POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

APAE ANÁPOLIS

2021

Sede à Rua Galileu Batista Arantes, n.º 296, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570
(62) 3098-2525 | apae@apaeaps.org.br

Vander Lúcio Barbosa da Silva
Presidente

Daise dos Santos Rodrigues Lourenço
1ª Diretora Secretária

Maria da Penha Lima
2ª Diretora Secretária

Argemiro Alves Ribeiro
1º Diretor Financeiro

João Amélio da Silva Júnior
Diretor Médico

Josafá Cândido de Sousa
Diretor de Patrimônio

Lauriton Gonçalves Holanda
Diretor Social

Conselho de Administração

Antenor Ribeiro Pantaleão
Ednaldo Pereira Braga
Hélia Maria da Costa Pietrobon
José Lúcio Borges
José Wanderlei Martins de Oliveira
Kleicivânia Augustinho Silva
Luiz Wilton Barros
Maria da Silva Cabral – *In Memorian*
Ovídio do Prado Neto
Vandir Estácio Maia
Wilson de Oliveira

Autodefensores

Ana Flávia da Silva Araújo
Marcus Divino Ferreira Campos

Equipe Elaboradora

Alcides Pereira da Mata Neto – Analista de Redes
Edilson Rezende Júnior – Assessor Jurídico
Helenjusse Macedo Machado da Silva – Gerente Administrativa e Financeira
Mirian Cleidiane Queiroz Cunha – Procuradora Jurídica
Nancy Ferreira Barbosa de Oliveira – Superintendente
Samuel da Costa Vicente – Analista de Sistemas

Sede à Rua Galileu Batista Arantes, n.º 296, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570
(62) 3098-2525 | apae@apaeaps.org.br

SUMÁRIO

Sede à Rua Galileu Batista Arantes, n.º 296, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570
(62) 3098-2525 | apae@apaeaps.org.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI DA APAE ANÁPOLIS

(Aprovado em reunião da Diretoria Executiva e Conselho de Administração do dia 13/07/2021)

CAPÍTULO I – DA APRESENTAÇÃO E OBJETIVOS

Art. 1º. A informação é um ativo de grande valor, e a **ASSOCIAÇÃO DE PAIS E AMIGOS DOS EXCEPCIONAIS DE ANÁPOLIS – APAE ANÁPOLIS**, buscando medidas efetivas para proteger-se de vulnerabilidades, riscos e ameaças adota uma política com procedimentos que visem garantir a segurança de todas as suas informações, sendo esta uma prioridade deste manual;

Art. 2º. Esta Política de Segurança da Informação – PSI, tem como um de seus pilares a Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709 de 14 de agosto de 2018), e terá por finalidade primordial assegurar que a Instituição APAE Anápolis esteja segura com relação aos seus dados, seja através dos negócios realizados junto a outras empresas, seja aqueles oriundos do atendimento aos pacientes e alunos, ou ainda outros que venham a integrar seus arquivos;

Art. 3º. A PSI se aplica a todos os funcionários que laborem na APAE Anápolis, inclusive temporários ou prestadores de serviços terceirizados, remunerados ou não, e se regerá pelos seguintes princípios básicos:
a) Confidencialidade: somente indivíduo devidamente autorizado poderá ter acesso a determinadas informações, sendo por ela responsável direto em caso de desvio, alteração ou perda, desde que comprovada sua culpabilidade;
b) Integridade: deve-se buscar que garantia de que a informação seja mantida em seu estado original, ou seja, alterações, supressões e adições às informações somente poderão ser realizadas caso haja autorização expressa do responsável indicado pela Instituição;
c) Disponibilidade: as informações devem estar sempre disponíveis para os indivíduos autorizados;
Parágrafo único – É vedado alocar pessoa que não seja diretamente contratada, mediante regime celetista pela Instituição, como sendo proprietária das informações;

