APROVA Instrução Normativa CGGDIESP-8/PPDP referente ao Anexo III, 3 – Tabela de Providências Complementares e Responsáveis – Finalidades e Bases legais para Tratamento de Dados Pessoais: **Guia Orientativo e Modelo - 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**, da Deliberação Normativa CGGDIESP-2, de 30/12/2021.

GUIA ORIENTATIVO

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

1. Objetivos

Este guia orientativo tem os seguintes objetivos:

- Recomendar procedimento para elaboração de 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, primeira providência requerida pela Política de Proteção de Dados Pessoais (PPDP), no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021.
- Orientar a utilização do modelo de documento em formato de planilha eletrônica, disponibilizado com esta orientação, para identificação e registro das bases legais dos serviços prestados ao cidadão, da competência na matéria para o tratamento e dos dados pessoais tratados.
- Esclarecer conceitos inerentes ao inventário dos serviços executados e ao registro das atividades de tratamento de dados pessoais realizadas em razão desses serviços, conforme modelo disponibilizado com esta orientação.

2. Sumário

8.1. Preenchimento da aba "Capa"
8.2. Preenchimento da aba "RoPA geral"
8.3. Preenchimento da aba "Atualizações"
8.4. Conceito de serviço público finalístico ou serviço finalístico
8.5. Conceito de processo
8.6. Conceito de processo crítico
8.7. Conceito de procedimento
8.8. Conceito de dado crítico
8.9. Conceitos de dado pessoal e dado pessoal sensível
8.10. Conceito de forma de tratamento de dados pessoais
8.11. Conceito de finalidade
8.12. Conceitos de base normativa e base legal
8.13. Instrumento fornecido
8.14. Inventário das demais atividades de tratamento de dados

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI).
- de Proteção de Dados Pessoais (PPDP), considerando, em seu Anexo III, a primeira providência, Documento com a relação das finalidades e atribuição das bases legais, contendo informações sobre: serviços prestados ao cidadão; competência na matéria para o tratamento; e quais dados pessoais serão coletados.
- Decreto Estadual nº 48.897, de 27 de agosto de 2004, que dispõe sobre os Arquivos Públicos, os documentos de arquivo e sua gestão, os Planos de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo, define normas para a avaliação, guarda e eliminação de documentos de arquivo.
- 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).
- ANPD. Guia orientativo – Tratamento de dados pessoais pelo Poder Público. [Brasília]: ANPD, jan. 2022.

5. Glossário

Termos e siglas	Definição
ANPD	Autoridade Nacional de Proteção de Dados. Órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Termos e siglas	Definição
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.
Gestão de Riscos	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.
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.
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).
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. Introdução e contexto

"Conhece-te a ti mesmo" é um aforismo grego que revela a importância do autoconhecimento e que cabe muito bem na governança de dados. Não há certeza em relação ao autor dessa máxima, mas muitos a atribuem ao sábio grego Tales de Mileto.

"Não é possível gerenciar o que não se conhece." Essa máxima foi reproduzida inúmeras vezes na história, sendo a citação mais famosa a de William Edwards Deming (1900-1993) que, no início dos anos 1950 disse: "Não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende, e não há sucesso no que não se gerencia".

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, a instituição 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.

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

O 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, primeira providência requerida pela PPDP, é resultado da ação de inventariar os serviços para permitir que outros processos de proteção de dados pessoais, inclusive dados pessoais sensíveis, sejam implementados ou adequados com base nas informações levantadas. No âmbito da LGPD, tal documento é conhecido como RoPA e deve ser uma base de conhecimento para a aplicação da governança de dados e informações.

7. Estrutura do documento RoPA (modelo padrão)

- Coleta/processamento.
- Acesso aos dados.
- Compartilhamento/transferência de dados.
- Armazenamento de dados.
- Eliminação.
- Exceções do processo.
- Classificação do processo.
- Análise de impacto do processo.

8. Orientações para utilização do modelo

Orienta-se mapear os serviços finalísticos executados pelo órgão ou entidade e registrar as atividades de tratamento de dados pessoais por meio da planilha eletrônica "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", disponibilizada com esta orientação. Trata-se de modelo de inventário de serviços e processos, composto de campos para preenchimento por meio de digitação ou seleção de item em lista predefinida, construído com objetivo de nortear e padronizar a elaboração 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, tendo em vista a implementação da PPDP em toda a Administração Pública estadual e a adequação à LGPD do tratamento de dados pessoais realizado por seus órgãos e entidades.

