1 OBJETIVO

Estabelecer diretrizes que permitam firmar padrões de comportamento relacionados à segurança da informação, adequados às necessidades da instituição e à proteção legal dos dados pessoais, além de nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento, em adequação à Lei Anticorrupção, à Lei Geral de Proteção de Dados (LGPD) e ao Código de Conduta Ética da IBASP Gestão em Saúde.

É responsabilidade de todos os integrantes, colaboradores, terceiros e parceiros conhecer, disseminar e cumprir todos os termos desta política.

A presente Política de Tecnologia da Informação tem como objetivos específicos:

a) Estabelecer diretrizes estratégicas e operacionais para a governança e o uso responsável dos recursos de tecnologia da informação (TI), promovendo a integridade, confidencialidade, disponibilidade e autenticidade das informações institucionais;

b) Normatizar o uso de sistemas, equipamentos, redes, serviços de conectividade e ferramentas digitais com vistas à proteção da infraestrutura tecnológica e à prevenção de incidentes de segurança;

c) Assegurar a conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a Lei Anticorrupção (Lei nº 12.846/2013), o Marco Civil da Internet (Lei nº 12.965/2014) e demais normativos aplicáveis às organizações do terceiro setor e aos serviços de saúde;

d) Promover a cultura de segurança da informação, por meio da conscientização, capacitação e monitoramento contínuo dos colaboradores, parceiros e usuários, reduzindo riscos cibernéticos e operacionais;

e) Integrar a Política de TI às demais políticas institucionais da IBASP, especialmente àquelas relacionadas à proteção de dados, compliance, governança, execução de projetos e comunicação organizacional;

f) Fortalecer o Programa de Integridade da instituição, garantindo rastreabilidade, ética digital, uso seguro de tecnologias e responsabilização por condutas inadequadas.

2 APLICAÇÃO

Esta Política compõe o Programa de Integridade da IBASP Gestão em Saúde, sendo aplicável a todos os integrantes, colaboradores, terceiros e parceiros, dirigentes e gestores, sendo extensivo, no que couber, a doadores e patrocinadores. Aplica-se a todos os setores, unidades, sistemas e usuários que utilizem, acessem ou administrem recursos de tecnologia da informação no âmbito da instituição, abrangendo:

a) Colaboradores próprios, terceirizados, estagiários, consultores, prestadores de serviço e quaisquer outras pessoas físicas ou jurídicas com acesso autorizado a dispositivos, sistemas ou redes da instituição;

b) Unidades administrativas e operacionais, incluindo o escritório central, unidades de saúde, centros de formação e quaisquer outros ambientes institucionais que utilizem infraestrutura tecnológica da IBASP;

c) Soluções tecnológicas adotadas ou desenvolvidas pela IBASP, tais como sistemas de gestão, plataformas de comunicação, aplicações corporativas, servidores, dispositivos móveis, redes internas, e serviços em nuvem;

d) Parceiros institucionais e fornecedores de tecnologia, nos contratos que envolvam coleta,

armazenamento, tratamento, compartilhamento ou análise de dados institucionais ou sensíveis, conforme obrigações previstas na legislação vigente e nas cláusulas contratuais.

A presente Política deve ser observada em todas as etapas de uso da tecnologia da informação, incluindo aquisição, implantação, manutenção, atualização, monitoramento, descarte e suporte, garantindo o alinhamento com os princípios de segurança, ética, legalidade e eficiência operacional da IBASP.

3 BASE LEGAL

Esta Política está fundamentada na legislação brasileira vigente e em normativos que regem a governança da tecnologia da informação, a proteção de dados pessoais e a segurança da informação, notadamente:

a) Lei nº 13.709/2018 – *Lei Geral de Proteção de Dados Pessoais (LGPD)*, que estabelece princípios, bases legais, direitos dos titulares e obrigações das organizações no tratamento de dados pessoais;

b) Lei nº 12.965/2014 – *Marco Civil da Internet*, que disciplina o uso da internet no Brasil, assegurando princípios como a proteção à privacidade, à neutralidade da rede e à segurança dos dados;

c) Lei nº 12.846/2013 – *Lei Anticorrupção*, que responsabiliza administrativamente e civilmente pessoas jurídicas por atos lesivos cometidos contra a administração pública, inclusive em meios digitais;

d) Decreto nº 10.046/2019 – que trata do compartilhamento de dados no setor público e estabelece diretrizes de interoperabilidade e governança de dados;

e) Decreto nº 10.332/2020 – que institui a Estratégia de Governo Digital 2020–2022, orientando a transformação digital dos serviços públicos com base em segurança e proteção de dados;

f) Normas técnicas da ABNT (Associação Brasileira de Normas Técnicas), especialmente as séries NBR ISO/IEC 27000 sobre gestão da segurança da informação, e ISO/IEC 20000 sobre gestão de serviços de TI;

g) Boas práticas de governança e gestão de TI, conforme os frameworks internacionalmente reconhecidos, como COBIT, ITIL, PMBOK e os Guias de Boas Práticas em Tecnologia da Informação do Tribunal de Contas da União (TCU);

h) Demais normativos internos da IBASP, incluindo a Política de Proteção de Dados, o Código de Conduta Ética e o Programa de Integridade Institucional.