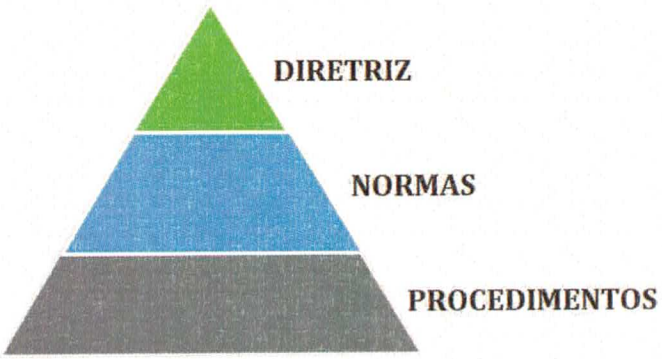
Art. 4º. É de responsabilidade direta do departamento de Tecnologia da Informação – TI gerenciar que os dados estejam protegidos contra roubos, fraudes, perdas, acidentes, vazamentos, bem como demais ameaças que possa identificar, devendo levar periodicamente ao conhecimento da Superintendência da Instituição as medidas que vêm sendo adotadas, bem como sugerir ações que possam aprimorar o controle, buscando sempre a proteção dos dados gerais;

Art. 5º. A Instituição buscará os meios adequados para proteger seus dados, agindo na estrutura organizacional, emitindo normas e procedimentos relacionados à segurança, aprimorando os controles e processos internos, e orientando os funcionários através de comunicados internos, assessoramento direto para que possam seguir padrões de comportamento seguro, e aplicação de medidas punitivas com igualdade e isonomia;

Art. 6º. O objetivo principal deste documento é reafirmar o compromisso da APAE Anápolis com as informações que trafegam em seus arquivos, estabelecendo diretrizes básicas para uma rotina interna segura e confiável com proteção dos ativos de informação e prevenção de responsabilidade para os usuários;

CAPÍTULO II – DA ESTRUTURA NORMATIVA DA SEGURANÇA

Art. 7º. Toda a estrutura normativa da PSI será baseada em três níveis hierárquicos, da seguinte forma:
a) 1º Nível – Política de Segurança da Informação (Diretriz): define a estrutura e obrigações referentes à segurança das informações. É a própria Política de Segurança da Informação – PSI;
b) 2º Nível – Normas de Segurança da Informação (Normas): estabelece as obrigações e procedimentos definidos de acordo com as diretrizes acima, devendo ser seguidas em diversas situações em que as informações serão tratadas;
c) 3º Nível – Procedimentos de Segurança da Informação (Procedimentos): instrumentaliza o disposto nos níveis supracitados, permitindo uma direta aplicação nas atividades da Instituição;



Art. 8º. A PSI e seus normativos devem ser divulgados a todos as pessoas que prestem serviços à Instituição, devendo ser dispostas de maneira clara e direta, podendo ser consultada a qualquer momento;

Art. 9º. Os procedimentos de segurança são previstos para setores específicos, de maneira distinta e direta, devendo ser divulgados aos setores pertinentes, com a devida orientação em caso de dúvida em sua aplicação;

Art. 10. Esta normativa geral deverá estar sempre à disposição no setor de Recursos Humanos da Instituição, devendo ser disponibilizada ainda aos colaboradores quando contratados, preferencialmente através do e-mail institucional, tendo o recebimento expresso do colaborador no ato de sua admissão, mediante **Termo de Responsabilidade**, juntamente com o Regimento Interno e outros documentos porventura existentes;

CAPÍTULO III – DAS ATRIBUIÇÕES E RESPONSABILIDADES

Art. 11. Caberá a todos os colaboradores (funcionários, estagiários, prestadores de serviços, profissionais cedidos por órgãos públicos, voluntários) da APAE Anápolis:
a) Cumprir fielmente todos os níveis hierárquicos citados nesta normativa, sendo incabível a alegação de desconhecimento;
b) Buscar orientação de seu superior hierárquico em caso de dúvidas e, caso persista a insegurança, comunicar-se diretamente com o departamento de Tecnologia da Informação – TI da Instituição;
c) Comunicar imediatamente seu superior hierárquico e o departamento de Tecnologia da Informação – TI em caso de identificação de infração às normativas internas de segurança das informações;

d) Assinar **Termo de Responsabilidade** acerca das normativas pertinentes a segurança dos dados da Instituição aos quais tenha acesso;
e) Proteger as informações da Instituição, agindo diretamente evitando acessos indevidos, modificações e destruições de dados;
f) Utilizar os recursos tecnológicos para preservação e promoção da Instituição;
g) Cuidar para que as propriedades intelectuais da Instituição estejam protegidas;
h) É da inteira responsabilidade de cada colaborador e afins todo prejuízo ou dano que vier a sofrer ou causar à Instituição ou a terceiros em decorrência da não obediência à diretriz, normas e procedimentos de segurança das informações;