Esse modelo é composto de três abas: "Capa", "RoPA geral" e "Atualizações". Para auxiliar a compreensão e o registro das informações requeridas, a seguir estão elencadas orientações para seu preenchimento e, na sequência, são apresentados conceitos relacionados a campos do documento acompanhados, quando pertinente, de considerações (notas) concernentes à Gestão de Riscos, ao inventário de processos e serviços finalísticos e à política de privacidade e tratamento de dados pessoais.

8.1. Preenchimento da aba "Capa"

Na parte superior os campos devem ser preenchidos manualmente.

- Campo "Data da criação": informar a data de criação do RoPA.
- Campo "Data da atualização": informar a data da última atualização do RoPA.
- Campo "Bloco de serviços/programas/ações": informar o nome do serviço ao qual se refere o RoPA.
- Campo "Área responsável": informar o nome da área responsável pelo serviço.
- Campo "Órgão ou entidade": informar o nome do órgão ou da entidade que executa o serviço.
- Campo "Secretaria vinculada": informar o nome da Secretaria à qual o órgão/entidade está vinculado.
- Campo "Responsável pelo preenchimento": informar o nome da pessoa que preencheu o RoPA.
- Campo "Responsável pela proteção de dados": informar o nome do encarregado de dados pessoais.

Na parte inferior os campos não requerem preenchimento manual.

- Coluna "Tratamento de dados": contém as oito ações de tratamento de dados que deverão ser preenchidas na aba "RoPA geral".
- Coluna "Preenchimento": é preenchida de forma automática de forma a evidenciar o *status* de preenchimento das ações de tratamento de dados na aba "RoPA geral".
- Coluna "É necessária uma avaliação de impacto?": é preenchida de forma automática de acordo com o preenchimento da aba "RoPA geral". Quando apresenta "Sim", em vermelho, indica alerta para avaliação de impacto. Quando apresenta "Não", indica que, aparentemente, a avaliação de impacto não será necessária, porém, deve ser realizada análise das respostas registradas no documento. De maneira complementar, deve-se observar a trigésima providência da PGDI e a sétima providência da PPDP, que orientam quanto à Gestão de Riscos e ao Relatório de Impacto (RIPD), respectivamente.
- Gráfico "Atividades concluídas x Total a realizar": representa os avanços no preenchimento da planilha na aba "RoPA geral", para cada um dos temas.
- Gráfico "Evolução do preenchimento": apresenta o percentual de preenchimento da aba "RoPA geral" já realizado em relação ao total necessário.

8.2. Preenchimento da aba "RoPA geral"

Todas as colunas da aba "RoPA geral" devem ser preenchidas de acordo com os serviços e processos executados pelo órgão/entidade. Aquelas que, em seu canto superior direito, contêm uma indicação vermelha apresentam, em nota *pop-up*, uma explicação sobre o preenchimento. As demais colunas têm títulos autoexplicativos.

8.3. Preenchimento da aba "Atualizações"

A aba "Atualizações" deve ser preenchida de acordo com as alterações feitas no processo ao qual o RoPA se refere.

- Campo "ID": informar o ID do processo alterado.
- Campo "Data": informar a data da alteração do processo.
- Campo "Alterações": descrever as alterações ocorridas no processo.
-

8.4. Conceito de serviço público finalístico ou serviço finalístico

Diz respeito à atividade-fim prestada pela Administração Pública estadual, diretamente (incluindo as funções públicas) ou em regime de autorização, concessão ou permissão, e voltada aos cidadãos ou aos usuários do serviço público. Corresponde ao processo de negócios do setor privado. Em geral, um serviço finalístico é compreendido por diversos processos (ver item 8.5 desta orientação).

