GUIA ORIENTATIVO

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

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

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

Diagnóstico de Maturidade em Proteção de Dados Pessoais

São Paulo
2025

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

ABNT	*Associação Brasileira de Normas Técnicas*
ANPD	*Autoridade Nacional de Proteção de Dados*
AUDI	*Auditoria Geral do Município*
CGM-SP	*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*
CSA	*Control Self-Assessment*
IEC	*International Electrotechnical Commission*
IN	*Instrução Normativa*
ISO	*International Organization of Standardization*
LAI	*Lei de Acesso à Informação*
LGPD	*Lei Geral de Proteção de Dados Pessoais*
MCI	*Marco Civil da Internet*
MGI	*Ministério da Gestão e da Inovação em Serviços Públicos*
NBR	*Normas Brasileiras Regulamentadoras*
NIST	*National Institute of Standards and Technology*
OT	*Orientação Técnica*
PDCA	*Plan-Do-Check-Act*
PEPDP	*Política Estadual de Proteção de Dados Pessoais*
PMGTIC	*Política Municipal de Governança de Tecnologia da Informação e Comunicação*
PMSP	*Prefeitura Municipal de São Paulo*
SCGE-PE	*Secretaria da Controladoria Geral do Estado de Pernambuco*
SGD	*Secretaria de Governo Digital*
SMIT	*Secretaria Municipal de Inovação e Tecnologia*
TCU	*Tribunal de Contas da União*
TI	*Tecnologia da Informação*

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. Através desta mensuração é possível gerar diversos benefícios à Administração Pública, uma vez que ela possibilita: orientar os gestores a respeito dos principais requisitos de conformidade da 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 geral dos órgãos no contexto de adequação à LGPD.

Considerando o contexto atual de adaptação à cultura da privacidade e da proteção de dados pessoais no país, a CMG-SP desenvolveu metodologia personalizada com o objetivo principal 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, buscando-se 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].

[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.

2. CONSIDERAÇÕES INICIAIS

A metodologia desenvolvida busca fornecer uma ferramenta de auxílio à gestão municipal. Nesse cenário, é importante enfatizar que:

a) Os aspectos verificados representam uma seleção baseada em critérios de relevância, não contemplando a totalidade dos controles exigidos pelos normativos e pelas boas práticas sobre o tema. Assim, a utilização desta metodologia não isenta os órgãos de se adequarem a outras determinações legais existentes na própria LGPD e em outros normativos. Deve-se atentar principalmente a requisitos específicos aplicáveis aos diferentes setores de atuação.

b) Os aspectos verificados possuem foco no tema de privacidade e proteção de dados pessoais. Nota-se que este tema não se confunde com o tema da segurança da informação, porém, é necessário ressaltar que eles estão intimamente relacionados. Nesse aspecto, observa-se que algumas medidas e controles de segurança da informação são considerados também essenciais para a garantia da privacidade e da proteção de dados pessoais. Levando-se em consideração a sinergia entre controles de ambos os temas, optou-se por inserir também na metodologia desenvolvida a verificação de alguns controles de segurança da informação relacionados à privacidade e à proteção de dados pessoais. No entanto, ressalta-se que isto não isenta os órgãos de seguirem as orientações técnicas, diretrizes e boas práticas específicas elaboradas por SMIT sobre segurança da informação, como por exemplo, a Orientação Técnica nº 013 – Diretrizes básicas de segurança da informação .

c) Os aspectos verificados podem ser adaptados pelos órgãos para o seu contexto e realidade. A abordagem proposta à PMSP oferece uma sugestão de implementação de controles, porém é importante que cada instituição compreenda sua própria postura em relação ao risco. Assim, é possível adaptar os controles sugeridos, de modo a adequá-los ao porte, às necessidades e aos objetivos da instituição.

d) A metodologia desenvolvida contempla a verificação de aspectos de adequação à LGPD, ou seja, tratam aspectos de conformidade. Nesse sentido, ressalta-se que não se contempla a verificação de aspectos de desempenho, os quais estariam relacionados à medição do rendimento do processo sob a ótica da economicidade, da eficácia, da eficiência e da efetividade.

e) Os resultados obtidos na mensuração devem ser interpretados sob a ótica da gestão, para auxílio na tomada de decisão dos gestores públicos. Nesse sentido, é importante que a mensuração seja preenchida observando-se a boa-fé, buscando-se a veracidade, a fidedignidade e a exatidão das respostas. Ressalta-se que a mensuração não tem foco na constatação de irregularidades ou na aplicação de penalidades, porém, isso não significa isentar os órgãos de suas obrigações e responsabilidades. Salienta-se que é dever do agente público ter sua conduta permeada pela pelos valores da ética, devendo ainda observar o princípio da responsabilização e prestação de contas (Art. 6º, X, LGPD).

[4] Disponível em: <https://tecnologia.prefeitura.sp.gov.br/arquivos/ot-volumes/OT_vol3.pdf#page=35> Acesso em: 21/03/2024

2. CONSIDERAÇÕES INICIAIS

f) Os resultados obtidos na mensuração não devem ser interpretados como um “selo” de garantia de cumprimento à LGPD, uma vez que a própria ANPD não reconhece nenhuma metodologia capaz de atestar tal situação. O cenário de proteção de dados pessoais no país é dinâmico e encontra-se em constante evolução, de modo que os órgãos devem adotar práticas de revisões e de melhoria contínua em um processo de constante monitoramento.

g) A metodologia desenvolvida não representa ou se manifesta em nome de nenhuma das referências de normas técnicas e/ou boas práticas utilizadas. Sugere-se que os órgãos que desejarem se aprofundar no estudo a respeito dos controles e práticas adotadas pelas referências analisadas consultem diretamente as fontes oficiais de informação ofertadas pelas próprias instituições.

