	REDUÇÃO			VALORES EM REAIS
ÓRGÃO/QUOTAS MENSAIS/DOTAÇÃO CONTINGENCIADA		FR	GD	VALOR
08000	SECRETARIA DA EDUCAÇÃO			
	T O T A L	03	3	7.666.117,00
	DEZEMBRO			7.666.117,00
	T O T A L	05	3	169.722.653,00
	DEZEMBRO			169.722.653,00
	T O T A L	43	3	10.760.191,00
	DEZEMBRO			10.760.191,00
08046	FUND.PARA O DESENV.DA EDUCAÇÃO - FDE			
	T O T A L	81	3	3.328.299,00
	DEZEMBRO			3.328.299,00
	T O T A L	85	3	3.000.000,00
	DEZEMBRO			3.000.000,00

TABELA 3	MARGEM ORÇAMENTÁRIA	VALORES EM REAIS
	RECURSOS DO RECURSOS TESOURO EPRÓPRIOS	

ESPECIFICAÇÃO					VALOR TOTAL		VINCULADOS
LEI	ART	PAR	INC	ITEM			
17286	13				673.254.246,00	673.254.246,00	0,00
17286	28	5			266.705,00	266.705,00	0,00
TOTAL GERAL					673.520.951,00	673.520.951,00	0,00

DECRETO Nº 66.405, DE 28 DE DEZEMBRO DE 2021

Retificação do D.O. de 29-12-2021

Na tabela leia-se como segue e não como constou:

TABELA 3	MARGEM ORÇAMENTÁRIA	VALORES EM REAIS
	RECURSOS DO RECURSOS TESOURO EPRÓPRIOS	

ESPECIFICAÇÃO					VALOR TOTAL		VINCULADOS
LEI	ART	PAR	INC	ITEM			
17309	9º		I		2.000.000.000,00	2.000.000.000,00	0,00
TOTAL GERAL					2.000.000.000,00	2.000.000.000,00	0,00

Atos do Governador

DESPACHOS DO GOVERNADOR

DESPACHO DO VICE-GOVERNADOR, EM EXERCÍCIO NO CARGO DE GOVERNADOR DO ESTADO, DE 30-12-2021

No processo SEDUC-PRC-2021-17227, sobre convênio: "À vista dos elementos de instrução constantes dos autos, notadamente da representação do Secretário da Educação e do Parecer 861-2021, da A.J.G./P.G.E., autorizo a celebração de convênio entre o Estado, por intermédio da Pasta citada, e a Fundação de Amparo à Pesquisa do Estado de São Paulo - Fapesp, tendo por objeto a execução do Programa de Pesquisa em Educação Básica - PPEDUC/ FAPESP-SEDUC, condicionada a formalização do termo à observância das recomendações indicadas no pronunciamento jurídico referido, bem como das normas legais e regulamentares aplicáveis à espécie."

Governo

GABINETE DO SECRETÁRIO

Deliberação Normativa CGGDIESP-1, de 30-12-2021

Institui a Política de Governança de Dados e Informações – PGDI, 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 Governança de Dados e Informações – PGDI, a que se refere o inc. III do art. 3º do Dec. 65.347-2020, fica instituída nos termos desta deliberação, visando estabelecer parâmetros para as boas práticas em segurança da informação, para a privacidade e proteção de dados pessoais e para a gestão de dados e informações, no âmbito da Administração Pública estadual.

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

§ 2º – Normas, procedimentos e padrões específicos serão desenvolvidos e divulgados pela Administração Pública estadual, conforme o Anexo II – Providências e Documentos Complementares.

CAPÍTULO I

Das Disposições Iniciais

Artigo 2º – Para proporcionar um nível adequado de segurança das informações, armazenadas tanto em suporte físico quanto digital, a PGDI estabelece diretrizes de orientação à governança de dados e informações e à estruturação de processos e procedimentos para utilização confiável e segura das informações e dados.

Parágrafo único – As diretrizes a que alude o "caput" deste artigo são estabelecidas em conformidade, no que couber, com os instrumentos de planejamento do Sistema Estadual de Tecnologia da Informação e Comunicação – SETIC, reformulado pelo Decreto nº 64.601, de 22 de novembro de 2019.

Artigo 3º – Esta PGDI se aplica aos órgãos e entidades da Administração Pública estadual, devendo ser observada pelos agentes públicos no exercício de suas atribuições.