São exemplos de serviço finalístico:

- habilitação ou regularização do fornecimento de água no Jardim Primavera em Jundiaí;
- confecção de Carteira Nacional de Habilitação (CNH) ou atualização do cadastro de condutor com informações sobre sua deficiência física;
- aprovação de contratação de financiamento imobiliário, renegociação de dívida ou amortização de saldo devedor de apartamento na Vila Galvão em Guarulhos;
- confecção de Relatório de Impacto Ambiental para projeto de implantação de usina de cana-de-açúcar no Vale do Paraíba ou inspeção de denúncia ambiental em área rural próxima ao Rio Paraná em Rubineia;
- aferição de bombas de combustível nos postos de abastecimento da Grande São Paulo.

Nota a respeito do serviço finalístico na Gestão de Riscos

A Gestão de Riscos avalia o impacto (estimado) ao serviço finalístico. Ela deve estimar e avaliar as consequências (impactos) para o Estado e os titulares de dados pessoais (caso sejam afetados), que possam prejudicar ou interromper a condução natural do serviço finalístico como um todo em caso de ocorrência de falha ou de exploração de vulnerabilidade.

São exemplos de impacto a serviços finalísticos:

- para o Estado: a impossibilidade de cumprir seu papel e de prestar serviços públicos;
- para o cidadão: a impossibilidade de receber um serviço de direito e/ou o fato de ter seus dados pessoais vazados e utilizados para fins que o prejudiquem.

8.5. Conceito de processo

Processo é um conjunto de atividades/tarefas que têm sequência lógica e são estruturadas para a produção de resultado que gere valor ao cidadão e à sociedade por meio da entrega de um produto ou serviço.

São exemplos de processo:

- aqueles executados, rotineira ou excepcionalmente, para possibilitar a habilitação ou a regularização do fornecimento de água, que é de fato objeto do serviço finalístico, entre eles:
    - verificação da documentação enviada;
    - comprovação do pagamento correspondente;
    - aprovação ou reprovação da solicitação;
    - acionamento da equipe técnica para ligação inicial do fornecimento de água;
    - verificação de causa da interrupção do fornecimento de água;
    - acionamento das equipes de manutenção e reparo;
    - constatação de ausência de pendências financeiras do cliente;
    - aprovações e atualização do cadastro de clientes;
    - emissão de boleto de cobrança correspondente.
- aqueles executados, rotineira ou excepcionalmente, para possibilitar a confecção de CNH ou atualização do cadastro de condutor com informações sobre deficiência física, que são de fato os objetos do serviço finalístico, entre eles:
    - verificação da documentação enviada;
    - conferência de comprovação de pagamento da taxa correspondente;
    - conferência de comprovação de aprovação em exame de direção emitido por Centro de Formação de Condutores credenciado;
    - conferência de aprovação de exames médicos (oftalmológico ou toxicológico) e psicotécnicos exigidos para a categoria de habilitação solicitada;
    - constatação via laudo pericial, para caso de indicação de deficiência física;
    - aprovação ou reprovação da solicitação;
    - atualização do cadastro de condutor;
    - emissão da CNH (nova ou com a indicação de deficiência física do condutor).

- aqueles executados, rotineira ou excepcionalmente, para possibilitar a aprovação de contratação de financiamento imobiliário, renegociação de dívida ou amortização de saldo devedor, que são de fato objetos do serviço finalístico, entre eles:
    - verificação da documentação enviada;
    - análise de crédito do solicitante;
    - aprovação de contratação;
    - aprovação da renegociação de dívida;
    - emissão de contrato de mutuário;
    - análise e acionamento de inadimplentes;
    - emissão de boleto de cobrança correspondente;
    - comprovação do pagamento correspondente;
    - encaminhamento para gestão de pagamentos e recebíveis;
    - emissão de comprovante de quitação de dívida;
    - suspensão ou revogação de contrato;
    - emissão de escritura definitiva do imóvel.
- aqueles executados, rotineira ou excepcionalmente, para possibilitar a confecção de Relatório de Impacto Ambiental ou a inspeção de área objeto de denúncia ambiental, que são de fato objetos do serviço finalístico, entre eles:
    - verificação da documentação enviada;
    - análise de impacto ambiental;
    - compilação das aprovações ambientais;
    - verificação de incidentes ambientais ocorridos no período;
    - determinação dos impactos sofridos;
    - detalhamento das ações de contenção e regularização empregadas;
    - confecção e aprovação do Relatório de Impacto Ambiental;
    - emissão de multas;
    - emissão da relação de Relatórios de Impacto Ambiental emitidos no período.
- aqueles executados, rotineira ou excepcionalmente, para possibilitar a aferição de instrumentos e equipamentos, regulamentados e certificados, conforme os requisitos técnicos exigidos pela legislação, que é de fato o objeto do serviço finalístico, entre eles:
    - inventário de bombas de combustível;
    - inventário de balanças;
    - histórico das medições executadas em bombas de combustível;
    - histórico das medições executadas em balanças;
    - detalhamento das inconsistências ou irregularidades encontradas;
    - detalhamento das ações de ajuste empregadas e/ou recomendadas;
    - emissão de multas;