3. CONTROLES INTERNOS RELACIONADOS À PROTEÇÃO DE DADOS PESSOAIS

A metodologia desenvolvida pela CGM-SP consiste na verificação da implementação de controles relacionados a requisitos da LGPD e boas práticas no tema pelos órgãos da PMSP. Trata-se de um processo no qual o controle interno das unidades é avaliado com o objetivo de se fornecer razoável segurança de que os principais requisitos relacionados à proteção de dados pessoais estão sendo observados.

Foram selecionados 70 controles para verificação, contemplando os níveis estratégico, tático e operacional dos órgãos, divididos em 8 temas e 5 fases para mensuração. A divisão em temas busca melhor organização para direcionar a resposta das unidades. Já a divisão em fases proporciona vantagens como a priorização dos controles, a melhor distribuição da avaliação no tempo, a melhor compreensão da situação de cada unidade avaliada, a maior agilidade na implementação dos controles e a maior profundidade nas análises.

3.1. DO AGRUPAMENTO DOS CONTROLES POR TEMAS

A fim de se promover melhor organização dos controles, foi realizado agrupamento por temas, totalizando os 08 temas descritos a seguir (o detalhamento dos controles por tema encontra-se no Apêndice 2):

1. Estrutura organizacional: A LGPD estabelece no Art. 50 que os controladores e operadores poderão formular regras de boas práticas e de governança que definam as condições de organização, o regime de funcionamento, procedimentos e outras ações referentes à governança em privacidade e proteção de dados pessoais. Espera-se que seja definida a estrutura organizacional para executar as funções relacionadas ao tratamento de dados pessoais, com a determinação dos principais colaboradores dessa estrutura, suas competências e suas responsabilidades.

2. Governança: O Art. 50 da LGPD prevê que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições gerais de organização e funcionamento da unidade com relação ao tratamento de dados pessoais. O órgão deve desenvolver e implementar políticas para gerenciar e monitorar os requisitos regulatórios, legais, de risco e operacionais da organização, de modo que sejam compreendidos por todos e que direcionem as ações de tratamento de dados pessoais de forma organizada e coordenada.

3. Tratamento de dados pessoais: Com base no Art. 50 da LGPD, os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam procedimentos relacionados ao tratamento de dados pessoais. Nesse sentido, espera-se que o órgão tenha mapeado e desenhado os principais fluxos sobre a execução de funções relacionadas ao tratamento de dados pessoais, de acordo com o Art. 37 da LGPD.

4. Direitos dos titulares: CConforme os princípios do livre acesso e qualidade dos dados estabelecido no Art. 6º da LGPD e os direitos do titular de dados pessoais, previsto no Art. 18, o controlador deve garantir aos titulares o acesso facilitado e gratuito a seus dados pessoais, com direito a correção de dados incompletos, inexatos ou desatualizados. Deve-se ainda garantir exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e a finalidade de seu tratamento.

5. Resposta a incidentes: De acordo com o Art. 50, § 2º, I, g, LGPD, o órgão deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais. É importante estabelecer uma estrutura adequada para executar esta função e implementar procedimentos de identificação, registro, tratamento de incidentes e comunicação às autoridades competentes e aos titulares dos dados pessoais, nos casos que possam acarretar risco ou dano relevante.

6. Transparência: O princípio da transparência está previsto no Art. 6º, VI, LGPD. O controlador, ao tratar dados pessoais, deve atender a este princípio, assegurando a disponibilização de informações claras, precisas, atuais e facilmente acessíveis aos titulares sobre o tratamento de seus dados. As informações exigidas pela LGPD devem ser disponibilizadas de forma adequada, ostensiva, em linguagem simples e acessível, de modo a assegurar o efetivo conhecimento do titular a respeito das atividades de tratamento realizadas pelo controlador, bem como sobre os seus direitos e a forma de exercê-lo, preferencialmente na página eletrônica do órgão.

7. Segurança da Informação: Os dados pessoais sob os cuidados e custódia do Poder Público devem ser protegidos conforme orientações previstas na LGPD em seus Arts. 46, 47, 49 e 50. O órgão deve adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade.

8. Gestão de terceiros: O Art. 39 da LGPD estabelece que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. A supervisão em terceiros visa garantir a implementação de ações previstas pelo controlador no intuito de atender aos requisitos de conformidade com as leis e regulamentos de proteção de dados em vigor e requisitos de privacidade.

3.2. DAS FASES PARA VERIFICAÇÃO DOS CONTROLES

O processo de adequação à LGPD não ocorre de uma só vez, trata-se de um movimento contínuo, que pode ser feito de forma seriada. Nesse sentido, observa-se que a implementação de alguns controles depende da adoção de controles anteriores, de modo que o processo de adequação deve ocorrer de forma gradual. Um exemplo é a realização do inventário de dados pessoais, que depende do prévio mapeamento de processos da instituição (vide Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo).

