SÃO PAULO
GOVERNO DO ESTADO

CONTROLADORIA GERAL DO ESTADO
Ouvidoria Geral do Estado

Metodologia para Autoavaliação da Aderência à Política de Proteção a Dados Pessoais - PPDP

Versão 1

JANEIRO/2026

Sumário

Metodologia para Autoavaliação da Aderência à Política de Proteção a Dados Pessoais – PPDP

1. Introdução

A Controladoria Geral do Estado de São Paulo, por meio da Ouvidoria Geral do Estado, apresenta esta metodologia com o propósito de orientar os órgãos da Administração Direta na realização da autoavaliação do nível de aderência à Política de Proteção de Dados Pessoais (PPDP).

O instrumento foi concebido para fortalecer a governança de dados pessoais, estimular a cultura de privacidade e promover a melhoria contínua das práticas de conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e com as normas estaduais complementares.

Ao aplicar esta metodologia, os órgãos públicos poderão identificar seu nível de maturidade em proteção de dados, planejar ações de aprimoramento e consolidar práticas institucionais alinhadas aos princípios da transparência, responsabilidade e segurança da informação.

2. Objetivo

A avaliação da aderência à Política de Proteção a Dados Pessoais (PPDP) será realizada com base nas respostas obtidas através do questionário proposto. O objetivo é apresentar um panorama do nível de conformidade da organização em relação aos requisitos legais e boas práticas de governança de dados e proteção da privacidade, de acordo com o Anexo III– Deliberação Normativa 02 - CGGDIESP.

3. Estrutura da Metodologia

A metodologia será dividida em etapas para garantir uma autoavaliação abrangente, conforme segue:

1. Coleta de Dados
2. Pontuação das Respostas
3. Identificação do Nível de Aderência
4. Análise Detalhada
5. Relatório de Aderência à Política de Proteção de Dados
6. Plano de Ação

4. Etapas da Avaliação

4.1. Coleta de Dados

O questionário será distribuído aos pontos focais indicados pelas chefias de gabinete de cada órgão da Administração Direta, respeitando o período estabelecido no calendário

definido por Resolução. Em seguida, as respostas serão coletadas e compiladas para análise subsequente.

4.2. Pontuação das Respostas

Cada resposta do questionário será pontuada de acordo com a seguinte escala:

- Sim: 2 pontos
- Parcialmente/Em Implementação: 1 ponto
- Não: 0 pontos

A pontuação de aderência à PPDP é calculada com base na média simples das respostas em cada categoria temática do questionário e, posteriormente, na média simples global entre todas as categorias.

A média de cada categoria é obtida somando-se os pontos das perguntas e dividindo-se pelo total de perguntas da categoria.

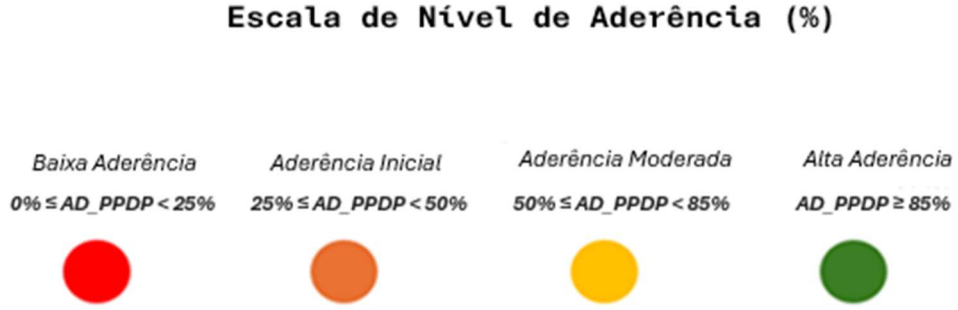
A média global é calculada somando-se todos os pontos obtidos e dividindo-se pelo total de perguntas do questionário.

Para apresentação final, as médias são convertidas em percentuais, considerando o valor máximo possível (2 pontos) como equivalente a 100%. Assim, utiliza-se a seguinte fórmula:

$$\text{Nível de Aderência (\%)} = \left(\frac{\text{Média obtida}}{2}\right) \times 100$$

4.3. Faixa indicativa de Aderência

Com base na pontuação total obtida, será identificada a faixa indicativa de aderência, que se enquadrará em uma das seguintes categorias:



4.4. Análise Detalhada

Para uma análise mais granular, cada seção do questionário será organizada em cinco categorias principais, que serão avaliadas individualmente e em conjunto. Essa abordagem permitirá identificar com maior precisão as áreas que demandam melhorias.