- emissão do Relatório de Instrumentos de Medição aferidos no período.

Existem processos que não são etapas nem elementos que componham diretamente um serviço finalístico, a saber:

- Atividade-meio: Conforme nomenclatura dada pelo Arquivo Público do Estado de São Paulo, tanto no Plano de Classificação, quanto na Tabela de Temporalidade, atividade-meio se refere a ação, encargo ou serviço que um órgão leva a efeito para auxiliar e viabilizar o desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter instrumental e acessório (Decreto Estadual nº 48.897/2004, artigo 17, inciso I). Essas atividades também podem ser entendidas como processos, pois dão suporte aos serviços finalísticos. Devem, então, ser objeto de avaliação com vistas a verificar se os mecanismos de proteção e controle existentes se encontram adequados e suficientes para a preservação da disponibilidade dos serviços finalísticos, dos sistemas e dos dados, bem como para a preservação da autenticidade, integridade e confidencialidade dos dados e das informações.
- Atividade-fim: Conforme nomenclatura dada pelo Arquivo Público do Estado de São Paulo, tanto no Plano de Classificação, quanto na Tabela de Temporalidade, atividade-fim se refere a ação, encargo ou serviço que um órgão leva a efeito para o efetivo desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter substantivo e essencial para o seu funcionamento (Decreto Estadual nº 48.897/2004, artigo 17, inciso II).

São exemplos de processo-meio associado à tecnologia da informação:

- Processo de Gestão de Mudanças (ao qual é atribuída a maioria das interrupções não programadas em ambientes produtivos);
- Processo de Gestão de Incidentes de Segurança da Informação;
- Processo de Gestão da Capacidade Produtiva;
- Processo de Gestão da Produção;
- Processo para Gestão da Atualização Periódica de *Software*;
- Processo para Gestão de Proteção contra Código Malicioso ou Nocivo (Antivírus, Antimalware etc.);
- Processo de Contratação e Gestão de Fornecedores;
- Processo para Operações e Armazenamento de Dados;
- Processo para Gerenciamento de Metadados;
- Processo para Execução e Controle de Inventário de Sistemas e Tecnologias;
- Processo para Gestão do Controle de Acessos Físicos;
- Processo para Gestão da Proteção Perimetral de Ambientes Críticos e de Acesso Controlado;
- Processo para Gestão do Controle de Acessos Lógicos e Autenticação de Identidades;
- Processo para Definição de Perfis e Autorização de Privilégios;

- Processo de Gestão da Configuração de Sistemas e Equipamentos;
- Processo para Gestão e Controle da Virtualização de Recursos;
- Processo para Gestão de Cópias de Segurança (*Backups*);
- Processo de Gestão e Monitoramento de Redes;
- Processo para Controle de Recepção e Descarte de Equipamentos;
- Processo para Controle de Mídias Móveis (Fitas, Discos Removíveis, *Pen-drives* etc.);
- Processo para Controle de Dispositivos Pessoais (*Notebooks*, *Tablets* e Celulares);
- Processo para Desenvolvimento de Sistemas e Aplicativos;
- Processo para Aquisição de Produtos (HW e SW);
- Processo para Gestão da Segurança da Informação;
- Processo para Monitoramento de Controles;
- Processo para Gestão de *Compliance*;
- Processo para Continuidade de Negócio e Recuperação de Desastres.

Os processos podem determinar o tratamento de dados pessoais e/ou dados pessoais sensíveis. Nesses casos, eles são objeto da LGPD e devem estar adequados às suas normas e exigências.

