1. OBJETIVO

Estabelecer as diretrizes para proteção das informações que estão armazenadas ou que circulam no âmbito dos recursos de Tecnologia da Informação (T.I.) do Hospital Porto Dias (HPD), buscando resguardá-las de acesso lógico não autorizado, da ação de vírus de computador, de erros ou omissões em sua utilização, de uso indevido, do extravio ou vazamento de informações, de sabotagem, de falhas de *hardware* e da indisponibilidade de serviços ou informações.

2. RESPONSABILIDADES

2.1. PRESIDÊNCIA, DIRETORIAS E GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Elaborar, aprovar, revisar e disponibilizar as diretrizes que assegurem a segurança da informação no HPD.

2.2. COLABORABORES E USUÁRIOS ATUANTES NO HOSPITAL

Utilizar os Recursos de T.I. para fins estritamente profissionais, alinhados a Política de Segurança da Informação e em conformidade com a moral e as leis vigentes.

3. DIRETRIZES

- A presente Política de Segurança da Informação está em conformidade com a legislação brasileira correlata, em especial a Lei 13.709/2018 Lei Geral de Proteção de Dados Pessoais (LGPD). As normas constantes da Política de Segurança da Informação são aplicáveis a todas as unidades do grupo HPD e é de observância obrigatória a todos os usuários.
- Os Recursos de T.I., bem como toda informação do hospital ou para ela/nela gerada, adquirida, armazenada, processada ou transmitida são de propriedade do HPD.

- Os Usuários deverão observar todas as normas de conduta previstas na Política de Segurança da Informação e deverão tomar todos os devidos cuidados para que as informações que circulam ou que estejam armazenadas no âmbito dos Recursos de T.I. somente possam ser acessadas conforme autorizado.
- Os Usuários não poderão, em nenhuma hipótese, utilizar os Recursos de T.I. para o acesso, a visualização, a divulgação, a transmissão ou o armazenamento de qualquer tipo de conteúdo ou informação que possa se enquadrar nos seguintes casos:
  - Conteúdo que possa ser considerado inadequado, imoral ou ilegal;
  - Conteúdo que contenha ou faça referência a qualquer forma de discriminação, ao racismo, à pedofilia, à pornografia, à prática de crimes, à incitação à violência, ou a informações falsas, caluniosas, injuriosas ou difamatórias;
  - Conteúdo que viole a propriedade intelectual de terceiros, notadamente direitos de patentes ou marcas, segredos industriais, regras de licenciamento de softwares ou direitos autorais, ou ainda que configure concorrência desleal ou outros crimes tipificados na Lei de Propriedade Industrial e na Lei de Direito Autoral (Lei. n. 9.610/98);
  - Conteúdo que caracterize a produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador que tenham como objetivo invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dado ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita;
  - Conteúdo que caracterize a produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador que tenham como objetivo interromper serviço telemático ou de informação de utilidade pública, ou

impedir e dificultar seu restabelecimento (vírus, Worms - é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar, cavalos de tróia, malware - é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações, etc. (confidenciais ou não);

- Caso o Usuário se depare com qualquer dos conteúdos mencionados acima, deverá proceder, imediatamente, à notificação do HPD através dos canais de comunicação
- O HPD reserva para si o direito de monitorar e de interferir no uso dos Recursos de T.I., com o propósito de verificar o cumprimento dos padrões de segurança estabelecidos pela Política de Segurança da Informação sempre que julgar necessário e sempre que possível armazenará os dados e os registros relativos a todas as atividades realizadas por cada Conta de Usuário dentro dos Recursos de T.I.

• No âmbito da presente Política de Segurança da Informação, os seguintes termos, expressões e palavras serão empregados, no singular ou no plural, de acordo com as definições ora estabelecidas:

- **Colaborador:** são os membros da diretoria, os empregados e os estagiários, por ela diretamente contratados com base na legislação trabalhista.
- **Prestador de Serviço:** é a pessoa física ou jurídica que, por força de contrato firmado com este objetivo, preste serviços de qualquer natureza a qualquer uma das unidades.
- **Fornecedor:** é a pessoa física ou jurídica que, por força de contrato firmado com este objetivo, forneça bens ou produtos de qualquer natureza a qualquer uma das unidades.

- **Paciente:** é a pessoa física, particular ou conveniada, que contrata os serviços de saúde prestados pelo HPD.
- **Corpo clínico**: é o conjunto de médicos, fisioterapeutas, psicólogos, odontólogos, fonoaudiólogos, e profissionais da saúde que prestam assistência aos pacientes do HPD, particulares ou conveniados, que gozam de autonomia profissional, técnica, científica, política e cultural.
- **Visitante:** é a pessoa física que não se enquadre em qualquer outra definição e que, por breve período, tenha acesso aos recursos de Tecnologia da Informação.
- **Usuário:** é o Colaborador, Prestador de Serviço, Fornecedor, membro do Corpo Clínico ou Visitante que, por qualquer meio e ainda que momentaneamente, tenha acesso à Infraestrutura de Tecnologia de Informação.
- **Recursos de Tecnologia da Informação (T.I.):** é o conjunto de bens ou recursos materiais ou imateriais que integra o sistema de tecnologia da informação de qualquer das unidades do HPD, tais como os computadores de mesa (*desktop*) e seus acessórios, os computadores portáteis (tais como *notebooks, laptops, palmtops, tablets*), os servidores de rede, as redes de dados, as redes de telefonia, as redes de conexão à *internet*, os Sistemas Corporativos, os *softwares*, os dispositivos de armazenamento, os *scanners*, as impressoras, os aparelhos de áudio, bem como quaisquer outros recursos tecnológicos utilizados para execução das atividades profissionais.
- **Sistemas Corporativos:** são todos os sistemas e aplicativos utilizados, no âmbito do HPD, para o exercício das atividades profissionais: rede corporativa, Correio Eletrônico Corporativo, Tasy, Sênior, PACs CareStream dentre outros.
- **Correio eletrônico corporativo (*e-mail* corporativo):** é o endereço de *e-mail* corporativo adotado pela empresa.

