APAS Andradina	REGIMENTO DO COMITÊ DE PROTEÇÃO DE DADOS

Da Natureza

Art. 1º O presente regimento interno cria estabelece o Comitê de Proteção de Dados (CPD) da **Associação Policial de Assistência à Saúde – Apas Andradina**, define sua estrutura corporativa e regula suas atividades e atribuições com o objetivo de com o propósito reduzir a probabilidade da ocorrência de incidentes que possam afetar a integridade, disponibilidade e segurança das informações corporativas e dos individuos que estão sob sua guarda, bem como minimizar qualquer impacto referente à ocorrência de incidentes desta natureza.

Capítulo I Da Aplicação

Art. 2º Este regimento aplica-se aos membros integrantes do CPD.

Capítulo II Das Siglas e Definições

Art. 3º São utilizadas as seguintes siglas no texto deste regimento.

Sigla ou Termo	Definição
CPD	Comitê de Proteção de Dados
NSI	Núcleo de Segurança da Informação
LGPD	Lei Geral de Proteção de Dados
EMPRESA	Refere-se à **EMPRESA** Associação Policial de Assistência à Saúde
DPO	Encarregado de proteção de dados da **EMPRESA**
TI	Tecnologia da Informação

Capítulo III Dos objetivos do CPD

Art. 4º Constitui objetivos especificos do CPD:

I. Elaborar e manter atualizada a política de proteção e dados e segurança da informação.

II. Melhorar continuamente a gestão de segurança da informação da **EMPRESA**.

III. Tratar incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

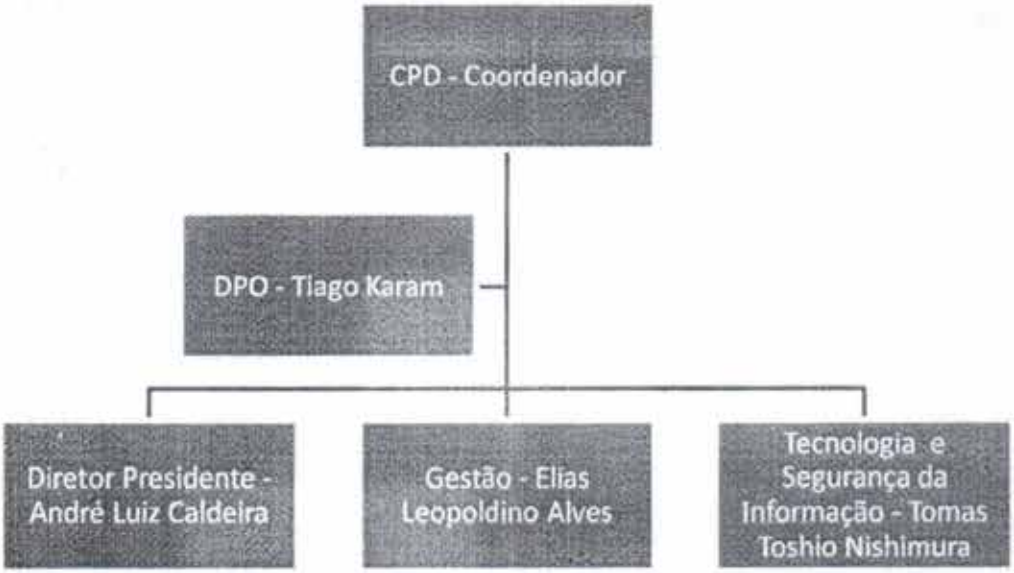
IV. Estabelecer contatos com autoridades, organismos reguladores e entidades técnicas especializadas sempre que necessário para tratamento rápido de incidentes graves de segurança.

V. Garantir que os processos de gestão de crise estejam estabelecidos e atualizados para pô-los em prática quando necessário.

Capítulo IV Dos membros participantes do CPD

Art. 5º O CPD é um colegiado de profissionais de diferentes áreas organizacionais com a seguinte estrutura organizacional:

Capítulo V Das responsabilidades e atribuições dos membros participantes do CPD



Art. 6º O membro **Coordenador do CPD** tem por responsabilidade manter atuante o CPD conforme este regimento. Ele será indicado pelos integrantes do comitê, de acordo com o perfil profissional dos participantes, e não terá poder hierárquico sobre os demais membros que se mantém reportando-se à sua estrutura funcional.