Foram definidas cinco fases de verificação, descritas a seguir (o detalhamento dos controles por fase encontra-se no Apêndice 3):

a) Fase 01 - Preparatório: todos os órgãos são inicialmente classificados nesta fase, que se caracteriza pela execução de atividades de tratamento de dados pessoais de forma não estruturada. Após a implementação dos controles exigidos nesta fase, espera-se que as instituições já executem as principais atividades relacionadas à privacidade e à proteção de dados pessoais, possuindo seus processos de negócio mapeados. Contudo, sua atuação ainda deve estar baseada em competências previstas na lei, dependendo de habilidades específicas de indivíduos que ocupam determinadas posições.

b) Fase 02 - Básico: os órgãos devem completar a implementação de todos os controles previstos na fase anterior para progredir à Fase 02. Após a implementação dos controles exigidos nesta fase, as instituições devem ter seus processos de negócio formalizados em procedimentos e fluxos, havendo documentação que demonstre como o trabalho deve ser realizado. Espera-se que o órgão tenha revisado seus principais processos e atividades relacionados à privacidade e à proteção de dados pessoais.

c) Fase 03 - Intermediário: os órgãos devem completar a implementação de todos os controles previstos nas fases anteriores para progredir à Fase 03. Após a implementação dos controles exigidos nesta fase, as instituições devem ter seus processos de negócio definidos em regulamento próprio, havendo políticas e normas disciplinando os procedimentos. Espera-se que o órgão tenha controle e documentação sobre seus principais processos e atividades relacionados à privacidade e à proteção de dados pessoais. Após a conclusão da Fase 03, considera-se que as instituições possuem controles robustos relacionados à implementação da LGPD, de modo que as próximas fases de verificação terão foco em aspectos de monitoramento e de melhoria contínua.

d) Fase 04 - Avançado: os órgãos devem completar a implementação de todos os controles previstos nas fases anteriores para progredir à Fase 04. Após a implementação dos controles exigidos nesta fase, as instituições devem possuir gerenciamento sobre os seus processos através de indicadores de desempenho, monitorando a implementação dos controles com maior profundidade. Espera-se que as instituições realizem o monitoramento periódico sobre os planos elaborados anteriormente (ex.: capacitação, implementação de controles, vulnerabilidades técnicas, entre outros).

e) Fase 05 – Institucionalização: os órgãos devem completar a implementação de todos os controles previstos nas fases anteriores para progredir à Fase 05. Nesta etapa, há verificação da institucionalização na operação de todas as práticas previstas para o tratamento de dados pessoais, havendo constantes revisões, atualizações e busca por melhoria contínua. Esta etapa possui verificação contínua e não possui previsão de encerramento ou conclusão definitiva, em alinhamento ao ciclo PDCA.

3.3. RESUMO DA ESTRUTURAÇÃO DOS CONTROLES

Conforme explicado, os controles foram agrupados por temas e divididos em fases para verificação. O quadro a seguir ilustra a estrutura dos controles esquematizada (o detalhamento dos controles esquematizado encontra-se no Apêndice 4):

Tema	Fase 01 – Preparatório	Fase 02 - Básico	Fase 03 – Intermediário	Fase 04 – Avançado	Fase 05 – Institucionalização	Total de controles por tema
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 controle por fase	**15**	**15**	**14**	**11**	**15**	**70**

Fonte: CGM/CPD

4. PROCEDIMENTO DE VERIFICAÇÃO DOS CONTROLES

O procedimento de verificação dos controles está dividido em quatro etapas principais:

a) Autoavaliação pelos órgãos da PMSP: A autoavaliação permite que os gestores públicos avaliem seu próprio sistema de controle interno, fornecendo evidências de implementação dos controles avaliados.

b) Análise da existência dos controles por CGM/CPD: A análise da existência dos controles por CGM/CPD é predominantemente uma análise documental, com objetivo de verificar a existência dos controles pelos órgãos. A análise da existência dos controles por CGM/CPD será feita de forma amostral sobre os órgãos que concluírem alguma das fases.

c) Monitoramento por CGM/CPD: O monitoramento será realizado por CGM/CPD, através de novas análises de fases já concluídas, selecionadas de forma amostral sobre os órgãos que já passaram pela análise da existência dos controles por CGM/CPD, constituindo etapa importante na busca pela atualização da implementação dos controles e pela melhoria contínua.

Para além do procedimento descrito neste tópico, destaca-se que CGM/AUDI poderá realizar trabalhos de auditoria de forma independente e objetiva sobre a temática de proteção de dados pessoais nos órgãos da PMSP.

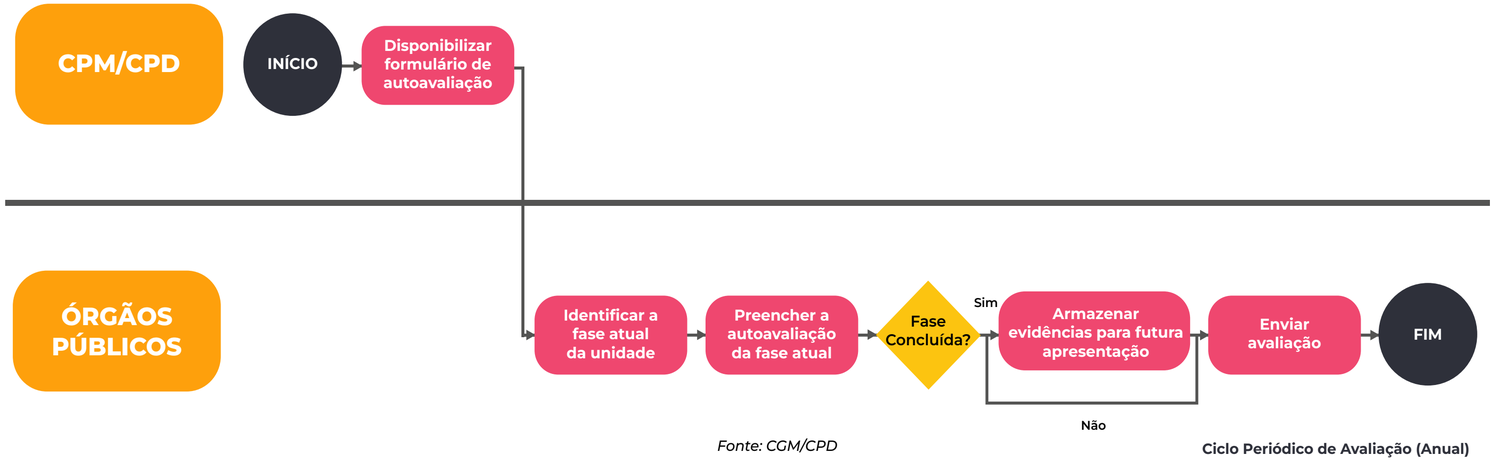
Figura 01 – Procedimento de verificação dos controles

Fonte: CGM/CPD

5. DA AUTOAVALIAÇÃO PELOS ÓRGÃOS DA PMSP

A autoavaliação é a primeira etapa do procedimento de verificação dos controles.