- **Conta de Usuário:** é a conta utilizada pelos Usuários para acesso aos Sistemas Corporativos, vinculada a um nome de *login* atribuído individualmente a cada Usuário pelo setor de tecnologia da informação.
- **Setor de Tecnologia da Informação (Setor de T.I.):** é o setor responsável pelo gerenciamento e pela administração dos recursos de T.I.
- **Mídias sociais:** são todas as estruturas pertencentes à rede mundial de computadores que permitem o compartilhamento de informações via redes sociais, ferramentas, *wikis, blogs, microblogs*, sites de compartilhamento de vídeos, entre outras. São exemplos de tais mídias: *Facebook, Instagram, Twitter, Snapchat, Blogger, Wordpress, LinkedIn, Youtube, Wikipedia, Flickr.*
- **Mídias de Armazenamento:** são os recursos materiais ou eletrônicos utilizados para o armazenamento de informações, incluindo dispositivos eletrônicos como fitas, discos, HDs externos (dispositivos de armazenamento magnético), *pen drives* (além de outros dispositivos que utilizam memória *flash*), CDs e DVDs (dispositivos de armazenamento óptico), bem como documentos impressos ou manuscritos;
- **Ativos intangíveis:** são uma grande variedade de informações armazenadas em formato digital, compreendendo documentos, imagens, áudio, vídeo, bancos de dados e outros bens imateriais cujo conteúdo é de titularidade exclusiva do HPD.
- **Dados pessoais:** informações relacionadas a uma pessoa natural identificada ou identificável.
- **Tratamento de dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Informações estratégicas:** são todos os dados e informações que possuem relevância estratégica para a HPD, tais como, mas não limitadas a informações financeiras, contratuais, planos de ação, dados de pacientes, dentre outras.
- **Incidente de segurança da informação:** é indicado por um ou vários eventos de segurança da informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança das informações.
- **Fragilidades em Sistemas ou Serviços:** são vulnerabilidades encontradas em *softwares* e aplicativos que podem ser exploradas por ameaças colocando em risco a confidencialidade, disponibilidade e integridade das informações.

3.1. CRIAÇÃO DAS CONTAS DE USUÁRIOS

- O Setor de T.I. atribuirá a cada um dos Usuários uma Conta de Usuário, que deverá ser utilizada exclusivamente para fins profissionais.
- A cada Usuário, devidamente identificado e individualizado, somente poderá ser atribuída uma única Conta de Usuário para acesso aos Sistemas Corporativos.
- Em caráter excepcional, o Setor de T.I. poderá criar contas de usuário genéricas, isto é, que podem ser acessadas por mais de um Usuário. Cada uma dessas contas ficará sob a responsabilidade do Gestor da área que a utilizar.
- O Usuário é responsável pelas movimentações e utilizações da Conta de Usuário que lhe for atribuída, cabendo-lhe sempre observar as normas integrantes da Política de Segurança da Informação e demais normas da Rede.
- Todos os Usuários somente poderão ter acesso aos Sistemas Corporativos por meio de suas respectivas Contas de Usuário.

Os Usuários, ao utilizarem a rede corporativa do HPD, não poderão:

- Acessar, visualizar, armazenar, divulgar ou repassar qualquer site, portal,

página da internet ou material com conteúdo inadequado ou ilegal, tais como aquele que contenha ou faça referência a qualquer forma de discriminação, ao racismo, à pedofilia, à pornografia, à prática de crimes, à incitação à violência, a fatos que não sejam verdadeiros, a fatos ou informações caluniosas, a fatos ou informações injuriosas, a fatos ou informações difamatórias, a fatos ou informações que contrariem a moral e os bons costumes, a fatos ou informações que violem direitos autorais, regras de licenciamento de *softwares* e direitos relativos à propriedade, à privacidade e à proteção da propriedade industrial;

- Acessar, visualizar, armazenar, divulgar ou repassar qualquer site, portal, página da internet ou material, tais como salas de bate-papo (*chat*), blogs, aplicativos de mensagens instantâneas e redes sociais, para acessar conteúdo alheio às atividades profissionais, tais como arquivos de som e vídeo que não tenham relação com o ambiente corporativo;
- Armazenar ou trocar dados de conteúdo autorais não autorizados nos termos da Lei 9.610/98 e normas correlatas;
- Fazer *download* ou distribuição de quaisquer *softwares* sem autorização prévia e formal do Setor de T.I.;
- Efetuar upload de qualquer software licenciado do HPD sem a expressa autorização do Setor de T.I.;
- Acessar e propagar deliberadamente qualquer tipo de conteúdo malicioso, como vírus, worms, cavalos de tróia ou programas que permitam o controle de outros computadores, bem como spam de propagandas de quaisquer produtos ou assemelhados;
- Utilizar ferramentas e/ou serviços de troca de mensagens não autorizados pelo Setor de T.I.;

- Utilizar qualquer ferramenta com o intuito de burlar a segurança dos Recursos de T.I. do HPD, visando o acesso a sites bloqueados ou o acesso não autorizado à internet;

- Publicar, em nome do HPD, comentários em mídias sociais, sites, blogs ou qualquer outra rede de relacionamento ou colaboração;

3.2. SENHAS

A senha de acesso vinculada à Conta de Usuário tem caráter pessoal e intransferível, sendo vedado ao Usuário revelá-la a quem quer que seja, bem como solicitar a senha de outros usuários.

