PSIDE

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO E DADOS ELETRÔNICOS

Com as adaptações a Lei Geral de
Proteção de Dados
LGPD 13.709/18

A Política de Segurança da Informação, também referida como PSIDE, é o documento que orienta e estabelece as diretrizes corporativas do Instituto Brasileiro de Terapias Holísticas – Instituto Brasileiro de Terapias Holísticas, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSIDE está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002/2005, reconhecida mundialmente como um código de pratica para a gestão da segurança da informação, bem como está de acordo com a lei geral de proteção de dados (LGPD) 13.709-18.

OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores, terceiros, clientes e fornecedores do Instituto Brasileiro de Terapias Holísticas seguirem padrões de comportamento relacionados à segurança da informação adequados as necessidades de negócio e de proteção legal da empresa 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 do Instituto Brasileiro de Terapias Holísticas quanto à:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-lá, 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.

APLICAÇÕES DA PSIDE

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço e terceiros e se aplicam à informação em qualquer meio ou suporte. Esta politica dá ciência a cada um de que os ambientes,

sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com previa informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSIDE e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerencia de IT e o DPO (Data Protection Officer) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSIDE

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo Instituto Brasileiro de Terapias Holísticas pertence à referida instituição. As exceções devem ser explicitas 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.

O Instituto Brasileiro de Terapias Holísticas, por meio da Gerencia de IT e DPO, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS DA PSIDE

Para a uniformidade da informação, a PSIDE deverá ser comunicada a todos os colaboradores e terceiros do Instituto Brasileiro de Terapias Holísticas a fim de que a política seja cumprida dentro e fora da empresa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança de dados e informação, doravante designado como Comitê de Segurança de dados e Informação.

Tanto a PSIDE quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança de dados e informação.

Deverá constar em todos os contratos do Instituto Brasileiro de Terapias Holísticas como anexo o Acordo de Confidencialidade ou Clausula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela Empresa.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores e terceiros. Todos os colaboradores e terceiros 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.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à gerencia direta, e esta deverá encaminhar posteriormente ao Comitê de Segurança da Informação para o dashboard de KPIs e ocorrências.

Um **plano de mitigação operacional** 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 e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo Instituto Brasileiro de Terapias Holísticas ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A Instituto Brasileiro de Terapias Holísticas exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSIDE será implementada no Instituto Brasileiro de Terapias Holísticas por meio de procedimentos específicos, obrigatórios para todos os colaboradores e terceiros, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSIDE e das Normas de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral e PJ (Pessoas Jurídicas)

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 instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao Instituto Brasileiro de Terapias Holísticas e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o PSIDE que está previsto no aceite contratual, concedido pelo Comitê de Segurança da Informação.

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 PSIDE do Instituto Brasileiro de Terapias Holísticas .

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do Instituto Brasileiro de Terapias Holísticas , e que toda informação sobre a

empresa não poderá ser divulgada sobre hipótese alguma, por cinco anos após o seu desligamento.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSIDE, é um requisito básico de suas funções como gestor da organização ou que exerça algum papel de responsabilidade e comando sobre outros colaboradores.

4 - Dos Custodiantes da Informação

4.1 - 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 (SLA) 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 PSIDE.

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, por exemplo, a manutenção de computadores, a realização de cópias de Segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e comerciais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou 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 (clientes), incluindo o ambiente de CRM (gestão de clientes) e operacional (ERP), 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 para o Instituto Brasileiro de Terapias Holísticas .
Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação (Gerente de IT interno ou externo) 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 pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, 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 (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa 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.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa, é uma atribuição especifica do gerente de IT (interno ou externo da empresa), que responderá diretamente ao Gerente Geral da Instituto Brasileiro de Terapias Holísticas .

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 empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os horários oficiais do Brasil.

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 do Instituto Brasileiro de Terapias Holísticas ;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Instituto Brasileiro de Terapias Holísticas ;
- incidentes de Segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante, e qualquer outro que possa ser identificado);
- 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);

4.2 - 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 do Instituto Brasileiro de Terapias Holísticas .

Publicar e promover as versões da PSIDE e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da Segurança da informação para o negócio do Instituto Brasileiro de Terapias Holísticas , mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de Segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o Instituto Brasileiro de Terapias Holísticas .

Buscar alinhamento com as diretrizes corporativas da instituição, em relação a temas de atualizações sobre a LGPD (Lei geral de Proteção de dados), e buscar junto ao DPO todas atualizações e comunicações em bases regulares sobre temas de segurança.

