Descrição	Responsáveis	Providências
Backup		
Modelo para procedimentos de *backup*	CGGDIESP	Orientação técnica
	Órgãos e entidades	Especificação técnica com implementação em sistema
Gestão de mudanças		
Modelo para procedimentos para acompanhamento do andamento e dos resultados de mudanças	CGGDIESP	Orientação técnica
	Órgãos e entidades	Especificação técnica com implementação em sistema
Resposta a Incidentes de Segurança da Informação		
Plano de Resposta de Incidentes de Segurança, promovendo: • Comunicação de desvios e falhas de segurança; • Mobilização da equipe de combate; • Registro dos incidentes e das evidências; • Procedimentos para proteção das evidências de forma adequada; • Análise forense computacional e; • Ações de resposta ao incidente, com combate, controle e recuperação.	CGGDIESP	Modelo, Orientação técnica e Fluxo procedimental
	Órgãos e entidades	Plano de Resposta de Incidentes de Segurança conforme Modelo, Orientação técnica e Fluxo procedimental
Gerenciamento de Riscos		
Melhores práticas de gerenciamento de riscos, promovendo: • Identificação de vulnerabilidades e potenciais de exploração; • Estimativa de impacto;	CGGDIESP	Orientação técnica sobre melhores práticas

Descrição	Responsáveis	Providências
• Determinação de alternativas de mitigação e contingência; • Decisão quanto aos riscos identificados; e • Priorização das Ações.		
Procedimento de identificação e avaliação dos riscos	Órgãos e entidades	Manual técnico procedimental com documentação das práticas adotadas
Continuidade de negócios		
Planos de contingência e de recuperação de desastres, promovendo: • Identificação de Sistemas e equipamentos críticos; • Estimativa de impacto; • Determinação de alternativas de redundância, mitigação e contingência; • Decisão quanto aos investimentos necessários e; • Planejamento e execução de testes de contingência e de recuperação.	CGGDIESP	Orientação técnica sobre melhores práticas
Procedimentos de Gestão de Continuidade do Negócio	Órgãos e entidades	Manual técnico procedimental contendo Plano de contingência e de recuperação de desastres que observe a Orientação técnica
Monitoramento, Revisão e Atualização		
Procedimentos para monitoramento dos ambientes físicos e lógicos, promovendo: • Identificação dos Controles implantados; • Determinação de limites de tolerância para não-conformidade dos Controles; • Monitoramento de Alertas; • Desenvolvimento e publicação de relatórios operacionais de conformidade; • Ações de Correção: ▪ Ajustes nos limites de Alertas; ▪ Ajustes (adição/eliminação) de Controles;	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental

Descrição	Responsáveis	Providências
▪ Ajustes na configuração de Sistemas; e • Submissão de recomendações para revisão e atualização de políticas, normas, processos e procedimentos operacionais.		
Programa de revisão e atualização de políticas, normas, processos e procedimentos	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental

Deliberação Normativa CGGDIESP-2, de 30-12-2021

Institui a POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS – PPDP no âmbito da Administração Pública Estadual e dá providências correlatas

O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, no uso das atribuições que lhe foram conferidas pelo Dec. 64.790-2020, delibera:

Artigo 1º - A POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (PPDP), a que se refere o inciso III do artigo 3º do Decreto nº 65.347, de 13 de fevereiro de 2020, fica instituída nos termos desta deliberação, em conformidade com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e alinhada às diretrizes da Política de Governança de Dados e Informações do Estado de São Paulo – PGDI.

§ 1º – Para os fins desta PPDP, são adotadas as definições constantes do Glossário que integra este documento como Anexo I.

§ 2º – A Política de Privacidade e Tratamento de Dados Pessoais integra esta PPDP como Anexo II.

§ 3º – Normas, procedimentos e padrões específicos serão desenvolvidos e divulgados pela Administração Pública estadual, conforme o Anexo III – Providências e Documentos Complementares.