Os Usuários deverão criar senhas que:

- Sejam fáceis de lembrar e difíceis de serem descobertas por terceiros;
- Não contenham caracteres idênticos consecutivos ou grupo de caracteres somente numéricos ou alfabéticos;
- Não sejam baseadas em dados de fácil adivinhação ou obtenção a partir de informações pessoais, tais como nome, sobrenome, datas importantes, placas de carros, números de documentos, entre outras.

São exemplos de senhas seguras aquelas que não contenham mais de 2 (dois) caracteres consecutivos do nome completo do titular da Conta de Usuário e que contenham caracteres das quatro categorias seguintes:

- Caracteres maiúsculos (de “A” a “Z”);
- Caracteres minúsculos (de “a” a “z”);
- Base 10 dígitos (0 a 9);
- Caracteres não alfabéticos (ex: !, $, #, %).

As senhas criadas para acesso aos Sistemas corporativos deverão ser utilizadas exclusivamente para este fim, e nunca em sistemas de outras empresas ou serviços, como e-mails pessoais, redes sociais, internet banking, entre outros.

O Usuário deverá se atentar para os locais de guarda das senhas criadas para acesso aos sistemas corporativos, evitando anotá-las e deixá-las expostas a terceiros, assumindo a responsabilidade sobre elas e a mesma deverá ser trocada a cada 90 dias.

Caso haja a necessidade de redefinir a senha vinculada à Conta de Usuário, o Usuário deverá solicitar ao Setor de Tecnologia da Informação apresentando suas identificações de colaborador ou prestador de serviço.

3.3. BLOQUEIO E DESATIVAÇÃO DE CONTAS DE USUÁRIO

- As Contas de Usuários relativas a Usuários que não mantenham mais vínculo com o HPD serão desativadas na data do término do vínculo, cabendo o setor de Recursos Humanos e Credenciamentos notificar a T.I.
- Em caso de desligamento da liderança do setor, caberá ao diretor responsável pela área notificar o setor de Recursos Humanos e de T.I.
- Os dados e informações referentes à Conta de Usuário desativada deverão ser preservados por um prazo de trinta dias após o término do vínculo do usuário.
- Ainda que, por algum motivo, a Conta de Usuário não tenha sido desativada na data do término do vínculo entre o Usuário e o HPD, o Usuário não poderá utilizá-la para acessar os Sistemas Corporativos.
- Em caso de bloqueios emergenciais, o setor de R.H. ou Diretoria responsável deverá entrar em contato com o Setor de T.I. solicitando o bloqueio.

3.4. CANAIS OFICIAIS DE COMUNICAÇÃO

Constituem canais oficiais de comunicação do HPD todas as funcionalidades disponibilizadas pelos:

- Sistemas homologados;
- E-mails corporativos;
- Sistema de telefonia interna

Os Usuários devem fazer uso dos canais oficiais de comunicação sempre que for necessária a transmissão de quaisquer informações relativas às atividades do HPD, sendo expressamente vedado o envio por canais alternativos.

O Usuário assume a responsabilidade pelas informações por ele compartilhadas ou trafegadas por meio de canais não oficiais de comunicação, por exemplo: e-mail particular e aplicativos de mensagens instantâneas (como o Whatsapp ou Telegram).

3.5. USO DE CORREIO ELETRÔNICO CORPORATIVO

É dever do Usuário fazer uso adequado da conta de e-mail corporativo que lhe for atribuída, sendo vedado:

- O envio de mensagens com informações particulares, ou seja, que digam respeito às informações íntimas do Usuário;
- O envio de mensagens com informações confidenciais, sem a devida autorização formal de seu Gestor ou pessoa responsável por aquela informação;
- O cadastramento da conta de e-mail corporativo em sites com finalidades particulares (como sites de mídias sociais ou de compra e venda online);
- Utilizar o correio eletrônico corporativo durante o período de férias e de afastamento por licença.

Cabe ao Usuário realizar verificações frequentes em sua conta de e-mail, eliminando arquivos e mensagens desnecessárias à execução das atividades.

São de responsabilidade do Usuário as mensagens transitadas em sua conta de e-mail corporativo e, no caso de contas genéricas, do Gestor da área.

3.6. USO DA INTERNET

O serviço de internet é disponibilizado no HPD exclusivamente para atividades relacionadas aos seus negócios e serviços, para a comunicação com clientes e fornecedores e para pesquisas de tópicos pertinentes e obtenção de informações empresariais úteis, no sentido de manter os níveis mais altos de produtividade, qualidade e atualização tecnológica e de promover o desenvolvimento profissional de seu pessoal.

O acesso à rede de internet, por qualquer meio, somente deve ser possibilitado ao usuário devidamente autenticado em sua Conta de Usuário.

O HPD poderá restringir ou bloquear o acesso a determinados sites ou categorias de sites por meio da adoção de filtros de conteúdo. Poderá ser restringido ou bloqueado o acesso a sites que:

- Veiculem qualquer tipo de conteúdo ilícito ou imoral;
- Apresentem risco de comprometimento da produtividade, tais como sites que demandam alto consumo de banda (streaming, vídeo, peer-to-peer e outros);
- Apresentem risco à segurança das informações ou dados do HPD, possuindo alto índice de disseminação de vírus computacionais.