Art. 7º O membro **DPO** refere-se ao encarregado de proteção de dados que foi nomeado pela organização e tem por responsabilidades perante o CPD:

I. Manter o CPD informado sobre as mudanças e exigências estabelecidas pela LGPD e outras leis pertinentes.

II. Informar ao CPD sobre a estratégia e andamento das ações de combate aos riscos de segurança da informação.

III. Garantir que as políticas de proteção de dados e suas normas complementares estejam devidamente descritas e em conformidade legal.

IV. Assegurar que os termos de privacidade e proteção de dados pessoais estejam devidamente implantados em todos os canais de coleta e uso de dados pessoais da **EMPRESA**.

V. Conscientizar e treinar colaboradores e contratados da **EMPRESA** a respeito das práticas a serem adotadas em relação à proteção de dados pessoais através de cursos, palestras e material educativo.

VI. Receber, tratar e responder solicitações de informações, reclamações ou queixas sobre incidentes relativos ao tratamento de dados pessoais ou comunicações advindas de titulares de dados ou seus representantes legais, controladores ou operadores de tratamento de dados e autoridades estabelecidas para a proteção de dados pessoais e adotar as providências cabíveis.

VII. Monitorar o cumprimento dos prazos legais para o atendimento de consultas sobre tratamento de dados pessoais feitas por titulares.

VIII. Avaliar as atividades de tratamento de dados pessoais da **EMPRESA** sob a luz da LGPD.

IX. Organizar, prestar suporte e atuar na avaliação de impacto de proteção de dados dos produtos e serviços oferecidos pela **EMPRESA** em sua concepção e manutenção.

X. Acompanhar o andamento dos planos de ação e projetos que tratam os riscos de proteção de dados que foram levantados em decorrência da avaliação de impacto sobre a proteção de dados pessoais.

XI. Garantir, através de auditorias regulares, o registro atualizado das operações de tratamento de dados.

XII. Suportar as áreas técnicas de segurança da informação com requisitos que devam ser cumpridos em seus processos para garantir a conformidade legal da proteção de dados.

Art. 8º O membro **Núcleo de Segurança da Informação – NSI** refere-se ao setor, departamento ou apenas o profissional responsável por implantar e controlar os mecanismos de segurança estabelecidos pelo CPD. Sua linha de report deve estar definida no organograma da **EMPRESA** de forma que ele fique independente das equipes de desenvolvimento e infraestrutura de TI visando ter autonomia de auditoria quanto às melhores práticas de segurança da informação. São suas responsabilidades:

I. Proteger a informação e os recursos computacionais contra incidentes de origem interna ou externa que ponham em risco a organização.

II. Cumprir e fazer cumprir as definições desta política, mantendo o CPD informado sobre qualquer vulnerabilidade ou incidente que justifique ação deste colegiado.

III. Definir procedimentos específicos que complementam a Política de Proteção de Dados.

IV. Avaliar e auditar sistemática e rotineiramente todos os processos de TI sob a luz dos procedimentos e melhores práticas de segurança, mantendo um processo de avaliação de riscos de segurança, determinando sua grandeza, probabilidade e impactos nos negócios.

V. Prover o CPD com informações e dados técnicos necessários a tornar a aplicação desta norma eficaz e eficiente.

VI. Prover análise investigativa sempre que houver qualquer incidente, denúncia ou indicação de vulnerabilidades de segurança.

VII. Estabelecer medidas complementares de segurança sempre que um incidente vier a ocorrer.

VIII. Avaliar sob o aspecto da segurança todo e qualquer novo recurso computacional que venha a ser incorporado ao parque de informática.

IX. Prevenir o acesso físico e lógico indevido a qualquer informação ou recurso computacional.

X. Propor a contratação, sempre que necessário, de trabalho técnico especializado que mantenha a informação adequadamente protegida.

Art. 9º O membro **Setor de Tecnologia da Informação – TI** refere-se à liderança de TI da **EMPRESA**. Suas responsabilidades são:

I. Coordenar, implantar e suportar software, hardware e processos definidos pelo NSI que atinjam os objetivos desta política.

