PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este documento contém diretrizes da área de Tecnologia da Informação

Versão 4 - Inicial 20/08/2022 Documento inicial **Versão 5 - Revisão 29/03/2023** Adicionada informação sobre monitoramento	**Elaboração:** Daniel Carvalho Gianni
	Contribuições: Mateus Rodrigues Romanini
	Revisão: Carolina Reis e Silva Tomaz de Oliveira
	Aprovação: Marcelo César Carboneri

Política de Segurança da Informação

A Política de Segurança da Informação, também referida como PSI, da FHSL **Fundação Hospital Santa Lydia** incluindo todas as unidades por ela geridas, tem por objetivo descrever Diretrizes, Procedimentos e Normas que atendam às necessidades da proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve-se, portanto, ser cumprida e aplicada em todas as áreas da FHSL. A presente PSI está baseada nas melhores práticas propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da Segurança da Informação, bem como está de acordo com as leis vigentes em nosso país e para atender a LGPD (Lei Geral de Proteção de Dados) 13.709/2018.

I. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores, representantes e terceiros, seguirem padrões de comportamento relacionados à Segurança da Informação adequados às necessidades de negócio e de proteção legal da FHSL e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações quanto à:

• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

II. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política visa informar a cada colaborador que os ambientes, sistemas, computadores e redes da FHSL poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Coordenação de T.I.. (ou pessoa designada como DPO) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de equipamentos e informações.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

III. PRINCÍPIOS

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela FHSL pertence à mesma. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A FHSL, por meio da Gerência T.I., poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

IV. REQUISITOS

Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um Termo de Responsabilidade e todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente à Coordenação de T.I.. / DPO e ela, se julgar necessário, deverá encaminhar a diretoria. Um Plano de Contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução. Deverão ser criados controles apropriados, registros de atividades, em todos os pontos e sistemas em que a FHSL julgar necessário para reduzir os riscos dos seus ativos de informação tais como, as estações de trabalho, notebooks, acessos à internet, correio eletrônico, sistemas comerciais e financeiros desenvolvidos pela FHSL ou por terceiros. Os ambientes de produção devem ser segregados e controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A FHSL reserva-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar medidas legais cabíveis no caso de uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores.

Esta PSI será implementada na FHSL por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da FHSL e sujeitará o usuário às medidas administrativas e legais cabíveis.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

V. RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da FHSL. Será de inteira responsabilidade de cada colaborador, preservação dos ativos a ela disponibilizados, bem como obedecer às regras de utilização dos recursos (Rede, Internet, Sistemas etc.), visando evitar danos ou prejuízos aos equipamentos / FHSL.

2 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pela FHSL. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

3 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI na FHSL.

Exigir dos colaboradores a assinatura do Termo de Comprometimento, assumindo o dever de seguir as normas estabelecidas, bem como, se comprometer a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da FHSL.

4 – Dos Responsáveis pela T.I.

a) Da Área de Tecnologia da Informação
   Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e Normas de Segurança da Informação complementares. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como,

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente. Configurar permissões de acesso a fim de restringir ao mínimo necessário os poderes de cada indivíduo e ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes à FHSL. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela T.I., nos ambientes totalmente controlados por ela. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pela T.I. Quando ocorrer movimentação interna dos ativos de T.I., garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

• os usuários (login) individuais de funcionários serão de responsabilidade do próprio funcionário;

• os usuários (login) de terceiros serão de responsabilidade do gestor da área contratante. Proteger continuamente todos os ativos de informação da FHSL contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado (passar antivírus). Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da FHSL em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros (bloqueio USB, acesso restrito a rede Wifi). Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da FHSL (as instalações de software dever ser realizada pela T.I.). Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da FHSL,

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da FHSL. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da FHSL operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:
• uso da capacidade instalada da rede e dos equipamentos;
• tempo de resposta no acesso à internet e aos sistemas críticos da FHSL;
• períodos de indisponibilidade no acesso à internet e aos sistemas críticos do FHSL;
• incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
• atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

b) Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da FHSL. Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pela FHSL. Promover a conscientização dos colaboradores em relação à relevância da Segurança da Informação para o negócio da FHSL, mediante campanhas, palestras, treinamentos e outros meios. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços. Analisar criticamente incidentes. Apresentar as atas e os resumos das reuniões.

c) Da área de Coordenação de T.I.