O HPD reserva para si o direito de monitorar o uso de qualquer dado ou informação que trafegue na infraestrutura de Tecnologia da Informação conforme proposto na Lei nº 12.965/14, denominada Marco Civil da Internet.

3.7. USO DE REDES SEM FIO

O acesso via tecnologia de acesso à rede sem fio das unidades do HPD por equipamentos móveis é um serviço de comunicação disponibilizado exclusivamente

para atividades relacionadas aos seus negócios e serviços, e deverá ser utilizado para fins corporativos apenas durante o expediente de trabalho.

O HPD reserva para si o direito de cancelar ou restringir o acesso de qualquer Usuário à rede sem fio por decisão administrativa, razões técnicas ou violações das regras definidas na Política de Segurança da Informação. Qualquer acesso via tecnologia sem fio à rede de *internet* poderá ser rastreado.

Somente os dispositivos de propriedade do HPD e os disponibilizados por terceiros, nos casos previstos em contrato, que estejam em conformidade com o padrão estipulado pelo setor de Tecnologia da Informação devem ser utilizados para acesso à rede corporativa.

3.8. USO E ADMINISTRAÇÃO DA REDE CORPORATIVA

A Rede Corporativa somente deverá ser utilizada pelos Usuários que tiverem permissão para acessá-la, que estiverem devidamente autenticados em suas respectivas Contas de Usuário, a partir de aparelhos também autorizados, e para fins estritamente profissionais.

O Usuário somente poderá acessar as informações e os arquivos cujo acesso lhe for permitido pelo próprio sistema, por orientações de seu Gestor ou por disposições do contrato que o vincula ao HPD.

O Usuário deve usar adequadamente a Rede Corporativa, utilizando-a exclusivamente para a consulta de dados e informações relacionados às atividades profissionais, sendo vedada sua utilização para o armazenamento de qualquer conteúdo ilícito ou imoral.

Qualquer acesso à Rede Corporativa e qualquer atividade nela realizada pelo Usuário poderão ser rastreados.

3.9. ACESSO REMOTO EXTERNO (VPN)

O acesso remoto à Rede Corporativa somente poderá ocorrer mediante VPN, cuja liberação será realizada pelo Setor de T.I. com a assinatura de termo de responsabilidade pelo Usuário.

As normas são aplicáveis aos Usuários que acessem remotamente os Recursos de T.I. do HPD. O acesso remoto somente poderá ser concedido aos Usuários nos casos em que o exercício pleno de suas funções assim o exigirem, mediante assinatura de termo de acesso.

A T.I disponibilizará o acesso remoto ao Usuário com o único intuito de facilitar sua atuação quando em trânsito, em casos de força maior ou quando for inviável o acesso presencial à rede local nas dependências do HPD fora do horário de expediente, em detrimento da necessidade de eventual deslocamento.

A HPD reserva para si o direito de monitorar e interferir no acesso remoto, com os fins de verificar e de garantir o cumprimento dos padrões mínimos de segurança estabelecidos nesta Política de Segurança da Informação.

O equipamento utilizado para o acesso remoto deverá atender ainda aos seguintes requisitos mínimos de segurança:

- Ter instalado sistema operacional licenciado e atualizado;
- Ter instalado programa antivírus licenciado e atualizado.

O HPD reserva para si o direito de incluir regras sistêmicas que impeçam o acesso por meio de equipamento em desacordo ao disposto nos artigos anteriores, quando julgar que a falta destes requisitos esteja colocando em risco seu ambiente operacional.

O acesso remoto somente será permitido se realizado em conformidade com as orientações do Setor de T.I., que objetivarão garantir maior integridade no processo de autenticação do Usuário e proteção ao sistema contra acessos não autorizados.

Durante a sessão de acesso remoto, o Usuário deverá executar apenas atividades condizentes com suas respectivas funções, não utilizando os Recursos de T.I. para fins pessoais.

O direito ao acesso remoto será revogado permanentemente ou temporariamente nas seguintes situações:

- Desligamento do Empregado ou Colaborador;
- Detecção da não necessidade do acesso remoto;
- Não observância das regras de acesso remoto.

3.10. USO E MANUSEIO DE ESTAÇÕES DE TRABALHO, EQUIPAMENTOS E SOFTWARES

A utilização de estações de trabalho ou de equipamentos, conectados ou não à rede de *internet* ou à rede de dados, por qualquer meio, somente deve ser possibilitada ao Usuário devidamente autenticado em sua Conta de Usuário.

Os usuários devem fazer uso adequado dos equipamentos de informática (*hardware*) e programas de computador (*software*) conforme as seguintes orientações:

- Para conectar qualquer equipamento de informática (computadores, notebooks, switches, hubs etc.) na rede de dados ou na rede de internet, o Usuário deverá consultar previamente o Setor de T.I., via ordem de serviço, que autorizará ou não a solicitação;
- O Usuário não poderá alterar as configurações padrão de hardware e software dos equipamentos;
- O Usuário não poderá violar os lacres dos computadores e demais equipamentos eletrônicos, a fim de não comprometer a segurança e a garantia destes recursos;
- O Usuário não poderá compartilhar pastas ou arquivos dos computadores e demais equipamentos eletrônicos que permitam o armazenamento de informações sem a utilização de senhas de proteção e a definição dos demais Usuários autorizados a acessá-los;

- O Usuário não poderá utilizar instalar softwares não autorizados ou sem licença de uso nas estações de trabalho ou nos equipamentos eletrônicos, tais como: Jogos ou softwares de entretenimento; Softwares gratuitos, temporários ou compartilhados (freewares ou sharewares) que não se relacionem às atividades do HPD e que não sejam homologados pelo Setor de T.I.