4.3 - Do Comitê de Dados e Segurança da Informação (CDSI)

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, e empresas terceiras que poderão atuar como (DPO – Data protection Officer) e outros nomeados pelos diretores, nomeados para participar do grupo pelo período de um ano, podendo ser renovados automaticamente pelo mesmo período.

Deverá o CDSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o Instituto Brasileiro de Terapias Holísticas . O CDSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico. Cabe

ao CDSI:

- propor investimentos relacionados à Segurança da informação com o objetivo de reduzir mais os riscos;

- propor alterações nas versões da PSIDE 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 PSIDE e/ou das Normas de Segurança da Informação complementares.
- Cumprimento das normas de segurança LGPD, e garantir o seu cumprimento, e avaliar os KPIs de segurança de dados.

5 – Do monitoramento e da auditoria de ambiente

Para garantir as regras mencionadas nesta PSIDE, o Instituto Brasileiro de Terapias Holísticas poderá:

- 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;
- tornar publicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- 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.

CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores do Instituto Brasileiro de Terapias Holísticas quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do Instituto Brasileiro de Terapias Holísticas é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais não é permitida.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do Instituto Brasileiro de Terapias Holísticas :

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;

- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Instituto Brasileiro de Terapias Holísticas 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;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do Instituto Brasileiro de Terapias Holísticas 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 do Instituto Brasileiro de Terapias Holísticas ;*
  - *contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;*
  - *contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à Segurança;*
  - *vise obter acesso não autorizado a outro computador, servidor ou rede;*
  - *vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;*
  - *vise burlar qualquer sistema de Segurança;*
  - *vise vigiar secretamente ou assediar outro usuário;*
  - *vise acessar informações confidenciais sem explícita autorização do proprietário;*
  - *vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;*
  - *contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet) tenha conteúdo considerado improprio, obsceno ou ilegal;*
  - *seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico;*
  - *contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;*
  - *tenha fins políticos de qualquer natureza (propaganda política);*
  - *inclua 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
- Gerência ou departamento

- Nome da empresa
- Telefone(s) (Celular e Telefone da central de atendimento)
- Endereço de e-mail
- Endereço da empresa (matriz)
- Logomarca da empresa

- Dados de proteção da informação sempre ao final da assinatura do e-mail como segue :

“ O conteúdo desta mensagem de e-mail e quaisquer anexos se destinam exclusivamente ao (s) destinatário (s) e podem conter informações confidenciais e / ou privilegiadas e podem ser legalmente protegidos contra divulgação. Se você não for o destinatário pretendido desta mensagem ou de seu agente, ou se esta mensagem foi endereçada a você por engano, por favor, avise imediatamente o remetente pelo e-mail de resposta e exclua esta mensagem e quaisquer anexos. Se você não é o destinatário pretendido, você está notificado que qualquer uso, disseminação, cópia ou armazenamento desta mensagem ou de seus anexos é estritamente proibido, nos termos da lei 13.709/18, podendo desta forma ser aplicadas as sansões dentro das circunstâncias penais e legais. “

INTERNET DENTRO DA REDE INTERNA

Todas as regras atuais do Instituto Brasileiro de Terapias Holísticas visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição 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, o Instituto Brasileiro de Terapias Holísticas , 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 empresa, 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.

A Instituto Brasileiro de Terapias Holísticas ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de Segurança, por qualquer colaborador, sem o devido 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 instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela empresa aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não infrinja normas de segurança.

Como é do interesse do Instituto Brasileiro de Terapias Holísticas que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores das áreas de marketing, copyrighting, influencers e vendas, podem falar em nome do Instituto Brasileiro de Terapias Holísticas para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, lives, e redes sociais (instagram, facebook, Linkedin, Twiter, Youtube e assim por diante), entre outros, as áreas adminsitrativas não estão autorizadas a publicar em redes sociais em nome da Instituto Brasileiro de Terapias Holísticas.

Apenas os colaboradores autorizados pela instituição 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, e Lei geral de Proteção de Dados (LGPD) 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, salas de bate- papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades da Instituto Brasileiro de Terapias Holísticas e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas,desde que autorizados pela gerência de IT.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de IT.

