GUIA ORIENTATIVO

DOCUMENTAÇÃO DA AUTOAVALIAÇÃO NO SEI

Instrução Normativa CGM/SP nº 02/2024
Diagnóstico de Maturidade em Proteção de Dados Pessoais

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Cidade de São Paulo
Controladoria Geral do Município
Coordenadoria de Proteção de Dados Pessoais

Guia Orientativo: Documentação da autoavaliação no SEI

Instrução Normativa CGM/SP nº 02/2024

Diagnóstico de Maturidade em Proteção de Dados Pessoais

FICHA TÉCNICA

Prefeitura do Município de São Paulo
Prefeito
Ricardo Nunes

Controladoria Geral do Município
Controlador Geral do Município
Encarregado da Proteção de Dados Pessoais
Daniel Falcão

Chefe de Gabinete
Thalita Abdala Aris

Equipe da Coordenadoria de Proteção de Dados Pessoais
Elaboração
Fábio Fernandes Libonati
Thiago Ryuichi Hirata

Colaboração
Gabriela da Silva Camargo
João Victor Palhuca Braz
Marcus Vinicius Marins
Maria Victoria Teodoro Raimundo
Mateus dos Santos Vieira

Arte e Diagramação
Marília Miquelin de Oliveira

Versão 01
Janeiro de 2025

Este manual foi elaborado em cumprimento aos termos do Decreto Municipal nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo do Município de São Paulo.

Controlador Geral do Município

Daniel Falcão

VERSÃO

Versão	Descrição	Data
1.0	Versão inicial	02/2025

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

ABNT	*Associação Brasileira de Normas Técnicas*
ANPD	*Autoridade Nacional de Proteção de Dados*
CGM	*Controladoria Geral do Município de São Paulo*
CIS	*Center for Internet Security*
CONACI	*Conselho Nacional de Controle Interno*
CPD	*Coordenadoria de Proteção de Dados Pessoais*
IEC	*International Electrotechnical Commission*
ISO	*International Organization of Standardization*
LGPD	*Lei Geral de Proteção de Dados Pessoais*
MGI	*Ministério da Gestão e da Inovação em Serviços Públicos*
NBR	*Normas Brasileiras Regulamentadoras*
NIST	*National Institute of Standards and Technology*
OT	*Orientação Técnica*
PEPDP	*Política Estadual de Proteção de Dados Pessoais*
PMSP	*Prefeitura Municipal de São Paulo*
SCGE-PE	*Secretaria da Controladoria Geral do Estado de Pernambuco*
SGD	*Secretaria de Governo Digital*
TCU	*Tribunal de Contas da União*

SUMÁRIO

1. INTRODUÇÃO

A mensuração do nível de adequação à LGPD é atividade fundamental no processo de adaptação dos órgãos da PMSP à cultura da privacidade e da proteção de dados pessoais. Por meio desta mensuração será possível gerar diversos benefícios à Administração Pública, uma vez que ela possibilita:

- orientar os gestores a respeito dos principais requisitos de conformidade com a LGPD;
- acompanhar o progresso dos órgãos no cumprimento desses requisitos;
- identificar vulnerabilidades, dificuldades e pontos de atenção na implementação das ações;
- identificar boas práticas e casos de sucesso;
- priorizar e direcionar ações da política de implementação; e
- compreender o panorama dos órgãos no contexto de adequação à LGPD.

Considerando o contexto atual de adaptação e fomento à cultura da privacidade e da proteção de dados pessoais no país, a CGM desenvolveu uma metodologia personalizada com o objetivo de realizar o diagnóstico de maturidade em proteção de dados pessoais de todos os órgãos da PMSP, com foco na verificação da adequação aos principais requisitos da LGPD e às boas práticas no tema. Espera-se que a metodologia seja utilizada como ferramenta de auxílio à gestão municipal e permita alcançar melhores resultados no processo de adaptação à cultura de proteção de dados pessoais.

A elaboração da metodologia teve como base:

(i) a análise da legislação vigente e identificação dos principais requisitos de conformidade aplicáveis aos órgãos da PMSP[1];

(ii) a análise de normas técnicas e de referências de boas práticas de instituições especializadas em matérias de privacidade, proteção de dados pessoais e segurança da informação[2]; e

(iii) a análise de modelos de mensuração de adequação à LGPD já existentes, elaborados por outras instituições no âmbito do setor público[3].