Art. 12. Caberá à Diretoria Executiva da APAE Anápolis:
a) Aprovar e modificar a Política de Segurança da Informação – PSI da APAE Anápolis;
b) Instituir em ata de reunião os colaboradores responsáveis pela propriedade das informações;
c) Estabelecer as punições em razão de infração à PSI ou normativas derivadas, devendo ser levadas pela Procuradoria Jurídica da Instituição em reunião, com o assessoramento direto do departamento de Tecnologia da Informação – TI, com lavratura de ata;

Art. 13. São obrigações do departamento de Tecnologia da Informação – TI da APAE Anápolis:
a) Propor ajustes, projetos, melhorias, investimentos e modificações das normativas atinentes a segurança das informações da Instituição;
b) Propor as normas de segurança as quais serão aprovadas pela Diretoria Executiva;
c) Identificar os casos de violações ocorridas na segurança interna, encaminhando diretamente à Procuradoria Jurídica e Diretoria Executiva da APAE Anápolis;
d) Auxiliar no planejamento, indicação de recursos humanos e tecnológicos, alocação de recursos financeiros, inclusive apresentando orçamentos, para o aprimoramento constante da segurança das informações;
e) Emitir relatórios, levantamentos e análises;
f) Acompanhar o andamento dos projetos pertinentes à segurança das informações, comunicando à Superintendência;
g) Propor à Diretoria Executiva os nomes de colaboradores responsáveis pela propriedade das informações;
h) Divulgar a PSI e seus derivados a todos os colaboradores da Instituição;
i) Ser responsável pela orientação e treinamento de todos os setores acerca desta PSI e normativas afins;
j) Estabelecer procedimentos e realizar a gestão direta dos sistemas de controle de acesso da Instituição, incluindo concessões, manutenções, revisões de licença e suspensão ou interrupção de acessos;
k) Analisar a vulnerabilidade da Instituição, aferindo o nível de segurança dos sistemas contendo informações e ambientes de circulação de informações;
Parágrafo único – É de exclusividade do departamento de Tecnologia da Informação – TI, o acesso à sala do servidor da Instituição, ainda instalações utilizadas para armazenamento e tráfego de informações, salvo exceções autorizadas pela Superintendência;

Art. 14. São atribuições das gerências, gestores e coordenadores:
a) Ter postura exemplar em relação à segurança das informações, servindo como modelo de conduta não somente para suas equipes, mas também para toda a Instituição;
b) Fazer cumprir a PSI e suas derivações, garantindo que as equipes sob sua responsabilidade tenham acesso a toda a normativa;

Sede à Rua Galileu Batista Arantes, n.º 296, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570
(62) 3098-2525 | apae@apaeaps.org.br

c) Verificar se o colaborador, ou terceiro sob sua responsabilidade, assinou o **Termo de Responsabilidade** perante o setor de Recursos Humanos antes de conceder o acesso às informações;
d) Orientar os colaboradores, ou terceiros, informando que a confidencialidade se mantém mesmo após o desligamento ou finalização dos serviços perante a Instituição;
e) Comunicar imediatamente ao departamento de Tecnologia da Informação – TI sobre toda violação de segurança da informação, ou possível identificação de falha;

Art. 15. Compete ao setor de Recursos Humanos:
a) Colher a assinatura no **Termo de Responsabilidade** para todos os colaboradores (celetistas, estagiários, voluntários, terceiros, profissionais cedidos, ou qualquer outro que porventura preste serviço na Instituição), devendo fazê-lo no ato da contratação, antes que inicie os serviços;
b) Manter comunicação constante com o departamento de Tecnologia da Informação – TI acerca das movimentações (entradas, afastamentos, alterações de cargos, saídas e outros) de colaboradores, para atualização nos acessos a informação;

CAPÍTULO IV – DOS RISCOS IDENTIFICADOS

Art. 16. São fatores de riscos negativos:
a) Não cumprimento das atribuições e responsabilidades;
b) Falha no monitoramento da PSI e suas derivações;
c) Ausência de punição após constatação e apuração de infração cometida;
d) Descrédito dos colaboradores em relação à importância da segurança das informações;
e) Escassez de recursos humanos para monitoramento da execução da PSI;
f) Gastos financeiros para aprimoramento das tecnologias;
g) Falha na instrução aos colaboradores;