Figura 02 – Da autoavaliação pelos órgãos da PMSP



Fonte: CGM/CPD

Ciclo Periódico de Avaliação (Anual)

5.1. DO PREENCHIMENTO DA FERRAMENTA

Na autoavaliação de controles (do inglês CSA – Control Self Assessment), a instituição deverá preencher questionário através de formulário online disponibilizado anualmente pela CGM/CPD. A autoavaliação é uma ferramenta útil para a difusão do conhecimento sobre os controles relacionados à privacidade e à proteção de dados pessoais no ambiente interno das instituições. Sua utilização permite que os gestores públicos avaliem seu próprio sistema de controle interno (relacionado a aspectos de adequação à LGPD), aumentando seu grau de conhecimento sobre a operação e identificando pontos fortes e fracos.

5.2. DO RESPONSÁVEL PELO PREENCHIMENTO

O responsável pelo preenchimento da autoavaliação é o Chefe de Gabinete do respectivo órgão, por força do Art. 7 do Decreto Municipal nº 59.767/2020, podendo contar com o auxílio de representantes de outros setores, como a Assessoria Jurídica, a Tecnologia da Informação, entre outros. A CGM/CPD permanecerá disponível para orientar as unidades e solucionar dúvidas no preenchimento da ferramenta.

5.3. DAS MÉTRICAS PARA VERIFICAÇÃO DOS CONTROLES

Para a verificação de cada controle presente no questionário, o órgão deve responder em sua autoavaliação com "Sim" (informa a existência do controle, sinalizando a conformidade), "Não" (informa a inexistência e/ou não conclusão da implementação do controle, sinalizando a não conformidade) ou "Não se aplica" (desde que justificado, informa a inaplicabilidade do controle à instituição avaliada, a fim de se personalizar a avaliação).

5.4. DA FASE DE AVALIAÇÃO

Ao preencher a autoavaliação, a unidade deverá identificar a fase em que se encontra e realizar a avaliação dos controles apenas desta fase. É importante salientar que os controles de uma fase somente serão mensurados após a conclusão da implementação dos controles da fase anterior. Isto porque eles estão organizados de forma lógica e devem seguir a prioridade determinada.

5.5. DAS EVIDÊNCIAS DE ATENDIMENTO AOS CONTROLES

A autoavaliação é atividade realizada através de procedimento formal e documentado (em atendimento ao princípio da responsabilização e prestação de contas), seguindo-se as orientações de CGM/CPD. Todos os controles devem estar acompanhados de evidência apropriada e suficiente, que de fato ateste a sua existência (evidências documentais). A anexação das evidências será solicitada apenas quando o órgão concluir a implementação de todos os controles da fase em que estiver. Nota-se que essas evidências são importantes também para facilitar acordos com parceiros de negócios quando o tratamento de dados pessoais é mutuamente relevante, além de serem importantes para instruir respostas a ações de controle interno e externo a que a unidade esteja submetida.

5.6. DA PERIODICIDADE

O ciclo de avaliação é anual. Ao final de cada ciclo, CGM/CPD disponibilizará um Guia Orientativo com o detalhamento dos requisitos necessários para conclusão de cada fase de avaliação atualizados. Cada órgão deverá submeter a sua avaliação no formulário, escolhendo a fase de medição em que se encontrar.

6. DA ANÁLISE DA EXISTÊNCIA DOS CONTROLES POR CGM/CPD

A análise da existência dos controles por CGM/CPD será predominantemente uma análise documental. Seu objetivo é verificar a existência dos controles implementados pelos órgãos.

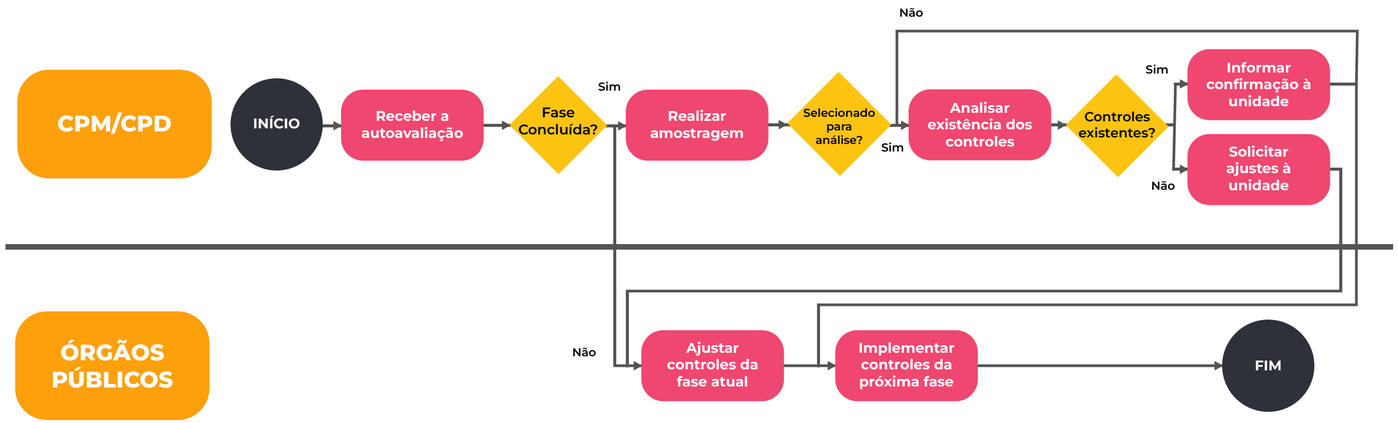
Todos os órgãos deverão preencher o formulário disponibilizado por CGM/CPD na fase de avaliação em que se encontrarem, porém, a anexação das evidências será solicitada apenas quando o órgão concluir a implementação dos controles da respectiva fase avaliada.