Nota a respeito do processo na Gestão de Riscos

A Gestão de Riscos avalia a exposição (vulnerabilidade) na tecnologia (infraestrutura, equipamentos ou sistemas) ou nos procedimentos que instrumentalizam o processo. Ela deve identificar e avaliar as exposições ou deficiências (vulnerabilidades) presentes na infraestrutura, nos equipamentos, nos sistemas ou nos procedimentos, as quais tornem o processo vulnerável e exposto à situação de exploração intencional ou frágil, bem como à ocorrência acidental, e tragam, por conseguinte, um risco à boa execução do serviço finalístico ou à privacidade dos titulares de dados pessoais envolvidos.

São exemplos de vulnerabilidade na tecnologia ou no procedimento:

- armazenamento de todos os dados necessários à execução do processo (dados comuns, dados críticos, dados pessoais e/ou dados pessoais sensíveis) em única bateria de discos, o que expõe o processo a interrupção em caso de quebra dos discos;
- *data center* secundário sem proteção perimetral (barreiras físicas) adequada ou sem controles de acesso físico (controladores de acesso ou vigilantes) suficientes para inibir a entrada de pessoas não autorizadas, o que expõe os dados a acesso não autorizado e uso indevido;
- sistema ABC sem controle nem supervisão de acesso, o que expõe os dados a acesso não autorizado e uso indevido;
- rede de telecomunicações sem *firewall* ativado, o que expõe os dados a acesso não autorizado e uso indevido;
- procedimento de remoção dos dados não mais necessários ao serviço finalístico sem dispositivo que verifique ou assegure que todas as informações foram realmente

destruídas e não podem mais ser recuperadas por engenharia reversa ou outro artifício, o que expõe os dados a acesso não autorizado e uso indevido;

- funcionários de administração da base de dados não capacitados para a execução da criptografia dos dados armazenados, o que expõe os dados a perda de disponibilidade caso a criptografia não possa ser corretamente revertida (decriptografia) para uso regular dos sistemas.

Nota a respeito do processo no inventário de processos e serviços finalísticos

A necessidade de execução de inventário recai, em especial, sobre o serviço finalístico, pois a LGPD faz exigências explícitas à identificação e à transparência da finalidade do tratamento de dados pessoais, e a finalidade é uma característica intrínseca ao serviço finalístico. Entretanto, na prática, são os processos – componentes ou de apoio a um serviço finalístico – que devem ser avaliados acerca dos mecanismos de proteção e controle adequados à sua missão e natureza a fim de se mitigar sua exposição. Para tanto, deve-se considerar todos os processos que fazem tratamento de dados (incluindo dados pessoais e/ou dados pessoais sensíveis) ou atuam na gestão e no controle dos equipamentos e sistemas responsáveis por fornecer suporte e apoio aos serviços finalísticos.

As atividades-meio devem ser incluídas no inventário em duas situações: quando elas são parte de um processo crítico para a execução do serviço finalístico e/ou quando nelas ocorrem tratamento de dados pessoais, dados pessoais sensíveis ou dados pessoais de crianças e adolescentes.

Nota a respeito do processo na política de privacidade e tratamento de dados pessoais

A política de privacidade e tratamento de dados pessoais deve ser elaborada apenas para os serviços finalísticos prestados aos cidadãos ou aos usuários do serviço público pelo órgão ou entidade, pois é ao serviço finalístico que é atribuída base normativa (ver orientação técnica relativa à décima segunda providência da PPDP).

8.6. Conceito de processo crítico

Processo crítico é todo processo cuja interrupção pode causar a paralização do serviço finalístico, impedindo que ele seja disponibilizado, bem como todo processo que utilize dados críticos, uma vez que, quando o processo é mal controlado ou impactado, pode-se colocar os dados críticos em situação de vulnerabilidade.

8.7. Conceito de procedimento

Trata-se do detalhamento técnico e sequencial de todas as atividades necessárias à execução de um processo.

