DIAGNÓSTICO DE MATURIDADE EM PROTEÇÃO DE DADOS PESSOAIS DA PREFEITURA DO MUNICÍPIO DE SÃO PAULO

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

AGENDA

- Parte I: Apresentação da Metodologia
- Parte II: Instrução Normativa CGM nº 02/2024
- Parte III: Ofício Circular CGM
- Parte IV: Formulário da Autoavaliação
- Parte V: Documentação da Autoavaliação no SEI
- Parte VI: Controles da Fase 01 – Preparatório

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

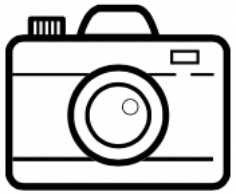
Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

O QUE É O DIAGNÓSTICO DE MATURIDADE?



Fotografia do estágio de adequação à LGPD

Diagnóstico da situação atual de adequação

Ações para adequação à LGPD

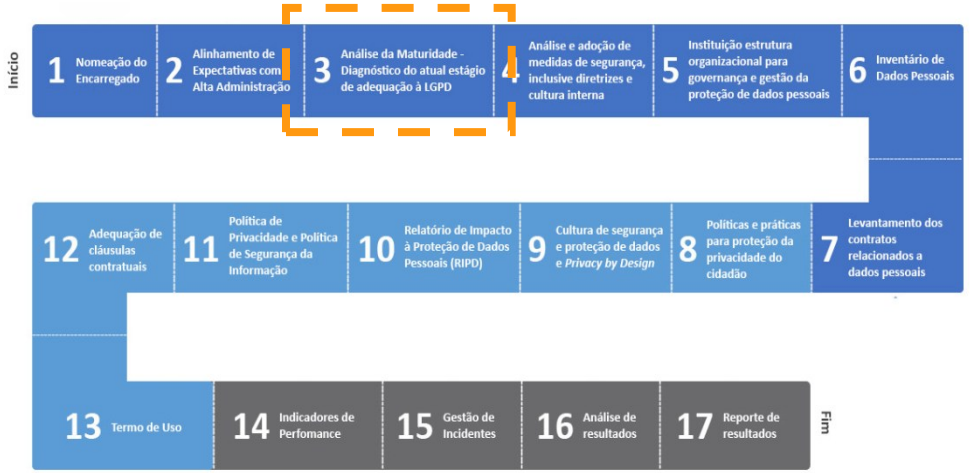
CONTEXTO

Cenário atual

- Diversos entes públicos e privados já criaram procedimento para mensuração da adequação[1];
- O diagnóstico de adequação à LGPD é atividade inicial do processo de conformidade.

1. *Exemplos analisados: CONACI, SCGE-PE, TCU, SGD/MGI, CGE-MG, TCE-RJ*

Exemplo de *roadmap* de implantação da LGPD



Exemplo do caso de SGD/MGI, cujo diagnóstico consta na etapa 3

OBJETIVOS E VANTAGENS ESPERADAS

Objetivos

- Mensurar a adequação à LGPD na PMSP e direcionar as ações necessárias para acelerar todo o processo, através da criação de uma ferramenta de auxílio à gestão.

Vantagens

- Orientação aos gestores públicos com priorização das ações;
- Compreensão do panorama geral da PMSP e da sua evolução no tempo;
- Identificação de pontos de atenção e de boas práticas;
- Auxílio para respostas a ações de fiscalização e sanção (ANPD, TCM, etc.).

CONSIDERAÇÕES INICIAIS

Ressalvas

- Metodologia não contempla todos os controles existentes e aplicáveis;
- Necessidade de o gestor continuar observando os requisitos legais específicos aplicáveis;
- Requisitos em constante atualização/ revisão;
- Diagnóstico não fornece "atestado" de conformidade às referências consultadas.

Escopo

- Foco no contexto da unidade, com possibilidade de adaptação para contextos distintos;
- Foco em Privacidade e Proteção de Dados Pessoais, apesar de tangenciar a Segurança da Informação;
- Foco em aspectos de conformidade e não de desempenho;
- Foco na gestão e não na repreensão.

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

INSTRUÇÃO NORMATIVA CGM Nº 02/2024

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.

