TÍTULO	CONTROLE	REVISÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PI-INSGQ-011	002
ÁREA RESPONSÁVEL		VIGÊNCIA
TECNOLOGIA DA INFORMAÇÃO		2024

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

2.1. DEFINIÇÃO

Segurança da Informação é a proteção da Informação contra ameaças internas e externas, garantindo a continuidade do negócio e minimizando os riscos para a instituição ou seus clientes.

A Segurança da Informação é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos e a própria estrutura organizacional da empresa.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente, sempre que necessários, e melhorados continuamente para garantir que os objetivos sejam atendidos.

Internamente, considera-se como informação toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagens, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e Informações de propriedade, interesse ou posse da instituição e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos clientes sob nossa custódia.

Para os efeitos desta PSI são estabelecidos os seguintes conceitos e definições:

- Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
- Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;
- Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

- Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;
- Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;
- Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;
- Classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados;
- Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- Custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- Ética: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;
- Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, falta de controle ou situação previamente desconhecida que possa ser relevante para a segurança da informação;
- Gerenciamento de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- Gerenciamento de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;
- Gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- Incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
- Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação

e comunicações;

- Proprietário de ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;
- Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;
- Responsabilidade: os agentes públicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;
- Risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao HIFA;
- Tratamento de incidentes: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas; e realizar as prováveis correções dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;
- Usuário: qualquer pessoa que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;
- 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.

2.2. REFERÊNCIAS LEGAIS E NORMATIVOS

Esta PSI está em conformidade com as principais normas que regem a segurança da informação e aplica-se no âmbito do HIFA e suas unidades.

São referências legais e normativas para esta PSI:

- ISO 27000;
- Lei Nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet;
- Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- Código de Conduta e Ética do HIFA;
- Contrato de Trabalho;
- Contratos de prestação de serviços;

2.3. PRINCÍPIOS DA INSTITUIÇÃO

Aplica-se a esta PSI os seguintes princípios:

- Celeridade: As ações de SIC devem oferecer respostas rápidas à incidentes e falhas de segurança;
- Ética: Os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;
- Clareza: As regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
- Legalidade: As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do HIFA e suas unidades;
- Publicidade: Transparência no trato da informação, observados os critérios legais.

2.4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- Confidencialidade: garantir que a informação seja acessível apenas àqueles autorizados a ter acesso. Isso significa dizer que, literalmente, determinadas informações são confidenciais e só dispõe de seu acesso aqueles que possuem autorização para tal.

- Integridade: a informação não foi alterada de forma não autorizada ou indevida. O princípio de integridade garante que todas as informações estejam em seu formato original e verdadeiro, a fim de servir para os propósitos para o qual foram designadas

- Disponibilidade: Diz respeito ao acesso dos dados sempre que este for necessário. Está diretamente relacionado à eficácia do sistema e do funcionamento da rede para que, consequentemente, a informação possa ser acessada quando for necessário.

2.5. DIRETRIZES GERAIS

As diretrizes desta PSI constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração dos seguintes documentos:

- Manual de Contingência para serviços de Tecnologia da Informação Dados (MP-SAINF-003);
- Manual de Backup e Restauração de Dados (MP-SAINF-001);

3. TRATAMENTO DA INFORMAÇÃO

A informação sob custódia do HIFA, mesmo que pertencente a clientes, colaboradores ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação da informação devem ser feitas de acordo com as necessidades da instituição, sendo que estes processos devem estar devidamente documentados.

O HIFA reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

A informação deve ser armazenada por tempo determinado legislação ou regulação vigente.

3.1. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação criada, manuseada, armazenada, transportada ou descartada pelo HIFA será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011, sendo:

- PÚBLICAS: quando pode ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio.

- INTERNAS: quando não for desejável que ela se torne conhecida por pessoas de fora da organização.

- RESTRITAS: quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio.

- CONFIDENCIAL: quando sua exposição fora do ambiente da organização possa acarretar perdas financeiras, de imagem, de competitividade etc.

