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.

Instrução Normativa PGDI-2, de 27-12-2022

APROVA Instrução Normativa PGDI 2 referente Ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Análise dos processos e Ativos de Dados e Informação: Orientação Técnica - Procedimento de Análise Periódica dos Processos e Ativos de Dados e Informações, da Deliberação Normativa CGGDIESP 1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA
Orientação Técnica - Procedimento de Análise Periódica dos Processos e Ativos de Dados e Informações

9. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimentos e práticas à implementação do processo Análise Periódica dos Processos e Ativos de Dados e Informações; Controle do Inventário dos Processos e Ativos de Dados e Informações; e Identificação dos Gestores dos Processos e Ativos de Dados e Informações, 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.
- Disseminar a importância da revisão, da atualização e da classificação periódicas dos inventários de processos e ativos de dados e informações, dada a natureza dinâmica da prestação de serviços, das mudanças normativas, da evolução tecnológica e das mudanças em ambientes produtivos, visando garantir disponibilidade e conformidade com a operação e manter a padronização, a estabilidade e a previsibilidade na execução das regras e atividades operacionais envolvidas.
- Instruir sobre o monitoramento e o acompanhamento das medidas de controle instituídas.

10. Sumário

11. Abrangência

Órgãos e entidades da Administração Pública estadual.

12. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI), considerando, em seu Anexo II, a décima providência, voltada à análise periódica dos processos e ativos de dados e informações, tendo como base o artigo 16 da PGDI – "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 [...]".
- Política de Proteção de Dados Pessoais (PPDP), em especial seu Anexo III.
- Orientação Técnica do CGGDIESP que define modelo padrão e instrui sobre "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", conforme primeira providência requerida pela PPDP, em seu Anexo III.
- Orientação Técnica do CGGDIESP que instrui sobre como fazer o "inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos", conforme quarta providência requerida pela PGDI, em seu Anexo II.
- Norma Técnica ABNT NBR ISO 9001:2015 – Sistemas de Gestão da Qualidade – Requisitos.
- Norma Técnica ABNT NBR ISO 10013:2021 – Sistemas de Gestão da Qualidade – Orientação para Documentação Orientada.
- 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.
- MARQUES, Pedro. Guia completo para ITIL® 4. Desenho de Serviços, [s.d]. Disponível em https://desenhodeservicos.com.br/guia-completo-para-itil4/. Acesso em: 29 jun. 2022.
- CENTER FOR INTERNET SECURITY (CIS). Controles CIS – Versão 8. [s.l.]: CIS, 2021. Disponível em: https://learn.cisecurity.org/cis-controls-download. Acesso em: 28 jun. 2022.

13. Glossário

Termos e siglas	Definição
ABNT	Associação Brasileira de Normas Técnicas.
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.
Checklist	Lista de verificação.
CIS	*Center for Internet Security*, organização sem fins lucrativos com a missão de tornar o mundo tecnológico mais seguro nas questões cibernéticas.
***CIS Controls*® ou Controles CIS®**	Conjunto de melhores práticas, atualmente na versão 8, composto por 18 controles, conhecidos também como salvaguardas, com objetivo de mitigar os ataques cibernéticos mais prevalentes contra sistemas e redes de tecnologia atuais.
Framework	Estrutura composta por um conjunto de códigos genéricos que permite o desenvolvimento de sistemas e aplicações. Funciona como *template* ou modelo que, quando utilizado, oferece elementos estruturais básicos para a criação de uma aplicação ou software, bem como para a aplicação de métodos e controles.
IG	*Implementation Group* (Grupo de Implementação dos Controles CIS®).
Internet das Coisas (IoT)	Sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, e objetos aos quais são vinculados UIDs e que possuem a habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador.
ISO	*International Organization for Standardization* (Organização Internacional de Normalização).
ITIL®	*Information Technology Infrastructure Library* (Biblioteca de Tecnologia da Informação e Infraestrutura).
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.
Lista mestra	Documento do tipo catálogo com lista atualizada de todos os documentos que os órgãos e as entidades utilizam internamente, contendo, no mínimo, o código, a descrição e as datas de revisão desses documentos.
***Log* ou *Log* de dados**	Expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional.
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.
OGC	*Office of Government Commerce* (Escritório de Comércio do Governo do Reino Unido).
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.