Parágrafo Único – Os órgãos e entidades a que se refere o "caput" deste artigo:

1. devem elaborar as normas e procedimentos específicos indicados no Anexo II – Providências e Documentos Complementares, não se limitando às expressamente mencionadas;

2. devem promover as devidas adequações em seus respectivos programas, processos, procedimentos e ferramentas para a governança de dados e informações, de modo a observar a PGDI instituída por esta deliberação, adaptando eventuais especificidades;

3. podem, motivadamente, propor modificações à PGDI à análise do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

Artigo 4º – Sem prejuízo da publicação em Diário Oficial, esta PGDI e respectivos anexos devem ser disponibilizados nos sítios eletrônicos da Central de Dados do Estado de São Paulo – CDESP e dos órgãos e entidades da Administração Pública estadual.

Parágrafo único – Na hipótese a que alude o item 3 do parágrafo único do artigo 3º, as modificações setoriais à PGDI também devem ser disponibilizadas no sítio eletrônico do respectivo órgão ou entidade.

CAPÍTULO II

Dos Princípios

Artigo 5º – A PGDI observa os princípios que regem a atividade administrativa, bem como o seguinte:

I – proporcionalidade: adoção de medidas necessárias, adequadas e possíveis para atendimento do interesse público;

II – confidencialidade: garantia de que a informação não pública não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada ou credenciada;

III – disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por pessoa física ou sistema, órgão ou entidade da Administração Pública estadual devidamente autorizados;

IV – integridade: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V – autenticidade: garantia de que a informação é livre de adulteração;

VI – finalidade: garantia de tratamento da informação para propósitos legítimos, específicos, explícitos e informados ao titular;

VII – adequação: compatibilidade do tratamento da informação com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

VIII – necessidade: limitação do tratamento ao mínimo necessário para o alcance da respectiva finalidade, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;

IX – livre acesso: garantia, aos titulares dos dados, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

X – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade do respectivo tratamento;

XI – transparência: fornecimento, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização de operações de tratamento e os respectivos agentes, respeitados os segredos comercial e industrial;

XII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

XIII – prevenção: garantia de adoção de medidas para prevenir a ocorrência de danos em virtude ou durante a realização de operações de tratamento de dados pessoais;

XIV – não discriminação: impossibilidade de realização de operações de tratamento com fins discriminatórios, ilícitos ou abusivos;

XV – responsabilização e prestação de contas: demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO III

Dos Objetivos

Artigo 6º – A PGDI tem os seguintes objetivos:

I – estabelecer as diretrizes estratégicas, responsabilidades e competências na implementação de medidas de segurança da informação;

II – preservar e proteger de vulnerabilidades e ameaças as informações contidas em qualquer suporte ou formato, em todo o respectivo ciclo de vida;

III – prevenir e reduzir impactos gerados por incidentes de segurança da informação, de modo a preservar a disponibilidade, confidencialidade, integridade e autenticidade da informação;

IV – cumprir as leis e regulamentos atinentes à segurança da informação e privacidade;

V – promover a conscientização e a capacitação em segurança da informação, dos agentes públicos;

VI – planejar, gerir, supervisionar e controlar informações, incentivando o ciclo de melhoria contínua de processos internos e a observância de boas práticas de governança de dados e informações, evitando incidentes de segurança e reduzindo custos;

VII – propiciar que a Administração Pública estadual gerencie dados como ativos, com a adoção de práticas aderentes e sustentáveis de governança de dados e informações, devidamente incorporadas nas atividades-fim;

VIII – utilizar e fomentar o uso da governança de dados e informações para aperfeiçoar as políticas públicas do Estado;

IX – auxiliar e aperfeiçoar os processos de tomada de decisão pelos gestores estaduais.

CAPÍTULO IV

Diretrizes Gerais

Título I

Governança de Dados e Informações

Seção I

Política de Governança de Dados e Informações

Artigo 7º – Os órgãos e entidades da Administração Pública estadual devem observar, no âmbito de suas atribuições, as diretrizes específicas para a Governança de Dados e Informações, conforme Anexo II, exercendo autoridade e controle, mediante planejamento, monitoramento e execução, sobre a gestão de ativos de dados, com o objetivo de garantir que estes sejam gerenciados de forma adequada, de acordo com esta PGDI e as melhores práticas, em prol da tomada de decisão responsável e qualificada.

Parágrafo único – As diretrizes específicas sobre governança de dados e informações constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre:

1. Segurança de Dados e Informações;
2. Integração e Interoperabilidade de dados;
3. Gerenciamento de Documentos e Conteúdo;
4. Arquitetura de Dados;
5. Modelagem e Design de Dados;
6. Armazenamento e Operações de Dados;
7. Dados de Referência e Dados Mestre;
8. Data Warehousing e Business Intelligence;
9. Metadados;
10. Qualidade dos Dados;
11. Big Data e Data Science; e
12. Inteligência Artificial.