Os colaboradores não poderão em hipótese alguma utilizar os recursos do Instituto Brasileiro de Terapias Holísticas para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação brasileira.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de Segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao Instituto Brasileiro de Terapias Holísticas 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 do Instituto Brasileiro de Terapias Holísticas 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) serão permitidos desde que para fins profissionais. Os serviços de comunicação instantânea (WhatsApp, Google Chat, e demais chats corporativos) estão totalmente liberados desde que para uso corporativo. São proibidos os acessos a chats de bate papo, para fins não profissionais (BOL, UOL, AOL, etc...) onde caso seja detectado o uso indevido uma notificação será emitida ao CDSI, como alerta de segurança de dados.

Atualizações e uso do website da Instituto Brasileiro de Terapias Holísticas:

- O website da Instituto Brasileiro de Terapias Holísticas , com o URL Instituto Brasileiro de Terapias Holísticas deverá obedecer às politicas de segurança da informação e proteção de dados (LGPD), e deverá solicitar a cada usuário no momento do acesso, o aceite de Cookies (arquivo de rastreamento e controle de identificação de usuário no momento do acesso, identificando desta forma o IP, localização, e demais dados do usuário) neste caso o site deverá realizar a pergunta sobre o aceite ou não dos cookies de forma simples e fácil.

- O website da Instituto Brasileiro de Terapias Holísticas, também deverá contar uma política de privacidade, contendo de forma clara e objetiva, as políticas Instituto Brasileiro de Terapias Holísticas, e deverá ser de fácil acesso dentro do website.

IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Instituto Brasileiro de Terapias Holísticas e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. Todos os dispositivos de identificação utilizados no Instituto Brasileiro de Terapias Holísticas , como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a empresa, e legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas. O RH e Administração geral do Instituto Brasileiro de Terapias Holísticas são os responsáveis pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores. A Gerência de IT responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do **Procedimento para Gerenciamento de Contas de Grupos e Usuários**.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local ou na nuvem (em ambiente de rede ou webaplication), o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

COMPUTADORES E RECURSOS TECNOLÓGICOS

(Apenas aplicável a equipamentos da Instituto Brasileiro de Terapias Holísticas em poder de terceiros ou colaboradores).

Os equipamentos disponíveis aos colaboradores são de propriedade do Instituto Brasileiro de Terapias Holísticas , cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, 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 Gerência de IT do Instituto Brasileiro de Terapias Holísticas , ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de IT e/ou à Gerência Administrativa, ficando responsáveis jurídica e tecnicamente pelas ações realizadas. Todas os notebooks terão as suas saídas para armazenamento em dispositivos externos (PenDrive) bloqueadas. Para fins de segurança de Dados.

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 permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

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 do Instituto Brasileiro de Terapias Holísticas (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede (física ou nuvem), pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem a comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores do Instituto Brasileiro de Terapias Holísticas 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 de IT.

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

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de IT do Instituto Brasileiro de Terapias Holísticas , 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 da Gerência de Sistemas do Instituto Brasileiro de Terapias Holísticas ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos 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.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela empresa, seguindo os devidos controles de Segurança exigidos pela

Politica de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

- Todos os recursos tecnológicos adquiridos pelo Instituto Brasileiro de Terapias Holísticas 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 Instituto Brasileiro de Terapias Holísticas .
- 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, sexista, ou de cunho político ou qualquer outro que viole a legislação em vigor no pais, a moral, os bons costumes e a ordem pública.

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação brasileira.

DISPOSITIVOS MÓVEIS

(Apenas aplicável a equipamentos da Instituto Brasileiro de Terapias Holísticas em poder de terceiros ou colaboradores).

O Instituto Brasileiro de Terapias Holísticas deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores e terceiros. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido

por sua Gerência de IT, como: notebooks, smartphones. Todas os smartphones terão as suas saídas para armazenamento em dispositivos externos (PenDrive) bloqueadas. Para fins de segurança de Dados.

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.

O Instituto Brasileiro de Terapias Holísticas , na qualidade de proprietário 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 no Instituto Brasileiro de Terapias Holísticas , mesmo depois de terminado o vínculo contratual mantido com a instituição.

O backup dos dados armazenados em notebooks deverá ser realizado em drivers dentro da nuvem, em bases diárias por meio de webservices, determinados pelo gerente de IT da Instituto Brasileiro de Terapias Holísticas, nas políticas de backup da Instituto Brasileiro de Terapias Holísticas.

O suporte técnico aos dispositivos móveis de propriedade do Instituto Brasileiro de Terapias Holísticas e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.
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 Gerência de Sistemas.

