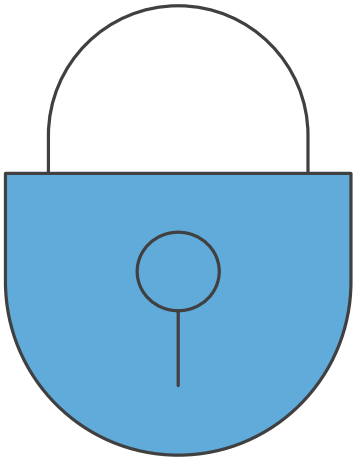
POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS LOCAL

P P D P L

2021

SUAPE

SUMÁRIO



Capítulo I

DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Proteção de Dados Pessoais Local (PPDPL) tem por finalidade estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a proteção dos dados pessoais aos planos estratégicos, programas, projetos e processos da empresa Suape e será composta pelo disposto neste documento, bem como pelo plano de ação proposto pela Comissão de Trabalho da Lei Geral de Proteção de Dados (LGPD).

Art. 2º A PPDPL e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se a todos os setores da empresa, abrangendo os servidores, prestadores de serviços, colaboradores, estagiários, jovem aprendiz, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais, estendendo-se para aqueles que realizam tratamento de dado pessoal em nome da estatal.

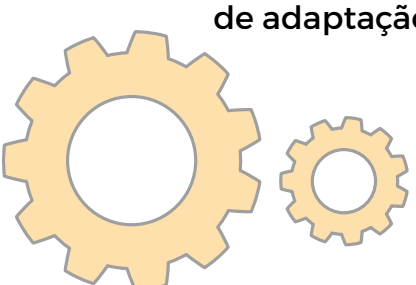
Capítulo II

DOS PRINCÍPIOS E OBJETIVOS

Art. 3º As atividades de proteção de dados pessoais no âmbito da empresa, bem como seus instrumentos resultantes, devem se guiar pelos seguintes princípios, além dos previstos no Decreto Estadual nº 49.265, de 6 de agosto de 2020:

I - Aderência à integridade e aos valores éticos no tratamento de dados pessoais;

II - Adequado suporte de tecnologia da informação para apoiar os processos de adaptação dos tratamentos de dados pessoais;



III - Disseminação de informações necessárias ao fortalecimento da cultura do tratamento de dados pessoais em respeitos à Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

IV - Realização de avaliações periódicas internas para verificar a eficácia da proteção de dados pessoais, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive à alta administração;

V - Estruturação do conhecimento e das atividades em metodologias, normas, manuais e procedimentos;

VI - Aderência dos métodos e modelos de tratamento de dados às exigências regulatórias da LGPD.

Art. 4º A PPDPL tem por objetivos:

I - Proporcionar adequação das atividades desenvolvidas pela empresa Suape à LGPD e regulamentos emitidos pela ANPD, em consonância com atingimento dos objetivos estratégicos;

II - Produzir informações íntegras, confiáveis e completas das demandas dos titulares do dado;

III - Salvaguardar o direito à proteção dos dados pessoais dos titulares;

IV - Possibilitar a adequada apuração dos responsáveis, em todos os níveis, que tenham acesso impróprio aos dados pessoais, em especial, aqueles considerados sensíveis, considerando o disposto no Código de Ética e Conduta de Suape, bem como no Programa de Integridade de Suape e demais Políticas Internas relacionadas e a Lei Estadual nº 6.123, de 20 de julho de 1968 (Estatuto do Servidor Público Estadual);

V- Reduzir os riscos relacionados a incidentes envolvendo dados pessoais, com a implantação de medidas de controle de segurança da informação;

VI - Orientar e servir de diretriz para os agentes de tratamento.

Capítulo III

DAS DIRETRIZES

Art. 5º São diretrizes da PPDPL:

I - A gestão da integridade com a promoção da cultura ética focada na preservação da privacidade;

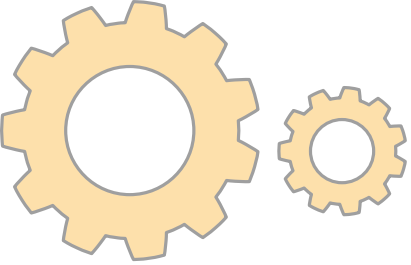
II - O fortalecimento da integridade institucional a partir do diagnóstico de vulnerabilidades na segurança da informação;

III – A capacitação adequada do encarregado e sua equipe de apoio e dos agentes de tratamento;

IV - O fortalecimento dos mecanismos de comunicação de possíveis incidentes deve ser pautado pela tempestividade, a implementação de melhorias de segurança e a obtenção de informações sobre as origens da vulnerabilidade; e

V - A gestão de riscos será sistematizada e suportada pelas premissas de metodologias técnicas;

Parágrafo único. O modelo de gestão de gerenciamento de riscos deve seguir o método de priorização de processos, considerando sua relevância e impacto na estratégia da empresa.