A análise da existência dos controles por CGM/CPD será feita de forma amostral sobre os órgãos que concluírem alguma das fases. Independentemente de ter sido selecionado ou não para análise após a conclusão de uma fase, os órgãos podem seguir com a implementação dos controles da fase seguinte no próximo ciclo de avaliação.

A análise de CGM/CPD busca garantir maior segurança e alinhamento às boas práticas sobre os resultados da autoavaliação dos diferentes órgãos. O resultado da análise será informado ao órgão:

- Se a CGM/CPD entender pela confirmação da autoavaliação após o procedimento de análise de existência dos controles, isto será informado à unidade.
- Caso a CGM/CPD conclua pela não confirmação da autoavaliação, será formalizada lista de ajustes necessários para a unidade, correspondente aos controles que apresentaram alguma irregularidade na sua implementação. Os órgãos deverão implementar os ajustes necessários para o próximo ciclo de avaliação.

Figura 03 – Da análise da existência dos controles por CGM/CPD



Fonte: CGM/CPD

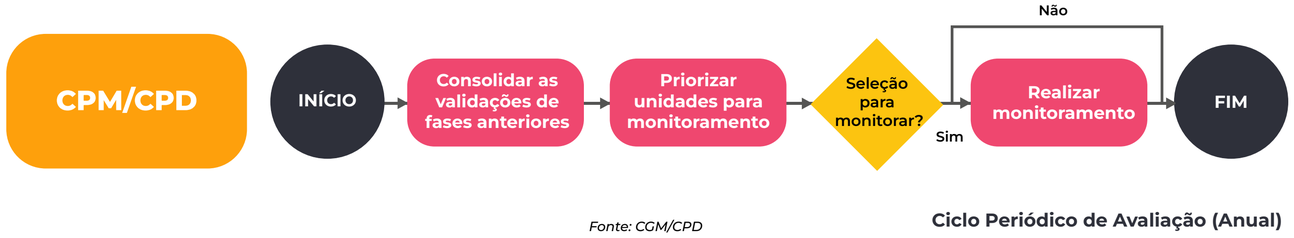
7. DO MONITORAMENTO POR CGM/CPD

Após o órgão obter a confirmação da autoavaliação de alguma das fases, ela entrará em procedimento de monitoramento por CGM/CPD.

No procedimento de monitoramento, será feita uma nova análise sobre fases que já foram avaliadas, de modo que as unidades devem manter os controles avaliados em fases anteriores sempre implementados e atualizados. O cronograma das ações de monitoramento será definido a critério de CGM/CPD, devendo ser divulgado às unidades da PMSP previamente à sua realização.

Caso o procedimento de monitoramento avalie que a unidade não possui mais os controles de fases anteriores adequadamente aplicados, CGM/CPD irá solicitar os ajustes necessários e será concedido prazo para que o órgão implemente as correções. Desta forma, não haverá regressão da unidade à fase anterior. Porém, caso a unidade não implemente os ajustes necessários no devido prazo, no próximo ciclo de avaliação, haverá regressão para a fase que se encontrar pendente.

Figura 05 – Do monitoramento por CGM/CPD



Fonte: CGM/CPD

8. CICLO DE AVALIAÇÃO

O ciclo de avaliação é composto de duas partes.

A primeira é composta pelo ciclo interno, no qual a própria instituição preenche a sua autoavaliação, realiza análise de lacunas, planeja as ações e as implementa. A condução destas atividades é inspirada no ciclo PDCA, buscando-se a melhoria contínua dos processos.

Por sua vez, a segunda parte é composta pelo ciclo externo, no qual a CGM/CPD irá realizar a análise da existência dos controles, além de conduzir outras atividades, como o acompanhamento e apoio das instituições, o monitoramento e o diagnóstico amplo da PMSP.

8.1. CICLO INTERNO DE AVALIAÇÃO – ATIVIDADES DOS ÓRGÃOS DA PMSP

O ciclo interno de avaliação é conduzido pela própria instituição avaliada. Trata-se de procedimento que possui quatro etapas principais, inspiradas no ciclo PDCA, buscando-se a melhoria contínua, com periodicidade anual.

a. Autoavaliação: O ciclo se inicia com a autoavaliação pela instituição acerca da implementação dos controles da fase em que se encontrar no período. Nesta etapa, a finalidade é obter autoconhecimento sobre a situação da implementação dos controles da instituição.