O Diagnóstico de Maturidade em Proteção de Dados Pessoais desenvolvido pela CGM estabelece cinco fases de maturidade para classificação dos órgãos da PMSP, cada uma prevendo a verificação da implementação de diferentes controles relacionados a requisitos da LGPD e boas práticas no tema. Dessa forma, cabe a cada órgão, anualmente, identificar a fase em que se encontra e preencher a autoavaliação sobre os controles exigidos para a respectiva fase. Para auxiliar os gestores no procedimento de autoavaliação, foram criados Guias Orientativos para detalhar os controles avaliados em cada fase do diagnóstico.

---

[1] Os principais normativos analisados para identificação dos requisitos de conformidade foram: Lei Federal nº 13.709/2018 (LGPD), Decreto Municipal nº 59.767/2020 e Instrução Normativa CGM nº 01/2022.

[2] Entre as normas técnicas e referências de boas práticas analisadas destacam-se os documentos citados a seguir: Controles CIS Versão 8, NIST Privacy Framework, Publicações da ANPD, Normas ABNT NBR ISO/IEC nº 27001:2022 27002:2022 e 27701:2020 e Orientação Técnica nº 013 – Diretrizes básicas de segurança da informação.

[3] Foram considerados como referências: Diagnóstico de Adequação à LGPD do CONACI, Monitoramento da Política Estadual de Proteção de Dados Pessoais (PEPDP) da SGCE-PE, Acórdão TCU nº 1384/2022 – Plenário e Guia do Framework de Privacidade e Segurança da Informação da SGD/MGI.

O presente Guia Orientativo detalha o procedimento anual para documentação da autoavaliação no SEI pelos órgãos públicos da PMSP.

2. DOCUMENTAÇÃO DA AUTOAVALIAÇÃO NO SEI

Cada órgão deverá preencher a autoavaliação em formulário disponibilizado anualmente pela CGM/CPD por meio de Ofício Circular.

Sugere-se que os órgãos criem processo SEI específico, para trâmite interno no próprio órgão, com a finalidade de reunir as informações necessárias para responder a autoavaliação, uma vez que isto pode envolver diferentes setores e servidores (conforme art. 4º, §3º da Instrução Normativa CGM nº 02/2024).

Como boa prática, é recomendado que cada órgão crie um novo processo SEI específico a cada ano, o qual deverá reunir as informações referentes ao período contemplado na respectiva autoavaliação, evitando-se misturar documentos de autoavaliações de anos diferentes no mesmo processo SEI.

Ressalta-se que este processo SEI não deve ser encaminhado à CGM, tratando-se de um processo SEI de tramitação interna ao próprio órgão. Entretanto, caso o órgão seja escolhido para análise amostral pela CGM/CPD (conforme art. 5º da Instrução Normativa CGM nº 02/2024), o processo SEI com as respectivas evidências de implementação dos controles e justificativas dos controles inaplicáveis poderá ser solicitado pela CGM.

A seguir encontram-se detalhados os procedimentos para a criação, instrução e encerramento do processo SEI pelos órgãos da PMSP para fins de preenchimento da autoavaliação do Diagnóstico de Maturidade em Privacidade e Proteção de Dados Pessoais.

1. **Criação do Processo SEI:**
    a. O Chefe de Gabinete deverá iniciar novo Processo SEI com as seguintes especificações:
        i. Iniciar Processo: Comum
        ii. Tipo de processo: Comunicações Administrativas: Memorando
        iii. Especificação: Diagnóstico de Maturidade em Proteção de Dados Pessoais – *SIGLA DO ÓRGÃO* - 20*XX*
        iv. Classificação por Assuntos: Autoavaliação do Diagnóstico de Maturidade em Proteção de Dados Pessoais
        v. Nível de Acesso: Restrito
        vi. Hipótese Legal: Atividades de Controle Interno (Art. 30, inc. IX, do Decreto nº 56.623/2012)