São exemplos de procedimento:

a. relacionados a interrupção no fornecimento de água:

- recebimento de chamado com reclamação sobre a interrupção do fornecimento de água;
- verificação de possível inadimplência no pagamento por parte do usuário do serviço público:
    - verificação, no sistema financeiro, de pagamento ou não da última conta de água;
    - solicitação de envio do comprovante de pagamento da última conta de água;
    - contato com agente financeiro para verificar possíveis erros;
    - solicitação de regularização da situação de inadimplência no sistema financeiro;
    - emissão de segunda via da conta de água e solicitação do pagamento;
    - confirmação de regularização de pagamento;
- conferência da localidade reportada com falta de água:
    - verificação, na Central de Atendimento, da existência ou não de notificação anterior para a localidade;
    - verificação de identificação ou não da causa do problema na localidade;
    - verificação de acionamento ou não de equipe de atendimento técnico para investigação do problema na localidade;
    - acionamento de equipe de investigação da possível causa da interrupção do fornecimento de água;
    - registro de data e hora do acionamento das equipes de investigação;
    - aviso sobre o acionamento da equipe de investigação e a estimativa de prazo para a análise, em horas;
- aviso sobre a existência de notificação anterior para a localidade, o acionamento da equipe de investigação e a estimativa de prazo para a análise, em horas;
- aviso sobre a existência de notificação anterior para a localidade, a identificação do problema pela equipe de investigação e a estimativa de prazo para a solução (regularização do fornecimento de água), em horas;
- confirmação de causa-raiz (depois de confirmada a causa da interrupção do fornecimento de água):
    - acionamento de equipe de manutenção para correção;
    - registro de data e hora do acionamento de equipe de manutenção;
- confirmação de regularização do reparo (depois de confirmada a regularização do fornecimento de água):
    - documentação da causa-raiz;

        - documentação da solução empregada no reparo;
        - registro de data e hora da regularização;
        - registro de período de interrupção do fornecimento de água (horas passadas desde o primeiro acionamento até a regularização final);

    - comunicação da regularização do fornecimento para o cidadão;
    - encerramento do atendimento.

b. relacionados a alteração cadastral para inclusão de condição de deficiência física de condutor:

    - recepção e conferência da documentação recebida do solicitante;
    - agendamento de perícia médica;
    - consulta com avaliação médica;
    - emissão do laudo pericial;
    - conferência do laudo pericial;
    - solicitação das aprovações correspondentes;
    - atualização do cadastro do condutor com deficiência física;
    - emissão da CNH com as devidas alterações;
    - armazenamento das aprovações e dos documentos desenvolvidos pelo tratamento para efeito comprobatório.

c. relacionados a contratação de financiamento imobiliário:

    - recepção e conferência da documentação recebida do solicitante;
    - verificação do histórico de crédito e de pagamento de empréstimos no próprio órgão ou em bases de cadastro positivo ou em outras referências comerciais;
    - verificação da capacidade de pagamento (conferência de holerite e outras fontes de renda);
    - verificação do nível atual de endividamento (em instituições financeiras);
    - verificação da existência de bens que podem ser utilizados como garantia de dívida;
    - especificação do valor máximo de crédito;
    - levantamento da lista de imóveis disponíveis para financiamento que estejam na região indicada pelo solicitante e possuam valor de financiamento abaixo do limite máximo de crédito especificado;
    - agendamento de vistoria do imóvel selecionado;
    - estabelecimento das condições do financiamento;
    - aprovação/rejeição da negociação contratual;
    - elaboração do contrato de financiamento;
    - assinatura do contrato de financiamento;
    - emissão do boleto com a fatura inicial e encaminhamento para o setor de cobrança.

8.8. Conceito de dado crítico

Diversos fatores podem levar a instituição a classificar um dado como crítico. Em geral, são considerados dados críticos institucionais ou corporativos:

- informações, números, textos, índices, documentos, métodos e procedimentos operacionais que sejam essenciais para o bom funcionamento dos órgãos e entidades ou tenham relação direta com os serviços finalísticos prestados pela Administração Pública estadual ou com os serviços e produtos vendidos por uma empresa privada:
    - sem que esses dados estejam disponíveis, íntegros e protegidos de acesso ou uso indevido, o serviço finalístico sofre impactos temporários ou pode ser interrompido.
- aqueles que, por sua natureza, não podem ser facilmente criados ou reproduzidos em caso de destruição, roubo ou perda:
    - sem que esses dados estejam disponíveis, íntegros e protegidos de acesso, uso indevido ou destruição, o serviço finalístico sofre impactos permanentes ou pode ser definitivamente interrompido.
- informações, análises, estratégias, documentos ou relatórios confidenciais cuja interceptação ou captura possa comprometer um ativo importante, pois se trata de capital intelectual:
    - sem que esses dados estejam disponíveis, íntegros e protegidos de acesso, uso indevido, subtração ou destruição, a instituição sofre impactos severos que certamente prejudicarão sua capacidade de prestação de serviços e poderão, no limite, levar a seu desmantelamento.