4 DEFINIÇÕES

Para os fins desta Política, consideram-se as seguintes definições:

a) **Acesso Autenticado**: forma de controle que exige identificação segura do usuário (ex: login e senha) para acesso aos sistemas e redes da instituição;

b) **Backup**: cópia de segurança de dados armazenados com a finalidade de recuperação em caso de falhas, perdas ou danos;

c) **Dado Pessoal Sensível**: dado pessoal que revele origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde, vida sexual, dados genéticos ou biométricos;

d) **Dados Pessoais**: toda informação relacionada a pessoa natural identificada ou identificável, conforme definido na Lei Geral de Proteção de Dados (LGPD);

e) **Dispositivos Corporativos**: equipamentos fornecidos ou autorizados pela IBASP para fins institucionais, como computadores, notebooks, celulares, tablets, servidores, entre outros;

f) **Governança de TI**: estrutura de processos, políticas, responsabilidades e controles que asseguram que os recursos de tecnologia estejam alinhados às estratégias organizacionais e aos princípios de eficiência, risco e conformidade;

g) **Incidente de Segurança da Informação**: evento adverso, confirmado ou sob suspeita, relacionado à violação da política de segurança, que comprometa dados, sistemas ou infraestrutura de TI;

h) **Operador de Dados**: pessoa natural ou jurídica que realiza o tratamento de dados em nome do controlador;

i) **Segurança da Informação**: conjunto de ações e controles voltados a garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais e pessoais;

j) **Tecnologia da Informação (TI)**: conjunto de recursos tecnológicos e computacionais utilizados para armazenamento, processamento, transmissão, segurança e gestão de dados e informações, incluindo *hardware*, *software*, redes e sistemas integrados;

k) **Titular de Dados**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

l) **Tratamento de Dados**: toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, armazenamento, eliminação, avaliação, entre outras;

m) **Usuário de TI**: toda pessoa física ou jurídica que, de forma autorizada, utiliza recursos de tecnologia da informação da instituição, incluindo colaboradores, estagiários, prestadores de serviço e parceiros.

5 DIRETRIZES

No atendimento ao que é requerido pela LGPD e nesta Política, a IBASP Gestão em Saúde seguirá, em seus processos, as seguintes premissas:

a) Proteção às operações e atividades da instituição, buscando evitar e/ou minimizar incidentes e impactos que possam vir a causar danos ao relacionamento com colaboradores, fornecedores, clientes, doadores, patrocinadores, investidores e público, no que diz respeito à capacidade, continuidade e monitoramento de redes e processamento de responsabilidade da área de Tecnologia da Informação;

b) Gestão preventiva da área de Tecnologia da Informação (TI) da instituição, aculturando e capacitando as equipes, aprimorando os processos e metodologias de desenvolvimento de sistemas para torná-los mais ágeis e seguros;

c) Conformidade, confiabilidade e segurança da infraestrutura dos serviços prestados pela instituição, por meio de boas práticas, padrões internacionais e/ou certificações, realizando periodicamente o controle e acompanhamento das recomendações e exigências relativas à proteção de dados.

Esta Política está fundamentada em princípios de segurança, ética, legalidade, eficiência operacional e inovação, e deve orientar as ações de todos os usuários e gestores da área de TI, conforme as diretrizes a seguir:

5.1 Alinhamento Estratégico

As ações de TI devem estar alinhadas ao planejamento estratégico institucional, contribuindo para a eficiência organizacional, a inovação, a sustentabilidade digital e a melhoria contínua dos processos.

5.2 Segurança da Informação

Devem ser implementadas medidas técnicas e administrativas para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais. A proteção contra ameaças cibernéticas, perda de dados, acessos não autorizados e outros riscos tecnológicos deve ser tratada como prioridade permanente.

5.3 Controle e Proteção de Dados

O tratamento de dados pessoais e sensíveis deve seguir os princípios e fundamentos da Lei Geral de Proteção de Dados (LGPD), com respeito aos direitos dos titulares e às bases legais aplicáveis. Devem ser adotadas práticas de minimização de dados, acesso restrito por perfil, registro de consentimentos e políticas de retenção e descarte seguro.