Artigo 8º – A PGDI tem como pilares:

I - Gestão de Riscos, compreendendo análise, identificação, gerenciamento e mitigação de riscos de uso indevido de dados e aos direitos e liberdades individuais, no que se refere à privacidade e proteção de dados pessoais;

II - Segurança de Dados, com vistas à proteção da informação, mediante adoção de controles que assegurem a sua confidencialidade, integridade, disponibilidade e autenticidade;

III – Privacidade, abrangendo a proteção de dados pessoais e de dados pessoais sensíveis, por meio de exercício de controles apropriados, monitorados via aplicação de avaliações sistemáticas da governança de dados e informações, propiciando ciclos de melhoria contínua.

Seção II

Segurança de Dados e Informações

Artigo 9º – As atividades de planejamento, desenvolvimento e execução de políticas públicas devem observar a segurança de dados, com observância de normas e procedimentos de autenticação, autorização, acesso e auditoria adequados de dados e informações, de modo a:

I – prevenir acessos não autorizados a dados e informações da Administração Pública estadual;

II – assegurar a conformidade com regulamentos e leis de privacidade, proteção e confidencialidade vigentes no país; e

III – respeitar direitos e garantias das partes interessadas, no que tange à privacidade e à confidencialidade.

Parágrafo Único – As diretrizes específicas sobre segurança de dados da Administração Pública estadual constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre segurança:

I – das instalações;

II – dos dispositivos;

III – de credenciais; e

IV – da comunicação eletrônica.

Seção III

Integração e Interoperabilidade

Artigo 10 – Sempre que possível, os dados devem ser mantidos em formato interoperável e estruturados com vistas ao uso compartilhado, para a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo público em geral, com observância da legislação aplicável.

§1º – As atividades de integração e interoperabilidade devem ser planejadas, desenvolvidas, testadas e implementadas conforme as diretrizes estabelecidas pelo Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo e do Conselho Estadual de Tecnologia da Informação e Comunicação – COETIC.

§2º – Os sistemas integrados e as bases de dados utilizadas pela Administração Pública devem ser objeto de melhoria contínua.

§3º – A estrutura dos dados deve ser arquitetada de modo a torná-los acessíveis a partir de mecanismos de busca, leitura, consulta e recuperação de dados.

§4º – Os órgãos e entidades responsáveis pela custódia de documentos físicos, nos casos em que não seja possível convertê-los em digitais ou em que exista obrigação legal de armazenamento em meio físico, devem adotar as medidas cabíveis para a preservação da integridade e da inviolabilidade dos dados.

§5º – As diretrizes de integração e interoperabilidade do Estado de São Paulo constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre:

I – interconexão;

II – segurança;

III – meios de acesso;

IV – organização e intercâmbio de informações;

V – áreas de integração para a Administração Pública.

Seção IV

Gestão de Documentos e Informações

Artigo 11 – Os órgãos e entidades devem criar, usar, recuperar e descartar documentos e informações com observância:

I – da legislação de proteção de dados aplicável;

II – das políticas, normas e procedimentos estabelecidos pelo Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo;

III – das demais regras de conformidade editadas pelo órgão ou entidade integrante da Administração Pública, no âmbito de suas atribuições.

Parágrafo Único – A gestão de documentos e informações deve garantir:

1. a respectiva recuperação e uso em formatos não estruturados;

2. recursos de integração entre dados não estruturados e estruturados.

Título II

Segurança da Informação

Seção I

Ativos da Informação

Artigo 12 – As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pela Administração Pública estadual, bem como os demais ativos da informação, devem ser utilizados unicamente para finalidades públicas na persecução do interesse público.

Seção II

Sigilo

Artigo 13 – É vedada a revelação de informações sob a responsabilidade do Estado de São Paulo, excetuando-se aquelas de caráter público, nos termos do Decreto nº 58.052/2012.

Parágrafo Único – Os órgãos e entidades estaduais devem:

1. observar as disposições do Decreto nº 48.897/2004, no que se refere aos documentos de arquivo e sua gestão, aos Planos de Classificação e à Tabela de Temporalidade de Documentos;

2. definir ou atualizar as respectivas normas para a avaliação, guarda e eliminação de documentos de arquivo e providências correlatas;

3. estabelecer ou atualizar os respectivos Planos de Classificação de Documentos e de Tabelas de Temporalidade;

4. providenciar, visando à uniformização de critérios, a integração dos controles de classificação e indexação de dados não estruturados implementados pelo Plano de Classificação e pela Tabela de Temporalidade de Documentos aos controles de classificação e indexação de dados estruturados, nos termos do Decreto nº 58.052/2012.

Seção III

Classificação da Informação

Artigo 14 – As informações sob a responsabilidade do Estado de São Paulo devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida.

Parágrafo Único – A classificação a que se refere o "caput" deste artigo deve observar o disposto no Decreto nº 48.897/2004 quanto ao arquivamento, criando uma associação entre dado ou informação e a respectiva classificação e origem.

Artigo 15 – Os órgãos e entidades da Administração Pública estadual devem classificar os dados sob sua responsabilidade, de modo a identificar, no mínimo, a finalidade do tratamento, o tempo necessário de armazenamento da informação e a categoria, na seguinte conformidade:

I - dados públicos;

II - dados sigilosos;

III - dados confidenciais;

IV - dados críticos;

V - dados pessoais;

VI - dados pessoais sensíveis;

VII - dados pessoais de criança e adolescente.

Seção IV

Análise dos Processos e Ativos de Informação

Artigo 16 – Os órgãos e entidades, em intervalos regulares, devem analisar os respectivos processos e ativos de informação, visando assegurar que estejam devidamente inventariados e classificados, com identificação e ciência dos respectivos gestores, controladores e operadores, assim como que sejam mapeadas as vulnerabilidades e ameaças de segurança.

Seção V

Uso dos Ativos de Informação

Artigo 17 - Os ativos de informação sob responsabilidade do Estado de São Paulo devem ser utilizados para o exercício da função pública pelos órgãos e entidades, em conformidade com a legislação aplicável e as diretrizes desta PGDI.

Artigo 18 - A gestão dos ativos de tecnologia da informação da Administração Pública estadual deve atender, além das recomendações de fabricantes e desenvolvedores, as regras estabelecidas pelo processo de gestão de mudanças a que alude o artigo 33 desta PGDI.

Artigo 19 - Os órgãos e entidades da Administração Pública estadual devem realizar e manter devidamente atualizado inventário de hardwares e softwares de sua propriedade.

Artigo 20 - Para armazenar ou transmitir informações sob a responsabilidade do Estado de São Paulo, é vedado o uso de repositórios digitais ou dispositivos removíveis não autorizados ou que não tenham sido homologados para uso pelo órgão ou entidade estadual.

Artigo 21 – O uso de mídias sociais e de aplicativos de comunicação instantânea para o desempenho de atribuições do agente público, bem como para a troca de informações organizacionais é permitido, desde que necessário ao desenvolvimento das atividades do órgão ou entidade e com observância das regras estabelecidas pelo Secretário Extraordinário de Comunicação do Estado de São Paulo.

Artigo 22 – É vedado aos agentes públicos e colaboradores realizar qualquer atividade relacionada à captura de áudio, vídeo ou imagens dentro das dependências das repartições públicas do Estado de São Paulo, sem a prévia e formal autorização do respectivo órgão ou entidade que integrem.

Seção VI

Treinamento e Conscientização

Artigo 23 – Os órgãos e entidades devem realizar treinamentos periódicos e promover a conscientização e a disseminação da cultura da governança de dados e informações, proteção de dados e segurança da informação aos respectivos agentes públicos.

Parágrafo único - Os planos de treinamento e conscientização devem estimular a educação continuada, atualização periódica e realização de campanhas internas de comunicação a fim de promover a sensibilização para temas relacionados à segurança da informação, à governança de dados e informações e à proteção de dados e informações.

Artigo 24 – A capacitação e constante aperfeiçoamento de agentes públicos ocorrerá preferencialmente por meio do Centro de Excelência em Transformação Digital, ambiente digital mantido e operacionalizado pelo COETIC, de que trata o Decreto nº 64.601, de 22 de novembro de 2019, em articulação com a Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação, da Secretaria de Governo.

Título III

Digital

Seção I

Controle de Acesso

Artigo 25 – Os órgãos e entidades devem estabelecer regras de autenticação para acesso lógico, inclusive com a adoção de mecanismos de segurança que garantam acesso exclusivo por meio de credenciais, nível hierárquico e função compatíveis com o grau de classificação de cada dado ou informação.

§ 1º – As regras a que se refere o "caput" deste artigo devem estipular mecanismos para a revisão periódica das autorizações de acesso a dados e informações, no mínimo em razão de contratações, exonerações ou alterações de cargos e funções.

§ 2º – O acesso aos dados e informações que integram a Central de Dados do Estado de São Paulo – CDESP observará as disposições do Decreto nº 64.790, de 13 de fevereiro de 2020.

Artigo 26 – Os agentes públicos devem acessar os dados estritamente necessários ao desempenho de atividades no âmbito do órgão ou entidade que integrem.

Artigo 27 – Todo acesso a dados e informações terá registro histórico passível de auditoria, contendo, no mínimo:

I – identificação do agente responsável;

II – data e horário;

III – dispositivo de origem;

IV – objeto do acesso;

V – operação realizada.

Parágrafo único – Os princípios do privilégio de acesso e da segregação de funções devem ser observados na estruturação dos processos de trabalho e do acesso aos sistemas, de forma a reduzir o risco de acesso e de modificação de dados não autorizados, não intencionais ou indevidos.

Seção II

Ambientes Físicos e Lógicos

Artigo 28 - Os ativos e ferramentas que suportam informações e processos devem ser confiáveis, íntegros, seguros e disponíveis para o desempenho de atividades no âmbito da Administração Pública estadual.

Parágrafo único – Para garantir a segurança a que se refere o "caput" deste artigo, os sistemas de proteção serão mantidos operacionais e atualizados.

Artigo 29 – Os órgãos e entidades devem estabelecer perímetros de segurança para proteção dos respectivos ativos, bem como implementar controles para identificação e registro de acessos aos seus ambientes físicos.

Seção III

Armazenamento Seguro

Artigo 30 – Os órgãos e entidades devem armazenar dados em meio eletrônico com observância da segurança física e lógica de acesso, bem como da segurança no armazenamento de dados, a partir de mecanismos de criptografia e controle de acesso.

Parágrafo único – Os dados e informações em formato eletrônico devem ser encaminhados para a Central de Dados do Estado de São Paulo – CDESP, no prazo e formato indicados em requisição do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, nos termos do Decreto nº 64.790 de 13 de fevereiro de 2020.

Seção IV

Desenvolvimento de Software

Artigo 31 – O desenvolvimento interno ou externo e as aquisições de softwares devem garantir o cumprimento dos requisitos de segurança da informação, proteção de dados e controle de acesso previstos nesta PGDI e nas demais normas do órgão ou entidade responsável pelo desenvolvimento ou aquisição.

Seção V

Backup

Artigo 32 - Os órgãos e entidades devem manter processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (Backup), a fim de atender a requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes, bem como a recuperação o mais rápido possível.

Seção VI

Gestão de Mudanças

Artigo 33 – Os órgãos e entidades devem estabelecer procedimentos próprios para acompanhamento do andamento e dos resultados de mudanças principalmente em seus respectivos sistemas e infraestrutura tecnológica, e preservar os controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade das informações.

Parágrafo único – Os processos de gestão de mudanças devem ser registrados em um repositório centralizado na Central de Dados do Estado de São Paulo – CDESP, para fins de consulta, padronização e melhorias, nos termos do Decreto nº 64.790/2020.

Seção VII

Resposta a Incidentes de Segurança da Informação

Artigo 34 – Os órgãos e entidades devem manter equipe multidisciplinar de gerenciamento de crises e incidentes de segurança e elaborar Plano de Resposta de Incidentes de Segurança, com observância ao procedimento específico de gestão de incidentes, o qual será oportunamente elaborado e publicado pelo Estado de São Paulo, conforme Anexo II – Providências e Documentos Complementares.

Artigo 35 – Os órgãos e entidades devem orientar os respectivos agentes públicos a reportar de imediato às áreas responsáveis possíveis incidentes de segurança da informação, conforme Anexo II – Providências e Documentos Complementares.

§1º - Na hipótese de incidentes de segurança envolvendo dados pessoais:

1. as áreas responsáveis devem comunicar os seus respectivos Encarregados pelo Tratamento de Dados Pessoais;

2. os Encarregados, sem prejuízo das demais atribuições, devem reportar, tão logo quanto possível, todos os casos de incidentes, suspeitos ou comprovados, ao Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

§2º - Os desvios, as vulnerabilidades e as falhas de segurança identificados não devem ser explorados ou utilizados indevidamente.

§3º Os incidentes de segurança informados ou detectados devem ser registrados e as evidências, caso encontradas, devem ser protegidas de forma adequada, visando a subsidiar