4. REQUISITOS DE SEGURANÇA DO AMBIENTE

4.1. FÍSICO

Os servidores de dados estão em área protegida fisicamente em data center próprio localizado no Hospital Maternidade.

A entrada ao Data Center tem acesso restrito a colaboradores da TI. e Terceiros previamente autorizados e/ou acompanhados, com controle através de senha de liberação.

4.2. LÓGICO

Todo acesso às informações e aos ambientes lógicos deve ser controlado por credenciais, de forma a garantir acesso apenas às pessoas autorizadas.

Os dados, as informações e os sistemas de informação devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

4.2.1. COMPUTADORES ESTAÇÃO DE TRABALHO

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

Quando se ausentar da mesa, o usuário deverá bloquear sua estação de trabalho, com desbloqueio por senha.

Apenas pessoal da área de Tecnologia da informação pode instalar softwares nas estações de trabalho dos usuários e devem utilizar apenas softwares licenciados.

4.2.2. EQUIPAMENTOS MEDICINA DIAGNÓSITICA

Os equipamentos da medicina diagnóstica como RX, US, TC e em como equipamentos do laboratório, devem estar protegidos da internet, com barreira criada no firewall, por regra de negação de permissão de acesso. A comunicação destes dispositivos se dará apenas com computadores e servidores da rede local, habilitados para troca de informação.

4.2.3. UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES / TERCEIROS DENTRO DA EMPRESA

Notebooks particulares não tem acesso à rede corporativa, neste caso é liberado um acesso à internet Wi-fi fora da rede interna.

Computadores de terceiro ou de funcionários não acessam à rede de arquivos da instituição.

O acesso de equipamentos de terceiros se dará somente via VPN, solicitada previamente na central de serviços HIFA, e quando autorizados.

5. CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS

O Backup/Restore será realizado conforme descrito no Manual de Backup e Restauração de Dados (MP-SAINF-001), de acordo com o plano de backup/restauração de cada sistema.

A política de Backup será executada em Storage (online), fita LTO (offline), e em Nuvem (softwares de terceiros) de acordo com a criticidade estabelecida no plano de backup de cada sistema;

A restauração é feita sob demanda por solicitação ou periódica de acordo com plano de restore de cada aplicação, a fim de garantir a integridade dos dados.

6. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Todo o tráfego de dados, entre rede interna e externa, é filtrado através de políticas de segurança definidas que controlam o fluxo de entrada e saída de informações entre a rede do HIFA e a internet, incluindo regras de prevenção / detecção de intrusão e de proteção contra softwares maliciosos.

O HIFA conta com proteções contra códigos maliciosos através da utilização de Firewall e antivírus em todas as estações de trabalho.

7. GESTÃO DE IDENTIDADE DE ACESSOS

Toda permissão de acesso é de responsabilidade da área de TI e é concedido conforme a necessidade do perfil do colaborador para a execução de suas atividades profissionais, tais como:

- Credenciais de acesso a sistemas;
- Gestão de Privilégios;
- Permissão ou Negação de acesso aos Sistemas;
- Política de senhas;
- Acesso Remoto por VPN;
- Acesso Físico.

Durante a integração do colaborador, o mesmo receberá as credenciais para acesso aos sistemas de sua área.

O acesso ao prontuário informatizado deverá ser realizado via usuário com login e senha com o seu respectivo perfil de acesso, sendo, portanto, pessoal e intrasferível.

Colaboradores inativados ou remanejados para outros setores deverão ter suas permissões atualizadas.

7.1. ACESSO E USO DA INTERNET

O acesso à internet será permitido sempre de acordo com a política de Segurança da Informação, com bloqueios de sites classificados como inseguros ou não confiáveis.

É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área de Tecnologia de Informação do HIFA.

Somente usuários autenticados com credenciais próprias terão acesso à internet. Credenciais genéricas não terão acesso a internet.

