológicos e consultivos, devendo:

- Realizar qualificação e avaliação formal de fornecedores;
- Garantir que terceiros cumpram a Política de Segurança e requisitos da Qualidade;
- Formalizar contratos com cláusulas de confidencialidade e segurança.

**CLOUD COMPUTING — Versão Revisada**
Contratações de serviços em nuvem devem garantir:

- Segurança, privacidade e compliance;
- Backups, salvaguardas e mecanismos de recuperação;
- Planos de resposta a incidentes;
- Gestão do ciclo de vida da informação;
- Documentação formal e controle de mudanças;
- Rastreamento, monitoramento e auditabilidade;
- SLAs compatíveis com os requisitos críticos do HIFA.

**DATA LOSS PREVENTION (DLP) — Versão Revisada**
Para mitigar riscos de perda de dados, o HIFA deve:

- Manter sistemas e procedimentos atualizados;
- Definir níveis de acesso conforme necessidade;
- Garantir padrões de segurança em dispositivos móveis e acessos remotos;
- Utilizar VPN ou redes controladas;
- Identificar e classificar dados conforme estado (uso, trânsito, repouso).

**ATUALIZAÇÃO DE SOFTWARES**
Novos sistemas, versões ou atualizações devem seguir processo formal de homologação, comprovando:

- Desempenho adequado;
- Resiliência, recuperação de erros e planos de contingência;

- Procedimentos operacionais definidos;
- Conjunto de controles de segurança revisados;
- Impacto zero nos sistemas existentes;
- Testes e validação das áreas críticas (ex.: sistema MV).

**PENALIDADES**

A violação desta Política poderá resultar em:

- Sanções administrativas;
- Medidas disciplinares;
- Rescisão contratual;
- Responsabilização civil e penal.

Ocorrências devem ser reportadas imediatamente para:
**si@hifa.org.br**
**ouvidoriainterna@hifaci.org.br**

**VIGÊNCIA**

Esta Política entra em vigor na data de sua aprovação pela Superintendência e Conselho Administrativo, permanecendo vigente por prazo indeterminado.

**REGRAS DE CONSEQUÊNCIAS**

As consequências decorrentes de violações às normas desta Política serão tratadas conforme diretrizes institucionais e poderão incluir deliberação da Superintendência, a partir de pareceres das áreas envolvida.

## 3. *REFERÊNCIAS BIBLIOGRÁFICAS*

**1. Referências Legislativas e Regulatórias (Brasil)**

- **Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)**
  Disponível no Portal do Planalto. [barradvisory.com]
- **Marco Civil da Internet (Lei nº 12.965/2014)**
  (Referência indireta via LGPD). [barradvisory.com]
- **Resolução CD/ANPD nº 15/2024 — Regulamento de Comunicação de Incidente de Segurança**
  Define prazos, critérios de risco e obrigações de notificação. [www2.senado.leg.br], [youtube.com], [youtube.com]
- **Portaria GM/MS nº 3.232/2024 — Programa SUS Digital**
  Institui diretrizes para transformação digital e uso responsável de tecnologias em saúde. [gov.br]

**2. Conselho Federal de Medicina — Normas sobre IA e Ética Médica**

- **Resolução CFM nº 2.454/2026 — Normatiza o uso da Inteligência Artificial na Medicina**
  Define que a decisão final é sempre do médico, exige supervisão humana e impõe classificação de risco dos sistemas de IA.
  [csrc.nist.gov], [PI-INSGQ-0...VISÃO 2026 | Word]

**3. ANVISA — Regulamentação de Software como Dispositivo Médico (SaMD)**

- **RDC nº 657/2022 — Software como Dispositivo Médico (SaMD)**
  Regulamenta classificação, requisitos de segurança, eficácia e regularização.
  [elevateconsult.com]
- **RDC nº 751/2022 — Classificação de risco e regras gerais de dispositivos médicos**
  (Referenciada no manual atualizado da Anvisa). [www1.tozzi...ire.com.br]
- **RDC nº 848/2024 — Requisitos essenciais de segurança e desempenho para dispositivos médicos e IVD**
  (Parte das atualizações regulatórias). [www1.tozzi...ire.com.br]

- **Manual de Regularização de Equipamento Médico e Software como Dispositivo Médico – Versão 2025**
  Atualização que incorpora RDC 657/2022, 751/2022 e 848/2024.
  [www1.tozzi...ire.com.br]
- **Revisão da RDC 657/2022 – Proposta de novas regras para IA adaptativa em saúde (2025)**
  [glocertint...tional.com]

**4. SBIS — Saúde Digital e Orientações sobre Prontuário Eletrônico**

- **SBIS — Sociedade Brasileira de Informática em Saúde**
  Páginas oficiais e materiais de referência sobre prontuário eletrônico, certificações e padrões de saúde digital.
  [vanzolini.org.br]
- **Estudos sobre prontuário eletrônico e melhoria do acesso (SciELO, 2024)**
  [acreditacao.com.br]

**5. Estudos e Publicações sobre IA em Saúde**

- **INTELIGÊNCIA ARTIFICIAL NA SAÚDE — Potencialidades, riscos e perspectivas para o Brasil (CETIC.br / CGI.br, 2024)**
  Aborda riscos, governança e desafios éticos da IA na saúde brasileira.
  [ibes.med.br]
- **White Paper — "Inteligência Artificial nas Organizações de Saúde: Implementação Integrada, Segura e Ética" (SPMS, 2025)**
  Documento robusto sobre governança, segurança e práticas éticas em IA na saúde.
  [pinheironeto.com.br]
- **Estudos Fiocruz / ENSP — Saúde Digital e IA no SUS (2024)**
  [mattosfilho.com.br]

**6. Referências Complementares sobre Regulação, Equidade e SaMD**

- **Avaliação regulatória de SaMD com foco em inclusão e equidade (USP / Revista de Direito Sanitário, 2025)**
  [hightable.io]
- **Artigos e análises sobre o Marco Legal da IA e impactos na saúde (Saúde Business, 2025)**
  [secureframe.com]

## 4. ANEXOS E DOCUMENTOS DE APOIO

Não se aplica.

| ELABORAÇÃO | | |
|---|---|---|
| DATA:<br>*04/2026* | CARGO:<br>*Coordenador Geral de TI* | RESPONSÁVEL:<br>*Higor Bankerdt* |

| APROVAÇÃO | | |
|---|---|---|
| DATA: | CARGO: | AUTORIZADOR: |
| *04/2026*<br>*04/2026* | *Gerente TI*<br>*Gerente de Estratégia* | *Miter Mayer*<br>*Verônica Moten* |
| *04/2026* | *Superintendente* | *Jailton Pedroso* |

| *TÍTULO* | *CONTROLE* | *REVISÃO* |
|---|---|---|
| ***POLÍTICA DE SEGURANÇA DA INFORMAÇÃO*** | *PI-INSGQ-011* | *003* |
| *ÁREA RESPONSÁVEL* | | *VIGÊNCIA* |
| *TECNOLOGIA DA INFORMAÇÃO* | | *2026* |

| HISTÓRICO DE REVISÕES | | |
|---|---|---|
| DATA: | REVISÃO: | DESCRIÇÃO: |
| *06/2023* | *000* | *Implantação* |
| *07/2024* | *001* | *Revisão do conteúdo descrito no documento* |
| *07/2024* | *002* | *Inclusão do tópico 4.2.2* |
| *04/2026* | *003* | *Revisão do conteúdo descritivo no documento e conteúdo de IA* |