Art. 17. Buscando minorar os riscos citados, o departamento de Tecnologia da Informação – TI, deve cumprir as seguintes medidas práticas:
a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis, componentes de rede, podendo usar tais informações coletadas para identificar usuários, acessos realizados e ainda materiais manipulados;
b) Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria em caso de exigência judicial, solicitação da Superintendência ou Diretoria Executiva;
c) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e perímetros de acesso;
d) Realizar, a qualquer tempo, inspeção física nas máquinas;
e) Testar constantemente a eficácia dos controles utilizados, informando à Superintendência acerca dos riscos residuais;
f) Trabalhar em conjunto com os gestores e coordenadores organizando os níveis de acessos prestados, e eventuais procedimentos a serem adotados em caso de violação;
g) Configurar os equipamentos, ferramentas, sistemas e demais que são disponibilizados aos colaboradores, coordenando os controles necessários para cumprimento da PSI;
h) Administrar, proteger e testar as cópias de segurança dos programas e seus dados;

i) Sempre que ocorrer movimentação interna de dados, deve-se garantir que as informações não sejam retiradas de forma abrupta do usuário anterior, para que se possa rastrear os dados desde sua origem, e compará-los identificando onde houveram alterações;
j) Proteger continuamente todos os ativos de informação da Instituição contra códigos maliciosos;
k) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades nos ambientes da Instituição;
l) Definir as regras para instalações de hardware e software;
m) Informar previamente a Superintendência acerca do fim dos prazos de retenção de dados, buscando uma organização sob cronograma, para que os dados possam ser salvos ou alterados antes de seu descarte;
n) Realizar auditorias periódicas nos sistemas utilizados;
o) Manter constante auditoria e controle sobre as assinaturas e certificados digitais utilizados;
p) Realização e manutenção de backups constantes, bem como recuperação de dados;
q) Assegurar que os dados coletados de pacientes, usuários e alunos somente sejam utilizados para a finalidade que foi autorizada por estes, mediante **Termo de Consentimento;**

Art. 18. O departamento de Tecnologia da Informação – TI deverá monitorar o ambiente de segurança das informações com a geração constante dos seguintes relatórios:
a) Uso da capacidade instalada na rede e equipamentos;
b) Tempo de resposta no acesso à internet e aos sistemas críticos;
c) Períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
d) Incidentes de segurança identificados (vírus, furtos, acessos indevidos, inclusive tentativas, e outros);
e) Sites visitados por todos os colaboradores;
f) E-mails recebidos por todos os colaboradores, incluindo seus arquivos;
g) Downloads e uploads;

Art. 19. É primordial que o departamento de Tecnologia da Informação – TI, mantenha contato permanente junto ao setor de Recursos Humanos para que haja o bloqueio imediato de colaboradores desligados, prestadores de serviços com contratos finalizados ou rescindidos, ainda incidentes, investigações, e demais situações em que haja necessidade de salvaguardar dados e ativos da Instituição;

Art. 20. O departamento de Tecnologia da Informação – TI, deverá realizar atribuições a cada conta ou dispositivo de acesso aos computadores, sistemas, bases de dados ou qualquer outro ativo de informação a um responsável identificável (pessoa física), utilizando dados de identificação previstos legalmente;
a) Os usuários (logins) individuais dos funcionários serão de responsabilidade do próprio funcionário;
b) Os usuários (logins) de terceiros serão de responsabilidade do coordenador imediato que concedeu o acesso, devendo, portanto, supervisionar a utilização desses dados;

Art. 21. O departamento de Tecnologia da Informação – TI, em sendo o administrador de sistemas da Instituição, terá privilégio para acessar as informações pertinentes a todos os setores. Entretanto, deverá utilizar de forma responsável, buscando tal acesso somente nos casos em que for realizar a manutenção, realização de cópias de segurança, auditorias e testes em ambiente. A responsabilidade pelo setor de Tecnologia da Informação – TI será de atribuição direta de colaborador designado pela Superintendência juntamente com o Presidente, cabendo a este a supervisão de seus colaboradores imediatos;
Parágrafo único – O setor da Tecnologia da Informação deverá implantar controles que gerem registros auditáveis para retirada e transporte das informações (dados) sob custódia de seu departamento, buscando sempre identificar o responsável por seu acesso ou modificação;