4.5. Relatório de Aderência à Política de Proteção de Dados

(Produto – KR previsto para 2027)

Sumário Executivo:
Visão geral da avaliação, metodologia empregada e principais conclusões sobre o grau de aderência à PPDP do Estado de São Paulo.

Resultados Detalhados:
Apresentação dos resultados obtidos, com nível de aderência e classificação global e por categoria.

Análise de Lacunas:
Identificação dos elementos ou categorias com menor aderência, fragilidades ou pontos de atenção para o aprimoramento da governança de dados pessoais, incluindo o nível de impacto e os riscos associados a cada lacuna.

Recomendações:
Ações específicas para aprimorar a aderência à PPDP, organizadas por prioridade (curto, médio e longo prazo). Esse item contempla os planos de ação elaborados pelos pontos focais dos órgãos, com base nos resultados do questionário de aderência e em conformidade com o calendário definido na Resolução de que regulamenta a matéria.

4.6. Plano de Ação

Com base na análise das lacunas identificadas, serão definidas as prioridades de intervenção, dando foco às categorias que demandam atenção imediata. As ações corretivas necessárias serão especificadas de forma clara, com a designação dos responsáveis pela sua execução e a definição de prazos para conclusão. Além disso, será instituído um processo de monitoramento contínuo para acompanhar a evolução da aderência até a plena conformidade, promovendo melhorias permanentes.

5. Categorias de Avaliação.

Governança de Dados Pessoais
Avaliação da existência da conformidade e aplicação efetiva de políticas e normas que orientam o tratamento de dados pessoais, alinhadas à PPDP.

Coleta e Uso de Dados Pessoais
Verificação da conformidade das práticas institucionais com os princípios da LGPD, com ênfase na finalidade, necessidade, adequação e transparência no tratamento de dados pessoais.

Encarregado de Dados Pessoais
Avaliação dos fluxos institucionais de comunicação e de atuação do Encarregado de Dados Pessoais, em conformidade com as atribuições previstas na LGPD e nas instruções normativas estaduais.

Armazenamento, Transferência e Eliminação
Avaliação das práticas institucionais relacionadas ao armazenamento seguro, à transferência e ao uso compartilhado de dados pessoais, bem como aos procedimentos de eliminação, em conformidade com a LGPD e as instruções normativas estaduais.

Segurança e Incidentes com Dados Pessoais
Avaliação da existência de procedimentos técnicos para identificação, comunicação e tratamento de incidentes envolvendo dados pessoais, em conformidade com os princípios da LGPD e as diretrizes institucionais estaduais.

6.Conclusão

A metodologia proposta para a avaliação da aderência à Política de Proteção de Dados Pessoais (PPDP) adota uma abordagem estruturada, técnica e transparente, permitindo identificar o nível de aderência dos órgãos da Administração Direta do Estado de São Paulo com as diretrizes da Deliberação Normativa 02 - CGGDIESP, de 30 de dezembro de 2021. Ao combinar questionários temáticos com critérios de pontuação objetivos, classificação padronizada e análise por categoria, o modelo oferece um diagnóstico para subsidiar a definição de planos de ação voltados à melhoria contínua.

A conversão das pontuações em níveis percentuais de aderência, associada à elaboração de relatórios analíticos e à elaboração de plano de ação, fortalece a governança pública de dados, estimula o desenvolvimento de uma cultura institucional voltada à privacidade e à proteção de dados e apoia as unidades na evolução de suas práticas, em sintonia com as exigências legais e sociais por maior proteção das informações pessoais dos cidadãos. A inclusão de mecanismos de monitoramento e o foco na priorização de fragilidades demonstram o compromisso da Controladoria Geral do Estado com uma cultura institucional de melhoria contínua e evolução na proteção de dados pessoais.