Capítulo IV

DOS INSTRUMENTOS

Art. 6º São instrumentos da PPDPL:

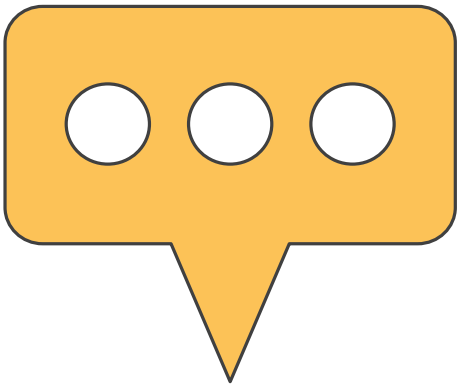
I - As Instâncias de supervisão: Diretoria Executiva e o Conselho de Administração;

II - A metodologia: o modelo de gestão de riscos deve ser estruturado com base nas boas práticas produzidas pela International Organization for Standardization, em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100;

III - A capacitação continuada: o Plano Anual de Capacitação, incluindo o eixo temático de Segurança da Informação e Proteção de Dados Pessoais;

IV - As normas, manuais e procedimentos: documentos devem ser formalmente definidos e aprovados pelo Dirigente Máximo;

V - A solução tecnológica: o processo de gestão de riscos deve ser apoiado por adequado suporte de tecnologia da informação.



Capítulo V

DAS INSTÂNCIAS DE SUPERVISÃO, COMPOSIÇÃO E DAS ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Do controlador, encarregado e operador

Art. 7º A empresa Suape é a controladora dos dados pessoais por ela tratados, nos termos das suas competências legal e institucional.

Art. 8º O dirigente máximo, enquanto representante legal, terá responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD na empresa, nos termos do art. 12 do Decreto Estadual 49.265, de 6 de agosto de 2020, com supervisão do Conselho de Administração.

Art. 9º O encarregado terá responsabilidade pelo gerenciamento do projeto de implantação e dos riscos e controles internos quanto à adequação à LGPD na empresa, conforme art 13 do Decreto Estadual 49.265, de 6 de agosto de 2020.

Parágrafo Único. Para assessorar o encarregado, deve ser considerada como equipe de apoio: Assessoria Jurídica, Compliance, Ouvidoria, Unidade de Tecnologia da Informação e Unidade de Planejamento e Gestão, além da Comissão de Trabalho sobre LGPD.

Art. 10º Os provedores de serviços de Tecnologia da Informação e Comunicação (TIC) e demais prestadores de serviços à estatal, que vierem a tratar dado pessoal em nome desta, poderão ser considerados operadores e deverão aderir a essa Política, além de cumprir os deveres legais, contratuais e de parceria respectivos, dentre os quais se incluirão, mas não se limitarão aos seguintes:

I. Assinar contrato ou termo de compromisso com cláusulas específicas sobre

proteção de dados pessoais requeridas por Suape;

II. Apresentar evidências e garantias suficientes nas quais se aplica adequado conjunto de medidas técnicas e administrativas de segurança, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

III. Manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

IV. Seguir fielmente as diretrizes e instruções transmitidas por Suape;

V. Facultar acesso a dados pessoais somente para a equipe autorizada, que demonstre estrita necessidade e assuma compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição à empresa, mediante solicitação;

VI. Permitir a realização de auditorias de Suape e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII. Auxiliar, em toda providência que estiver ao seu alcance, no atendimento por Suape de obrigações perante Titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII. Comunicar formalmente e de imediato à Suape a ocorrência de qualquer risco, ameaça ou incidente de segurança que possam acarretar comprometimento ou dano potencial ou efetivo a titular de dados pessoais, evitando atrasos por causa de verificações ou inspeções;

IX. Descartar de forma irrecuperável, ou devolver para Suape, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Seção II

Instituições

Art. 11º A Comissão de Trabalho sobre LGPD é responsável por realizar estudos, desenvolver projeto de implantação, adaptação, estruturação e monitoramento da adequação de Suape à LGPD.