AUTOAVALIAÇÃO PELOS ÓRGÃOS DA PMSP

- **Definição:** Preenchimento de questionário sobre os controles da fase
- **Método**: CSA (*Control Self-Assesment*) - Autoavaliação de controles
- **Objetivo**: Verificação dos controles internos relacionados à LGPD
- **Escopo**: Órgãos da Administração Direta – avaliação dos controles somente da fase em que estiver
- **Periodicidade**: Anual
- **Responsável**: Chefe de Gabinete / Ponto Focal
- **Documentação**: Instrução de Processo SEI

Referência: Arts. 3º e 4º da IN CGM nº 02/2024

VERIFICAÇÃO DA EXISTÊNCIA DOS CONTROLES POR CGM/CPD

- **Definição:** Análise das evidências no SEI sobre a existência dos controles
- **Método**: Análise documental
- **Objetivo**: Verificação de existência dos controles
- **Escopo**: Apenas sobre os órgãos que concluírem a respectiva fase (seleção amostral)
- **Periodicidade**: Anual
- **Responsável**: CGM/CPD
- **Documentação**: Aprovação / Recomendação de ajustes

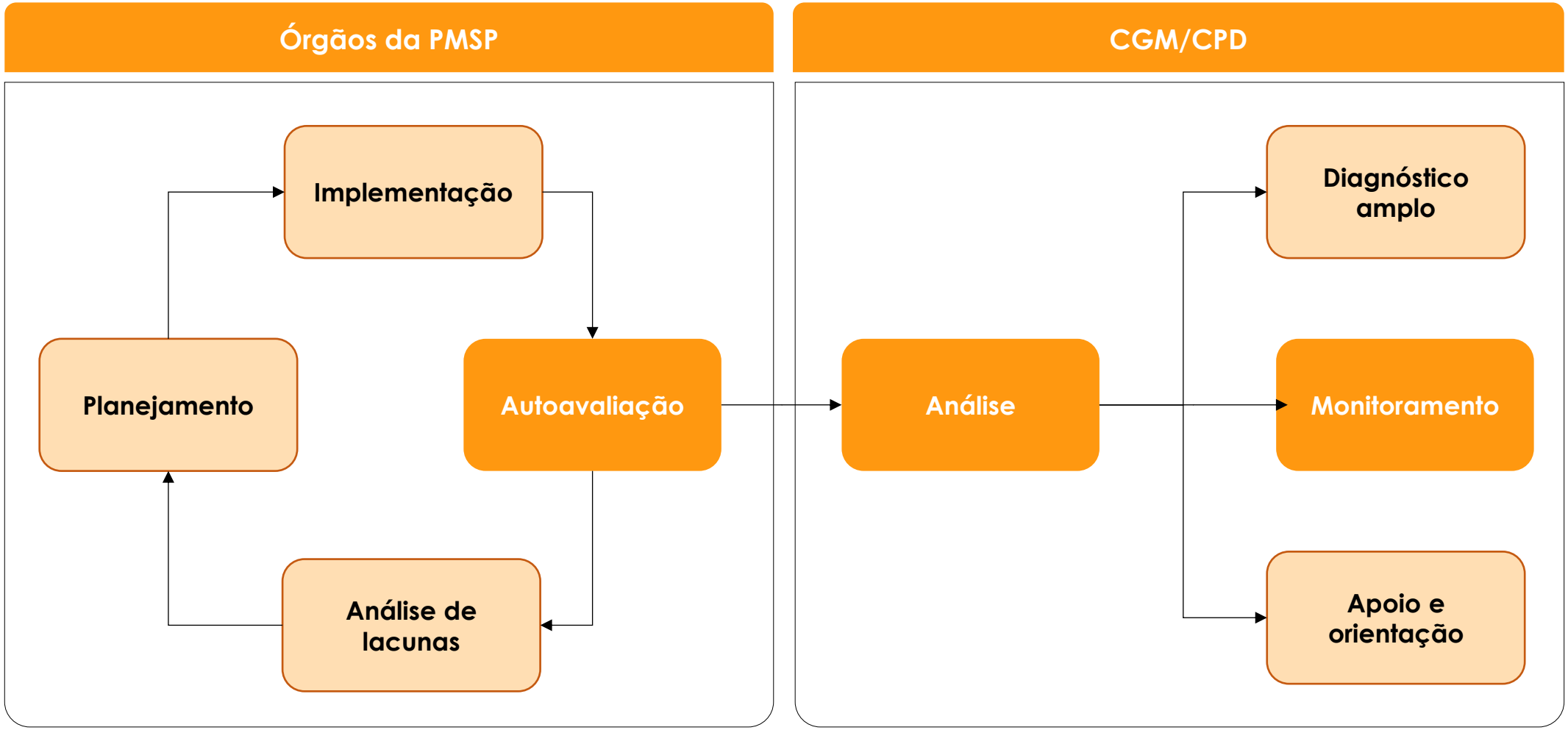
Referência: Art. 5º da IN CGM nº 02/2024