Anexo I – Questionário a ser aplicado

1. Governança de Dados Pessoais

1.1 Políticas, Normas e Regras para Tratamento de Dados Pessoais

O órgão disponibiliza em sua página eletrônica a Política de Privacidade e Tratamento de Dados Pessoais instituída pelo CGGDIESP, ou política própria adaptada, nos termos do artigo 5º do Decreto nº 65.347/2020?

- ( ) Sim
- ( ) Parcialmente/ em implementação
- ( ) Não

1.2 Finalidade de Tratamento

O órgão identifica de forma clara as finalidades do tratamento de dados pessoais informando-as em sua página eletrônica, com as respectivas bases legais aplicáveis aos tratamentos de dados que realiza?

- ( ) Sim
- ( ) Parcialmente/ em implementação
- ( ) Não

1.3 Competência para Tratamento

O órgão informa em sua página eletrônica a competência legal ou normativa para realizar o tratamento de dados pessoais no âmbito das suas atividades?

- ( ) Sim
- ( ) Parcialmente/ em implementação
- ( ) Não

1.4 Termo de Consentimento

Na hipótese em que o consentimento é requerido para o tratamento de dados pessoais, o órgão possui um modelo de termo de consentimento a ser disponibilizado ao titular?

- ( ) Sim / hipótese não aplicável ao órgão
- ( )Parcialmente/ em implementação
- ( ) Não

1.5 Mapeamento de Processo e Procedimentos

O órgão possui mapeamento dos processos de trabalho e respectivos procedimentos relacionados ao tratamento de dados pessoais, alinhados à Política de Proteção de Dados Pessoais estadual?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

1.6 Direitos dos Titulares

O órgão possui fluxo interno para responder às solicitações, reclamações e comunicações dos titulares de dados pessoais, por meio da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.SP, quando relacionadas ao tratamento de seus dados?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

1.7 Regras de boas práticas de governança

O órgão formulou regras de boas práticas e de governança que incluam, entre outros aspectos, mecanismos internos de supervisão e de mitigação de riscos relacionados ao tratamento de dados pessoais?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

2. Coleta e Uso de Dados Pessoais

2.1 Regras para Coleta de Dados Pessoais

O órgão possui documento que descreva os procedimentos adotados para a coleta inicial de dados pessoais?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

2.2 Limites para a Coleta de Dados Pessoais

O órgão possui procedimentos para a coleta de dados pessoais, de forma a garantir que apenas os dados necessários ao desempenho de suas atribuições sejam coletados?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

2.3 Uso Compatível de Dados Pessoais

O órgão possui procedimento para revisar e, se necessário, adequar serviços físicos ou digitais, com o objetivo de identificar dados pessoais tratados e verificar se estão adequados aos limites da coleta de dados?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

2.4 Inventário de Dados Pessoais

O órgão elaborou inventário de dados pessoais?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

3. Encarregado de Dados Pessoais

3.1 Fluxo de Comunicação

O órgão possui fluxo interno formalizado de interlocução com o encarregado de dados pessoais da Administração Direta para tratar questões relacionadas a proteção e dados?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

3.2 Gestão das Comunicações

O órgão acompanha as comunicações realizadas pelo encarregado de dados pessoais da Administração Direta, assegurando o controle do histórico de atendimento, solicitações e providências adotadas junto a agentes internos, titulares de dados, ANPD e demais órgãos competentes?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

3.3 Procedimento de Elaboração do Relatório de Impacto à Proteção de Dados (RIPD)

O órgão possui procedimento de elaboração e publicação do RIPD, quando identificados processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

4. Armazenamento, Transferência e Eliminação de Dados Pessoais

4.1 Armazenamento de Dados

O órgão armazena seus dados pessoais em conformidade com as regras do Plano de Classificação e da Tabela de atividades-meio, considerando o período de armazenamento vinculado à finalidade específica do tratamento? O órgão possui e aplica Tabela de Atividades-Fim para disciplinar os prazos de guarda e as regras de eliminação de dados após o término do período determinado, conforme orientação do Anexo III da Deliberação Normativa 02 - CGGDIESP, de 30 de dezembro de 2021?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

4.2 Compartilhamento de Dados

O órgão possui um manual técnico ou documento equivalente que oriente o uso compartilhado de dados pessoais com outros órgãos e entidades da Administração Pública estadual, incluindo compartilhamento internacional, quando aplicável, conforme previsto na Tabela de Providências Complementares e Responsáveis, constante do Anexo III da Deliberação Normativa 02 - CGGDIESP, de 30 de dezembro de 2021?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