2. **Instrução do Processo SEI:**
    a. O Chefe de Gabinete deverá inserir documento de abertura de processo SEI (sugere-se utilizar o modelo do Capítulo 3):
        i. Tipo de Documento: Memorando SEI
        ii. Nível de Acesso: Restrito

iii. Hipótese Legal: Atividades de Controle Interno (Art. 30, IX, do Decreto nº 56.623/2012)

b. Após isso, o processo SEI deverá ser encaminhado aos setores competentes, conforme a necessidade, para resposta à autoavaliação, anexando, para cada controle avaliado:
   i. As evidências de existência;
   ii. Previsão de prazo para implementação; ou
   iii. As justificativas para a sua não aplicabilidade.

c. Após coletar as respostas a todos os controles avaliados, será possível responder a autoavaliação

3. **Encerramento do Processo SEI:**
   a. Após responder a autoavaliação, deve-se inserir no processo SEI uma cópia das respostas
   b. Na sequência, compete ao Chefe de Gabinete ratificar as respostas que foram anexadas ao processo SEI (sugere-se utilizar o modelo do Capítulo 4).
      i. Tipo de Documento: Informação
      ii. Nível de Acesso: Restrito
      iii. Hipótese Legal: Atividades de Controle Interno (Art. 30, inc. IX, do Decreto nº 56.623/2012)
   c. Por fim, o órgão pode encerrar o processo SEI, armazenando o número do processo caso seja solicitado posteriormente para análise pela CGM (ressalta-se que este processo SEI somente deverá ser encaminhado à CGM se e quando solicitado)

3. MODELO DE DOCUMENTO PARA ABERTURA DO PROCESSO SEI

Tipo de documento: Memorando SEI

São Paulo, *XX* de *XX* de *202X*.

Trata-se de processo SEI criado para instruir o procedimento de autoavaliação do Diagnóstico de Maturidade em Proteção de Dados Pessoais da *Secretaria/Subprefeitura XXX* no ano de *2025*.

O procedimento de autoavaliação seguirá os termos do Ofício Circular CGM (doc. SEI *XXX*), a Instrução Normativa CGM nº 02/2024 e os Guias Orientativos disponibilizados pela CGM.

Para o atual ciclo de avaliação, esta unidade irá avaliar os controles da Fase *01*. Para cada controle avaliado, o respectivo responsável pela análise deverá anexar ao presente processo SEI:

- As evidências suficientes e adequadas de existência;
- Previsão de prazo para implementação; OU
- As justificativas da inaplicabilidade para o órgão.

O quadro a seguir indica os setores e os servidores responsáveis pela avaliação de cada controle:

Controles da Fase *01*	**Responsáveis pela avaliação de cada controle**
Controle *01*	*Setor/Responsável*
Controle *02*	*Setor/Responsável*
Controle *03*	*Setor/Responsável*
Controle *04*	*Setor/Responsável*
Controle *05*	*Setor/Responsável*
Controle *06*	*Setor/Responsável*
Controle *07*	*Setor/Responsável*
Controle *08*	*Setor/Responsável*
Controle *09*	*Setor/Responsável*
Controle *10*	*Setor/Responsável*
Controle *11*	*Setor/Responsável*
Controle *12*	*Setor/Responsável*
Controle *13*	*Setor/Responsável*
Controle *14*	*Setor/Responsável*
Controle *15*	*Setor/Responsável*

Ano	**Referência a Processos SEI de autoavaliação anteriores**
2025	*SEI XXXX.XXXX//XXXXXXX-X (se houver)*

2026	*SEI XXXX.XXXX//XXXXXXX-X (se houver)*
2027	*SEI XXXX.XXXX//XXXXXXX-X (se houver)*

O responsável pela consolidação de todas as respostas do órgão e pelo preenchimento da autoavaliação no formulário indicado no Ofício Circular CGM será o agente público *XXX*. O prazo para resposta é *XX/XX/XXXX*.

Assinatura do Chefe de Gabinete

4. MODELO DE DOCUMENTO PARA RATIFICAÇÃO DA AUTOAVALIAÇÃO

Tipo de documento: Informação

São Paulo, *XX* de *XX* de *202X*.