CAPÍTULO V – DAS NORMAS GERAIS

Art. 22. É terminantemente proibida a transmissão às pessoas e/ou organizações alheias à Instituição, bem como divulgar, reproduzir, copiar, utilizar, explorar, por qualquer meio, os conhecimentos, dados e informações da APAE Anápolis, utilizáveis para execução do trabalho, sem a prévia autorização da Diretoria Executiva, com lavratura em ata de reunião, estendendo-se tal vedação além da relação empregatícia ou de contratação terceirizada, mesmo após sua finalização;

Art. 23. Todas as informações que tramitam na Instituição, seja pela rede, e-mails, sistemas e outros, são de propriedade da APAE Anápolis, e possuem caráter sigiloso, devendo ser manuseada somente por pessoas com acesso previamente concedido, a qual poderá ser responsabilizada por perda, extravio, furto, cópia, cessão e divulgação não autorizada, sendo vedado utilizar em ambiente estranho à Instituição;

Art. 24. É vedado adquirir, reproduzir, utilizar ou ceder cópias dos dados ou sistemas em nome da APAE Anápolis sem que haja autorização expressa da Diretoria Executiva, em ata de reunião;

Art. 25. Cada setor é responsável direto pelas suas informações e devida utilização;

Art. 26. É proibido divulgar, encaminhar ou armazenar em disco rígido e afins particulares os dados e informações de pacientes. Transmissão desses dados serão realizadas por departamento próprio, sob a supervisão do departamento de Tecnologia da Informação – TI, e Departamento Jurídico;

Art. 27. Todas as solicitações de criação de usuários, liberações e alterações de acessos, deverão ser encaminhadas pelo coordenador imediato, via e-mail, com cópia ao setor de Recursos Humanos, o qual, por sua vez indicará se o **Termo de Responsabilidade** foi assinado, para que haja a providência do departamento de Tecnologia da Informação – TI;

a) Mudanças na função dos colaboradores deverão ser informadas pelo setor de Recursos Humanos através de sistema próprio;

b) Na solicitação deverá constar o nome completo do usuário, número de matrícula, departamento e outras informações que julgar pertinentes para sua identificação;

c) Não poderão ser criados usuários genéricos ou fantasmas;

d) Os acessos serão concedidos conforme orientação do coordenador responsável da área requisitante;

e) Será criada uma senha padrão, devendo ser alterada no primeiro acesso do usuário;

Art. 28. O acesso à internet deverá ser realizado de forma ética, profissional e responsável, não sendo permitido o acesso a sites pornográficos, bate papo, jogos, ou outros que não sejam atinentes à atividade do colaborador ou seu desenvolvimento pessoal, e principalmente perigosas para a segurança dos dados da Instituição;

a) Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a auditoria;

b) É de responsabilidade pessoal do colaborador os acessos realizados em seu login;

c) Os acessos realizados pelo colaborador não serão confidencias, devendo, entretanto, serem repassados somente ao seu Coordenador imediato, setor de Recursos Humanos, Departamento Jurídico, Superintendência e Diretoria Executiva, evitando constrangimentos;

d) Os equipamentos, tecnologia e serviços ofertados para o acesso à internet são de propriedade da APAE Anápolis, podendo analisá-los e efetuar bloqueios;

e) Eventuais punições por acessos indevidos constarão no Regimento Interno da Instituição;

Art. 29. A Instituição disponibilizará correio eletrônico (e-mail) a todos os colaboradores, desde que contratados pelo regime celetista ou cedidos por órgãos públicos, ainda estagiários e voluntários, não sendo permitido a terceirizados;

a) A forma de cadastramento do e-mail será definida pelo departamento de Tecnologia da Informação – TI;

b) O e-mail deverá ser utilizado para fins profissionais, não sendo permitida a utilização pessoal;

c) Deverá ser usada uma linguagem cordial, clara e direta, evitando-se termos coloquiais;

d) É vedado alterar o cartão profissional, assinatura, e mensagem de confidencialidade, sendo permitido apenas ao departamento de Tecnologia da Informação – TI, juntamente com o setor de Recursos Humanos;