MONITORAMENTO POR CGM/CPD

- **Definição:** Análise das evidências no SEI sobre a existência dos controles de outras fases
- **Método**: Análise documental
- **Objetivo**: Atualização e melhoria contínua
- **Escopo**: Seleção amostral
- **Periodicidade**: Não definida
- **Responsável**: CGM/CPD
- **Documentação**: Aprovação / Recomendação de ajustes

Referência: Arts. 6º e 7º da IN CGM nº 02/2024

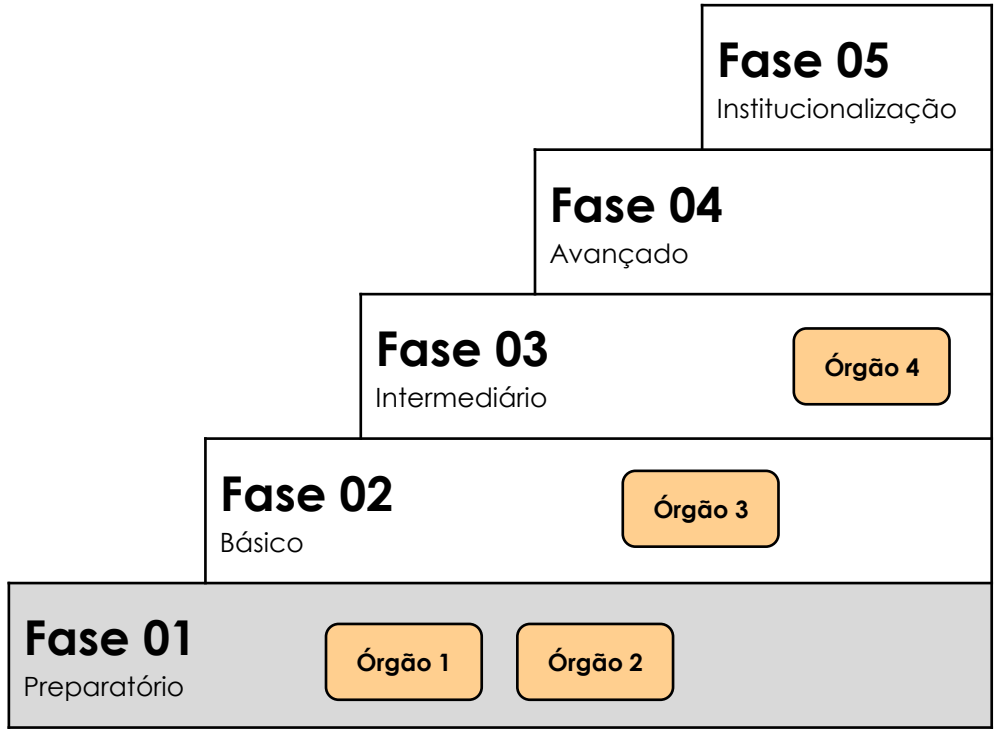
CICLO DE AVALIAÇÃO



DIAGNÓSTICO AMPLO DA PMSP

Classificação final PMSP

- Os órgãos serão avaliados individualmente;
- A PMSP será classificada de acordo com o órgão na menor fase.



Referência: Art. 8º da IN CGM nº 02/2024

APOIO E ORIENTAÇÃO

Principais ações previstas

Ilustrativo / Não exaustivo / Preliminar

Instrução Normativa

- **Guia Orientativo para cada Fase**
- **Formulário para cada Fase**

Manuais sobre os controles

- Manual sobre privacidade e proteção de DP
- Manual de mapeamento de processos
- Manual de mapeamento de dados pessoais
- Manual sobre gestão de riscos [...]

Modelos de documentos

- Modelo de mapeamento de processos
- Modelo de mapeamento de dados pessoais
- Modelo de gestão de riscos [...]