• propor investimentos relacionados Segurança da Informação com o objetivo de reduzir riscos;

• propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;

• avaliar os incidentes de segurança e propor ações corretivas;

• definir as medidas cabíveis nos casos de descumprimento da PSI - Política de Segurança da Informação.

5 - MONITORAMENTO DO AMBIENTE

Para garantir as regras mencionadas neste PSI, a FHSL poderá:

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como, material manipulado;

• Demonstrar as informações obtidas pelos sistemas de monitoramento, no caso de solicitação do gerente (ou superior) ou solicitação judicial.

• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

VI. POLÍTICA DE SENHAS

O objetivo da política de senhas é estabelecer um padrão de criação e utilização de senhas fortes, no intuito de evitar que pessoas mal-intencionadas as descubram e se passem por outras pessoas, acessando, por exemplo: contas de correio eletrônico, de rede, de computador e de sistemas; sites indevidos ou informações privilegiadas.

A Política de senhas estabelecida contempla:

- 8 dígitos (Letras, Números, caracteres especiais)

- Expira 60 dias

VII. CORREIO ELETRÔNICO – E-mail

O objetivo desta norma é informar aos colaboradores da FHSL quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo. O uso do correio eletrônico da FHSL é para fins corporativos e relacionados às atividades do colaborador usuário dentro do local de trabalho.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da FHSL:

• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da FHSL desde que o volume não ultrapasse o permitido pelos nossos servidores;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a FHSL ou suas unidades vulneráveis a ações civis ou criminais;

• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

• apagar mensagens pertinentes de correio eletrônico quando a FHSL estiver sujeita a algum tipo de investigação.

• produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da FHSL e contenha ameaças eletrônicas, como: spam, vírus de computador; ou contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .src, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança; obter acesso não autorizado a outro computador, servidor ou rede; interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; burlar qualquer sistema de segurança; vigiar secretamente ou assediar outro usuário; acessar informações confidenciais sem explícita autorização do proprietário; acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; incluir imagens criptografadas ou de qualquer forma mascaradas; anexo(s) superior(es) a 30 MB para envio (interno e internet) e 30 MB para recebimento (internet) conteúdo considerado impróprio, obsceno ou ilegal; de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros; perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; fins políticos locais ou do país (propaganda política); material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

• Nome do colaborador

• Cargo conforme grafado no Sistema do Departamento Pessoal

• Unidade da FHSL

• Telefone(s) se aplicável

VIII. INTERNET

Todas as regras atuais da FHSL visam basicamente o desenvolvimento de um comportamento ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a FHSL, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da FHSL, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, pretende-se garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a FHSL cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela FHSL aos seus colaboradores, independentemente de sua relação contratual, deve ser utilizada com exclusividade para desempenho de suas atividades profissionais. Somente os colaboradores que estão devidamente autorizados a falar em nome da FHSL para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, seja por documento físico, entre outros. Apenas os colaboradores autorizados pela FHSL poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia correlata que venha surgir na internet. Os colaboradores com acesso à internet não estão autorizados a instalar software em seus equipamentos. Quando necessário devem solicitar a T.I., evitando desta forma instalar software sem licenciamento. Os colaboradores não poderão em hipótese alguma utilizar os recursos da FHSL para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado pela FHSL ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados. Os colaboradores não poderão utilizar os recursos para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) podem ser permitidos a grupos específicos. Não é permitido acesso a sites bloqueados pelo proxy.

IX. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da FHSL, comodato ou locação, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da FHSL, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da T.I. da FHSL, ou de quem este determinar. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da FHSL (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores e consequentemente o backup. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário. Documentos imprescindíveis para as atividades dos colaboradores da FHSL deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C: ou Área de Trabalho), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário. Os colaboradores da FHSL e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da ~~Gerência~~ Coordenação de T.I.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

• Todos os computadores de uso individual deverão ter senha de Administrador para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Coordenação de T.I. da FHSL, que terá acesso a elas para manutenção dos equipamentos.

• Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

• É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico indicado pela FHSL ou por terceiros devidamente contratados para o serviço.

• Todos os modems internos ou externos, roteadores e wifi devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

• O colaborador deverá manter a configuração do equipamento disponibilizado pela FHSL, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas, assumindo a responsabilidade como responsável das informações.

• Deverão permanecer não autenticados (logoff/logout) todos os softwares ou site que o colaborador não estiver utilizando no momento ou qualquer sistema após seu uso.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

• Todos os recursos tecnológicos adquiridos pela FHSL devem ter imediatamente suas senhas padrões (default) alteradas.

• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do FHSL.

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• Burlar quaisquer sistemas de segurança, acessar informações confidenciais sem explícita autorização do proprietário.

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

X. DISPOSITIVOS MÓVEIS

A FHSL pode permitir que usem equipamentos portáteis, com definição de mobilidade para fluxo de informações entre seus colaboradores. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da FHSL, ou aprovado e permitido pela Coordenação de T.I., como: notebooks, smartphones e pendrives etc. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A FHSL, na qualidade de proprietário, locatário ou comodatário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na FHSL. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos. O suporte técnico aos dispositivos móveis de propriedade da FHSL e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado por ela.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da FHSL. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da FHSL. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela FHSL constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela FHSL, notificar imediatamente seu gestor direto. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO). O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a FHSL e/ou a terceiros.

Todos os colaboradores independentemente do nível hierárquico ficam proibidos de utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da FHSL deverá submeter previamente tais equipamentos ao processo de autorização da Coordenação de T.I.

Equipamentos portáteis ou não, como smartphones, pen-drives, notebook de qualquer espécie, quando não fornecidos ao colaborador pela FHSL, não serão validados para uso e conexão em sua rede corporativa.

Em situações excepcionais a Coordenação de T.I. poderá homologar uso de equipamentos pessoais ou de terceiros provisoriamente, em rede segregada e sem acesso à rede corporativa da FHSL, tão somente para uso de internet, mas seguindo os mesmos termos desta PSI quanto auditoria e monitoramento.

XI. TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

A T.I., Departamento Jurídico e o RH, podem disponibilizar informativos educativos orientando a segurança da informação nos moldes da FHSL.

Treinamentos de especialização e cursos livres EAD podem ser direcionados pelo RH para aprimorar a qualificação profissional etc.

As orientações do DPO podem ser encaminhadas através de comunicados internos, esclarecendo sempre a importância de notificar as ocorrências encaminhando e-mails ao responsável como DPO da FHSL.

XII. SALA SERVIDORES

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

O acesso somente deverá ser feito por pessoa autorizada para troca de fitas de backup, suporte em eventuais problemas, no cabeamento de rede, switches, modens, servidores etc.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto inflamável.

A entrada ou retirada de quaisquer equipamentos somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

XIII. GERENCIAMENTO DE ATIVOS (inventário)

Todo gerenciamento do inventário deve ser implementado no controle OCS (Open Computer and Software) pela equipe de T.I. da FHSL. O gerenciamento é Web e o armazenamento é realizado banco de dados.

XIV. GERENCIAMENTO CHAMADOS SUPORTE TÉCNICO

A FHSL disponibiliza um Sistema de Chamados o qual permite registro do chamado técnico, bem como seu acompanhamento, o direcionamento do chamado será automatizado, as tarefas e logs podem ser auditadas. O gerenciamento é Web e o armazenamento é realizado banco de dados.

XV. BACKUP

Todos os backups devem ser realizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros. As mídias de backup (como LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em maleta apropriada) e distantes o máximo possível da Sala dos Servidores.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial. Mídias que apresentam erros devem primeiramente ser formatadas e testadas.

Caso o erro persista, deverão ser inutilizadas. É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup. As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da FHSL, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup. Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Administrador, nos termos do Procedimento de Controle de Backup e Restore.