Parágrafo único – É terminantemente proibido apagar mensagens eletrônicas quando estiver em curso qualquer tipo de investigação na Instituição;

Art. 30. Não é permitido o envio de mensagem eletrônica (e-mail):

a) Que contenha informações estratégicas ou negociais da Instituição sem a prévia autorização da Diretoria Executiva e Superintendência, devendo esta última estar sempre alocada como destinatária da mensagem;

b) Com materiais que possam infringir direitos autorais ou de propriedade intelectual;

c) Que preveja informações prejudiciais a Instituição;

d) Com conteúdo impróprio, pornográfico, obsceno, vedado moralmente, situações vexatórias, ilegais, preconceituosas, constrangedoras e afins, e que possam assediar outros usuários;

e) Que faça parte de "correntes virtuais";

f) Com materiais particulares, não condizentes com o trabalho realizado;

g) Que contenha informações delicadas, contenciosas, que possam gerar discussões judiciais, implicações legais, exceto nos casos em que o departamento jurídico esteja envolvido, desde que restrito o trânsito da mensagem aos Gestores, Coordenadores, Departamento Jurídico, Superintendência e Diretoria Executiva da Instituição;

h) Que possa tornar o remetente ou qualquer colaborador vulnerável a ações civis ou criminais;

i) Que divulgue informações não autorizadas ou imagens de tela, sistemas, documentos e afins, sem autorização expressa concedida pelo coordenador, com cópia à Superintendência;

j) Com falsificações de endereçamento e adulteração de cabeçalhos;

k) Que vise acessar informações confidenciais sem autorização do responsável;

l) Que inclua mensagens criptografadas, códigos, ou outras formas mascaradas;

Parágrafo único – Quando houver o recebimento de mensagem indevida, deverá remeter imediatamente ao departamento de Tecnologia da Informação – TI;

Art. 31. As senhas de acesso são pessoais e intransferíveis, sendo de inteira responsabilidade do colaborador sua guarda;

a) Em havendo utilização de senhas ou dispositivos de outras pessoas poderá incorrer-se em crime de falsa identidade previsto no Art. 307 do Código Penal Brasileiro e punição administrativa pela Instituição;

b) O colaborador deverá realizar a alteração das senhas no mínimo a cada 90 (noventa) dias, exceto nos casos em que o sistema não o permita, podendo, entretanto, alterar em tempo menor, caso queira;

c) Orienta-se que a senha possua um certo nível de complexidade;

d) Caso sejam realizadas 03 (três) tentativas de acesso alocando a senha incorreta o acesso ficará bloqueado durante 05 (cinco) minutos, exceto nos casos de sistemas que não permitam tal opção;

Art. 32. É de responsabilidade exclusiva do departamento de Tecnologia da Informação – TI a aquisição, manejo, instalação e desinstalação dos softwares e hardwares utilizados na Instituição, devendo a alienação, doação, transferência ou descarte serem autorizados pela Superintendência;

Art. 33. Quando houver a digitalização de documentos físicos, deverá ser imediatamente retirado da área comum a todos os colaboradores e alocado em pasta própria do setor responsável;
Parágrafo único – Documentos digitalizados que permaneçam na área comum pelo prazo de 05 (cinco) dias, poderão ser descartados pelo departamento de Tecnologia da Informação – TI;

Art. 34. Sempre que um colaborador se ausentar de seu posto de trabalho deverá colocar o computador em modo repouso, para que seja necessário efetuar novo login. Ao fim do expediente, é obrigação do colaborador desligar o computador, evitando utilização desnecessária da máquina e gasto de energia elétrica;

Art. 35. Utilização de recursos internos, tais como celulares da Instituição, notebooks, impressoras, fax, equipamentos de wi-fi e outros, serão regularizados no Regimento Interno;

Art. 36. Meio particulares de arquivamento, tais como pendrive, HD externo e afins, não poderão ser utilizados na Instituição, salvo autorizados expressamente pela Superintendência;
Parágrafo único – Não será de responsabilidade da APAE Anápolis a utilização de equipamentos estranhos à Instituição trazidos diretamente pelos colaboradores para seu uso pessoal;