Trata-se de processo SEI criado para instruir o procedimento de autoavaliação do Diagnóstico de Maturidade em Proteção de Dados Pessoais da *Secretaria/Subprefeitura XXX* no ano de *2025*.

Ratifico o resultado da autoavaliação anexado em doc. SEI *XXX*, que indica que o órgão *concluiu/não concluiu* a implementação dos controles da Fase *01*. As evidências de existência ou justificativas da inaplicabilidade de cada controle encontram-se indicados a seguir:

Controles da Fase *01*	**Evidência ou Justificativa**
Controle *01*	*Doc. SEI XXX (se houver)*
Controle *02*	*Doc. SEI XXX (se houver)*
Controle *03*	*Doc. SEI XXX (se houver)*
Controle *04*	*Doc. SEI XXX (se houver)*
Controle *05*	*Doc. SEI XXX (se houver)*
Controle *06*	*Doc. SEI XXX (se houver)*
Controle *07*	*Doc. SEI XXX (se houver)*
Controle *08*	*Doc. SEI XXX (se houver)*
Controle *09*	*Doc. SEI XXX (se houver)*
Controle *10*	*Doc. SEI XXX (se houver)*
Controle *11*	*Doc. SEI XXX (se houver)*
Controle *12*	*Doc. SEI XXX (se houver)*
Controle *13*	*Doc. SEI XXX (se houver)*
Controle *14*	*Doc. SEI XXX (se houver)*
Controle *15*	*Doc. SEI XXX (se houver)*

Assinatura do Chefe de Gabinete

5. REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27701:2020. Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. Tratamento de dados pessoais pelo Poder Público. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: < https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf > Acesso em: 05/03/2024

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia do Framework de Privacidade e Segurança da Informação, versão 1.1.2. Brasília, setembro de 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias-e-modelos> Acesso em: 04/03/2024

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 82, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI. Diário Oficial da União, 30 de março de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 14 de agosto de 2018.

BRASIL. Tribunal de Contas da União. ACÓRDÃO nº 1.384/2022. Plenário. Relator: Ministro Augusto Nardes. Sessão de 15/06/2022. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2521877> Acesso em: 04/03/2024

CENTER INTERNET SECURITY. Controles CIS, Versão 8, 2021. Disponível em: <https://www.cisecurity.org/> Acesso em: 04/03/2024

CONACI. Diagnóstico de Adequação à LGPD, Pesquisa 01/2022. Disponível em: <https://conaci.org.br/noticias/camara_tecnica/lgpd/> Acesso em: 04/03/2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, Versão 1.0, 2020. Disponível em: <https://doi.org/10.6028/NIST.CSWP.01162020pt> Acesso em: 04/03/2024

PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Portaria SCGE nº 41, de 07 de julho de 2023. Disponível em: <https://www.scge.pe.gov.br/lgpd-rede-de-encarregados/> Acesso em: 04/03/2024

SÃO PAULO (Cidade). Decreto nº 59.767, de 15 de setembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) – no âmbito da Administração Municipal direta e indireta. São Paulo, Diário Oficial da Cidade, 16 de setembro de 2020.

SÃO PAULO (Cidade). Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaPrivacidadeeaProtecaodeDadosPessoaisparaaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf> Acesso em: 21/03/2024

SÃO PAULO (Cidade). Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo, versão 01, 2023. Disponível em: < https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaInstrucaoNormativaCGM-SPn%C2%BA01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf> Acesso em: 21/03/2024

SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, Diário Oficial da Cidade, 22 de julho de 2022.

SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 02, de 23 de dezembro de 2024. Aprova a Metodologia de Diagnóstico de Maturidade em Proteção de Dados Pessoais e disciplina o procedimento de autoavaliação por parte dos órgãos da Administração Pública Municipal. São Paulo, Diário Oficial da Cidade, 27 de dezembro de 2024.

SÃO PAULO (Cidade). Orientação Técnica nº 013 – Diretrizes básicas de segurança da informação. Disponível em: <https://tecnologia.prefeitura.sp.gov.br/arquivos/ot-volumes/OT_vol3.pdf#page=35> Acesso em: 21/03/2024

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO