APROVA Instrução Normativa CGGDIESP-1/PGDI 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

8.9. Identificação dos processos que utilizam o dado

8.10. Instrumento fornecido

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.

Termos e siglas	Definição
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).
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.

7. Relação de temas abordados

- Dado e banco de dados.
- SGBD.
- Regras de validação ou fórmulas.
- Sistemas e processos que utilizam dado inventariado.
- RoPA.
- Diagrama de MER.
- *Log*.
- Formulário para inventário de dados.

8. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)

A classificação das informações e a identificação e adoção dos controles necessários, idealmente estabelecidos desde a concepção dos processos de trabalho, conferem maturidade ao órgão ou entidade, fortalecendo os princípios de confiabilidade, rastreabilidade, segurança, privacidade e qualidade do tratamento dos dados.

Os dados, as informações e os ativos de informação e de Tecnologia da Informação devem ser utilizados unicamente para as finalidades públicas. Depois de mapeados os processos relativos aos serviços executados pelo órgão ou entidade, deve-se inventariar todos os dados tratados, em especial os dados críticos, os dados pessoais e os dados pessoais sensíveis. Orienta-se que tal inventário (catalogação e classificação) seja realizado por meio da planilha eletrônica "Inventário de Dados PGDI Anexo II", disponibilizada com esta orientação técnica. Trata-se de formulário composto de campos para preenchimento, construído com objetivo de nortear e padronizar a elaboração de documento com a relação dos dados objeto de tratamento na instituição, tendo em vista a implementação da PGDI em toda a Administração Pública estadual e, consequentemente, a adequação à LGPD do tratamento de dados pessoais realizado por seus órgãos e entidades.

O trabalho com o inventário de dados não se limita à sua elaboração. Devem ser realizadas análises periódicas, conforme disposto na décima providência da PGDI. Estabelecer e executar procedimento de análise periódica dos dados tratados pelos processos é importante para manter o controle do inventário de dados sempre atualizado, o que configura conduta em prol da mitigação dos riscos associados ao tratamento de dados pessoais. Observa-se que no "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados – RoPA", procedente da primeira

providência da PPDP, existe uma aba destinada ao registro de toda e qualquer alteração realizada em tais processos, o que facilita a análise periódica dos dados tratados.

Conforme as normas técnicas ABNT-NBR ISO/IEC 27001:2022 e ABNT-NBR ISO/IEC 27002:2022, que oferecem orientações ou requisitos complementares sobre uma gama de controles para o processo global de segurança da informação, a atenção a estas orientações e requisitos é importante para o adequado processo de análise periódica dos inventários de dados. A norma técnica ABNT-NBR ISO/IEC 27002:2022 no capítulo 5.9, que trata do "Inventário de informações e outros ativos associados", orienta que os inventários sejam desenvolvidos e mantidos, bem como orienta que os inventários devem ser precisos, atualizados, consistentes e alinhados com outros inventários considerando as análises críticas regulares dos dados, informações e dos ativos identificados. Por esta norma os inventários devem ser realizados e mantidos por sua função relevante à segurança da informação, por isso orienta que a localização dos dados seja incluída como informação importante e de forma apropriada, indicando que a granularidade das informações dos inventários esteja em nível adequado a gestão dos dados e para as necessidades dos órgãos e entidades. Também orienta que os órgãos e entidades identifiquem e documentem os dados que estejam em posse de pessoal ou instituições contratadas, com o propósito de proteger e garantir o adequado tratamento, assim como controlar a devolução desses dados quando do encerramento dos contratos.

A seguir estão elencados os **itens obrigatórios** ao inventário dos dados objeto de tratamento no órgão ou entidade, acompanhados de definições e orientações para a utilização do formulário disponibilizado com esta orientação técnica.

8.1. Identificação do dado

O dado deve ser identificado por código, nome e descrição.

Orientações para preenchimento do formulário

- Campo "ID": informar o código identificador do dado. Sugere-se que esse código seja similar aos códigos de classificação do Plano de Classificação e da Tabela de Temporalidade, conforme disposto no Decreto Estadual nº 63.382/2018. Por exemplo, "004.05.02.001", em que a primeira sequência numérica (004) corresponde à função, ou seja, a determinado conjunto de atividades que o Estado exerce para a consecução de seus objetivos; a segunda sequência numérica (05), à subfunção, ou seja, ao agrupamento de atividades afins correspondente a uma vertente da função; a terceira sequência numérica (02), à atividade, ou seja, ações, encargos ou serviços decorrentes do exercício da função; e a quarta sequência numérica (001), ao tipo de documento produzido, recebido ou acumulado no órgão ou entidade.
- Campo "Nome do dado": informar o nome do dado ou nome fantasia que o represente. Por exemplo, "CPF".

- Campo "Descrição do dado": inserir texto que descreva o dado. Por exemplo, "Cadastro de Pessoa Física".