II. Comunicar o NSI sobre qualquer incidente ou processo relacionado à segurança da informação.

III. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

IV. Garantir a disponibilidade, segurança, desempenho e contingências dos sistemas implantados.

V. Garantir que os sistemas contratados estejam em conformidade com a LGPD, identificando vulnerabilidades e priorizando ações de melhorias visando torná-los aderente a esta política.

VI. Garantir que todos os dados armazenados em servidores de rede estejam cobertos por procedimentos de segurança e backup.

VII. Garantir que todos os backups de dados estejam devidamente executados e com certeza de recuperação se necessário.

VIII. Auxiliar o CPD na elaboração das normas de procedimentos que complementam esta política.

Art. 10º Os demais membros do CPD (Jurídico, Comunicação e Marketing, Diretoria, RH) devem atuar esclarecendo questões relativas à LGPD conforme sua área de atuação e conhecimento bem como contribuindo de forma a enriquecer o programa de proteção de dados da **EMPRESA**.

Capítulo VI Das reuniões do CPD

Art. 11º O CPD deverá reunir-se ordinariamente no mínimo 1 vez por trimestre, ou extraordinariamente quando algum assunto exigir, com pauta pré-estabelecida, com um quórum mínimo de 3 participantes, cobrindo pelo menos os seguintes temas:

I. Acompanhamento operacional: Avaliar os seguintes indicadores: colaboradores treinados, incidentes de segurança registrados, indisponibilidade de serviços causados por problemas relativos à segurança;

II. Informação sobre novos projetos em desenvolvimento e a abordagem de privacidade adotada;

III. Monitoramento da evolução da gestão de riscos de privacidade decorrente da sustentação da LGPD implantada;

IV. Acompanhamento do número de manifestações realizados através do canal DPO;

V. Mudanças ou adaptações necessárias à LGPD implantada;

VI. Casos de gravidade maior que mereçam destaque.

Capítulo VII Da confidencialidade dos assuntos tratados

Art. 12º Toda informação, seja de forma escrita ou falada, revelada, transmitida, tratada e/ou discutida pelo CPD é considerada confidencial e restrita, sendo vetada a sua propagação sem a devida autorização em ambientes externos.

Capítulo VIII Da Aprovação deste regimento

Art. 13º A elaboração e revisão deste regimento são de responsabilidade do CPD e sua aprovação do Diretor Presidente da **EMPRESA**.

Art. 14º Este regimento deverá ser revisado no máximo com periodicidade anual ou a critério do CPD quando assim for necessário.

Capítulo IX Do Histórico de revisões

Revisão	Data	Elaborado/Revisado por:	Descrição da Alteração
00	08/10/2021	CPD	Criação do documento
01	01/06/2023	Edmar Primio	Substituição do DPO
02	21/12/2023	Tiago Karam	Substituição do DPO

Andradina, 21 de dezembro de 2023.

Aprovo o Regimento do Comitê de Proteção de Dados e autorizo as ações de processo que sejam necessárias à sua conformidade.

André Luiz Caldeira
Diretor Presidente

ANEXO I – TERMO DE NOMEAÇÃO DO COMITÊ DE PROTEÇÃO DE DADOS

Pelo presente termo de nomeação e a partir da presente data está instituído o COMITÊ DE PROTEÇÃO DE DADOS da Associação Policial de Assistência à Saúde com seus respectivos membros.

Para uma melhor execução desta função e respectivas obrigações, o comitê ora nomeado, deve se reportar diretamente ao Diretor Presidente.

O COMITÊ DE PROTEÇÃO DE DADOS tem a função de conduzir a efetivação do projeto de implementação da conformidade LGPD, realizando levantamentos, registros, reuniões de alinhamento, treinamento e monitoramento de ações relacionadas à proteção e privacidade de dados.

Membros nomeados:

Nome	Função	Departamento	Assinatura
Tiago Karam	DPO	Terceiro	
André Luiz Caldeira	Diretor Presidente	Diretoria	
Elias Leopoldino Alves	Gestor	Administração	
Tomas Toshio Nishimura	Tecnologia e Segurança da Informação	Administração	