7.2. E-MAIL / CORREIO ELETRÔNICO

A comunicação institucional do HIFA somente poderá ser realizada através emails oficiais, domínios hifa.org.br e hifaci.org.br, não sendo permitido o uso de nenhum outro domínio.

As Informações contidas nas mensagens eletrônicas são de propriedade do HIFA podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio do HIFA, conforme o item MONITORAÇÃO nesta mesma Política.

É expressamente proibido o envio de Informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail de outros domínios além do hifa.org.br e hifaci.org.br, exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no assunto da mensagem.

O colaborador desligado, independentemente de seu cargo, terá seu email bloqueado e/ou inativado. Este bloqueio deverá emitir mensagem resposta com orientações de contato com a instituição.

7.3. USO DE COMUNICADORES DE MENSAGENS INSTANTÂNEAS (WHATSAPP / TELEGRAN/OUTROS)

A comunicação realizada entre colaboradores e público externo e vice-versa, através de aplicativos de mensagens instantâneas, somente será permitida através dos canais oficiais da instituição.

Toda a troca de mensagens deverá ser provida da segurança necessária, com acompanhamento e gravação de toda a operação, resguardando o HIFA de quaisquer vazamentos não autorizados.

7.4. SENHAS DE ACESSO

A credencial de acesso aos recursos computacionais é pessoal e intransferível, sendo de inteira responsabilidade do colaborador, que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros.

Os usuários deverão utilizar senhas “fortes”, misturando letras e números, em todos os sistemas corporativos.

As senhas de usuário do domínio “hifa.corp”, rede interna, será renovada a cada período de 90 dias.

Os recursos departamentais controlados por permissões de acesso especiais, somente serão acessados com credenciais particulares, identificado o colaborador.

Credenciais genéricas, não poderão ter acesso a servidores de arquivos, navegação na internet, acesso a emails e comunicação por aplicativos oficiais.

7.5. CONTAS INATIVAS

Toda e qualquer credencial de acesso que não tiver atividade em até 30 dias serão bloqueadas em TODOS os sistemas corporativos.

7.6. DIRETRIZES QUANTO AO USO DE MÍDIAS REMOVÍVEIS

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção. Caso seja necessário o acesso a algum arquivo de mídia removível, o mesmo deve ser solicitado a área de TI.

Informações devem ser transmitidas usando as ferramentas corporativas (email, rede de dados, software de mensageria, etc.) que proveem a segurança requerida, evitando perda ou vazamento de informação institucionais.

O uso de dispositivos de conexão à internet, como modem 3G/4g ou outros, estando conectado à rede corporativa, não é permitido.

7.7. ACESSO REMOTO

O acesso remoto será provido por VPN (Rede Virtual Privada), a pessoas previamente autorizadas por seus respectivos setores, e mediante a abertura de chamado e assinatura do termo de responsabilidade.

7.8. MESA LIMPA

Todos os colaboradores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente informações classificadas como restritas, confidenciais e secretas.

Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas de forma a não expor seu conteúdo.

Esta regra vale para o ambiente de trabalho, incluindo a estação de trabalho, mesa, gavetas, arquivos e lixo.

7.9. BLOQUEIO DE DISPOSITIVO POR INATIVIDADE

Todo dispositivo corporativo de acesso aos sistemas do HIFA deve sofrer bloqueio automático depois de 10 minutos de inatividade (computadores, smartphones, tablets ou qualquer outro dispositivo, móvel ou não).

7.10. DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais fica restrito a rede de convidados do HIFA. Não é permitida a conexão de dispositivos não corporativos as redes internas, cabeadas ou sem fio.

Aos colaboradores que precisem fazer uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos fornecidos pela empresa, com os devidos controles e proteções técnicas aplicadas.

7.11. REDES SOCIAIS

É expressamente proibido que qualquer colaborador emita qualquer comunicado, opinião ou comentário EM NOME do HIFA sem a expressa aprovação e alinhamento com as áreas de marketing e comunicação.