8.2. Identificação do banco de dados

O banco de dados deve ser identificado por nome e local de hospedagem.

Orientações para preenchimento do formulário

- Campo "Nome do banco de dados": informar o nome do banco de dados onde o dado está armazenado.
- Campo "Local onde o banco de dados está hospedado (endereço do servidor)": informar o código numérico correspondente ao endereço *host* do servidor, também conhecido como endereço IP (Protocolo da Internet).

8.3. Identificação do Sistema Gerenciador de Banco de Dados

SGBD (em inglês, DBMS, de *Data Base Management System*) é o sistema de *software* responsável pelo gerenciamento de um ou mais bancos de dados. Seu principal objetivo é retirar da aplicação cliente a responsabilidade de gerenciar o acesso, a persistência, a manipulação e a organização dos dados. O SGBD disponibiliza uma interface para que seus clientes possam incluir, alterar ou consultar dados previamente armazenados. Em bancos de dados relacionais, a interface é constituída por protocolo de interface e de integração – por exemplo, API (*Application Programming Interface*) – ou *drivers* do SGBD, que executam comandos na linguagem SQL (*Structured Query Language*).

Orientações para preenchimento do formulário

- Campo "SGBD – Sistema Gerenciador de Banco de Dados": informar o SGBD responsável pelo gerenciamento do banco de dados onde o dado está armazenado. Por exemplo, "Oracle", "Mainframe" e "SQL Server".

8.4. Identificação das regras de validação ou fórmulas

Devem ser identificados *procedures* (rotinas, comandos ou instruções computacionais), *triggers* (procedimento automático ativado por determinado evento no banco de dados) e consistências (regras de validação de dados de entrada), entre outros procedimentos relativos à validação do dado quando de sua inserção no bando de dados.

Orientações para preenchimento do formulário

- Campo "Regras de validação ou fórmulas (BD) (*procedures*, *triggers*, consistências etc.)": informar a regra ou fórmula de validação de dado de entrada aplicada no bando de dados onde o dado está armazenado. Por exemplo, "Módulo 11".

8.5. Identificação dos sistemas que utilizam o dado

Devem ser elencados todos os sistemas do órgão ou entidade que utilizam o dado.

Orientações para preenchimento do formulário

- Campo "Sistemas que utilizam o dado": informar todos os sistemas que utilizam o dado. Por exemplo "Sistema 1", "Sistema 2", "Sistema 3".

8.6. Identificação do RoPA

O código de identificação do RoPA é atribuído quando do preenchimento do "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados – RoPA", procedente da primeira providência da PPDP.

Orientações para preenchimento do formulário

- Campo "ID do RoPA relacionado ao inventário": informar o código identificador do processo conforme RoPA que menciona o dado.

8.7. *Link* para acesso a diagrama de MER

O MER representa a arquitetura do banco de dados da aplicação. Por meio dele, é possível ilustrar como os dados são estruturados nos processos finalísticos e como são armazenados, com indicação de todos os parâmetros e propriedades de cada dado (qual o tipo, qual o tamanho, se aceita nulo ou não, se é obrigatório ou não etc.). Deve ser mantido um repositório específico para consulta que contenha o histórico dos MER extraídos do SGBD periodicamente ou em razão de mudança no banco de dados, de forma que o diagrama possa ser acessado a qualquer momento.

Orientações para preenchimento do formulário

- Campo "*Link* para acesso ao diagrama de MER (Modelo Entidade Relacionamento)": inserir o *link* para o arquivo que contém o diagrama do MER do SGBD que utiliza o dado.

8.8. *Link* para acesso a *log*

Log é o registro, em geral em arquivo de texto, dos eventos de interesse ocorridos no sistema, por meio do qual é possível, por exemplo, identificar as causas de um erro do sistema.

Orientações para preenchimento do formulário

- Campo "*Link* para acesso aos *logs* (histórico de transações)": inserir o *link* para o arquivo de *log* que contém todo o histórico de transações executadas no sistema que utiliza o dado.

8.9. Identificação dos processos que utilizam o dado

Todos os processos do órgão ou entidade que utilizam o dado devem ser elencados, por dado e respectivo banco de dados, e identificados pelo nome.

Orientações para preenchimento do formulário

- Campos "Nome do processo 1", "Nome do processo 2" etc.: informar o nome do processo que utiliza o dado. Por exemplo, "Cadastro de instituição de ensino credenciada", "Exame médico", "Efetivação da PPD", "Solicitação de renovação de CNH".

8.10. Instrumento fornecido

Com esta orientação técnica disponibiliza-se, como instrumento, o "Inventário de Dados PGDI Anexo II", planilha eletrônica em arquivo de Excel. Tal disponibilização é feita no Portal do COETIC(http://www.coetic.sp.gov.br/) na página de Governança de Dados e Informações.