4.3 Eliminação de Dados

O órgão possui regras para a eliminação dos dados pessoais após o prazo de armazenamento determinado, conforme previsto na Tabela de Providências Complementares e Responsáveis, constante do Anexo III da Deliberação Normativa 02 - CGGDIESP, de 30 de dezembro de 2021?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

5. Segurança e Incidentes com Dados Pessoais

5.1 Identificação de Incidente de Segurança

O órgão possui fluxo operacional que estabeleça critérios e procedimentos para identificação de incidentes envolvendo dados pessoais no âmbito de suas atividades?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

5.2 Comunicação de Incidente de Segurança

O órgão possui procedimento interno que oriente a comunicação de incidentes com dados pessoais ao encarregado de dados pessoais, de forma tempestiva e conforme diretrizes normativas vigentes?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

5.3 Gestão de Incidente de Segurança

O órgão possui procedimentos formalizados para análise, resposta e mitigação de incidentes envolvendo dados pessoais, incluindo a definição de responsabilidades, prazos e medidas corretivas?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

5.4 Treinamento e Conscientização

O órgão promove ações de capacitação e sensibilização voltadas à proteção de dados pessoais e à prevenção de incidentes, com foco na formação contínua de servidores e no fortalecimento da cultura de privacidade institucional?

- ( ) Sim
- ( )Parcialmente/ em implementação
- ( ) Não

Anexo II – Glossário de Termos e Definições

Aderência: Grau de conformidade de um órgão público em relação aos requisitos, princípios e diretrizes estabelecidos pela Política de Proteção de Dados Pessoais (PPDP) do Estado de São Paulo.

Administração Direta: Conjunto de órgãos e entidades que compõem a estrutura administrativa do Estado, sob a direção direta do Poder Executivo, sem personalidade jurídica própria.

Análise de Lacunas: Etapa da autoavaliação que identifica fragilidades, inconsistências ou pontos de atenção para o aprimoramento da governança de dados pessoais, permitindo o direcionamento de ações corretivas relacionadas à PPDP e à Lei Geral de Proteção de Dados - LGPD.

ANPD (Agência Nacional de Proteção de Dados): Autarquia de natureza especial, vinculada ao ministério da Justiça e Segurança Pública. Entre suas competências estão zelar pela proteção de dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de fiscalizar e aplicar sanções em caso de descumprimento da LGPD (Lei nº 13.709/2018).

Autoavaliação: Processo interno de análise conduzido pelo próprio órgão público, com base em um questionário estruturado, para mensurar o nível de conformidade com a Política de Proteção de Dados Pessoais estadual.

Base Legal: Fundamento jurídico que autoriza o tratamento de dados pessoais, conforme as hipóteses previstas nos arts. 7º e 11 da LGPD.

CGGDIESP: Comitê Gestor da Governança de Dados e Informações do Estado de São Paulo, responsável pela regulamentação e supervisão da Política Estadual de Proteção de Dados Pessoais.

Coleta de Dados: Ato de obtenção de dados pessoais de forma direta ou indireta, devendo observar os princípios previstos no artigo 6º da Lei nº 13.709/20.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Deliberação Normativa 02 - CGGDIESP: Ato normativo que institui a Política Estadual de Proteção de Dados Pessoais e define os parâmetros e instrumentos para a sua implementação e avaliação de aderência.

Dados Pessoais: Informação relacionada a pessoa natural identificada ou identificável, incluindo dados sensíveis, conforme definido na LGPD.

Encarregado de Dados Pessoais: Pessoa designada pelo órgão público para atuar como canal de comunicação entre o controlador, os titulares e a ANPD, nos termos do art. 41 da LGPD e do art. 6º do Decreto nº 65.347/2020.

Fluxo de Comunicação: Procedimento interno que define como as informações referentes ao tratamento de dados pessoais são comunicadas entre as áreas do órgão e o Encarregado.

Governança de Dados Pessoais: Conjunto de práticas, políticas e processos que gerenciam e controlam o tratamento adequado de dados pessoais e a conformidade com a legislação de proteção de dados.