Art. 37. Deve ser evitado o uso excessivo do arquivamento eletrônico. Arquivos de música particulares, imagens particulares, vídeo aulas particulares, e similares, não poderão ser armazenados na rede da Instituição;

CAPÍTULO VI – DA POLÍTICA DE PRIVACIDADE VOLTADA A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Art. 38. A APAE Anápolis buscará todos os meios acessíveis para efetivar a privacidade e segurança dos dados coletados de seus usuários, seja colaboradores, pacientes e alunos, prezando pelo cumprimento da Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709/2018), e demais normas pertinentes ao tema;

Art. 39. Para que haja a publicação de qualquer dado de usuário deverá haver o prévio consentimento, expresso, indicando qual o modo de publicação, tempo, público alvo e outras finalidades afins. Caso não haja tal autorização, fica vedada a exposição;

Art. 40. Entende-se por tratamento de dados toda e qualquer atividade que utilize um dado pessoal de determinado indivíduo na execução das operações da Instituição, tais como coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, sendo executado pelo Controlador, Encarregado e Operadores;
a) O Controlador é a própria Instituição APAE Anápolis, representada por sua Diretoria Executiva, a quem compete as decisões referentes ao tratamento dos dados pessoais, inclusive nomear o Encarregado e destacar Operadores;
b) O Encarregado deverá possuir conhecimento da LGPD, sendo preferencial a nomeação de colaborador do departamento de Tecnologia da Informação – TI, e será responsável por intermediar as relações entre as partes detentoras dos dados (usuários), e os agentes de tratamento (Operadores), devendo monitorar as atividades de tratamento de dados da Instituição, garantindo que estejam em conformidade com a LGPD e boas práticas de segurança;

c) Os Operadores serão todas as pessoas que, pelo trabalho que executam na Instituição, tenham acesso aos dados dos usuários, sendo responsáveis por realizar o tratamento segundo as orientações fornecidas pelo Controlador e pelo Encarregado, e aquela prevista na legislação atinente ao tema;

Art. 41. Deverão os Operadores agirem com diligência, segurança, transparência, responsabilidade e discrição, a fim de evitarem erros ou falhas que possam acarretar na indevida publicação de dados dos usuários, devendo ainda reportar diretamente aos seus superiores hierárquicos sobre toda e eventual intercorrência que porventura possa ocorrer;

Art. 42. É primordial que haja um treinamento constante, e orientação específica para os Operadores, tendo em vista que são eles os responsáveis diretos pelo tratamento e manuseio, dos dados coletados, e possíveis vazamentos incidirão na responsabilidade solidária da própria Instituição;

Art. 43. Excetuados os casos de dados de colaboradores, a Instituição coleta ou obtém os seguintes dados:
a) No caso de pacientes: nome completo, nome dos pais, números de RG, CPF, Cartão SUS, prontuários médicos, resultados de exames, telefone e endereço completo;
b) No caso de alunos: nome completo, nome dos pais, números de RG, CPF, Cartão SUS, telefone e endereço completo;
Parágrafo único – O uso de dados de colaboradores para questões empregatícias não exige o consentimento previsto na Lei Geral de Proteção de Dados – LGPD;

Art. 44. Os dados são coletados no ato do atendimento ou matrícula, momento no qual ocorre o consentimento da parte, devendo ser atualizados à medida que forem alterados. Deverá a APAE Anápolis disponibilizar **Termo de Consentimento**, o qual será assinado pela parte, ou seu representante legal, dando o expresso consentimento para tratamento dos dados informados;
a) Os dados somente poderão ser coletados, tratados e armazenados mediante prévio e expresso consentimento da parte ou seu representante legal;
b) A qualquer momento a parte ou seu representante legal poderão solicitar a revogação do **Termo de Consentimento**, sem que possa ocorrer qualquer empecilho da Instituição acerca de tal vontade;

Art. 45. Nos termos do Art. 18 da Lei Geral de Proteção de Dados – LGPD, são assegurados os seguintes direitos às partes detentoras dos dados pessoais:
a) Confirmar a existência de tratamento de seus dados, de forma simplificada, clara e completa;
b) Acessar seus dados informados à Instituição, em relatório físico ou eletrônico, seguro e idôneo;
c) Solicitar a correção, alteração, edição ou atualização de seus dados;
d) Rever o consentimento dado, podendo revogá-lo, mudá-lo total ou parcialmente;
e) Limitar os dados informados quando julgar desnecessários, excessivos, ou tratados em desconformidade com a legislação através de anonimato, bloqueio ou eliminação;
f) Solicitar a portabilidade de seus dados através de relatório cadastral;
g) Eliminar seus dados tratados a partir de seu consentimento, exceto nos casos previstos em lei;
h) Ser orientado acerca da impossibilidade de não fornecimento do consentimento e consequências deste ato, inclusive negativa de atendimento pela Instituição;

Art. 46. As partes proprietárias dos dados poderão exercer seus direitos de titulares, ou responsáveis legais, acessando diretamente a Instituição através do atendimento presencial na sede localizada na Rua Galileu Batista Arantes, n.º 350, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570, ou ainda pelos e-mails tecnologia@apaeaps.org.br e juridico@apaeaps.org.br, estando sujeita a identificação;

Art. 47. Os dados coletados ficarão armazenados seguindo os prazos previstos na legislação específica. O término do tratamento dos dados pessoais e sua consequente eliminação do banco de dados da Instituição ocorrerá quando:
a) A finalidade para o qual foi coletado tiver sido alcançada, ou não sendo mais necessários para aquela ação contratada;
b) Ocorrer a revogação do consentimento;
c) Nos casos de prontuários médicos, pelo prazo de 20 (vinte) anos contados do último registro realizado;

Art. 48. Após o término do vínculo empregatício devem ser excluídos todos os dados pessoais que não sejam obrigatórios, evitando falhas ou vazamentos;

Art. 49. São hipóteses de manutenção dos dados:
a) Para cumprimento de obrigação legal ou regulatória, sendo conservados apenas os dados atinentes ao cumprimento previsto, sendo excluídos os demais desnecessários;
b) Para fins de estudo ou pesquisa, desde que resguardado o anonimato;
c) Transferência a terceiro, desde que respeitados os requisitos de tratamento previstos legalmente;
d) Uso exclusivo do controlador, vedando o acesso a terceiros, respeitado o anonimato da parte;

Art. 50. Para uma manutenção segura das informações, devem ser utilizados os meios físicos, eletrônicos e gerenciais, com a devida orientação de proteção da privacidade;
a) Apenas pessoas autorizadas pela Diretoria Executiva poderão ter acesso aos dados coletados;
b) Os dados devem ser armazenados em ambiente seguro e idôneo;

Art. 51. A APAE Anápolis deverá adotar as melhores práticas para evitar incidentes de segurança. Como nenhuma página virtual é considerada totalmente segura e livre de riscos, mesmo apesar dos protocolos de segurança, ataques cibernéticos, hackers e problemas de culpa exclusiva de terceiros podem gerar riscos ou danos à Instituição e seus usuários, devendo o Encarregado comunicar a Autoridade Nacional de Proteção de Dados acerca de eventuais incidentes que venham a ocorrer;

Art. 52. Os dados coletados não poderão ser compartilhados com nenhum terceiro não autorizado pela Diretoria Executiva, assessorada pelo Departamento Jurídico da Instituição;
a) Parceiros comerciais, tais como laboratórios, receberão apenas os dados necessários para a execução do serviço contratado, devendo haver previsão contratual acerca das responsabilidades de segurança nos dados informados;
b) Os dados poderão ser informados a terceiros quando houver determinação judicial, ou outros casos legalmente previstos;

CAPÍTULO VII – DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 53. Esta Política de Segurança da Informação – PSI se aplica a toda a Instituição APAE Anápolis, aí incluídos seus colaboradores, terceirizados, voluntários, estagiários, e ainda usuários;

Art. 54. Eventuais dúvidas ou omissões porventura oriundas deverão ser dirimidas pela Diretoria Executiva em reunião, com lavratura de ata;

Art. 55. Este normativo entra em vigor na data de sua publicação, podendo ser revisto a qualquer momento, buscando a devida adequação a legislação aplicada.

Vander Lúcio Barbosa da Silva
Presidente

Sede à Rua Galileu Batista Arantes, n.º 296, Setor Bougainville, Anápolis – GO, CEP n.º 75.075-570
(62) 3098-2525 | apae@apaeaps.org.br