- Se a instituição concluir a implementação de todos os controles de uma fase, passa-se ao ciclo externo de avaliação, no qual haverá análise da existência dos controles por CGM/CPD. Independentemente de ter sido selecionado ou não para análise após a conclusão de uma fase, os órgãos podem seguir com a implementação dos controles da fase seguinte no próximo ciclo de avaliação.

b. Análise de lacunas: A segunda etapa do ciclo interno de avaliação é composta pela análise de lacunas. Nesta etapa, a instituição realiza uma análise dos controles que ainda não foram implementados de acordo com a sua autoavaliação, mapeando, portanto, as lacunas que necessitam de ações a serem tomadas. Caso a instituição não tenha implementado todos os controles de uma fase, a análise identificará quais controles ainda faltam ser implementados para a conclusão da fase. Havendo conclusão da implementação dos controles da fase, a análise identificará os controles da fase seguinte para verificação no próximo ciclo de avaliação. Se a análise da existência dos controles pela CGM/CPD identificar pendências, a análise de lacunas também deve mapear estes pontos para implementação.

c. Planejamento: A terceira etapa do ciclo interno de avaliação corresponde ao planejamento das ações. Neste momento, busca-se elaborar um plano de ação com as medidas a serem implementadas ou melhoradas, com base na análise de lacunas realizada anteriormente.

d. Implementação: Por fim, a quarta e última etapa do ciclo interno é a implementação dos controles e medidas identificadas e planejadas anteriormente, em busca do atingimento de todos os controles da fase de avaliação em que a instituição estiver. Após a finalização desta etapa, inicia-se novamente o ciclo interno através de uma nova autoavaliação, conduzindo-se, portanto, um ciclo de melhoria contínua.

8.2. CICLO EXTERNO DE AVALIAÇÃO – ATIVIDADES DE CGM/CPD

O ciclo externo de avaliação é composto por quatro atividades principais conduzidas por CGM/CPD:

a. Análise da existência dos controles por CGM/CPD: A análise da existência dos controles por CGM/CPD sobre a autoavaliação realizada pelos órgãos ocorrerá de forma amostral, selecionando-se para análise parte das instituições que concluírem a implementação de todos os controles da fase sob análise. Independentemente de ter sido selecionado ou não para análise após a conclusão de uma fase, os órgãos podem seguir com a implementação dos controles da fase seguinte no próximo ciclo de avaliação. Caso a CGM/CPD identifique pontos que necessitem de ajustes, a instituição deverá corrigir as pendências.

b. Diagnóstico amplo da PMSP: O diagnóstico amplo de toda a PMSP permite uma visão geral do nível de adequação dos órgãos à LGPD, de modo a fornecer informações importantes para a tomada de decisões estratégicas e a elaboração de políticas públicas, por exemplo. O diagnóstico amplo será realizado após a compilação de todas as autoavaliações preenchidas pelos órgãos da PMSP.

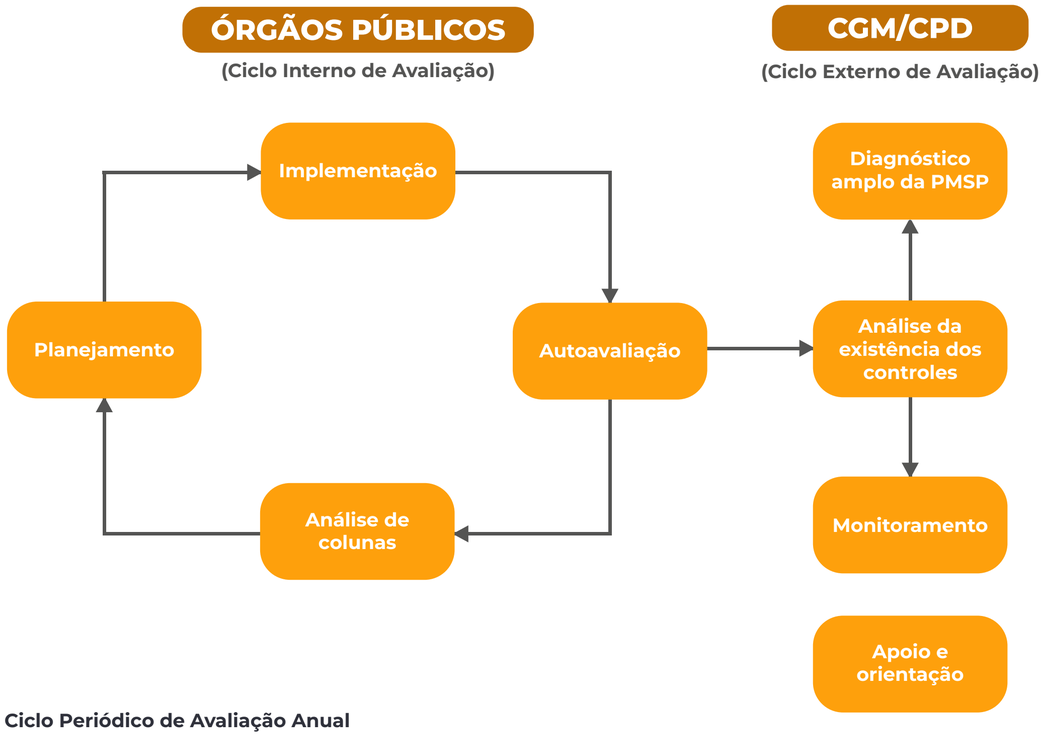
c. Monitoramento: A CGM/CPD também executará atividades de monitoramento, de modo que as fases anteriormente cumpridas pelos órgãos poderão ser novamente analisadas. O monitoramento será realizado através de novas análises de fases já concluídas, selecionadas de forma amostral sobre os órgãos que já passaram pela análise da existência dos controles por CGM/CPD. Isto implica na necessidade de que os controles anteriormente avaliados estejam sempre implementados e atualizados, em um procedimento de melhoria contínua.

d. Apoio e orientação: Ao longo do ciclo externo de avaliação, a CGM/CPD permanecerá disponível para orientar as unidades e solucionar dúvidas no preenchimento da ferramenta. Ademais, a fim de se aumentar o engajamento dos órgãos para que concluam a implementação dos controles de cada fase e realizem a inscrição para análise da existência dos controles, a CGM/CPD irá conduzir atividades de apoio e acompanhamento ao longo do ciclo.