Capacitações

- Capacitação sobre a Instrução Normativa
- Capacitação sobre o Guia e o Formulário
- Capacitação sobre controles / documentos

Referência: Arts. 8º e 12 da IN CGM nº 02/2024

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

OFÍCIO CIRCULAR CGM - 2025

1. Participação na capacitação de 11/02/2025

2. Resposta ao formulário do TCM-SP de 12/02/2025 a 28/02/2025

- Seguir as instruções de resposta e envio de evidências do TCM-SP

3. Resposta ao formulário da CGM-SP de 12/02/2025 a 28/02/2025

- Criação de Processo SEI pelo órgão:
  a) Anexação das respostas do arquivo Excel
  b) Anexação de evidências e justificativas

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

AUTOAVALIAÇÃO: RESPOSTAS E DOCUMENTAÇÃO

CONTROLE 04. O órgão elaborou e/ou atualizou no período o seu Planejamento para elaboração do Programa de Governança em Privacidade e Proteção de Dados Pessoais (documento com a descrição de atividades necessárias e os respectivos prazos para elaboração do Programa), para direcionar a iniciativa de adequação à LGPD?

No formulário		No SEI	
Sim	O controle foi implementado	**Evidência**	Anexar evidências da implementação do controle
Não	O controle não foi implementado (haverá implementação futura)	**Previsão**	Informar previsão de implementação do controle
Não se aplica	O controle não se aplica ao órgão	**Justificativa**	Justificar porque o controle não se aplica

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

QUADRO-RESUMO DOS CONTROLES

Tema	Fase 01 Preparatório	Fase 02 Básico	Fase 03 Intermediário	Fase 04 Avançado	Fase 05 Institucionalização	Total de controles
01. Estrutura organizacional	3	2	2	1	1	**9**
02. Governança	1	2	2	1	1	**7**
03. Tratamento de dados pessoais	3	1	2	2	7	**15**
04. Direitos dos titulares	1	2	2	1	1	**7**
05. Resposta a incidentes	1	2	2	1	1	**7**
06. Transparência	3	1	1	1	1	**7**
07. Segurança da Informação	1	3	1	2	1	**8**
08. Gestão de terceiros	2	2	2	2	2	**10**
Total de controles por fase	**15**	**15**	**14**	**11**	**15**	**70**

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

INSTAURAÇÃO DO PROCESSO SEI!

1. Criação do SEI!

- **Iniciar processo**: Comum
- **Tipo de processo**: Comunicações Administrativas: Memorando
- **Especificação**: Diagnóstico de Maturidade em Proteção de Dados Pessoais - *ÓRGÃO* - 2025
- **Classificação por Assuntos**: Autoavaliação do Diagnóstico de Maturidade em Proteção de Dados Pessoais
- **Nível de Acesso**: Restrito
- **Hipótese Legal**: Atividades de Controle Interno (Art. 30, IX, do Decreto Nº 56.623/2012)

2. Instrução do SEI!

2.1. Documento modelo de abertura

- **Tipo de Documento**: Memorando SEI
- **Nível de Acesso**: Restrito
- **Hipótese Legal**: Atividades de Controle Interno (Art. 30, IX, do Decreto Nº 56.623/2012)

2.2. Documentação pelos setores

- As evidências de existência;
- Os prazos para implementação dos controles; ou
- As justificativas para a sua não aplicabilidade.

ENCERRAMENTO DO PROCESSO SEI!

3. Ratificação das respostas

3.1. Cópia das respostas

- **Anexar:** cópia das respostas enviadas

3.2. Documento modelo de ratificação

- Tipo de Documento: Informação
- Nível de Acesso: Restrito
- Hipótese Legal: Atividades de Controle Interno (Art. 30, IX, do Decreto Nº 56.623/2012)

4. Encerramento do SEI

- Encerrar o processo SEI
- Armazenar o número do processo caso seja solicitado posteriormente para análise pela CGM
- Ressalta-se que **este processo SEI só deve ser encaminhado à CGM se e quando solicitado**