As interações de resposta, réplica aos comentários feitos por terceiros sobre a instituição, só podem ser feitas pelas áreas específicas de comunicação e gestão de mídias sociais, mesmo sendo postadas em redes pessoais.

A publicação de fotos em área internas também deve ser evitada, para evitar que informações restritas contidas nas áreas internas da empresa sejam publicadas inadvertidamente, a não ser que seja previamente autorizada pela área de comunicação.

7.12. SOFTWARE, APPS E PLUGINS

Não é permitido a instalação de softwares não aprovados pela área de TI e Segurança de Informação em quaisquer dispositivos que acessam os sistemas de Informação do HIFA que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plugins pagos ou gratuitos.

7.13. MONITORAÇÃO

O HIFA se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de informação para garantir o cumprimento desta e outras políticas da empresa.

Os ambientes internos do HIFA também podem sofrer gravação audiovisual com o propósito principal de gerenciar a segurança do perímetro interno da empresa contra incidentes de segurança de qualquer natureza.

7.14. ACESSO A UNIDADES INTERNAS E DE VISITANTES

O acesso às nossas unidades internas NÃO poderá ser feito por pessoas DESACOMPANHADAS. O agente de recepção do visitante deverá acompanhá-lo, DESDE a chegada nas recepções do HIFA, até a entrada nas unidades autorizadas para visitas, respeitando os protocolos de segurança da instituição.

O acesso deverá ser registrado em sistema de portaria, e ter biometria cadastrada ou crachá de acesso, e sempre terá que ser acompanhado pelo agente de recepção ou por outro colaborador do HIFA.

Os prestadores ou consultores externos também terão cadastro para identificação obrigatório, e deverão sempre estar acompanhados por um responsável pelo setor.

7.15. AVALIAÇÃO DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO

A área de Tecnologia da Informação deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação do HIFA.

A análise dos riscos deve atuar como ferramenta de orientação a área de Tecnologia da Informação, principalmente, no que diz respeito à:

- Identificação dos principais riscos aos quais as informações do HIFA estão expostas;

- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc. O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.;
- Implantação de ferramentas para identificação de riscos e compliance.

7.16. GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÃO E A OUTROS AMBIENTES

Todo acesso às informações e aos ambientes lógicos e físicos do HIFA deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação. A política de controle de acesso deve ser documentada e formalizada por meio de Normas e Procedimentos que contemplem, pelo menos, os seguintes itens:

- Procedimento formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas de informação;
- Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao propósito do negócio e se é consistente com a Política de Segurança da Informação, as Normas e Procedimentos;
- A remoção imediata de autorizações dadas a usuários desligados da empresa é feita automaticamente assim que o setor de RH desliga o funcionário, e toda vez que o usuário tem mudança de função é solicitado ao setor de TI a alteração do perfil de acesso desse usuário.
- Processo de revisão periódica das autorizações concedidas;
- Política de atribuição, manutenção e uso de senhas.

7.17. TREINAMENTO E CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

A área de Tecnologia da Informação deve garantir que todos do HIFA, incluindo fornecedores, clientes e prestadores de serviços, ao iniciar a relação com o HIFA ou quando tiverem alteração significativa na responsabilidade do trabalho, recebam treinamento sobre aspectos de segurança da informação relacionados a sua função.

8. TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais pelo HIFA é realizado em conformidade com a Lei Geral de Proteção de Dados Pessoais, sendo a guarda e eventual compartilhamento permitidos, apenas nas situações previstas na Lei.
Informações pessoais utilizadas para outras finalidades que não aquelas relacionadas à prestação de serviço, serviços administrativos, de apoio e de negócio são tratadas pelo HIFA apenas mediante aprovação, formal e explícita, realizada pelos titulares dos dados pessoais ou por seus representantes legais.