CAPÍTULO I

Âmbito de Incidência

Artigo 2º - A política instituída por esta deliberação:

I - observa as disposições da LGPD e do Decreto nº 65.347, de 13 de fevereiro de 2020;

II - não se aplica às operações de tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;

III – é de observância obrigatória por:

a) órgãos da Administração Pública direta, autarquias e fundações, sem prejuízo da aplicação subsidiária e complementar de normas e regras específicas;

b) empresas públicas e sociedades de economia mista controladas pelo Estado, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas;

c) pessoas jurídicas de direito privado em casos de execução descentralizada de atividade pública, quando houver previsão legal, contratual ou em convênio e instrumentos congêneres.

CAPÍTULO II

Objetivos

Artigo 3º - A PPDP tem por objetivos:

I – divulgar as diretrizes estabelecidas pelo Estado de São Paulo para operações de tratamento de dados pessoais;

II – estabelecer responsabilidades e limites de atuação aos agentes públicos;

III – declarar o compromisso do Estado de proteção do direito à privacidade no desempenho das atividades estatais.

Parágrafo único – As disposições desta PPDP aplicam-se a toda operação de tratamento de dados pessoais realizada pela Administração Pública estadual, sem limitações, devendo ser respeitadas por agentes públicos, bem como por aqueles que:

1. realizem operações de tratamento de dados pessoais em nome do Estado;

2. compartilhem dados pessoais com o Estado ou com terceiros em nome do Estado;

3. utilizem a infraestrutura fornecida pelo Estado para tratamento de dados pessoais.

CAPÍTULO III

Tratamento de Dados Pessoais

Seção I

Princípios da Proteção dos Dados Pessoais

Artigo 4º - Além daqueles relacionados no artigo 5º da PGDI, a PPDP observa os princípios gerais de proteção de dados pessoais e os direitos do titular previstos na LGPD.

Seção II

Finalidades e Bases legais para Tratamento de Dados Pessoais

Artigo 5º - O tratamento de dados pessoais pela Administração Pública observa as disposições previstas no Capítulo IV da LGPD, com vistas ao atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

§1º - A cada finalidade corresponde um fundamento legal, considerando o princípio da legalidade, que autoriza o tratamento de dados pessoais, inclusive de crianças e adolescentes, segundo as hipóteses:

1. execução de Políticas Públicas, previstas em leis e regulamentos ou respaldados em contratos, convênios ou instrumentos congêneres (artigo 7o, III da LGPD);

2. tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos (artigo 11, II, b da LGPD);

3. competências legais ou atribuições legais do serviço público (artigo 23 da LGPD).

§2º - A definição da finalidade e a atribuição dos fundamentos legais a que se referem os artigos 7º e 11 da LGPD considera:

1. o serviço a ser prestado ao particular;

2. a competência estadual na matéria;

3. os dados pessoais cuja coleta é necessária à luz da finalidade do tratamento.

§3º - Os fundamentos legais adotados para o tratamento de dados pessoais pela Administração Pública estadual são atribuídos de acordo com as finalidades do tratamento à luz do caso concreto.

§4º - O consentimento do titular de dados pessoais será exigido para desempenho de atividades excepcionais, em conformidade com o serviço público prestado e as diretrizes emanadas pelos órgãos e entidades com atribuição na matéria, mediante prévia consulta ao Comitê Gestor de Governança de Dados e Informações, conforme Anexo III – Providências e Documentos Complementares.

§5º - O tratamento de dados pessoais de crianças e adolescentes sempre deve ocorrer em seu melhor interesse.

§6º - As informações sobre o tratamento de dados de crianças e adolescentes devem ser fornecidas de maneira simples, clara e acessível, consideradas as características do titular, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança e adolescente.

§7º - As hipóteses de tratamento de dados pessoais pela Administração Pública, assim como a respectiva previsão legal, a finalidade, os procedimentos e as práticas utilizadas devem ser prévia e expressamente divulgadas em veículos de fácil acesso, preferencialmente nos sítios eletrônicos dos órgãos e entidades, observadas as disposições do Anexo II – Política de Privacidade e Tratamento de Dados Pessoais.