AGENDA

Parte I: Apresentação da Metodologia

Parte II: Instrução Normativa CGM nº 02/2024

Parte III: Ofício Circular CGM

Parte IV: Formulário da Autoavaliação

Parte V: Documentação da Autoavaliação no SEI

Parte VI: Controles da Fase 01 – Preparatório

QUADRO GERAL DOS CONTROLES

05. Institucionalização	56. Participação em fóruns especializados	57. Atualização do Programa de Governança	Controles sobre:	64. Tratamento automatizado 63.Exclusão ou destruição de dados 62. Dados de crianças e adolescentes 61. Formato interoperável e estruturado 60. Dados anonimizados 59. Dados em estudo ou pesquisa 58. Dados relacionados à saúde	65. Controles sobre a melhoria contínua no atendimento	66. Controles sobre a documentação e avaliação pós-incidente	67. Controles sobre os níveis de acesso no SEI	68. Controles sobre registros de eventos (logs)	70. Controles sobre a transferência de dados e criptografia 69. Controles sobre as medidas de proteção adotadas por terceiros
04. Avançado	45. Monitoramento do Plano de Capacitação	46. Monitoramento do Plano de Gestão de Riscos	48. Monitoramento do tempo de armazenamento dos dados pessoais 47. Gestão do Consentimento do Titular de Dados Pessoais		49. Monitoramento de Indicadores de Desempenho do atendimento aos titulares	50. Monitoramento de Indicadores de Desempenho de incidentes de segurança	51. Gerenciamento de dados pelo titular	53. Gestão do controle de contas e acessos 52. Monitoramento de vulnerabilidades técnicas	55. Monitoramento e comunicação de alterações a terceiros 54. Monitoramento de requisitos de terceiros
03. Intermediário	32. Conscientização 31. Funções e responsabilidades	34. Programa de Governança 33. Relatório de Impacto à Proteção de Dados Pessoais	36. Tabela de Temporalidade de Documentos 35. Política de Classificação da Informação		38. Registro dos atendimentos 37. Política de Atendimento	40. Registro dos incidentes 39. Política de Resposta a Incidentes	41. Política de Privacidade e Proteção de Dados Pessoais	42. Política de Segurança da Informação	44. Registro de compartilhamentos 43. Política de Contratações de Terceiros
02. Básico	17. Capacitação do Grupo de Trabalho 16. Capacitação do Encarregado	19. Política de Gestão de Riscos 18. Plano de Gestão de Riscos	20. Adequação de processos e atividades		22. Resposta às solicitações dos titulares 21. Fluxo de atendimento	24. Resposta aos incidentes 23. Fluxo de comunicação de incidentes	25. Adequação do Portal da Transparência	28. Cópias de segurança 27. Softwares antimalware 26. Arquitetura e infra de redes	30. Adequação de compartilhamentos e transferências 29. Adequação de contratos
01. Preparatório	03. Sensibilização 02. Grupo de Trabalho 01. Encarregado	04. Planejamento	07. Finalidades e hipóteses legais 06. Mapeamento de dados pessoais 05. Mapeamento de processos		08. Canal de atendimento aos direitos dos titulares	09. Canal de denúncias e/ou notificações de incidentes	12. Coleta de cookies 11. Informações do tratamento de dados 10. Informações do Encarregado	13. Inventário de software e de ativos de tecnologia da informação	15. Relação/lista dos contratos e compartilhamentos 14. Minutas padrão
Fase / Tema	**01. Estrutura organizacional**	**02. Governança**	**03. Tratamento de dados pessoais**		**04. Direitos dos titulares**	**05. Resposta a incidentes**	**06. Transparência**	**07. Segurança da Informação**	**08. Gestão de terceiros**

CONTROLE 01 - ENCARREGADO

CONTROLE	O órgão possui a indicação formal de um Encarregado pela proteção de dados pessoais?
DESCRIÇÃO	O órgão deve designar oficialmente o Encarregado por meio de nomeação por Portaria publicada no Diário Oficial da Cidade.
REQUISITOS	Designação de Encarregado e seu substituto por meio da publicação de portaria.
ORIENTAÇÕES	Resolução CD/ANPD nº 18/2024 e seu Guia Orientativo (Encarregado)

Observação: *Considerando o atual estágio de normatização na PMSP a respeito deste tema, todos os órgãos terão considerada a resposta "Sim", com a evidência cumprida pela própria CGM-SP, conforme Art. 5º do Decreto Municipal nº 59.767/2020. Caso haja alteração normativa, este controle poderá ser reavaliado.*

CONTROLE 02 – GRUPOS DE TRABALHO

CONTROLE	O órgão possui um Grupo de Trabalho ou estrutura equivalente, para apoiar na adequação à LGPD?
DESCRIÇÃO	Considera-se uma boa prática a criação de um grupo de trabalho para coordenar a implementação de ações necessárias à adequação da unidade à LGPD. Tal grupo não é subordinado e não se confunde com a figura do Encarregado. É importante que o grupo conte com o apoio e/ou a participação da alta direção da organização.
REQUISITOS	Designação de Grupo de Trabalho por meio da publicação de portaria.
ORIENTAÇÕES	Em elaboração.

