



Diário Oficial

Estado de São Paulo

Rodrigo Garcia - Governador

Poder
Executivo
seção I



Palácio dos Bandeirantes • Av. Morumbi 4.500 • Morumbi • São Paulo • CEP 05650-000 • Tel. 2193-8000

Volume 132 • Número 259 • São Paulo, quinta-feira, 29 de dezembro de 2022

www.prodesp.sp.gov.br

Governo

GABINETE DO SECRETÁRIO

Instrução Normativa PGDI-1, de 27-12-2022

APROVA Instrução Normativa PGDI 1 referente Ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Ativos da Informação: Orientação Técnica e Modelo - Inventário de Dados, da Deliberação Normativa CGGDIESP 1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA
INVENTÁRIO DE DADOS

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimento para elaboração de inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos, quarta providência requerida pela Política de Governança de Dados e Informações (PGDI), no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021.
- Subsidiar procedimento de manutenção da consistência de inventário de dados tratados na execução de serviços finalísticos, a fim de evitar que dados críticos escapem aos controles de proteção e segurança necessários à sua correta gestão e preservação.
- Orientar o uso do formulário em formato de planilha eletrônica, disponibilizado com esta orientação técnica, para elaboração de inventário de dados.
- Esclarecer definições inerentes ao inventário de dados.

2. Sumário

1.	Objetivos.....	1
2.	Sumário.....	1
3.	Abrangência.....	2
4.	Principais documentos relacionados e referenciais bibliográficos.....	2
5.	Glossário	2
6.	Contexto	3
7.	Relação de temas abordados.....	4
8.	Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)	4
8.1.	Identificação do dado	5
8.2.	Identificação do banco de dados.....	5
8.3.	Identificação do Sistema Gerenciador de Banco de Dados	6
8.4.	Identificação das regras de validação ou fórmulas.....	6
8.5.	Identificação dos sistemas que utilizam o dado.....	6
8.6.	Identificação do RoPA	7
8.7.	Link para acesso a diagrama de MER	7
8.8.	Link para acesso a log.....	7
8.9.	Identificação dos processos que utilizam o dado.....	7
8.10.	Instrumento fornecido.....	8

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI), considerando, em seu Anexo II, a quarta providência, na qual dispõe orientação técnica de como fazer o inventário de dados.
- Política de Proteção de Dados Pessoais (PPDP).
- Decreto Estadual nº 63.382, de 9 de maio de 2018, que substitui os anexos do Decreto nº 48.898, de 27 de agosto de 2004, que aprova o Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo: Atividades-Meio, e dá providências correlatas.
- Decreto Estadual nº 65.347, de 9 de dezembro de 2020, que dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito do Estado de São Paulo.
- Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- Norma Técnica ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.
- Norma Técnica ABNT-NBR ISO/IEC 27002:2022 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação.

5. Glossário

Termos e siglas	Definição
ABNT	Associação Brasileira de Normas Técnicas.
Ativos de informação	São ativos de tecnologia da informação, dados, documentos ou qualquer outro elemento que possua valor e esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível.
Ativos de Tecnologia da Informação	Quaisquer meios de armazenamento, transmissão e tratamento das informações, como softwares, hardwares e ambientes físicos.
CGGDIESP	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Órgão colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto Estadual nº 65.347/2020.
Dado crítico	Dado essencial para a manutenção dos serviços executados pela organização e/ou objeto da proteção regulamentada pela LGPD, alvo das políticas e controles de segurança de dados. Inclui informações e documentos da organização, dados não facilmente criados ou reproduzidos, capital intelectual e dados pessoais.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, genéticos ou biométricos, quando vinculado a uma pessoa natural.
ISO	International Organization for Standardization (Organização Internacional de Normalização).

Termos e siglas	Definição
LGPD	Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, essa Lei rege o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.
MER	Modelo Entidade e Relacionamento. Representa um banco de dados.
NBR	Norma Técnica.
Norma	Documento, estabelecido por autoridade reconhecida, que assegura as características desejáveis de produtos, serviços e comportamentos, visando a qualidade, segurança, confiabilidade e eficiência.
PGDI	Política de Governança de Dados e Informações. Instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, que estabelece 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, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Política	Documento que estabelece as diretrizes a serem aplicadas em uma organização tendo em vista os objetivos definidos para ela.
PPDP	Política de Proteção de Dados Pessoais. Instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, e corresponde à compilação de normas e regras de boas práticas de governança e proteção para tratamento de Dados Pessoais, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
RoPA	Record of Processing Activities (Registro das Atividades de Tratamento de Dados Pessoais).
SGBD	Sistema Gerenciador de Banco de Dados.
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
Tratamento de dados pessoais	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

6. Contexto

Uma política de governança de dados e informações bem estruturada deve definir e identificar claramente os dados críticos do negócio, os dados mais valiosos, os dados relacionados aos processos-chave, os dados associados a grandes riscos ou impactos corporativos e os dados pessoais sob custódia do Estado, pois são eles que devem receber a atenção dos controles de segurança da informação ditados pela política de segurança da informação.

Para definir e identificar esses dados, o órgão ou entidade deve necessariamente fazer um levantamento de todos os processos de negócio que executa. No caso da Administração Pública, deve-se identificar os serviços finalísticos prestados ao cidadão e os processos associados à prestação desses serviços finalísticos.

Levantadas, classificadas e registradas as informações referentes aos serviços finalísticos, processos e classificação dos dados críticos, é possível estabelecer a governança de dados e os controles de segurança da informação que devem ser empregados para sua proteção e preservação, conforme primeira providência da PPDP.