- Cópias sem licença de softwares autorizados;

- Os Usuários não poderão utilizar os equipamentos de informática do HPD para fazer envio e/ou armazenamento de arquivos de músicas, filmes e outros tipos de documentos não relacionado com suas atividades profissionais, salvo mediante expressa autorização;

- Os equipamentos de informática do HPD não devem ser utilizados para efetuar envio (upload) de dados e documentos que sejam confidenciais ou reservados, sem a autorização prévia e formal do Gestor ou da pessoa responsável.

O Usuário deverá realizar o encerramento da sessão sempre que houver a necessidade de se ausentar de sua estação de trabalho, de forma a evitar acessos indevidos.

O Usuário deverá tomar todos os cuidados necessários para a preservação dos Recursos de T.I. que lhe foram confiados.

3.11. USO DOS COMPUTADORES MÓVEIS

Somente computadores móveis de propriedade do HPD e os utilizados por terceiros, nos casos previstos em contrato, que estejam em conformidade com o padrão estipulado pelo Setor de T.I., devem ser utilizados para acesso à rede corporativa/internet.

Os computadores móveis são disponibilizados aos Usuários como uma ferramenta de apoio às atividades profissionais e seu uso deve ser restrito às atividades realizadas no âmbito do HPD.

O uso dos computadores móveis somente será permitido a Usuários autorizados e autenticados em suas respectivas Contas de Usuário, e a sua retirada de qualquer uma das unidades do HPD deverá ser autorizada pelo Gestor responsável e controlado pelo Setor de T.I.

O Usuário que utiliza computadores móveis disponibilizados pelo HPD deve observar as instruções dos fabricantes para sua proteção e seu manuseio, além das diretrizes do HPD previstas na Política de Segurança da Informação. Somente poderão ser instalados, nos computadores móveis, softwares, aplicações e plugins que atendam às seguintes regras:

- Nos notebooks, netbooks e laptops, somente os softwares homologados pelo Setor de T.I.;
- Nos tablets, palmtops e smartphones, softwares do fabricante necessários para o funcionamento do equipamento e seus periféricos e softwares homologados pelo Setor de T.I.

As informações do HPD armazenadas nos computadores móveis devem ser protegidas pelo Usuário contra vazamento e alterações não autorizadas.

O Setor de T.I. deve efetuar a configuração do antivírus, quando disponível para o computador móvel, celulares corporativos, ou qualquer outro recurso de T.I, de modo a realizar a atualização automática via *internet*, quando o Usuário estiver fora do local onde exerce suas atividades profissionais.

O uso externo em computador móvel de qualquer mídia removível, tais como cartões de memória, CDs, DVDs, pen drives e HD externo, entre outros, deve ter sua utilização limitada a:

- Cópia de Segurança (*backup*) de trabalho.
- Transferência de dados vindos de uma fonte externa confiável.

É vedado ao Usuário alterar as configurações de rede sem fio. Quando da devolução do computador móvel, o Usuário deverá entregar todos os acessórios recebidos incluindo assessórios e itens de alimentação externa).

3.12. MANUTENÇÃO E MOVIMENTAÇÃO DE EQUIPAMENTOS

Os serviços de manutenção dos equipamentos e acessórios do HPD, bem como de softwares, devem ser executados somente pelo Setor de T.I, assim como os serviços de movimentação que devem ser solicitados via Ordem de serviço.

Caso, durante a manutenção, seja identificada a existência de softwares não autorizados, o Setor de T.I. comunicará via ordem de serviço o fato ao Gestor ao qual o Usuário se vincula, que tomará as medidas cabíveis, conforme disposto neste documento.

O Usuário deve acompanhar a realização da manutenção preventiva ou corretiva de uma estação de trabalho sob sua responsabilidade, quando esta for realizada no seu ambiente de trabalho.

Antes do descarte de estações de trabalho, de computadores móveis danificados que demandarem substituição definitiva, ou de equipamentos alugados serem devolvidos, o Setor de T.I. deve providenciar a exclusão definitiva das informações neles contidas, tornando impossível sua recuperação.

3.13. USO DE MÍDIAS SOCIAIS

O Setor de Marketing é responsável pela administração dos perfis oficiais do HPD nas Mídias Sociais, reservando-se o direito de avaliar e responder a todo e qualquer comentário publicado nestes perfis.

Se, a qualquer tempo, algum Usuário publicar ou postar conteúdo que envolva o nome ou a imagem do HPD, deverá, primeiramente, deixar claro que o conteúdo publicado contém apenas sua opinião pessoal, desvinculada à do HPD e que assume toda a responsabilidade perante a publicação.

Os Usuários não devem fazer uso das mídias sociais de maneira que comprometa a confidencialidade de dados, imagens, informações sigilosas, segredos comerciais, reequacionais ou de quaisquer ativos de titularidade do HPD, sob pena de tal conduta ser considerada prática de concorrência desleal, nos termos do artigo 195 da Lei nº 9.279/96 (“Lei de Propriedade Industrial”), de constituir crime de calúnia, difamação ou injúria, conforme os artigos 138, 139 e 140 do Código Penal, ou de ensejar responsabilização civil, conforme os artigos 186, 187 e 927 do Código Civil.

Fica proibida a publicação, a qualquer tempo, de qualquer comunicação envolvendo assuntos internos do HPD, tais como informações estratégicas, financeiras, técnicas, administrativas, sem prejuízo de outras, nas Mídias Sociais e outras formas de divulgação pública na internet.