Referências: Art. 6º, X, Art. 50, LGPD.

CONTROLE 03 - SENSIBILIZAÇÃO

CONTROLE	O órgão realizou atividades de sensibilização de seus agentes públicos acerca da LGPD por meio de ações como disponibilização de informativos, condução de workshops, realização de palestras ou seminários, entre outros?
DESCRIÇÃO	A sensibilização dos agentes públicos do órgão é importante para a implantação e manutenção da cultura da privacidade e da proteção de dados pessoais na rotina dos colaboradores. Ações de sensibilização envolvem a organização de forma sistêmica, disponibilizadas para todos os colaboradores, ainda que nem todos tenham participado.
REQUISITOS	Realização de no mínimo uma ação de sensibilização com envolvimento de todo o órgão, não sendo necessária a participação de todos os funcionários.
ORIENTAÇÕES	Exemplo de cursos sobre Privacidade e Proteção de Dados Pessoais disponibilizado pela CGM/CPD

Referências: Art. 6º, X, Art. 50, LGPD. Art. 14, VI, IN/CGM nº 01/2022.

CONTROLE 04 - PLANEJAMENTO

CONTROLE	O órgão elaborou e/ou atualizou no período o seu Planejamento para elaboração do Programa de Governança em Privacidade e Proteção de Dados Pessoais, para direcionar a iniciativa de adequação à LGPD?
DESCRIÇÃO	O órgão deve documentar o diagnóstico de sua situação atual de conformidade à LGPD e as ações e medidas que são necessárias para implementação futura, visando a sua adequação às melhores práticas de proteção de dados. Espera-se que seja apresentado um cronograma para implementação das ações previstas.
REQUISITOS	Documento com a descrição das atividades necessárias e respectivos responsáveis e prazos.
ORIENTAÇÕES	Em elaboração.

Referências: Art. 6º, VIII, LGPD. Art. 4º, III, Art. 15, Decreto nº 59.767/2020.

CONTROLE 05 – MAPEAMENTO DE PROCESSOS ★

CONTROLE	**O órgão realizou, revisou ou atualizou no período o mapeamento de processos que tratam dados pessoais?** **Processo, nesse caso, é entendido como "*sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade*".**
DESCRIÇÃO	**O mapeamento de processos é etapa preliminar importante para se realizar o inventário de dados pessoais do órgão. É através do mapeamento de processos que se possibilita ter uma visão geral das atividades realizadas e em que etapas se concentram o tratamento de dados pessoais.**
REQUISITOS	**O mapeamento de processos resulta em uma lista com o repositório de todos os processos do ente. O nível de detalhamento pode variar de acordo com as suas necessidades.**
ORIENTAÇÕES	**Modelo de documento de mapeamento de processos da IN CGM nº 01/2022**

Referências: Art. 6º, VIII, LGPD. Art. 4º, I, Decreto nº 59.767/2020. Art. 2º, Art. 14, IV, b, IN/CGM nº 01/2022.

CONTROLE 06 – MAPEAMENTO DE DADOS PESSOAIS ★

CONTROLE	**O órgão realizou, revisou ou atualizou no período o mapeamento de dados pessoais dos processos mapeados?**
DESCRIÇÃO	**O mapeamento de dados pessoais deve conter as informações, de forma clara, adequada e ostensiva, sobre todo o ciclo de vida dos dados pessoais do titular (com a identificação dos dados pessoais utilizados em cada processo). A elaboração do mapeamento é importante para entender como os dados pessoais são coletados e por onde caminham dentro do órgão, facilitando a rápida localização de um dado mapeado em caso de incidente (vazamento), assim como o rápido atendimento a uma requisição do titular.**
REQUISITOS	**O art. 14, inc. IV, da Instrução Normativa CGM/SP nº 01/2022, dispõe sobre os requisitos necessários à elaboração do Mapeamento de Dados Pessoais.**
ORIENTAÇÕES	**Modelo de documento de mapeamento de dados pessoais da IN CGM nº 01/2022.**

Referências: Art. 6º, VIII, 37, LGPD. Art. 4º, I, Decreto nº 59.767/2020. Art. 2º, Art. 14, IV, IN/CGM nº 01/2022.