Art. 12º O Gestor de Processos corresponde a todo e qualquer responsável pela unidade de execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos.

Seção III

Das atribuições e responsabilidades

Art. 13º Compete ao dirigente máximo, enquanto representante legal:

I - Aprovar práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - Aprovar as alterações da PPDPL e submetê-las ao Conselho de Administração;

III - Deliberar sobre o Plano de Implementação de Controles Internos;

IV - Aprovar a estrutura, extensão e conteúdo do Inventário de Dados;

V - Realizar os ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL;

VI - Acompanhar o diagnóstico preliminar de controles internos;

VII - Tomar conhecimento do andamento e resultados da avaliação de controles internos;

VIII - Tomar ciência do monitoramento do PPDPL;

IX - Aprovar e promover o Plano de Tratamento de Incidentes com Dados Pessoais; e

X - Aprovar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade.

Art. 14° Compete ao encarregado:

I - Propor práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - Elaborar alterações da PPDPL;

III - Consolidar propostas de ações, avaliar e elaborar o Plano de Implementação de Controles Internos;

IV - Elaborar a estrutura, extensão e conteúdo do Inventário de Dados;

V - Promover a aderência às regulamentações, leis, códigos, normas e padrões na condução da PPDPL;

VI - Recomendar ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL;

VII - Definir o diagnóstico preliminar de controles internos;

VIII - Instituir e acompanhar a avaliação de controles internos;

IX - Monitorar o PPDPL;

X - Elaborar o Plano de Tratamento de Incidentes com Dados Pessoais;

XI - Elaborar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma

da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

XII - Cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Local;

XIII - Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria de cada órgão e entidade;

XIV - Receber comunicações da Agência Nacional de Proteção de Dados Pessoais (ANPD) e adotar providências;

XV - Orientar os funcionários e os operadores no cumprimento das práticas necessárias à proteção de dados pessoais;

XVI - Quando provocado, entregar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

XVII - Atender às normas complementares da ANPD;

XVIII - Informar à Agência Nacional de Proteção de Dados Pessoais e aos titulares dos dados pessoais eventuais incidentes de privacidade de dados pessoais, dentro da execução de um Plano de Tratamento de Incidentes com Dados Pessoais.

Art. 15º Compete à Assessoria Jurídica:

I - Prestar orientação jurídica ao encarregado e aos operadores sobre aplicação da LGPD e dos normativos dela decorrentes;

II - Elaborar os ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL;

III - Prestar consultoria jurídica na elaboração de normativos e instrumentos internos, em especial Termos de Uso e Termos de Consentimento, quanto à proteção de dados pessoais.

Art. 16º Compete à Unidade de Tecnologia da Informação:

I - Prestar orientação técnica ao encarregado e aos operadores sobre questionamentos e boas práticas em segurança da informação;

II - Apoiar as ações de capacitação nas áreas de Segurança da Informação e Proteção de Dados Pessoais;

III - Apoiar o diagnóstico preliminar;

IV - Apoiar a avaliação de controles internos dos processos priorizados;

V - Apoiar, com propostas técnicas de segurança da informação, a elaboração do Plano de Tratamento de Incidentes com Dados Pessoais;

VI - Apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais;

VII - Extrair estrutura e conteúdo de dados pessoais em sistemas informatizados para elaboração do Inventário de Dados;

VIII - Extrair conteúdo de dados pessoais em sistemas informatizados para atendimentos das demandas dos titulares;

IX - Apoiar, com propostas técnicas de segurança da informação, a elaboração instrumentos, em especial contratos e congêneres;

X - Apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 17º Compete ao Compliance:

I - Propor melhorias metodológicas no gerenciamento dos riscos associados à proteção de dados pessoais;

II - Apoiar o diagnóstico preliminar;

III – Apoiar a avaliação de controles internos dos processos priorizados;

IV - Apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais;

V - Apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 18º Compete à Ouvidoria:

I - Apoiar no recebimento de manifestações e comunicações dos titulares de dados pessoais;

II - Realizar a interlocução do titular de dados pessoais com o encarregado;

III - Mapear as principais possíveis demandas do titular de dado pessoal, considerando o Inventário de Dados;

IV - Apoiar o encarregado na elaboração de ações que facilitem o atendimento às demandas dos titulares de dados pessoais;

V - Promover a transparência dos tratamentos de dados pessoais sob responsabilidade de Suape.