XVI. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da FHSL, ou seja, qualquer incidente de segurança pode ser considerado como alguém agindo contra a ética e os bons costumes regidos pela FHSL.

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

GLOSSÁRIO

DPO – Data Protection Officer (responsável pela LGPD na FHSL)

LGPD – Lei Geral de Proteção de Dados

PSI – Política de Segurança da Informação

T.I. – Tecnologia da Informação

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

TERMO DE COMPROMISSO

Declaro que não há expectativa de privacidade com relação ao uso dos ativos e equipamentos da FHSL, tais quais, contas de e-mail, telefonia, ou qualquer outro recurso de propriedade da Fundação ou por ela locados ou adquiridos em comodato, devendo todos aqueles que os utilizarem estarem cientes de que todo o conteúdo trafegado, armazenado ou acessado, assim como a localização dos equipamentos, poderá ser monitorada a qualquer tempo.

Declaro que tenho pleno conhecimento da Política de Segurança da Informação da Fundação Hospital Santa Lydia, publicada e disponibilizada na eletronicamente na intranet.

Declaro estar ciente de que atos contrários à Política de Segurança da Informação poderão resultar na aplicação de medidas administrativas, inclusive na rescisão do contrato de trabalho ou de prestação de serviços, bem como na aplicação de medidas judiciais pertinentes.

Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência de meu vínculo contratual com a FUNDAÇÃO HOSPITAL SANTA LYDIA, mesmo após o seu encerramento.

Ribeirão Preto, _____ de _____ de _____.

DADOS DO COLABORADOR

Nome: _____

Nº de Matrícula: _____

DADOS DO PRESTADOR DE SERVIÇO/PARCEIRO

Nome da Empresa: _____

CNPJ: _____ E-mail: _____

Endereço Comercial: _____

Telefone Comercial: (___) _____-_____ Ramal: _____

Nome do gestor do contrato: _____

E-mail: _____

Unidade que irá prestar o serviço: _____

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01

TERMO DE CONFIDENCIALIDADE

Pelo presente termo, neste ato representada conforme seu contrato social ou pelo seu contrato de trabalho doravante denominada “OPERADOR”, a pessoal física e/ou jurídica assume o compromisso irrevogável e irretratável de manter o mais absoluto sigilo em relação a todas as informações que lhe forem disponibilizadas pela FUNDAÇÃO HOSPITAL SANTA LYDIA, sob qualquer forma, para o desenvolvimento dos serviços contratados ou na forma do seu contrato de trabalho.

As informações conferidas ao OPERADOR não poderão ser divulgadas, tampouco acessadas por pessoas não autorizadas, mesmo após finalizada a prestação de serviços ou contrato de trabalho.

O OPERADOR deverá indenizar a FUNDAÇÃO HOSPITAL SANTA LYDIA por perdas e danos sofridos em decorrência da falha de manutenção de sigilo por sua parte, bem como de qualquer pessoa à qual tenha dado devidamente ou indevidamente acesso às informações confidenciais e que falhou com a manutenção de sigilo dessas informações.

As informações disponibilizadas pela FUNDAÇÃO HOSPITAL SANTA LYDIA deverão ser restituídas imediatamente assim que requerido, juntamente com quaisquer cópias eventualmente realizadas por quaisquer meios.

Ribeirão Preto, _____ de _____ de _____.

DADOS DO COLABORADOR

Nome: _____

Nº de Matrícula: _____

DADOS DO PRESTADOR DE SERVIÇO/PARCEIRO

Nome da Empresa: _____

CNPJ: _____ E-mail: _____

Endereço Comercial: _____

Telefone Comercial: (___) _____-_____ Ramal: _____

Nome do gestor do contrato: _____

E-mail: _____

Unidade que irá prestar o serviço: _____

FUNDAÇÃO HOSPITAL SANTA LYDIA
Rua Tamandaré, 434 – CEP 14.085-070 - Campos Elíseos
Ribeirão Preto – S.P. – Tel.(16) 3605 4848
CNPJ-MF nº 13.370.183/0001-89 Inscr. Municipal nº 1499777/01