CONTROLE 07 – FINALIDADES E HIPÓTESES LEGAIS ★

CONTROLE	**O órgão realizou, revisou ou atualizou a identificação das finalidades e das hipóteses legais que são consideradas para o tratamento de dados pessoais?**
DESCRIÇÃO	**A identificação das finalidades e das hipóteses legais envolve o levantamento dos fundamentos que autorizam o tratamento de dados pessoais pelo órgão. Como exemplo, pode ser citada a identificação de obrigações legais e regulatórias, políticas públicas, contratos e normas específicas relativas às atividades do órgão. Nota-se que, além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser respeitados.**
REQUISITOS	**Documento consolidado com lista de todos as operações de tratamento de dados pessoais realizadas pelo órgão, com a indicação da respectiva finalidade e hipótese legal.**
ORIENTAÇÕES	**Em elaboração.**

Referências: Art. 6º, I, II, III, Art. 23, I, LGPD. Art. 10, Art. 14, IV, f, IN/CGM nº 01/2022.

CONTROLE 08 – CANAL DE ATENDIMENTO AO TITULAR

CONTROLE	O órgão disponibiliza canal específico para recebimento de demandas de atendimento aos direitos dos titulares referentes à LGPD?
DESCRIÇÃO	É importante e obrigatório disponibilizar canal específico para recebimento de demandas referentes à LGPD, como o atendimento dos direitos dos titulares, uma vez que a definição desta estrutura possibilita que o procedimento de resposta seja mais organizado e célere.
REQUISITOS	Indicação de forma de contato no sítio eletrônico para assuntos relacionados à LGPD.
ORIENTAÇÕES	Link para página da CGM

Referências: Art. 6º, IV, Arts. 17 a 20, LGPD. Art. 6º, Decreto nº 59.767/2020.

CONTROLE 09 – CANAL DE RECEBIMENTO DE DENÚNCIAS

CONTROLE	Existe um canal apropriado para o recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação?
DESCRIÇÃO	É importante que o órgão disponibilize canal apropriado para o recebimento de denúncias e encaminhamento de solução a respeito dos incidentes.
REQUISITOS	Existência de canal para recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação. Divulgação do canal nos meios de comunicação adequados para o público interno e externo.
ORIENTAÇÕES	Link para página da CGM Resolução CD/ANPD nº 15/2024 (Comunicação de Incidente de Segurança)

Referências: Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD.

CONTROLE 10 – TRANSPARÊNCIA DAS INFORMAÇÕES SOBRE O ENCARREGADO

CONTROLE	**O órgão divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?**
DESCRIÇÃO	**A identidade e as informações de contato (ex.: e-mail, telefone) do Encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico do órgão.**
REQUISITOS	**Divulgação do nome completo e contato do Encarregado Titular e Substituto no sítio eletrônico.**
ORIENTAÇÕES	**Link para página da CGM** **Resolução CD/ANPD n 18/2024 e seu Guia Orientativo (Encarregado)**

Referências: Art. 6º, VI, Art. 41, § 1º, LGPD. Art. 5º, parágrafo único, Decreto nº 59.767/2020.

CONTROLE 11 – TRANSPARÊNCIA DAS INFORMAÇÕES SOBRE O TRATAMENTO DE DADOS PESSOAIS

CONTROLE	**O órgão disponibiliza informações a respeito do tratamento de dados pessoais, especialmente sobre a previsão legal, a finalidade, os compartilhamentos, as transferências, os procedimentos e as práticas utilizadas para a execução dessas atividades, preferencialmente em seus sítios eletrônicos?**
DESCRIÇÃO	**Conforme Art. 9º, I, II e V da LGPD, o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva para o atendimento do princípio do livre acesso. Neste sentido, deve ser concedido acesso pleno e irrestrito a informações como a finalidade específica do tratamento de dados pessoais; a forma e duração do tratamento, observados os segredos comercial e industrial; e a informações acerca do uso compartilhado de dados pelo controlador e a sua finalidade.**
REQUISITOS	**Informações no sítio eletrônico do órgão a respeito da previsão legal, a finalidade, os compartilhamentos, as transferências, os procedimentos e as práticas utilizadas no tratamento de dados pessoais.**
ORIENTAÇÕES	**Em elaboração.**

Referências: Art. 6º, IV, VI, 9º, I, II, 23, I LGPD. Art. 11, II, Decreto nº 59.767/2020. Art. 10, IN/CGM nº 01/2022.