8.1. COLETA E USO DOS DADOS PESSOAIS

As informações pessoais tratadas pelo HIFA são aquelas necessárias para execução de atendimento dos pacientes, contratos firmados com seus clientes, funcionários, fornecedores e prestadores de serviço, compreendendo atividades como por exemplo:

- Abertura de atendimento nas recepções;
- Intercâmbio de dados com a SESA (Secretaria Estadual de Saúde);
- Intercâmbio de dados com operadoras de saúde;

- Manutenção do prontuário do paciente com evoluções, prescrições e demais documentos eletrônicos;
- Registro de acesso às dependências físicas das unidades hospitalares em sistema de gestão de acessos;
- Manutenção dos cadastros de prestadores, fornecedores, colaboradores.

9. DIREITOS DOS TITULARES DE DADOS PESSOAIS

Os titulares ou os representantes legais dos titulares dos dados pessoais que são tratados pelo HIFA possuem direito ao acesso a informações acerca de: tratamento de seus dados, podendo solicitar informações sobre a finalidade específica do tratamento; forma e duração do tratamento; identificação do controlador; informações do uso compartilhado de dados e sua finalidade; responsabilidades dos agentes que realizarão o tratamento.

Tais direitos incluem o direito a obter a 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 com a LGPD; portabilidade dos dados a outro fornecedor de serviço ou produto; eliminação dos dados tratados com o consentimento do titular; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento de uso dos dados pessoais.

A confirmação de existência ou o acesso a dados pessoais serão providenciados de forma imediata em formato simplificado, ou no prazo de até 15 (quinze) dias por meio de declaração completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial.

9.1. LIMITAÇÃO DOS DIREITOS DOS TITULARES

O direito do titular de solicitar o encerramento do tratamento de dados pessoais é válido apenas nas situações em que o dado tratado requer consentimento pelo titular. Contudo, nas situações em que o tratamento do dado é suportado por outra base legal, tais dados permanecerão sendo tratados pelo HIFA, sendo informado ao titular dos dados a base legal para manutenção do tratamento.

10. ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS

O DPO – Encarregado de Proteção de Dados Pessoais é o responsável pela comunicação do HIFA com os titulares dos dados. Entre suas funções estão:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O DPO será o profissional responsável por implementar, fiscalizar e reportar às autoridades quaisquer atividades relativas ao tratamento de dados pessoais.

As demandas ou solicitações serão recebidas pelo DPO, analisadas, tratadas e respondidas em conformidade com as regras e os prazos estabelecidos na LGPD, através do email ‘dpo@hifaci.org.br’ e canal digital disponibilizado no site do HIFA em ‘https://hifa.org.br/tratamento-de-dados-pessoais/’.

11. PENALIDADES

11.1.1. VIOLAÇÃO DAS POLÍTICAS

A violação desta Política de Segurança poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com o HIFA.

A observação do descumprimento desta política deve ser imediatamente reportada por meio do email si@hifa.org.br e pelos canais da ouvidoria interna em ouvidoriainterna@hifaci.org.br.

12. VIGÊNCIA

Esta Política entrará em vigor a partir da data de sua aprovação pela Superintendência e Conselho de Administrativo e permanecerá em vigor por prazo indeterminado.

13. REFERÊNCIAS BIBLIOGRÁFICAS

- Contrato de Trabalho;
- Código de conduta e ética;
- Política de Tratamento de Dados Pessoais;
- Lei 13.709 - Lei Geral de Proteção de Dados.

14. ANEXOS E DOCUMENTOS DE APOIO

Não se aplica.

ELABORAÇÃO		
DATA: *06/2023*	CARGO: *Gerente de TI*	RESPONSÁVEL: *Miter Mayer*

APROVAÇÃO		
DATA: *06/2023*	CARGO: *Gerente de Estratégia*	AUTORIZADOR: *Verônica Moten*
DATA: *06/2023*	CARGO: *Superintendente*	AUTORIZADOR: *Jailton Pedroso*

TÍTULO	*CONTROLE*	*REVISÃO*
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	*PI-INSGQ-011*	*002*
ÁREA RESPONSÁVEL		*VIGÊNCIA*
TECNOLOGIA DA INFORMAÇÃO		*2024*

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*