Caso o Usuário tenha interesse em divulgar informações que sejam de potencial interesse do público-alvo do HPD, inclusive seus clientes, deverá realizar solicitação de divulgação para análise do Setor de Marketing, indicando o conteúdo que deseja ver publicado nos canais oficiais.

Somente é permitida a publicação de imagens ou informações de pacientes do HPD caso haja a autorização prévia e por escrito do mesmo para tanto.

Caberá aos Gestores de cada setor gerenciar a coleta e assinatura dos termos de cessão de imagem, a serem disponibilizados pelo Setor de Marketing.

É vedado o uso do endereço de e-mail corporativo do HPD para fins de cadastramento em Mídias Sociais, *websites*, fóruns de discussão, sites de *e-commerce* e serviços de computação em nuvem, salvo quando utilizados pelo HPD.

O HPD monitorará todos os conteúdos e comentários publicados e compartilhados nas Mídias Sociais que envolvam o nome ou a marca do HPD.

O resultado do monitoramento permitirá o HPD impor sanções, tomando as medidas cabíveis quando necessário, conforme a presente Política de Segurança da Informação e demais normas internas existentes.

Não serão toleradas publicações que veiculem o nome do HPD a qualquer tipo de conteúdo mencionado na presente Política de Segurança da Informação; que veiculem dados pessoais, sobretudo de Pacientes, sem a autorização prévia e formal do titular; ou que digam respeito a informações estratégicas do HPD.

No que diz respeito a postagens realizadas por Colaboradores, membros do Corpo Clínico, Fornecedores e Prestadores de Serviços, em quaisquer Canais de Comunicação, caberá a este, exclusivamente, a responsabilidade pelo conteúdo da publicação e divulgação.

3.14. PROTEÇÃO FÍSICA DOS ATIVOS DE INFORMAÇÃO

As normas previstas regulamentam o uso e a proteção dos Recursos de T.I, visando resguardar os equipamentos de acesso físico não autorizado, da ação de vírus, de erros, de omissões e de uso indevido, bem como promover o descarte seguro de dados. Os Recursos de T.I. são de propriedade do HPD, não podendo ser extraviados, copiados, pirateados ou armazenados em dispositivos que não sejam de propriedade e utilização do HPD. Todo uso e acesso a sistemas críticos devem ser monitorados com o objetivo de detectar atividades não autorizadas.

3.15. DESCARTE SEGURO DE MÍDIAS DE ARMAZENAMENTO

As Mídias de Armazenamento devem ser descartadas nos seguintes casos:

- Mídias que passaram do prazo de validade ou tornaram-se inutilizáveis por alguma outra razão;
- Devoluções de dispositivos defeituosos que estejam no prazo de garantia;
- Discos ópticos com informações que deixaram de ser necessárias;

- Papéis com dados obsoletos para o HPD, que já não precisam estar impressos ou que são redundantes (ou seja, que estão presentes em outras Mídias de Armazenamento).

Os papéis que contenham dados pessoais ou quaisquer outras informações estratégicas do HPD deverão seguir o fluxo de descarte e não poderão ser utilizados como rascunho.

3.16. SEGURANÇA FÍSICA DO DATA CENTER

- As salas que contêm os servidores do HPD são áreas de acesso restrito a Colaboradores, Prestadores de Serviços ou Fornecedores autorizados, que devem se sujeitar às normas de utilização do ambiente. Caberá ao gestor de Tecnologia da Informação definir os acessos permitidos às salas de servidores, bem como revisar esses acessos periodicamente.
- Não será permitido o acesso às salas de servidores à pessoa que portar objetos pessoais como bolsas, mochilas, sacolas, cadernos, alimentos ou ferramentas, salvo necessidade e com o devido acompanhamento.
- Não será permitido o acesso às salas de servidores à pessoa que portar qualquer tipo de dispositivo eletrônico de processamento e armazenamento de informações, tais como *pen drives*, CDs ou DVDs, salvo necessidade e com o devido acompanhamento.
- Somente será permitida a entrada de equipamentos e ferramentas se comprovada a sua necessidade para execução de alguma atividade.
- É proibido fazer uso indevido de qualquer ferramenta dentro das salas que contenham os servidores do HPD que possa causar prejuízo para o ambiente, instalação ou qualquer equipamento da empresa.
- É proibido filmar ou fotografar nas dependências das salas que contenham os servidores, salvo autorização prévia da alta direção.

- Somente será liberado acesso às salas que contenham os servidores as pessoas devidamente identificadas por crachá em local visível, além do uso correto da senha das portas que lhe fazem a segurança;
- É proibido o fornecimento de senhas para acesso às salas que contenham servidores a pessoas não autorizadas.

3.17. USO DO SOFTWARE DE ANTIVÍRUS

O Setor de T.I. é responsável por instalar antivírus nos equipamentos móveis e estações de trabalho, com configuração que permita sua atualização recorrentemente.

É de responsabilidade do Setor de T.I. manter o antivírus e as correções de segurança do sistema operacional das estações de trabalho e equipamentos móveis atualizados.

É de responsabilidade do Setor de T.I. monitorar a existência de *softwares* não autorizados nas estações de trabalho e equipamentos móveis, removendo-os se identificados.

3.18. DADOS PESSOAIS

No que diz respeito ao tratamento de dados pessoais no âmbito do HPD, é proibido:

- O compartilhamento com pessoas não autorizadas, sobretudo que não integrem o HPD;
- A criação de cópias ou duplicatas de documentos com dados pessoais sem que haja necessidade para tanto, ou sem a autorização do gestor ou pessoa por eles responsável;
- A utilização para finalidade diversa daquela que justificou a sua coleta;
- A divulgação sem autorização expressa do titular;

- O armazenamento em mídias pessoais, como celulares e tablets de uso particular.