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 Gerência de Sistemas do Senac São Paulo.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição 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 pelo Instituto Brasileiro de Terapias Holísticas, notificar imediatamente seu gestor direto e a Gerência de IT. 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 a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao Instituto Brasileiro de Terapias Holísticas e/ou a terceiros. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Instituto Brasileiro de Terapias Holísticas deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de TI.

Smart phone e Notebooks de qualquer espécie, quando não fornecidos ao colaborador pela empresa, não serão validados para uso e conexão em sua rede corporativa.

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 13.709-18

A Lei Geral de Proteção de Dados (Lei no 13.709/18) já está em vigor desde setembro de 2020, trazendo direitos aos proprietários de dados pessoais e deveres aos agentes de tratamento e provedores, sejam controladores ou operadores de dados tanto pessoais como corporativos. A ANPD Autoridade Nacional de Proteção de Dados, é a responsável pela regulamentação e aplicação desta lei com base no art. 5o, XIX, da LGPD.

Com regra geral a Instituto Brasileiro de Terapias Holísticas guardará todos os dados de clientes, fornecedores e demais pessoas físicas e jurídicas e condomínios por 5 anos.

1 Processos gerais internos

A empresa adotará processos internos rastreáveis, aplicados a todas as áreas com impacto direto na coleta, uso e manuseio de dados de terceiros – fornecedores, clientes e terceiros. Estes processos deverão ser de uso constante e deverão ser revistos em bases periódicas, e suas alterações deverão ser rastreáveis, com o objetivo de aprimorar os procedimentos visando resguardar os interesses internos da organização e da confidencialidade dos dados de clientes, fornecedores e terceiros.

Estes processos deverão ser mantidos em formatos de fluxo de dados, simplificando o processo de aprendizado e deixar claro todas as funções, responsabilidades e proporcionar ao leitor a facilidade de aprendizado.

A criação e alteração destes fluxos e processos internos são de responsabilidade do comitê (CDSI - COMITÊ DE DADOS E SEGURANÇA DA INFORMAÇÕES), todos os membros do comitê deverão aprovar, tanto a sua criação como as devidas alterações nestes fluxos, processos e procedimentos.

1.1 Coleta de dados de clientes, fornecedores e terceiros em geral

A coleta de informações pessoais precisa obedecer aos cinco princípios: finalidade, adequação, necessidade, transparência e auditoria.

Para os casos de clientes, estes darão o aceite por meio do contrato em artigo específico, ou por meio do termo de confidencialidade, o mesmo princípio dos clientes será aplicado para os fornecedores.

Para os casos de : Prospecção de clientes, cotação com fornecedores, e ou solicitação de dados de terceiros com objetivos comerciais, estes deverão assinar o TERMO DE COLETA DE DADOS, onde este deverão aprovar a empresa a utilizar e tratar estes dados, e deixá-los em confidencialidade por 5 anos, sem a exposição destes dados por meios eletrônicos ou físicos.

Todos estes formulários deverão ser assinados pelas partes e deverá ser arquivado eletronicamente por 5 anos.

1.2 Uso dos dados coletados

O uso dos dados coletados segue o padrão estabelecido na MATRIZ DE RESPONSABILIDADES INTERNAS. Estas informações dos formulários assinados pelas partes NÃO poderão sofrer alterações após a sua assinatura.

Os dados de terceiros poderão ser classificados pela empresa, e deverão ser classificados como confidenciais seguindo os processos internos de segurança de dados, ora já estabelecidos neste documento.

Os dados de terceiros deverão sofrer um processo de revisão anual, onde os dados mais antigos ou julgados pela alta administração como sem uso prático para o negócio deverão ser excluídos de forma definitiva, e para isto o TERMO DE DESCARTE DE DADOS, deverá ser preenchido e aprovados pelos membros do comitê CDSI, e este termo deverá ser devidamente arquivados.

Para cada informação CPF ou CNPJ deverá haver uma aprovação por meio do termo de confidencialidade.

1.3 Auditoria dos dados

O DPO em bases anuais deverá realizar uma auditoria completa nos processos internos, documentos, arquivos, e demais documentos, e emitir um relatório sobre a aderência da empresa em relação aos processos e politicas baseados neste documento.