O Estado brasileiro, por meio da LGPD, estabeleceu mais duas categorias de dado crítico, na medida em que as determinações dessa Lei deram, para as instituições, o alerta de que, além dos critérios de criticidade já adotados – que avaliam, em geral, os impactos sofridos pela própria instituição –, o tratamento de dados pessoais, quando mal executado, pode causar prejuízos aos titulares dos dados, acarretando efeitos e consequências negativas para além das atividades-fim e das atividades administrativas da instituição. O tratamento de dados pessoais e de dados pessoais sensíveis deve, portanto, ser realizado com emprego de maior atenção e controle, a exemplo do que se faz com os demais dados críticos.

8.9. Conceitos de dado pessoal e dado pessoal sensível

De acordo com a LGPD, em seu artigo 5º, inciso I, **dado pessoal** é toda informação relacionada à pessoa natural identificada ou identificável. Trata-se de referenciais singulares que permitem a identificação de um indivíduo ou possibilitam, direta ou indiretamente a partir do cruzamento com outras informações, encontrar um indivíduo, isolá-lo de uma massa de pessoas e se referir a ele

de forma direta e inequívoca. São exemplos de dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP (Protocolo da Internet) e *cookies*.

Por sua vez, **dado pessoal sensível**, de acordo com a LGPD, em seu artigo 5º, inciso II, é todo 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, dado genético ou biométrico, quando vinculado a uma pessoa natural. Trata-se de dados privados que precisam de maior sigilo e cuidado ainda mais estrito por parte de quem os trata, pois podem ser utilizados para fins discriminatórios ou para prejuízo direto à pessoa a partir de julgamentos morais. São exemplos de dado pessoal sensível: origem racial ou étnica, prontuário de saúde, dados biométricos (genoma do DNA, impressão digital, fotografia do rosto, gravação do tom e timbre da voz) usados em autenticação de acesso, dados sobre orientação religiosa ou política e dados sobre a vida sexual.

8.10. Conceito de forma de tratamento de dados pessoais

Trata-se das operações realizadas para tratamento ou processamento de dados pessoais. O tratamento pode ser:

- recepção, coleta, captura, extração ou produção;
- acesso, visualização, leitura ou utilização;
- edição, alteração, manipulação, modificação, transformação, reprodução ou duplicação;
- comunicação, divulgação, difusão, distribuição, destinação, transferência internacional, transmissão, compartilhamento ou transporte;
- avaliação, análise, catalogação, tabulação ou classificação;
- arquivamento ou armazenamento;
- deleção, eliminação, descarte ou destruição;
- anonimização, criptografia, proteção ou controle da informação.

Nota a respeito da forma de tratamento no inventário de processos e serviços finalísticos

Deve-se identificar as operações realizadas no tratamento de dados do processo em análise e avaliar se os mecanismos de proteção e controle adotados são eficazes e suficientes para a preservação da disponibilidade, da integridade, da garantia de autenticidade e da confidencialidade dos dados em tratamento. Adicionalmente, pode-se verificar se o tratamento de dados é feito de maneira totalmente automatizada (por meio de sistemas autônomos, robotizados e/ou emprego de algoritmos de inteligência artificial) ou se há intervenção humana em estágios decisórios e/ou sensíveis do processo. Essa identificação é importante porque, para cada forma de tratamento ou tipo de operação realizada, deve ser estabelecido um conjunto específico de ações,

medidas ou mecanismos de proteção e controle apropriados para a preservação da disponibilidade, da integridade, da garantia de autenticidade e da confidencialidade dos dados em tratamento.