O compartilhamento de dados pessoais deve ser realizado através dos canais oficiais de comunicação disponibilizados e auditados.
Quando do tratamento de dados pessoais, os Usuários deverão sempre observar os seguintes princípios previstos na Lei 13.709/2018:

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Cabe ao Usuário zelar pela segurança e pelo sigilo dos dados pessoais que lhes são confiados, podendo o mesmo ser responsabilizado por quaisquer danos que venham a ser causados em caso de descumprimento das normas aqui previstas.

3.18.1. Geração e Preservação de Evidências

Esta seção estabelece procedimentos que regulamentam a notificação, o registro e o tratamento de Incidentes de Segurança da Informação e de Fragilidades em Sistemas ou Serviços identificadas pelos Usuários e que possam ter impactos na segurança dos Recursos de T.I, visando a permitir o controle e a adoção de medidas corretivas em tempo hábil.
Todos os Usuários devem, obrigatoriamente, notificar, conforme definido nesta seção, qualquer Incidente de Segurança da Informação ou Fragilidades em Sistemas

ou Serviços do HPD, imediatamente após sua identificação ou suspeita de sua identificação.

3.18.2. Incidentes de Segurança da Informação

São considerados exemplos de Incidentes de Segurança da Informação ou Fragilidades em Sistemas ou Serviços que devem ser notificados:

- Falhas de sistema de informação ou perda de serviços;
- Código malicioso;
- DDoS (Negação de serviço);
- Erros resultantes de dados incompletos ou inconsistentes;
- Violações de confidencialidade e integridade das informações;
- Uso impróprio de sistemas de informação;
- Perda de serviço, equipamento ou recursos;
- Erros humanos;
- Violações da Política de Segurança da Informação;
- Violações de procedimentos de segurança física;
- Mudanças não controladas ou não previstas de sistemas;
- Mau funcionamento de software ou hardware;
- Violações de acesso;
- Tentativas de invasão física ou lógica;
- Tentativas de fraude;

- Sinistros envolvendo ativos de informação;
- Vulnerabilidades em softwares ou aplicativos.

Os incidentes de Segurança da Informação deverão ser comunicados ao Gestor da área de sua ocorrência e ao Setor de T.I., da maneira mais rápida possível e, posteriormente, formalizada por meio dos canais de comunicação.

Ao reportar o incidente de Segurança da Informação, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações da Política de Segurança da Informação.

Os Usuários não devem testar Fragilidades em Sistemas ou Serviços, mas reportar sua suspeita ao Setor de T.I imediatamente, pois esse teste pode causar danos e ser interpretado como uso impróprio desses sistemas ou serviços.

Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser comunicado sobre as medidas tomadas para a solução do incidente.

Após a notificação, o Incidente de Segurança da Informação será categorizado (*hardware/software*), priorizado (urgência/impacto), e investigado, pela Gerência do Setor de T.I.

Sempre que tomar conhecimento de algum Incidente de Segurança da Informação, o setor ou a pessoa responsável pela informação ou pelo equipamento deverá preservar as informações relacionadas ao incidente, bem como informar o Setor de T.I. para que tome as providências cabíveis.

3.18.3. Incidentes envolvendo o Tratamento de Dados Pessoais

São considerados exemplos de Incidentes envolvendo o tratamento de dados pessoais que devem ser notificados:

- O vazamento de dados pessoais;
- A suspeita de vazamento de dados pessoais;

- A invasão ou tentativa de invasão do banco de dados pessoais;
- O compartilhamento ou cópia indevidos de dados pessoais;
- Violações da Política de Segurança da Informação do HPD envolvendo dados pessoais.

Qualquer incidente envolvendo o tratamento de dados pessoais deverá ser comunicado imediatamente através dos canais de comunicação, que irá reportá-lo ao encarregado pelo tratamento de dados pessoais e ao Comitê de Proteção de Dados.

Ao reportar o incidente envolvendo o tratamento de dados pessoais, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações da Política de Segurança da Informação.

O Usuário não deve tomar nenhuma ação própria para solucionar o Incidente envolvendo o tratamento de dados pessoais, mas reportá-lo imediatamente.

Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser comunicado sobre as medidas tomadas para a solução do incidente

3.19. INFRAÇÕES E PENALIDADES

A ação, omissão ou conivência de colaboradores e membros do corpo clínico que impliquem desobediência ou inobservância das disposições desta Política de Segurança da Informação sujeita o infrator às sanções abaixo descritas:

- Advertência por escrito;
- Suspensão não remunerada, conforme a legislação trabalhista, se colaborador for, ou suspensão, se membro do corpo clínico;
- Demissão por justa causa, se colaborador, ou exclusão do corpo clínico;

Colaboradores são considerados aqueles que mantêm vínculo trabalhista com o HPD, conceito que, para fins da presente Política, se aplica à Diretoria.

3.20. GESTÃO DA INFORMAÇÃO

O HPD tem como premissa o compromisso com a transparência e com o respeito nas relações com nossos clientes, visitantes e colaboradores. Com isso, o gerenciamento das informações é um componente essencial no processo de prestação de cuidados e segurança do paciente, bem como para a tomada de decisões, que abrangem diversos aspectos clínicos, técnico-científicos, administrativos, mercadológicos, econômicos, legais, ambientais e políticos. Assim, focados em Segurança da Informação, utilizamos de tecnologias e processos para garantir a privacidade e segurança de todas as informações armazenadas nos sistemas homologados, garantindo que estejam disponíveis somente aos usuários autorizados por níveis de acesso, ou seja, as informações são utilizadas por usuários autorizados e qualificados para o tratamento deste dado, dentro do desempenho das suas funções, inerentes às suas atividades.