Visando proteger os dados controlados ou operados, a IBASP Gestão em Saúde deverá:

a) Testar a eficácia dos controles utilizados na área de TI, e informar ao Comitê de Ética os riscos potenciais;

b) Disponibilizar equipamentos e sistemas aos integrantes, colaboradores, terceiros e parceiros, devidamente configurados e com os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política e pela Política de Proteção de Dados Pessoais;

c) Proteger de forma eficaz e permanente todos os dados e informações coletados e gerenciados pela instituição contra-ataques cibernéticos, além de garantir que todos os novos dados e informações que ingressem no ambiente de TI estejam protegidos de códigos maliciosos indesejados;

d) Definir as regras formais para instalação de software e hardware na rede corporativa, exigindo o seu cumprimento dentro da instituição;

e) Orientar e acompanhar a correta utilização e guarda de assinatura e certificados digitais;

f) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os dados e informações da instituição.

5.4 Acesso e Uso Responsável

O acesso aos sistemas e recursos de TI é pessoal, intransferível e restrito aos perfis autorizados. Cabe ao usuário zelar pela guarda de suas credenciais, utilizar os recursos de forma ética e comunicar incidentes de segurança.

O uso dos equipamentos e sistemas institucionais deve ocorrer exclusivamente para fins relacionados às atividades profissionais ou autorizadas, sendo vedada sua utilização para fins pessoais, ilícitos ou inadequados.

5.5 Infraestrutura Tecnológica

A aquisição, implantação, manutenção e descarte de equipamentos, softwares e sistemas deve ser feita de acordo com critérios técnicos, padrões de qualidade, sustentabilidade e compatibilidade com os objetivos institucionais.

Cabe ao setor de TI manter atualizados os inventários, licenças, contratos de suporte e planos de contingência da infraestrutura tecnológica.

5.6 Continuidade Operacional

Devem ser elaborados e atualizados os planos de contingência e recuperação de desastres, assegurando a continuidade dos serviços essenciais em situações críticas ou interrupções operacionais.

5.7 Capacitação e Conscientização

Todos os usuários de recursos de TI devem ser capacitados quanto às boas práticas de segurança digital, uso ético da tecnologia, proteção de dados e prevenção de incidentes.

A área de TI, em articulação com o setor de Recursos Humanos (RH) e o Núcleo de Educação Permanente e Humanização (NEPH), deverá promover ações contínuas de educação digital e sensibilização.

5.8 Monitoramento e Auditoria

Os sistemas e recursos tecnológicos serão objeto de monitoramento, auditoria e controle, visando identificar vulnerabilidades, rastrear incidentes, garantir conformidade e subsidiar decisões gerenciais.

5.9 Conformidade com Normas Internas e Externas

Todas as atividades de TI devem estar em conformidade com os normativos legais, contratuais e regulatórios aplicáveis, bem como com as demais políticas institucionais da IBASP.

5.10 Utilização da Internet

Todas as regras visam o desenvolvimento de um comportamento eminentemente ético e profissional também com relação ao 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 seja acessada, transmitida, recebida ou produzida na internet estará sujeita a auditoria, e quando for o caso, a divulgação para fins de transparência.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Proteção de Dados Pessoais.

Ao monitorar a rede interna, a instituição pretende garantir a integridade dos dados e programas utilizados, e qualquer tentativa de alteração dos parâmetros de segurança, por qualquer integrante, colaborador, terceiro ou parceiro sem a devida autorização, será considerada inadequada e os riscos relacionados serão informados ao Comitê de Ética para as devidas providências.

O uso de qualquer recurso para atividades ilícitas ou antiéticas poderá acarretar as ações administrativas e as penalidades previstas no Código de Conduta Ética da instituição, podendo ainda ensejar processos civil e criminal, sendo que nesses casos a IBASP Gestão em Saúde cooperará ativamente com as autoridades competentes.

5.11 Utilização do Correio Eletrônico institucional

É proibido aos integrantes e colaboradores o uso do correio eletrônico da IBASP Gestão em Saúde para:

a) Enviar mensagens em nome de outro usuário, ou utilizar endereço de correio eletrônico de outra pessoa, sem que haja autorização prévia;

b) Enviar mensagens por meios eletrônicos, cujo assunto ou teor torne seu remetente e/ou a instituição vulneráveis a ações civis ou criminais;

c) Divulgar informações, imagens, dados de sistemas e/ou documentos protegidos e confidencias, sem autorização expressa e formal concedida pela Diretoria Executiva;

d) Falsificar informações de endereçamento, adulterar títulos e mensagens para ocultar assuntos ou a identidade de remetentes e/ou destinatários, com o objetivo de dificultar investigações e/ou evitar as punições previstas;

e) Apagar ou ocultar mensagens de correio eletrônico, enviadas ou recebidas, durante a realização de investigações realizadas pela instituição ou por algum agente externo.

f) Produzir, transmitir e/ou divulgar mensagem que:

- Vise vigiar secretamente e/ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar de forma indevida, ou não autorizada, informações que possam causar prejuízos ou constrangimentos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal.