Seção III

Agentes de Tratamento

Artigo 6º - São agentes de tratamento, em conformidade com os conceitos estabelecidos pela LGPD, as orientações e regulamentação emanadas da Autoridade Nacional de Proteção de Dados (ANPD) e o disposto no Decreto nº 65.347/2020:

I - Estado de São Paulo, que exerce o papel de controlador de dados pessoais, por intermédio dos Secretários de Estado, do Procurador Geral do Estado e do Chefe do Poder Executivo;	No âmbito da Administração Pública Direta, as decisões referentes ao tratamento de dados pessoais cabem ao Estado de São Paulo, cujas atribuições de controlador, por força da desconcentração administrativa, são desempenhadas pelos órgãos públicos que o integram, respeitadas suas respectivas competências e campos funcionais.
II - Entidades da Administração Pública Indireta	As entidades, com personalidade jurídica própria, que compõem a Administração Pública Indireta assumem a posição de **controlador** – quando detêm poder de decisão sobre as finalidades e elementos essenciais de tratamento de dados pessoais – **ou de operador** – quando realizam o tratamento de dados pessoais de acordo com os interesses de outro agente de tratamento.
Pessoas naturais que ocupam cargo ou emprego ou exercem função na Administração Pública Direta ou Indireta	Não são considerados agentes de tratamento, pois atuam de forma subordinada em nome da pessoa jurídica à qual estão vinculados.
Terceiros	Terceiros que não integram a estrutura da Administração Pública Direta e Indireta do Estado de São Paulo, mas que com ela mantenham vínculo contratual ou de parceria, cujo instrumento jurídico específico estipule a realização de operação de tratamento de dados pessoais, na forma do artigo 26 da LGPD. Os terceiros podem atuar na condição de **controlador** – quando detiverem poder de decisão sobre as finalidades e elementos essenciais de tratamento de dados pessoais – **ou operador** – quando realizarem o tratamento de dados pessoais de acordo com os interesses do Estado de São Paulo ou das entidades da Administração Pública Indireta.

Seção IV

Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo

Artigo 7º - O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo atua como auxiliar do controlador, nos termos do artigo 3º do Decreto nº 65.347, de 9 de dezembro de 2020, cabendo-lhe examinar e aprovar as propostas de adaptação à PPDP, formuladas por órgãos e entidades estaduais.

Seção V

Encarregado de Dados Pessoais

Artigo 8º – A identidade e as informações de contato dos Encarregados pelo Tratamento de Dados Pessoais são divulgadas no sítio eletrônico da Central de Dados do Estado de São Paulo – CDESP.

Parágrafo único – Sem prejuízo do disposto no "caput" deste artigo, cabe às autarquias, fundações, empresas públicas e sociedades de economia mista designar e fazer publicar em sítio eletrônico próprio a identidade e as informações de contato do respectivo encarregado pelo tratamento de dados pessoais naquele âmbito.

Artigo 9º - Aos Encarregados pelo Tratamento de Dados Pessoais da Administração Direta e da Indireta, cabe exercer as atividades relacionadas no § 2º do artigo 43 da LGPD e outras que vierem a ser definidas pela ANPD, especialmente:

I – centralizar o recebimento das comunicações da ANPD direcionadas aos respectivos controladores e coordenar a adoção das providências necessárias ao atendimento;

II – orientar, com o apoio das Comissões de Avaliação de Documentos e Acesso (CADAs), os agentes públicos e os contratados da Administração Pública estadual a respeito das práticas a serem adotadas para a proteção de dados pessoais;

III – adotar as medidas necessárias à elaboração e publicação dos Relatórios de Impacto à Proteção de Dados (RIPD), na forma solicitada pela ANPD;

IV – receber e encaminhar ao órgão ou entidade responsável pela adoção de providências correlatas, as sugestões pertinentes e a relação das medidas voltadas à cessação de eventual violação à LGPD; e

V – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§1º - Ao Encarregado pelo Tratamento de Dados Pessoais da Administração Direta, nos termos do Decreto nº 65.347, de 9 de dezembro de 2020, cabe também:

1. subsidiar o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo com dados e informações que viabilizem a coordenação das ações de proteção de dados pessoais no âmbito da Administração Pública estadual; e

2. atuar em constante interlocução com os Serviços de Informação ao Cidadão (SICs), contando com o apoio técnico da Coordenadoria de Tecnologia da Informação e Comunicação – COORTIC, da Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação – SSCTI, da Secretaria de Governo e de quaisquer outras unidades administrativas que se fizerem necessárias.

§2º – Mediante requisição do Encarregado, os órgãos e as entidades da Administração Pública estadual devem