3.21. CONTROLE DE ACESSO AS INFORMAÇÕES DOS PACIENTES

- As informações dos pacientes são recolhidas sob consentimento e são armazenadas, única e exclusivamente com a finalidade de executar o tratamento assistencial, o faturamento, as estatísticas e a guarda dos prontuários dos pacientes.
- O HPD utiliza como ferramenta para o registro, armazenamento, guarda e gestão da informação o Sistemas EMR Tasy para dados e informações relacionados à assistência prestada.
- Para dados e informações referentes aos colaboradores o sistema utilizado é o Sênior. Além dessas das ferramentas, o software Weknow e PowerBI é utilizado para visualização dos dados de forma estruturada.

- O acesso a cada categoria de dados e às informações é restrito e limitado a cada perfil de usuário de acordo com sua função no processo assistencial e administrativo. O acesso destes profissionais é controlado por papéis (perfil padronizado de acesso no sistema EMR Tasy), conforme formação de cada área.
- O HPD assegura a proteção das informações contidas em seus Sistemas de Informações pelas leis e normas que regulamentam os direitos autorais, marcas registradas e patentes, não sendo permitidas modificações, reproduções, armazenamentos, transmissões, cópias, distribuições ou quaisquer outras formas de utilização para fins comerciais sem o consentimento prévio e formal ao Setor de Tecnologia da Informação.
- As informações administrativas do HPD são restritas, conforme liberação de acesso solicitada pela gestão e ou diretoria.
- Todos os sistemas do HPD possuem suas senhas individuais e formas de acesso. Desta forma o usuário é o único responsável pelo controle e utilização de cada uma de suas senhas de acesso, sendo exclusiva e intransferível e ficando o usuário inteiramente responsável em não a transmitir.

3.22. RELACIONAMENTO COM TERCEIROS

Ao contratar outras organizações para execução dos serviços de apoio, o HPD exige dele atenção quanto à privacidade, confidencialidade e segurança dos dados tratados. Sendo assim, quando um profissional terceira precisa de acesso a um dos sistemas do HPD, os mesmos são submetidos as nossas políticas, bem como com a assinatura do termo de responsabilidade.

3.23. AUDITORIAS DE SISTEMAS

Os sistemas do HPD possuem tabelas auditadas, ou seja, os processos gravados podem ser rastreados, permitindo identificar qual usuário foi responsável por tal alteração, data, hora etc. Apenas a TI tem privilégios de acesso para realização de

tais auditorias nos sistemas. Assim elas só podem ser executadas com solicitação por meio de Ordens de Serviços (O.S) registradas por gestores, conforme descrito abaixo:

- Auditoria de Prontuários: Alta gestão, Diretoria Médica e Gerência de Enfermagem.
- Auditoria de Processo Setorial: Gerência e Coordenação da área.
- Auditoria Geral: Alta Gestão.

3.24. INCIDENTES DE SEGURANÇA OU PARADAS GERAIS DOS SERVIÇOS E SISTEMAS

O HPD emprega técnicas, recursos e processos de segurança da informação para proteger todos os dados, porém temos ciência e trabalhamos com a prevenção, pois nenhuma das formas de transmissão de dados mesmo que criptografadas, seja via recursos de internet ou integrações de sistema, são 100% seguras.

O HPD possuí um plano de respostas aos incidentes, um plano de contingência durante as paradas dos sistemas (programadas e não programadas) e um plano de Continuidade do Negócio. Dessa forma, assegura-se a continuidade dos registros e prescrições em prontuário nos casos de indisponibilidade do sistema Tasy, ficando definida como contingência o uso de formulários impressos padronizados pelo Hospital para registro e prescrições manuais a serem utilizados pela equipe assistencial. Tais formulários ficam disponíveis nas unidades assistenciais armazenados em uma pasta na cor vermelha. A ativação e desativação da contingência só ocorre mediante sinalização da gerência de tecnologia da informação e autorização da diretoria técnica hospitalar, sendo comunicada para os profissionais operacionais por meio dos gestores diretos das áreas assistenciais e de apoio. Após desativação da contingência os registros são transcritos para o prontuário eletrônico pelos profissionais responsáveis.

4. REFERÊNCIAS

Padrões de Acreditação da Joint Commission International para Hospitais. Consórcio Brasileiro de Acreditação de Sistemas e Serviços de Saúde – Rio de Janeiro: CBA: 2021. 7ª edição.

Brasil, Lei Geral de Proteção de Dados Pessoais (LGPD), lei nº 13.709,

Brasil, Lei dos direitos autorais, lei nº 9.610/98,

Brasil, Lei de Propriedade Industrial, lei 9.279/96,

Brasil, Lei Marco Civil da Internet, lei nº 12.965/14.

5. ANEXOS

Não se aplica.

6. QUADRO RECAPITULATIVO

Descrição da Revisão	Versão	Data
Emissão inicial	01	01/06/2016
Revisão Geral para adequação com as revisões dos padrões do Manual de Acreditação JCI, 6º edição	02	01/06/2018
Revisão Geral conforme norma zero institucional.	03	01/06/2020
Revisão Geral para ajustes com base na lei geral de proteção de dados com atualização dos itens: 3.Diretrizes 4.Referências	04	22/08/2022
Revisão Geral para adequação com as revisões dos padrões do Manual de Acreditação JCI, 7º edição	05	30/05/2024