Incidente de Segurança: Evento adverso, confirmado ou sob suspeita, que comprometa a confidencialidade, integridade ou disponibilidade das informações ou sistemas de uma organização. Está relacionado à violação de dados pessoais, como acesso não autorizado, perda, vazamento ou destruição indevida de informações.

Inventário de Dados Pessoais: Instrumento que documenta os fluxos de tratamento de dados pessoais realizados por um órgão, incluindo finalidades, bases legais, responsáveis e medidas de segurança aplicadas.

LGPD (Lei Geral de Proteção de Dados Pessoais): Lei federal nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoas jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Média Global: Resultado obtido pela soma das pontuações de todas as categorias temáticas do questionário, dividido pelo total de perguntas, representando o nível geral de aderência à PPDP.

Monitoramento Contínuo: Mecanismo permanente de acompanhamento das ações de conformidade, visando avaliar a evolução da aderência e garantir a melhoria contínua.

Plano de Ação: Documento que define medidas corretivas e preventivas, prazos e responsáveis para sanar lacunas de conformidade identificadas na autoavaliação.

Plano de Classificação e Tabela de Temporalidade: Instrumentos de gestão documental que orientam o armazenamento e a eliminação de dados pessoais, conforme prazos e finalidades específicas.

Plataforma Fala.SP: Plataforma Integrada de Ouvidoria e Acesso à Informação do Estado de São Paulo, utilizada para o exercício dos direitos dos titulares de dados pessoais e recebimento de manifestações.

Política de Proteção de Dados Pessoais (PPDP): Documento normativo que estabelece diretrizes, princípios e responsabilidades para o tratamento de dados pessoais no âmbito da Administração Pública Estadual.

Pontuação de Aderência: Sistema de avaliação baseado em uma escala de 0 a 2 pontos, sendo 2 (Sim), 1 (Parcialmente/Em Implementação) e 0 (Não), que permite mensurar o grau de conformidade de cada categoria.

Relatório de Aderência: Produto da metodologia de autoavaliação, apresentando o panorama do nível de conformidade global e por categoria, acompanhado de análise e recomendações.

RIPD (Relatório de Impacto à Proteção de Dados): Documento que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e direitos fundamentais, indicando medidas de mitigação adotadas.

Segurança da Informação: Conjunto de medidas técnicas, administrativas e organizacionais destinadas a proteger os dados pessoais contra acesso não autorizado, destruição, alteração, perda, comunicação ou difusão indevida.

Tabela de Providências Complementares e Responsáveis: Instrumento previsto na Deliberação Normativa 02 - CGGDIESP, que orienta a implementação de ações específicas relacionadas ao tratamento, armazenamento e eliminação de dados pessoais.

Titular de Dados Pessoais: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Anexo III – Referências Normativas sugeridas

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o a proteção de dados pessoais e altera outras leis. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 17/10/2025.

SÃO PAULO. Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Deliberação Normativa 02 - CGGDIESP, de 30 de dezembro de 2021. Institui a Política Estadual de Proteção de Dados Pessoais – PPDP. Disponível em: *https://cggdiesp.sp.gov.br/wcm/connect/71942854-4c4d-4ac0-8ea5-9989c39e64d6/Pol%C3%ADtica+de+Prote%C3%A7%C3%A3o+de+Dados+e+Informa%C3%A7%C3%B5es+do+Estado+de+S%C3%A3o+Paulo+%28PPDP%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-71942854-4c4d-4ac0-8ea5-9989c39e64d6-pnJJSk3* .Acesso em 17/10/2025.

_____. Controladoria Geral do Estado. Manual Orientativo para conformidade com a LGPD. Disponível em: https://admin.sggd.sp.gov.br/dx/api/dam/v1/collections/d0be4569-1f67-492a-a3d3-447fef15c361/items/65b775d4-48f7-4e33-a6d4-ec65e25ea9c0/renditions/3ac8e7bd-2598-40b4-abdd-e8f222e4eb97?binary=true. Acesso em: 17/10/2025.

_____. Decreto nº 65.347, de 9 de dezembro de 2020. Regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais no âmbito da Administração Pública Estadual. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2020/decreto-65347-09.12.2020.html . Acesso em: 17/10/2025.