8.3. RESUMO DO CICLO DE AVALIAÇÃO

O quadro a seguir ilustra o ciclo de avaliação dos controles, conforme explicado neste tópico:

Figura 06 – Ciclo de avaliação dos controles



Fonte: CGM/CPD

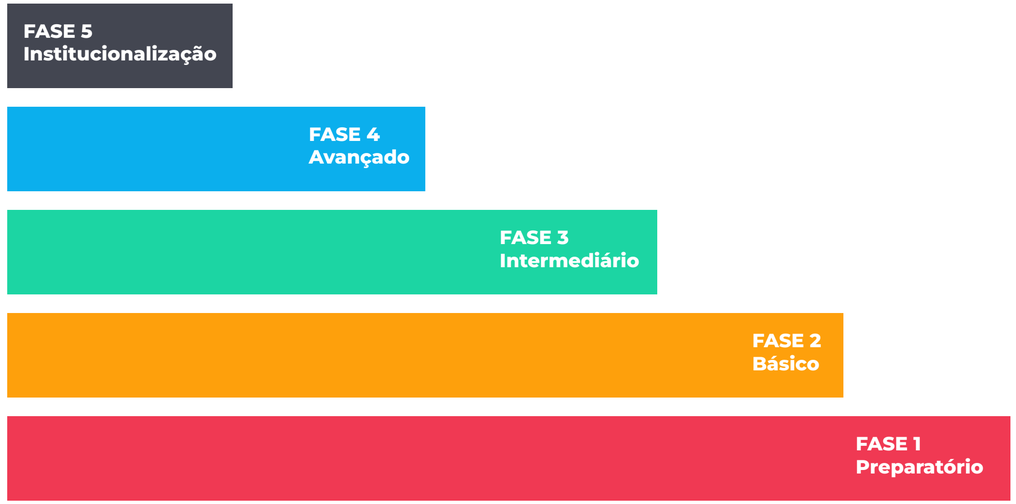
9. DIAGNÓSTICO AMPLO DA PMSP

A partir da compilação de todas as autoavaliações preenchidas pelos órgãos da PMSP, será possível obter o diagnóstico amplo da PMSP de maturidade em proteção de dados pessoais. O diagnóstico amplo tem como base as mesmas fases de avaliação dos controles, permitindo a classificação geral da PMSP em uma destas fases.

A PMSP será classificada conforme o órgão que estiver na fase mais inicial do diagnóstico (ex. Enquanto um órgão estiver na Fase 01, a PMSP será classificada também na Fase 01, mesmo que os demais órgãos estejam em fases mais avançadas). A seguir estão resumidas as cinco fases de classificação da PMSP no diagnóstico amplo de maturidade em proteção de dados pessoais:

a. **Fase 01 - Preparatório:** classificação inicial da PMSP independentemente do avanço dos órgãos na implementação dos controles.
b. **Fase 02 - Básico:** o diagnóstico amplo considera a classificação da PMSP na Fase 02 quando todos os órgãos avaliados concluírem a Fase 01.
c. **Fase 03 - Intermediário:** o diagnóstico amplo considera a classificação da PMSP na Fase 03 quando todos os órgãos avaliados concluírem a Fase 02.
d. **Fase 04 - Avançado:** o diagnóstico amplo considera a classificação da PMSP na Fase 04 quando todos os órgãos avaliados concluírem a Fase 03.
e. **Fase 05 - Institucionalização:** o diagnóstico amplo considera a classificação da PMSP na Fase 05 quando todos os órgãos avaliados concluírem a Fase 04.