CONTROLE 12 – BANNER DE *COOKIES*

CONTROLE	**O órgão, ao coletar *cookies*, identifica as hipóteses legais no banner de segundo nível, utilizando o consentimento como principal hipótese legal (exceção feita aos *cookies* estritamente necessários, que podem se basear no legítimo interesse ou no cumprimento de obrigações ou atribuições legais)?**
DESCRIÇÃO	**O Banner de *cookies* é um recurso visual utilizado para informar ao titular de dados sobre a utilização de *cookies* em sites ou aplicativos. O banner fornece ferramentas para que o usuário possa ter maior controle sobre o tratamento de dados, podendo consentir ou não com determinados tipos de cookies. Para mais informações recomenda-se a leitura do Guia Orientativo *Cookies* e Proteção de Dados Pessoais da ANPD.**
REQUISITOS	**Banner de *cookies* em dois níveis**
ORIENTAÇÕES	**Guia Orientativo da ANPD sobre *Cookies* e Proteção de Dados Pessoais**

Referências: Art. 6º, VI, Art. 9º, Art. 18, LGPD. Art. 10, IN/CGM nº 01/2022.

CONTROLE 13 – INVENTÁRIO DE *SOFTWARES* E ATIVOS DE TI

CONTROLE	O órgão mantém um inventário de *softwares* e de ativos de tecnologia da informação, executando também um processo de configuração segura de todos os ativos e *softwares*?
DESCRIÇÃO	É uma boa prática manter um inventário preciso, detalhado e atualizado periodicamente de todos os ativos institucionais que tenham potencial para armazenar ou processar dados pessoais, incluindo ativos que não estejam sob controle do órgão e também os *softwares* licenciados instalados nestes ativos. Adicionalmente, também é uma boa prática manter um processo de configuração segura para ativos corporativos e *softwares*.
REQUISITOS	Possuir um inventário de ativos de Tecnologia da Informação (físico e de *software*), atualizado periodicamente
ORIENTAÇÕES	Portaria SMIT nº 36/2018 (Sistema CITI) Orientações Técnicas SMIT nº 004 (Inventário de Ativos e Licenças de Software) Orientações Técnicas SMIT nº 013 (Diretrizes Básicas de Segurança da Informação)

Referências: Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD. OT nº 004 e 013 do Decreto nº 57.653/2017.

CONTROLE 14 – MINUTAS PADRÃO

CONTROLE	**O órgão adota minutas padrão para os instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres com requisitos mínimos relativos ao tratamento de dados pessoais?**
DESCRIÇÃO	**Uma boa prática de tratamento de dados pessoais envolve o estabelecimento de um procedimento de gestão de contratações de terceiros. Neste sentido, é importante definir as disposições específicas para cada modalidade de contratação, criar cláusulas contratuais padrão, instituir procedimentos de fiscalização, entre outras ações pertinentes.**
REQUISITOS	**Lista com os tipos mais frequentes de instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres com os seus respectivos requisitos mínimos relativos ao tratamento de dados pessoais.**
ORIENTAÇÕES	**Resolução CD/ANPD nº 19/2024 (Transferência Internacional de Dados Pessoais)**

Referências: Art. 6º, VIII, Art. 33, II, b, Art. 39, LGPD. Arts. 16 e 114, III do Decreto nº 62.100/2022.

CONTROLE 15 – MAPEAMENTO DE CONTRATOS E COMPARTILHAMENTOS

CONTROLE	O órgão realizou, revisou ou atualizou no período o mapeamento dos contratos firmados com terceiros, contemplando os registros de compartilhamentos e transferências internacionais de dados pessoais realizados, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?
DESCRIÇÃO	É importante que o órgão identifique os terceiros que possuem responsabilidades associadas ao tratamento de dados pessoais, mapeando os contratos firmados com operadores, controladores conjuntos e fornecedores, entre outros. É importante que o órgão tenha registro dos compartilhamentos e das transferências internacionais de dados pessoais realizados.
REQUISITOS	Documento com o mapeamento de contratos firmados com terceiros. Documento com o mapeamento de compartilhamentos e transferências de dados pessoais.
ORIENTAÇÕES	-

Referências: Art. 6º, VIII, Art. 26, Art. 27, Art. 37, Art. 39, LGPD. Art. 14, IV, j, k, l, IN/CGM nº 01/2022.

MUITO OBRIGADO!

Coordenadoria de Proteção de Dados (CGM/CPD)
privacidade@prefeitura.sp.gov.br
(11)3113-8288

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO