TÍTULO	CONTROLE	REVISÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PI-INSGQ-011	000
ÁREA RESPONSÁVEL		VIGÊNCIA
TECNOLOGIA DA INFORMAÇÃO		2023

ABRANGÊNCIA

Hospital Materno infantil Francisco de Assis

TERMOS E DEFINIÇÕES

PEP - Prontuário Eletrônico do Paciente;
GGSI - Grupo de Gestão da Segurança da Informação;
SI - Sistemas de Informação;
TI - Tecnologia da Informação;
PSI - Política de Segurança da Informação;
GTI - Gerência de Tecnologia da Informação;
POSIC - 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;
- Política de Tratamento de Dados Pessoais HIFA.

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. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD), n° 13.709/2018, tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.6. DIRETRIZES GERAIS

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

- Norma Geral de PSI do HIFA, destinado aos usuários;
- Plano de Gerenciamento de Riscos (PGR);
- Plano de Gerenciamento de Incidentes (PGI);
- Plano de Continuidade dos Negócios;
- Política de Backup e Restauração;
- Política de Tratamento de Dados Pessoais e Sensíveis
- Política de Privacidade de Dados.

Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta PSI, devem ser direcionados ao Grupo Gestor de Segurança da Informação (GGSI).

2.7. 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.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, por tempo determinado pela instituição, legislação ou regulação vigente, o que for maior e recuperável quando necessário. Já o local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

2.8. ACESSO À INFORMAÇÃO

O uso de redes externas de comunicação (Internet, redes privadas, etc.) deve ser controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

É vedado, a qualquer usuário do HIFA, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

2.9. GRUPO GESTOR DE SEGURANÇA DA INFORMAÇÃO

O GGSI terá uma atividade cooperativa, colaborativa e contínua. Este será composto pelos membros:

- Gerência de TI;
- Jurídico e Compliance;
- DPO.

São atribuições específicas do GGSI**:**

- Elaboração e revisões da Política de Segurança da Informação do HIFA, o qual servirá como guia para as ações de educação e difusão cultural do tema de Segurança da Informação e os controles técnicos aplicáveis;

- Revisão das ações educacionais já existentes no HIFA, como treinamento específico sobre SI para novos colaboradores além de iniciativas recorrentes de atualização para os demais colaboradores;

- Revisão dos procedimentos para continuidade dos negócios do HIFA (Plano de Continuidade de Negócios), bem como a produção e implantação de novos procedimentos que garantam a operação contínua dos negócios e do HIFA frente aos riscos mapeados pelo grupo gestor de riscos;

Para todos os demais, são responsáveis por:

- Conhecer e cumprir rigorosamente a Política de Segurança da Informação do HIFA, bem como toda a documentação correlata;
- Reportar ao se deparar com práticas em não conformidade com a Política de Segurança, ajudando, inclusive, na reeducação dos hábitos em não conformidade;
- Reportar ao Grupo de Segurança da Informação, ou ao canal disponibilizado pela mesma, a suspeita ou confirmação de descumprimentos de toda ou parte da PSI e seus Objetivos de Controle.

As seguintes práticas podem ser entendidas como incidentes de SI:

- Acesso não autorizado a recursos de TI, sistemas e banco de dados próprio ou de terceiros;
- Vírus;
- Ataques de navegação de serviços (DoS ou DDoS);
- Violação a esta Política ou procedimentos de SI correlatos;
- Acesso não autorizado ou vazamento de dados, inclusive de dados pessoais que estejam sob custódia do HIFA;
- Uso impróprio de Informações;
- Pirataria;
- Falha em equipamentos do HIFA.

2.10. 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.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo HIFA e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas. As informações sob gestão do HIFA terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração às informações exclusivas da instituição.

- PÚBLICAS: quando pode ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário nenhum tenha acesso a ela, a menos que precise de tal informação para o desempenho de suas atividades.

- INTERNAS: quando não for desejável que ela se torne conhecida por pessoas de fora da organização. Contudo, caso haja vazamento e ela se torne de conhecimento público, é característica da informação classificada como interna a impossibilidade da ocorrência de um grande prejuízo à organização. Como são informações relevantes para o funcionamento dos negócios, precisam principalmente ter sua integridade protegida.

- RESTRITAS: quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio. Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações confidenciais e por isso devem receber um grau de proteção ainda mais elevado. Só devem ter acesso a informações restritas, pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

- CONFIDENCIAL: quando sua exposição fora do ambiente da organização possa acarretar perdas financeiras, de imagem, de competitividade, etc. Para proteção de uma informação confidencial, se faz necessário, além de controles de acesso, controles que garantam sua integridade, pois são informações importantíssimas para as atividades do negócio. Informações confidenciais, por exemplo, jamais podem ser transmitidas via Internet sem o uso de criptografia e, quando descartadas, devem ser tomadas as providências cabíveis para que a informação seja de fato destruída, sem chance de recuperação.

2.11. ARMAZENAMENTO E TRANSMISSÃO DE INFORMAÇÕES CONFIDENCIAIS

Atendendo aos requisitos contratuais de sigilo, os meios de armazenamento previamente aprovados são: discos criptografados, transmissão por rede ou internet utilizando SSL (com certificado de origem e destino da transmissão pertencentes às partes acordadas em contrato), SSH ou SFTP (FTP via SSH).

Para transmissão de Informações confidenciais por e-mail em servidores e domínios diferentes, é necessário adicionar criptografia adicional em nível de arquivo (senha no arquivo utilizando criptografia forte de no mínimo AES 1024 bits ou equivalente). A proteção por senha deve ser aplicada INCLUSIVE para proteção de certificados privados de uso geral (por exemplo, ao se gerar pares de chaves SSH, é necessário aplicar senha FORTE nas chaves privadas).

Deverão ser classificadas como CONFIDENCIAIS as Informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas. Consideram-se Informações confidenciais todas as que assim forem classificadas, bem como – indistintamente – dados recebidos ou compilados de/sobre clientes, senhas, Informações financeiras ou de salários, código fonte, Informações sensíveis de usuários entre outras.

2.12. REQUISITOS DE SEGURANÇA DO AMBIENTE

2.12.1. AMBIENTE FÍSICO

As máquinas (servidores) que armazenam sistemas as informações do HIFA estão em área protegida fisicamente em data center próprio localizado no Hospital Maternidade.

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

A entrada nestas áreas para demais pessoas não autorizadas (visitantes, e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas do setor de Tecnologia da Informação.

2.12.2. AMBIENTE LÓGICO

Todo acesso às informações e aos ambientes lógicos deve ser controlado, 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.

2.12.3. SISTEMAS E SOFTWARES

Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a

leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa do HIFA.

Não enviar informações confidenciais para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de criptografia ou uma senha “robusta”.

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

2.12.4. MÁQUINAS - 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.

As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento. Exceto computadores que devem permanecer ligados 24 horas por dia.

Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

Apenas pessoal autorizado da área de Tecnologia da informação pode instalar softwares nas estações de trabalho dos usuários e devem utilizar apenas softwares licenciados. Em caso de dúvidas, deverá consultar a área de TI através dos canais de suporte.

A área de Tecnologia da Informação deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

2.12.5. 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.

2.13. DEVERES E RESPONSABILIDADES

2.13.1. ATRIBUIÇÃO INICIAL DA CLASSIFICAÇÃO À INFORMAÇÃO

Caberá ao colaborador AUTOR da Informação definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma Informação RESTRITA, CONFIDENCIAL ou SECRETA.

Será considerado como AUTOR da Informação o colaborador que primeiro produzir ou manipular a Informação

dentro do ambiente do HIFA.

Todo colaborador será responsável pela sua classificação e armazenamento, seguindo as recomendações contidas neste documento.

Caberá à área de Segurança da Informação de TI, prover o suporte técnico aos autores das Informações geradas e realizar os devidos treinamentos sobre proteção e armazenamento seguro de dados.

A área de Tecnologia da Informação é a provedora dos recursos e meios de armazenamentos seguro dessas informações, assim como as ferramentas de controle de acesso, proteção e criptografia.

Caberá ao colaborador armazenar os arquivos digitais da empresa obrigatoriamente no servidor de arquivos por meio dos compartilhamentos carregados em sua estação de trabalho. A área de Tecnologia da Informação não realiza nenhum tipo de backup de dados armazenados de forma local nos equipamentos e não se responsabiliza por arquivos salvos nos mesmos.

2.14. DADOS PESSOAIS SÃO COLETADOS

Dados cadastrais, tais como: nome, documentos de identificação, nacionalidade, endereço, data de nascimento, filiação, gênero, entre outros.

Dados pessoais de pacientes internos e externos

- Nome
- Dados de contato (Telefone, E-mail, Endereço)
- Empresa em que trabalha
- Profissão
- Filiação
- Responsável Financeiro
- Nacionalidade / Naturalidade
- Documentos de Identificação (CPF, RG, Nº Carteira Plano, Cartão SUS, Passaporte em caso de paciente estrangeiro)
- Gênero
- Raça/cor
- Cônjuge
- Data Nascimento
- Nome Social
- Estado Civil
- Dados biométricos (Foto)

Dados pessoais para cadastro de funcionários

- Nome
- Nome Social
- Dados de contato (Telefone, e-mail, endereço)
- Filiação
- Estado civil
- Gênero
- Cor/Raça
- Nacionalidade
- Grau de Instrução

- Documentos de Identificação (CPF, RG, Título de Eleitor, CTPS, Cartão SUS, Certificado Reservista, PIS/PASEP, CNH, Passaporte em caso de estrangeiros, Registro de conselho de classe)
- Dados biométricos (Foto e Biometria)

Dados pessoais de terceiros

- Nome
- Dados de contato (Telefone, e-mail, endereço)
- Documentos de Identificação (CPF, RG, Título de Eleitor, CTPS, Cartão SUS, Certificado Reservista, PIS/PASEP, CNH, Passaporte em caso de estrangeiros)

2.15. DIREITOS DOS TITULARES DE DADOS

Os titulares de dados pessoais têm direitos e garantias especificados pela LGPD. O HIFA assegura que sejam passíveis de serem acessados e exercidos desde o início do processo de tratamento de dados e ao longo de toda a vida do processamento, inclusive no término. São eles, conforme os artigos 6º, 18 e 20 da LGPD:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção dos dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação (apagamento) dos dados desnecessários, excessivos ou tratados em desconformidade;
- Portabilidade a outro fornecedor mediante requisição expressa;
- Eliminação dos dados tratados com o consentimento (pedido de apagamento);
- Informação das entidades com os quais houve compartilhamento dos dados pessoais;
- Informação sobre consequências de não fornecer o consentimento;
- Revogação de consentimento;
- Não discriminação no uso dos dados;
- Revisão de decisões automatizadas.

2.16. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Para que os procedimentos de anonimização e pseudonimização possam ser realizados de maneira efetiva e eficaz, é necessário observar alguns aspectos processuais e procedimentais, entre eles:

- Elencar os processos de trabalho;
- Identificar os dados a serem anonimizados ou pseudonimizados;
- Analisar o ciclo de vida dos dados sob o aspecto da mitigação de riscos, de modo a propor o arquivamento ou eliminação de informações desnecessárias;
- Avaliar o risco de identificação dos titulares dos dados anonimizados e/ou pseudonimizados;
- Definir um plano de comunicação de incidentes em caso de violação de dados;
- Documentar e relatar violações e incidentes;

2.17. PROTEÇÃO DOS DADOS

O HIFA estabelece diretrizes para o manuseio da informação, descrevendo condutas de segurança e confidencialidade para prevenção de vazamento de dados. Possui regras específicas para cópia e restauração de dados (backup e restore), bem como sobre criptografia.

- Backup realizado 1 vez por dia, às 20hs;
- A prática de Backup ocorre em Storage e fita LTO;

- Os cartuchos LTO são armazenados fora do data center em área protegida e segura no setor de Tecnologia da Informação, diariamente, Política de Backup e Restauração;
- A restauração é feita através de demanda e também realizada uma vez por mês para garantir a integridade dos dados.

2.18. GESTÃO DE IDENTIDADE DE ACESSOS

O HIFA estabelece diretrizes gerais para acesso a ativos e sistemas de informação. Toda permissão de acesso é de responsabilidade da área de informática e é concedido conforme a necessidade do perfil do funcionário para a execução de suas atividades profissionais, tais como:

- Criação de Logins;
- Gestão de Privilégios;
- Permissão ou Negação de acesso aos Sistemas;
- Política de senhas;
- Acesso Remoto;
- Acesso Físico.

No ato de admissão do funcionário na organização, o mesmo deverá assinar o contrato contemplando a cláusula de sigilo de todas as informações da organização.

No ato de admissão do funcionário e do corpo clínico, o mesmo deverá receber um login com senha de acesso.

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;

Os usuários devem seguir as seguintes práticas para proteção de senhas:

- Nunca podem ser compartilhadas ou apresentadas a terceiros.
- Nunca podem ser apresentadas/escritas em claro (com exceção de senha pré-expirada, utilizada no processo de senha inicial).

Os perfis de usuários utilizados pelo HIFA são criados e liberados de acordo com a atividade de cada setor, sendo de responsabilidade de cada funcionário um o correto uso destes acessos.

PERFIL	DESCRIÇÃO DAS PERMISSÕES PARA ACESSO AOS DADOS

Todo usuário é responsável por toda atividade associada com o login de usuário associados à sua identidade ou sob sua custódia.

2.19. PUBLICAÇÃO DE INFORMAÇÕES ABERTAS

Somente os gestores do HIFA, com assessoria devida da área de comunicação, poderão classificar Informações para divulgar externamente ou as definir como Informação Pública.

2.20. DESCARTE DE INFORMAÇÃO CLASSIFICADA

As Informações classificadas como RESTRITA, CONFIDENCIAL ou SECRETA devem sofrer tratamento especial no seu descarte.

O descarte de Informações, armazenadas em meio físico ou eletrônico, deverá ser realizado segundo o procedimento de descarte aplicável para garantir que a Informação descartada não possa ser recuperada de qualquer forma.

Além dos demais procedimentos aplicáveis:

(i) todas as Informações impressas deverão ser trituradas antes de seu descarte; aparelhos eletrônicos devem ser "resetados" antes de seu descarte;

(ii) Informações eletrônicas deverão ser deletadas mediante o uso de ferramentas apropriadas ao descarte de dados (*NIST 800-88 Data Sanitization)*, a ser disponibilizada pela área de TI/SI do HIFA.

2.21. EXTRAVIO DE INFORMAÇÃO

Qualquer evento de perda, extravio ou roubo de Informações, devem ser reportados IMEDIATAMENTE ao Grupo de Segurança da Informação, por meio do email si@hifa.org.br.

2.22. DO USO DOS ATIVOS DE TI (FERRAMENTAS CORPORATIVAS)

O HIFA poderá fornecer ao colaborador uma conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha celular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho.

O uso destas ferramentas estará sujeito a esta Política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Grupo de Segurança da Informação.

Como política de nível de acesso à informação, utilizamos a premissa de "menor privilégio possível". O colaborador somente terá acesso aos aplicativos e informações que forem estritamente necessários para a realização do seu trabalho.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.

O colaborador é responsável pelos ativos de TI do HIFA, bem como pelas Informações que inserir em tais ativos.

2.23. ACESSO E USO DA INTERNET

O HIFA poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e 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 Segurança da Informação do HIFA.

Essa aprovação é uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantirmos que somente ferramentas e fabricantes que possuam alta maturidade em Segurança da Informação, proteção de dados e políticas claras de privacidade, sejam incorporados à lista de ferramentas e fornecedores aprovados.

Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de Segurança da Informação.

Da mesma forma, não será permitido o *download* de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação. O colaborador deve consultar o departamento de TI antes de fazer o download de qualquer software de terceiros.

2.24. E-MAIL / CORREIO ELETRÔNICO

O correio eletrônico do HIFA, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

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.

As Informações classificadas, como “SECRETAS” não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é obrigatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos, através de solicitação à área de Segurança de Informação e autorização do superior imediato.

Quando um colaborador do HIFA for desligado, deverão ser observados os seguintes procedimentos em relação ao seu e-mail corporativo:

- O colaborador, independentemente de seu cargo, deverá ser informado de que seu e-mail corporativo foi suspenso e que o colaborador poderá, desde que acompanhado por um outro colaborador do HIFA designado para essa tarefa, retirar eventual e-mail pessoal e informações pessoais constantes em sua caixa de e-mails corporativa e/ou arquivos digitais e físicos;

- O e-mail corporativo do colaborador desligado deve emitir mensagem resposta ao receber e-mails informando que o e-mail está suspenso e que o remetente poderá entrar em contato com o HIFA por meio de outro canal de comunicação (por exemplo, e-mail de eventual gestor do colaborador desligado);

- O e-mail corporativo deve ficar ativo somente por um prazo razoável de até 30 dias e após esse período deve ser excluído juntamente com todas as informações e dados pessoais.

2.25. SENHAS DE ACESSO

A senha de acesso aos recursos computacionais do HIFA é 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 e o tamanho mínimo recomendado para as senhas é de 9 (nove) caracteres.

Informações classificadas como SECRETAS deverão obrigatoriamente utilizar uma sequência longa de pelo menos 16 caracteres, ou optar pela utilização de uma chave criptográfica de pelo menos 1024 bits (utilizando-se sempre uma senha adicional para a proteção da chave criptográfica).

Toda ação feita, dentro ou fora do ambiente computacional do HIFA, será de responsabilidade do colaborador associado às credenciais de acesso relacionado às ações.

2.26. CONTAS INATIVAS

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

2.27. AUTENTICAÇÃO DE MULTI FATOR (DOIS FATORES)

É obrigatório o uso de autenticação multi-fator (2FA ou MFA; Two factor Authentication ou Multi-Factor Authentication) para TODOS os serviços onde a opção estiver disponível.

2.28. 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.

O uso do modem 3G estando conectado à rede corporativa, não é permitido.

Os usuários de mídias removíveis, caso comprovado, serão responsabilizados quando os mesmos causarem dano aos ativos de informação do HIFA, seja por perda/vazamento de informação confidencial e/ou permitir a entrada de vírus ou softwares maliciosos na rede corporativa.

Caso seja necessário transportar arquivos através de mídias removíveis (HD Externo ou PenDrive) é recomendado que os arquivos sejam criptografados e apagados, posteriormente, a fim de evitar vazamento de informação sensível.

2.29. ACESSO REMOTO

Colaboradores previamente cadastrados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional do HIFA para trabalho fora de seu ambiente normal. Para isso, é necessário a abertura de chamado com aprovação da gestão.

Esse processo deve utilizar apenas equipamentos próprios fornecidos pelo HIFA com a aplicação dos controles de segurança vigentes. A conexão será estabelecida por meio de VPN privada corporativa.

2.30. 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.

Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.

Toda Informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável ou por qualquer outro colaborador que assim o quiser fazê-lo exercitando as boas práticas de proteção de Informações do HIFA.

Os documentos órfãos notoriamente importantes (que possuem assinaturas por exemplo) deverão ser depositados em um armário especial do tipo boca de lobo para que possam ser revisados posteriormente antes de sua destruição - cofre de documentos órfãos localizados ao lado das impressoras.

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

2.31. 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).

2.32. CAPTURA DE TRÁFEGO NA REDE

É expressamente proibida a captura de tráfego de rede dentro da rede corporativa do HIFA, salvo eventos devidamente autorizados pelo Grupo Gestor de segurança para fins exclusivos de diagnóstico, auditoria e monitoração previamente autorizados.

2.33. 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.

2.34. 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.

2.35. 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.

A área de TI deve possuir um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins.

A maioria dessas ferramentas já são previamente instaladas em todos os dispositivos corporativos.

2.36. POSTURA GERAL DE PRIVACIDADE

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio.

É expressamente proibido o acesso a quaisquer informações de clientes, colaboradores ou qualquer registro nos sistemas de informação do HIFA sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

É expressamente proibido o acesso a dados de pacientes, clientes, fornecedores por mera curiosidade, por exemplo:

- Acessar dados de celebridades, pessoas públicas, parentes, amigos ou qualquer outro cliente sem que haja um propósito de atendimento e principalmente, um chamado relacionado ao caso.

- Caso precise resolver algum problema na sua própria conta, como alterar uma informação de cadastro, abra um chamado e peça que um colega faça a alteração para você.

- Acessar o Prontuário Eletrônico do Paciente, sem que haja necessidade assistencial ou solicitação jurídica protocolada, e somente por colaborador autorizado e com funções específicas para manuseio de prontuário.

2.37. 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.

2.38. MODIFICAÇÃO / ROOT / JAILBREAKING

Com o propósito de proteger os dados do HIFA e seus clientes, não é permitido acessar qualquer ferramenta corporativa utilizando dispositivos que sofreram alterações nos sistemas nativos de segurança.

Exemplos práticos:

- Acesso utilizando celular ou tablet Android com alterações e desbloqueios, conhecidos também como "Root de Android";

- Acesso utilizando um iPhone ou iPad com "Jailbreak".

Devido a criticidade e o entendimento de que essas modificações afetam seriamente a segurança desses dispositivos, acessos feitos a partir de dispositivos pessoais (qualquer celular ou tablet pessoal) com essas modificações é expressamente proibido.

2.39. 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.

A porta de acesso às unidades internas de cada hospital, DEVE PERMANECER SEMPRE FECHADA. É vedado a presença de estranhos e não identificados nos corredores das unidades. Se necessário, peça à segurança da unidade para subir ao andar, verificar e escoltar a pessoa para o local correto para a devida identificação.

Não é permitido o atendimento a fornecedores fora do local reservado para a recepção de fornecedores.

2.40. CONFIDENCIALIDADE E INTEGRIDADE

Os gestores devem informar a todos do HIFA, os clientes e os fornecedores, usuários em geral dos sistemas de informação e dos processos que todas as informações armazenadas, transmitidas ou manuseadas por estes processos e sistemas são de propriedade do Hospital e de seus clientes ou licenciadas por terceiros. Sempre que permitido pela legislação, o HIFA reserva o direito de revisar e monitorar estas informações para fins administrativos, de segurança ou legais.

Informações confidenciais do HIFA, independentemente da mídia ou ambiente onde estejam sendo mantidas, devem ser protegidas contra acessos não autorizados e com as devidas aprovações. Este padrão se aplica, mas não está limitado, aos seguintes tipos de mídia ou ambiente, nos quais as informações estão contidas, registradas ou armazenadas: dados em cloud, cartões, CD, DVD, cópia impressa, disco magnético, fita magnética, pen drive, microfilme, disco ótico, documentos em geral, equipamentos de processamento, de rede, Internet, etc.

Para a proteção adequada das informações custodiadas pelo HIFA, que estão sendo manuseadas nas estações de trabalho, sempre que o colaborador se ausentar do ambiente, em particular fora do horário de trabalho, é sua responsabilidade bloquear a estação de trabalho, solicitar e utilizar os recursos disponibilizados pela área de Tecnologia da Informação para proteger as informações de acessos não autorizados. Para a proteção adequada das informações custodiadas pelo HIFA, que estão sendo manuseadas em equipamentos portáteis (notebook), todos os usuários devem cumprir os requerimentos definidos pela norma específica.

As informações classificadas como RESTRITA ou CONFIDENCIAL, quando não forem mais úteis ao HIFA ou seus clientes, considerados os períodos de retenção estabelecidos por lei, regulamento ou contrato, devem ser destruídas segundo os procedimentos definidos. Cada gestor deve assegurar que Terceiros (clientes ou fornecedores) protejam adequadamente as informações custodiadas pelo HIFA às quais eles têm acesso.

Monitorando os Terceiros que armazenam, processam, gerenciam ou acessam as informações do HIFA (exceto as informações classificadas como INTERNA ou PÚBLICA) ou têm conexão com os recursos de rede do Hospital, para que cumpram os padrões aqui definidos.

Formalizando acordos de confidencialidade NDA – “Non Disclosure Agreement” ou disposições equivalentes, aprovados pela área jurídica, com os Terceiros que armazenem, processem, gerenciem ou acessem informações custodiadas (exceto informações classificadas corno PÚBLICA).

2.41. ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações, com destaque para os seguintes itens:

Quotistas, colaboradores e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações.

Todos devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.

Todo tipo de acesso à informação do HIFA que não for explicitamente autorizado é proibido.

Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (ônibus, Uber, aviões, restaurantes, encontros sociais, elevadores, táxis, espaços de coworking, etc.).

As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido.

Somente softwares homologados pela equipe de TI do HIFA podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da Informação, respeitando as questões legais de licenciamento;

A política para uso de internet e correio eletrônico deve ser rigorosamente seguida;

Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;

Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.

Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Tecnologia da Informação;

Todas as normas de segurança da informação devem ser rigorosamente seguidas. Casos não previstos devem ser imediatamente submetidos para análise e a validação à área de Tecnologia da Informação.

2.42. 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.;
- Planejamento trimestral de identificação e análise dos riscos, podendo ser alterado o ciclo de análise conforme definido pela área de Tecnologia da Informação;
- Implantação de ferramentas para identificação de riscos e compliance.

2.43. 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;
- Comprovação da autorização do proprietário da 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.

2.44. SEGURANÇA EM REDES

O HIFA possui equipamentos específicos capazes de detectar e responder tentativas de intrusão em seu ambiente de rede.

Atualmente a segurança da rede é realizada através de Appliances de segurança de classe empresarial, na categoria NFGW.

2.45. RESPOSTA A INCIDENTES DE SEGURANÇA

A área de Tecnologia da Informação deve assegurar que todos os sistemas de informação que armazenam informações custodiadas (confidenciais) pelo HIFA usam trilhas de auditoria para registrar e reportar:

- Todas as tentativas de violação da segurança do sistema;
- Todos os eventos significativos relacionados à administração do sistema bem como a segurança das transações e informações custodiadas (confidenciais) pelo HIFA;
- O nível de detalhe das trilhas de auditoria deve ser compatível com o nível de risco do processo associado;
- Qualquer atividade suspeita deve ser imediatamente verificada e tomadas as ações corretivas necessárias.

Todas as áreas devem garantir que todos os produtos, serviços ou aplicativos sob gestão do HIFA, que usam a Internet para conexão ou comunicações, seguem o processo de avaliação de vulnerabilidade de aplicativos aprovado pela Área de Tecnologia da Informação.

Problemas classificados como de alto risco, identificados em teste de vulnerabilidade, devem ser resolvidos antes que o produto, serviço ou aplicativo entre em produção ou que as atualizações sejam implantadas no ambiente de produção. O gestor responsável pelo produto, serviço ou aplicativo deve manter registro de todas as ações tomadas para resolver os problemas de alto risco identificados.

A área de Tecnologia da Informação deve assegurar que, a cada mudança significativa e no mínimo anualmente,

sejam realizados testes de vulnerabilidade dos componentes sob sua responsabilidade.

2.46. TREINAMENTO E CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

A área de Tecnologia da Informação deve garantir que todos do HIFA e os fornecedores, 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.

2.47. PRODUTOS E SERVIÇOS DE GERENCIAMENTO DA SEGURANÇA

Sistemas de detecção de invasão e demais produtos e serviços de segurança da informação só podem ser contratados se aprovados pela área de Tecnologia da Informação.

Todos os alarmes de sistema associados a Segurança da Informação e eventos de segurança gerados sejam registrados e arquivados diariamente.

Quando ocorrer um Evento de Segurança, a área de Tecnologia da Informação deve ser acionada através do processo e procedimento definidos pela área de Segurança da Informação.

Os controles da área de Tecnologia da Informação devem assegurar que todas as conexões IP a Terceiros são protegidas por firewalls.

2.48. GESTÃO DE TERCEIROS

O HIFA pode contratar prestadores de serviços de informática para realização de assessorias, consultorias, elaboração de projetos, implantação e implementação de sistemas.

A prática de qualificação e avaliação de fornecedores deverá ser realizada conforme documento definido pela Qualidade - Qualificação e Avaliação de Fornecedores;

2.49. RECURSOS DE CLOUD COMPUTING

Em caso de contratação de serviço Cloud Computing (Serviço de Computação ou Armazenagem na Nuvem) deve-se verificar se o fornecedor escolhido disponibiliza de recursos como:

- Garantias de privacidade e segurança;
- Criação de backups e salvaguardas dos conteúdos das comunicações realizadas e a possibilidade de consulta de dados;
- Procedimentos e metodologias para contenção e resposta a incidentes de segurança da informação e dados pessoais;
- Garantia do ciclo de vida da informação;
- Documentações e processos formalizados de gestão e mudanças;
- Garantia de auditabilidade e rastreabilidade;
- Acordos de níveis de serviço (SLAs).

2.50. MECANISMOS DE PREVENÇÃO DE PERDA DE DADOS - DATA LOSS PREVENTION

No contexto da disseminação do uso de guarda de dados em nuvem, o HIFA deve adotar Mecanismos de Prevenção de Perda de Dados. Em suma, tais mecanismos são centrados na proteção dos dados e buscam evitar problemas de acesso ou armazenamento. Neste sentido deve-se:

- Manter os procedimentos e sistemas sempre atualizados: deste modo, é possível evitar ameaças e proteger os dados de maneira contínua;
- Adotar políticas de acesso personalizadas às necessidades da corporação: nem sempre é necessário que todos os funcionários tenham acesso ao ambiente geral da corporação, por isso, adotar políticas de permissão de acesso de acordo com níveis e necessidades reais é uma ótima estratégia;
- Garantir a adesão dos procedimentos de segurança da informação em todos os dispositivos com a possibilidade da mobilidade de acesso aos dados, nem sempre o colaborador vai acessar as informações por meio das ferramentas da instituição, por exemplo, podendo utilizar smartphones, tablets e computadores pessoais. Todavia, cabe ao HIFA garantir que em todos estes ambientes os padrões de segurança sejam adotados quando é feito o acesso aos dados, como conexões de rede privada (VPN) ou até mesmo localização do IP;
- Disponibilizar mecanismos de identificação dos dados: categorizar os dados de acordo com seu uso (em uso ou ocioso), movimento (trafegando pela rede) e armazenamento (local ou cloud) é essencial para garantir maior controle das informações.

2.51. ATUALIZAÇÃO DE SOFTWARES

Os critérios de aceitação de novos sistemas, englobando atualizações ou novas versões, deverão ser definidos de acordo com um processo formal de certificação e reconhecimento, para garantir que os requisitos de segurança tenham sido devidamente implantados, incluindo:

- Requisitos de desempenho e de demanda de capacidade computacional.
- Recuperação de erros, procedimentos de reinicialização e planos de contingência.
- Elaboração e teste de procedimentos operacionais de rotina para o estabelecimento de padrões.
- Concordância sobre o conjunto de controles de segurança utilizados.
- Manuais operacionais eficazes.
- Requisitos de continuidade do negócio
- Evidência de que a instalação do novo sistema não afetará de forma adversa os sistemas já existentes, particularmente nos períodos de pico de processamento, como, por exemplo, em final de mês.
- Evidência de que tenha sido considerado o impacto do novo sistema na segurança da organização como um todo.
- Treinamento na operação ou uso dos novos sistemas.
- Facilidade de uso, a fim de evitar perda de desempenho pelo usuário ou falhas humanas.

A atualização do sistema de gestão hospitalar (MV) é realizada de acordo com a liberação das versões pela fornecedora da solução. Após esta liberação são realizados vários testes de atualização e utilização do sistema pelas áreas críticas da instituição.

2.52. PENALIDADES

2.52.1. 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.

2.53. VIGÊNCIA

TÍTULO	CONTROLE	REVISÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PI-INSGQ-011	000
ÁREA RESPONSÁVEL		VIGÊNCIA
TECNOLOGIA DA INFORMAÇÃO		2023

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.

2.54. REGRAS DE CONSEQUÊNCIAS

As consequências em caso de descumprimento destas normas serão tratadas em conformidade com as diretrizes da instituição, para os casos previstos, ou em deliberação da Superintendência mediante posicionamento das áreas envolvidas.

3. 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.

4. ANEXOS E DOCUMENTOS DE APOIO

ANEXO 01 - TERMO DE RESPONSABILIDADE;
ANEXO 02 - TERMO DE RESPONSABILIDADE PARA TERCEIROS;
ANEXO 03 - TERMO DE COMPROMISSO ACESSO REMOTO;
ANEXO 04 - TERMO DE RESPONSABILIDADE E CONSENTIMENTO SOBRE O USO DE APLICATIVOS DE MENSAGENS INSTANTÂNEAS;

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*

HISTÓRICO DE REVISÕES		
DATA: *06/2023*	REVISÃO: *000*	DESCRIÇÃO: *Implantação*