Art. 19º Compete à Unidade de Recursos Humanos:

I - Apoiar a promoção da disseminação da cultura de proteção de dados pessoais;

II - Prover a capacitação dos agentes públicos no exercício do cargo, função e emprego no conteúdo de proteção de dados pessoais;

IV - Praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Art. 20º Compete aos Gestores de Processos:

I - Realizar, em conjunto com a Unidade de Tecnologia da Informação e Compliance, o diagnóstico preliminar;

II - Realizar, em conjunto com a Unidade de Tecnologia da Informação e Com-

pliance, a avaliação de controles internos dos processos priorizados;

III - Elaborar propostas de ação ao Plano de Implementação de Controles dos processos sob sua responsabilidade;

IV - Cumprir os objetivos e as prioridades estabelecidas pelo Plano de Implementação de Controles;

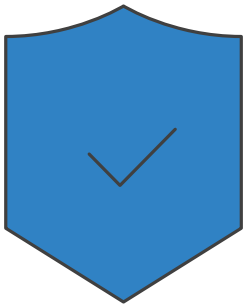
V - Gerenciar as ações do Plano de Implementação de Controles e avaliar os seus resultados dos processos sob sua responsabilidade;

VI - Disponibilizar o conteúdo de dados pessoais para elaboração do Inventário de Dados;

VII - Disponibilizar conteúdo de dados pessoais para atendimentos das demandas dos titulares;

VIII - Cumprir as recomendações e observar as orientações emitidas pelo dirigente máximo e pelo encarregado;

IX - Adotar princípios de conduta e padrões de comportamento no âmbito da sua estrutura organizacional.



Capítulo VI

DO TRATAMENTO DE DADOS PESSOAIS

Art. 21° O tratamento de dados pessoais por Suape será realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Parágrafo único. O Estatuto de Suape (Decreto Estadual n° 47.170/2019) e demais normas da organização definem as funções e atividades que constituem as finalidades e balizadores do tratamento de dados pessoais para fins dessa

política.

Art. 22º Em atendimento às suas competências legais, Suape poderá, no estrito limite de suas atividades, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares.

Parágrafo Único. Eventuais atividades que transcendam o escopo da função institucional estarão sujeitas à obtenção de consentimento dos titulares dos dados pessoais a serem objeto de tratamento.

Art. 23º Suape manterá contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários às operações, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível e ser consultada pelos interessados.

Art. 24º Os dados pessoais tratados por Suape são:

I. Protegidos por procedimentos internos para registrar autorizações e utilizações;

II. Mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade ou face a pedido de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de temporalidade de retenção de dados;

III. Compartilhados somente para o exercício das funções institucionais ou para atendimento de políticas públicas aplicáveis;

IV. Revistos em periodicidade mínima bianual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu de retenção.

Art. 25º A responsabilidade de Suape pelo tratamento de dados pessoais estará circunscrita ao dever de se ater ao exercício de sua competência legal e institucional e de empregar boas práticas de governança e de segurança.

DAS DISPOSIÇÕES FINAIS

Art. 26º Em função da complexidade e abrangência, a implementação dessa política será realizada de forma gradual e continuada pelo Plano de Implementação de Controles.

Parágrafo único. O Plano de Implementação de Controles deverá ser revisado anualmente e poderá sofrer alterações de ofício, após validação do dirigente máximo, a partir da redefinição de prioridades por parte da Política Estadual de Proteção de Dados Pessoais, conforme § 1º do art.6º do Decreto Estadual 49.265, de 6 de agosto de 2020.

Art. 27º O Plano de Implementação de Controles aprovado pelo dirigente máximo deverá ser inserido e gerenciado na solução tecnológica de gestão de riscos com adequado suporte do setor responsável.

Art. 28º Os casos omissos ou excepcionalidades serão deliberados pelo dirigente máximo, consultado o encarregado e a Comissão de Trabalho sobre LGPD.

SUAPE
Complexo Industrial Portuário
Governador Eraldo Gueiros

Secretaria de
Desenvolvimento
Econômico

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.