Caso a empresa tenha acima de 3 (três) não conformidades (não conformidade, é diferença entre os processos e politicas e a realidade) todas as pessoas da empresa deverão passar por uma revisão de treinamento interno sobre as politicas (PSIDE POLÍTICA DA SEGURANÇA DA INFORMAÇÃO E DADOS ELETRÔNICOS) e um acompanhamento e uma revisão dos processos e uma nova auditoria no prazo de três meses após o treinamento, onde caso, a empresa ainda tenha 3 (três) não conformidades, as pessoas responsáveis deverão sofrer penalidades e uma revisão de conhecimento sobre PSIDE.

1.4 Treinamento

É mandatório uma revisão anual de treinamento para os funcionários determinados pelo Comitê (CDSI), em bases anuais, e de novos funcionários ou terceiros que tenham relação direta na obtenção de dados de terceiros, clientes e fornecedores. O DPO poderá nomear uma pessoa interna para a realização destes cursos, podendo ser da administração ou recursos humanos, por ele designada, onde esta pessoa passará por um treinamento completo envolvendo as seguintes grades:

- ABNT NBR ISO/IEC 27002/2005 (abrangências gerais)
- Lei 13.709-18
- Politicas internas da empresa PSIDE
- Métodos de didática
- Processos internos de segurança de dados e informações

2 Responsabilidades do DPO (Art 39 Lei 13.709-18)

2.1 O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados.

b) Controla a conformidade com o PSIDE, com outras disposições de proteção de dados com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização

e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Presta aconselhamento ao chefe do comitê proteção de dados e informações, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º;

d) Coopera com a autoridade de controle Brasileiro

e) Ponto de contato para a autoridade de controle sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2.2 No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Em síntese, o DPO está incumbido de:

i) treinar e orientar os funcionários da organização em sobre os requisitos de conformidade com PDIDE e LGPD;
ii) realizar avaliações e auditorias regulares para garantir a conformidade com o PSIDE e PLPD;

iii) servir como ponto de contato entre a empresa e a autoridade supervisora;
iv) manter registros das atividades de processamento de dados realizadas pela organização;
v) responder e informar os titulares de dados pessoais sobre como seus dados estão sendo usados e quais medidas de proteção implementadas pela organização e,
vi) assegurar que os pedidos de acesso ou cancelamento de dados feitos por titulares de dados pessoais, sejam atendidos ou respondidos, conforme necessário.

De outro lado, a LGPD traz no parágrafo 2º de seu artigo 41 as atribuições do encarregado:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
>
> § 2º As atividades do encarregado consistem em:

I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - Receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

3 Plano de Mitigação LGPD

O (DPO) agente de tratamento de dados pessoais em conjunto com o CDSI estabelecem um plano e processo de resposta a incidentes envolvendo dados pessoais. Um processo claro de como saber o que fazer e como agir diante de incidentes que comprometam dados pessoais é fundamental, até mesmo porque a LGPD estabelece em seu art. 48 que o Gerente geral e o DPO deverão comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, bem como nas redes de comunicação locais. Neste aspecto, cumpre destacar a Diretriz 6.13 da norma ISO 27701 que dispõe, dentre outros pontos que:

a) Convém que a empresa estabeleça responsabilidades e procedimentos para identificação e registro de violações de dados pessoais;

b) Procedimentos relativos à notificação para as partes envolvidas e autoridades, considerando a legislação;

c) Realize uma análise critica, como parte de um processo de gestão da segurança da informação, para avaliar se medidas foram tomadas adequadamente. Assim, a comunicação aos envolvidos e à Autoridade Nacional de Proteção de Dados (ANPD) deverá se dar nos moldes do art. 48 da LGPD e prever:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados,
- observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;
- os motivos da demora, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

DISPOSIÇÕES GERAIS

Este documento passa a entrar em vigor na data de sua assinatura, a ata de treinamento, com a assinatura de todos os participantes com o termo de compreensão e aceite deverão fazer parte integrante deste documento, e devidamente arquivado.

Este documento é a versão inicial, para as demais versões a anterior deverá ser guardada por 10 anos para fins de rastreabilidade e auditoria. Todas as páginas deverão ser rubricadas por todos.

A última página será guardada para as assinaturas de todos os envolvidos.

Florianópolis, 4 de Agosto de 2022

DPO Data protection Office – Responsável pela proteção de dados Gilberto Coutinho
CPF

Membros do comitê, que aprovam esta PSIDE POLÍTICA DA SEGURANÇA DA INFORMAÇÃO E DADOS ELETRÔNICOS:

Michael Mendonça Diretor
CPF xxxxxx

Raphael Mendonça Diretor
CPF xxxxxxx