Nota a respeito do compartilhamento no inventário de processos e serviços finalísticos

Deve-se inserir as informações relativas ao compartilhamento de dados pessoais e de dados pessoais sensíveis com terceiros, sempre que ele ocorrer no serviço mapeado. Qualquer atividade de transferência, uso compartilhado e compartilhamento de dados pessoais deve observar as diretrizes da PPDP:

> **Artigo 17.** O uso compartilhado de dados pessoais pela Administração Pública estadual atende a finalidades específicas de execução de políticas públicas e atribuição legal e respeita os princípios de proteção de dados pessoais previstos na LGPD.
>
> §1º – Os dados pessoais devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos e à descentralização da atividade pública.
>
> §2º – Sem prejuízo dos dados pessoais armazenados em meios físicos, as operações de tratamento devem se dar preferencialmente por meio da Central de Dados do Estado de São Paulo (CDESP).
>
> §3º – O compartilhamento de dados pessoais no âmbito da Administração Pública estadual dar-se-á mediante acesso de agentes públicos designados e habilitados, por meio da CDESP, preferencialmente.

8.11. Conceito de finalidade

Trata-se de característica intrínseca ao serviço finalístico, visto que ele tem uma finalidade específica para servir ao cidadão ou à sociedade.

Nota a respeito da finalidade no inventário de processos e serviços finalísticos

Para que se cumpra a exigência da LGPD de informar com transparência ao cidadão a finalidade específica de um tratamento de dados e os dados pessoais que serão coletados e tratados no âmbito de um serviço finalístico, deve-se mapear esses atributos para cada serviço finalístico separadamente.

8.12. Conceitos de base normativa e base legal

A **base normativa** é aquilo que dá legitimidade à execução do serviço finalístico. Constitui-se de Lei, Decreto, Portaria, Resolução, Norma ou, ainda, respaldo em contratos, convênios e instrumentos congêneres a respeito de uma política pública ou atribuição e competência legal do órgão ou entidade.

A **base legal** refere-se à hipótese prevista na LGPD para o tratamento de dados pessoais nos processos dos serviços finalísticos. A ANPD, em seu *Guia orientativo* (2022), orienta que:

> Uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no artigo 7º ou, no caso de dados sensíveis, no artigo 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no artigo 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público.

Nota a respeito da base normativa e da base legal no inventário de processos e serviços finalísticos

Visto que a base normativa que legitima a execução do serviço finalístico é distinta da base legal para o tratamento de dados pessoais, é imprescindível a identificação de ambas. Por exemplo, qualquer que seja a base normativa ou o contrato, convênio ou instrumento congênere identificado para um serviço finalístico referente à execução de uma política pública, o tratamento de dados pessoais nele realizado terá como base legal o artigo 7º, inciso III, da LGPD:

> **Artigo 7º.** O tratamento de dados pessoais somente poderá ser realizado [...]
>
> III – pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

Por sua vez, o tratamento compartilhado de dados pessoais sensíveis terá como base legal prevista o artigo 11, inciso II, alínea b, da LGPD:

> **Artigo 11.** O tratamento de dados pessoais sensíveis somente poderá ocorrer [...]
>
> II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para [...]
>
> b) tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos.

Deve-se observar que a LGPD é mais restritiva quando se trata de dados sensíveis e que seu artigo 11 não faz referência às políticas públicas instituídas em ajustes contratuais, convênios ou instrumentos congêneres, mas sim àquelas instituídas por meio de leis e regulamentos. Nesse sentido, algumas diretrizes foram estabelecidas pela PPDP:

> **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 consideram:

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.

No modelo disponibilizado com esta orientação, o campo referente à base legal apresenta uma lista previamente elaborada com as possíveis bases legais e seus artigos estabelecidos pela LGPD para tratamento de dados pessoais e dados pessoais sensíveis, permitindo que o preenchimento se dê pela seleção do item adequado a cada serviço mapeado.

8.13. Instrumento fornecido

Com esta orientação disponibiliza-se, como instrumento, o "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", 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.

8.14. Inventário das demais atividades de tratamento de dados

Finalizado o inventário dos serviços finalísticos voltados ao cidadão, orienta-se mapear os demais serviços executados pelo órgão/entidade que tratam dados pessoais e dados pessoais sensíveis e

registrar as atividades desse tratamento, ações nas quais se pode utilizar o procedimento abordado nesta orientação.