6 VIOLAÇÕES E PENALIDADES

Qualquer dirigente, colaborador, terceiro ou parceiro que viole disposições desta Política estará sujeito às sanções disciplinares previstas no Código de Ética e Conduta da IBASP Gestão em Saúde, listadas abaixo:

I. Advertência verbal;
II. Advertência por escrito;
III. Suspensão;
IV. Demissão sem justa causa;
V. Demissão por justa causa;
VI. Exclusão do fornecedor, parceiro ou agente intermediário da instituição;
VII. Ação judicial cabível.

7 RESPONSABILIDADES

Cabe aos dirigentes da IBASP Gestão em Saúde cumprir e fazer cumprir com todas as disposições desta política, e assegurar que todos os integrantes, colaboradores, terceiros e parceiros de seu relacionamento sejam informados sobre seu conteúdo e a importância de sua implementação.

A adesão é obrigatória para todos os envolvidos, e suas regras e diretrizes devem ser colocadas em prática de imediato.

A efetividade desta Política exige o envolvimento coordenado de todos os níveis hierárquicos, sendo as responsabilidades distribuídas da seguinte forma:

7.1 Diretoria Executiva

a) Assegurar integração desta Política ao modelo de governança institucional;

b) Garantir a destinação de recursos humanos, financeiros e tecnológicos para a manutenção e aprimoramento da infraestrutura de TI;

c) Promover o alinhamento entre a estratégia organizacional e a gestão de tecnologia da informação.

7.2 Setor de Tecnologia da Informação (TI)

a) Planejar, implantar, operar e manter os sistemas, redes, equipamentos e recursos de tecnologia da informação da instituição;

b) Estabelecer e monitorar controles de segurança da informação, incluindo *backups*, criptografia, controle de acessos e prevenção de incidentes;

c) Garantir a conformidade técnica com as legislações aplicáveis (LGPD, Marco Civil da Internet, entre outras);

d) Avaliar riscos tecnológicos e propor medidas de mitigação;

e) Apoiar tecnicamente os setores da organização na utilização adequada de ferramentas digitais;

f) Monitorar o uso dos recursos tecnológicos e emitir relatórios de conformidade, desempenho e segurança.

7.3 Encarregado de Dados (DPO – *Data Protection Officer*)

a) Atuar em conjunto com a área de TI para garantir o cumprimento das normas da LGPD no tratamento de dados pessoais;

b) Responder às solicitações dos titulares de dados e aos órgãos reguladores;

c) Promover ações de orientação, governança e comunicação sobre proteção de dados pessoais.

7.4 Setor de Recursos Humanos

a) Incluir, nos processos de admissão, integração e desligamento de colaboradores, as orientações relacionadas ao uso ético e responsável dos recursos de TI;

b) Colaborar na promoção de treinamentos sobre segurança da informação e cultura digital institucional.

7.5 Colaboradores, Prestadores de Serviço e Usuários de TI

a) Utilizar os sistemas, redes, equipamentos e credenciais de acesso com zelo, responsabilidade e exclusividade;

b) Manter confidencialidade sobre informações institucionais e dados pessoais acessados em suas atividades;

c) Comunicar imediatamente à área de TI qualquer incidente, falha, suspeita de invasão, perda de dados ou comportamento suspeito;

d) Cumprir integralmente as diretrizes estabelecidas nesta Política e nos demais normativos correlatos.

8 COMUNICAÇÃO

A IBASP Gestão em Saúde incentiva a todos que comuniquem imediatamente ao Comitê de Ética quando suspeitarem ou detectarem violações a esta Política ou as legislações correlatas, cuja análise e investigação serão tratadas confidencialmente. Não serão admitidas retaliações e intimidações aos denunciantes.

9 DOCUMENTOS DE REFERÊNCIA

I. Estatuto;

II. Código de Conduta Ética;

III. Política de Integridade (*Compliance*);

IV. Política de Controles Internos e Gestão de Riscos;

V. Política de Proteção de Dados;

VI. Política de Privacidade e Proteção de Dados Pessoais;

VII. Política de Comunicação;

VIII. Política de Execução de Projetos e Prestação de Contas.