Figura 07 – Diagnóstico amplo de maturidade em proteção de dados pessoais



Fonte: CGM/CPD

APÊNDICE 1 – LISTA COMPLETA DOS CONTROLES

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
01. O órgão possui a indicação formal de um **Encarregado** da proteção de dados pessoais?	Art. 6º, X, Art. 23, III, LGPD	O órgão deve designar oficialmente o Encarregado, através da sua nomeação por Portaria publicada no Diário Oficial da Cidade.
02. O órgão possui um **Grupo de Trabalho** ou estrutura equivalente, para apoiar na adequação à LGPD?	Art. 6º, X, Art. 50, LGPD	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.
03. O órgão realizou no período atividade de **sensibilização** (estímulo à reflexão sobre a importância da LGPD com vistas à mudança de comportamentos) dos seus agentes públicos acerca da LGPD por meio de ações como disponibilização de informativos, condução de workshops, realização de palestras ou seminários, entre outros?	Art. 6º, X, Art. 50, LGPD Art. 14, VI, IN/CGM nº 01/2022	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. O objetivo da sensibilização é de promover mudanças no comportamento dos indivíduos, demonstrando a importância de cada um para o atingimento da mudança organizacional. Podem ocorrer na forma de campanhas institucionais, disponibilização de materiais educacionais (apresentações, vídeos, guias, cartilhas, etc.), comunicação contínua com os colaboradores (e-mails, cartazes, etc.), elaboração de atividades (desafios, programas de incentivos, quizzes, atividades interativas, etc.), avaliações de conhecimento (testes, dinâmicas, avaliações, etc.), entre outros.
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?	Art. 6º, VIII, LGPD Art. 4º, III, Art. 15, Decreto nº 59.767/2020 Art. 13, I, Art. 14, I, IN/CGM nº 01/2022	O órgão deve documentar o diagnóstico de sua situação atual de conformidade à LGPD e as ações e medidas necessárias para implementação futura, visando a sua adequação às melhores práticas de proteção de dados. Espera-se que seja apresentado cronograma para implementação das ações previstas.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
05. O órgão realizou, revisou ou atualizou no período o **mapeamento dos processos** que tratam dados pessoais?	Art. 6º, VIII, LGPD Art. 4º, I, Decreto nº 59.767/2020 Art. 2º, Art. 14, IV, b, IN/CGM nº 01/2022	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.
06. O órgão realizou, revisou ou atualizou no período o **mapeamento de dados pessoais** dos processos mapeados?	Art. 6º, VIII, Art. 37, LGPD Art. 4º, I, Decreto nº 59.767/2020 Art. 2º, Art. 14, IV, IN/CGM nº 01/2022	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. A elaboração do mapeamento é importante para entender como os dados pessoais são coletados e como se movem pelo órgão, facilitando a rápida localização de um dado mapeado em caso de vazamento, assim como o rápido atendimento a uma requisição do titular.
07. O órgão realizou, revisou ou atualizou no período a identificação das **finalidades e das hipóteses legais** que são consideradas para o tratamento de dados pessoais?	Art. 6º, I, II, III, Art. 23, I, LGPD Art. 10, Art. 14, IV, f, IN/CGM nº 01/2022	A identificação das finalidades e das hipóteses legais para o tratamento de dados pessoais envolve o levantamento das normas 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. As atividades de tratamento de dados pessoais devem ter propósitos legítimos e específicos, sendo informados ao titular.
08. O órgão disponibiliza **canal** específico para recebimento de demandas de atendimento aos direitos dos titulares referentes à LGPD?	Art. 6º, IV, Arts. 17 a 20, LGPD Art. 6º, Decreto nº 59.767/2020	É importante 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.
09. Existe um **canal** apropriado para o recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação?	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	É importante que o órgão disponibilize canal apropriado para o recebimento de denúncias e encaminhamento de solução a respeito dos incidentes.
10. O órgão divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?	Art. 6º, VI, Art. 41, § 1º, LGPD Art. 5º, parágrafo único, Decreto nº 59.767/2020	A identidade e as informações de contato (ex: e-mail, telefone) do Encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico do órgão.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
11. O órgão informa a respeito do **tratamento** de dados pessoais realizado no âmbito de suas competências, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os compartilhamentos, as transferências, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos?	Art. 6º, IV, VI, Art. 9º, I, II, Art. 23, I LGPD Art. 11, II, Decreto nº 59.767/2020 Art. 10, IN/CGM nº 01/2022	Conforme Art. 9º 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.
12. O órgão ao coletar **cookies** identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for o caso, no cumprimento de obrigações ou atribuições legais?	Art. 6º, VI, Art. 9º, Art. 18, LGPD Art. 10, IN/CGM nº 01/2022	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.
13. O órgão mantém um **inventário de software e de ativos de tecnologia da informação**, executando também um processo de configuração segura de todos os ativos e softwares?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD , OT nº 004 e 013 do Decreto nº 57.653/2017	É uma boa prática manter um inventário preciso, detalhado e atualizado periodicamente de todos os ativos institucionais com potencial para armazenar ou processar dado, 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 (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações).
14. 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?	Art. 6º, VIII, Art. 33, II, b, Art. 39, LGPD Art. 114, III do Decreto nº 62.100/2022	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.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
15. O órgão realizou, revisou ou atualizou no período o mapeamento dos contratos firmados com terceiros (operadores, co-controladores, provedores de serviço de TI, fornecedores, etc), contemplando os registros de **compartilhamentos e transferências internacionais** de dados pessoais realizados, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?	Art. 6º, VIII, Art. 26, Art. 27, Art. 37, Art. 39, LGPD Art. 14, IV, j, k, l, IN/CGM nº 01/2022	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 conveniente que o órgão tenha registro dos compartilhamentos e das transferências internacionais de dados pessoais realizados.
16. O **Encarregado** da proteção de dados pessoais participou no período de alguma capacitação específica direcionada à sua função?	Art. 6º, X, Art. 50, LGPD Art. 13, III, IN/CGM nº 01/2022	A atuação do Encarregado envolve conhecimentos multidisciplinares que devem estar em constante atualização. É importante que o Encarregado acompanhe as atualizações e orientações da Autoridade Nacional de Proteção de Dados (ANPD) a respeito de temas que impactem a sua atuação (guias orientativos, instruções técnicas), assim como aprimore os seus conhecimentos sobre a Lei de Acesso à Informação (LAI), o Marco Civil da Internet, Gestão de Riscos e Segurança da Informação, entre outros temas. Aconselha-se que o Encarregado ainda tenha conhecimento das normas técnicas e controles da International Organization for Standardization (ISO), em especial àquelas referentes a riscos, Segurança da Informação, tratamento de dados pessoais e privacidade.
17. O **Grupo de Trabalho** de apoio à Adequação à LGPD participou no período de algum treinamento relacionado com a temática de proteção de dados pessoais?	Art. 6º, X, Art. 50, LGPD Art. 13, III, IN/CGM nº 01/2022	É importante que o órgão elabore um Plano de Capacitação de seus agentes públicos que determine as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais, mapeando as lacunas de conhecimento associadas ao tema e planejando ações para redução dessas lacunas. Espera-se que recursos humanos envolvidos em atividades relacionadas à adequação do órgão à LGPD recebam treinamento além do nível básico fornecido aos demais colaboradores.
18. O Órgão elaborou e/ou atualizou no período o seu **Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais** (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?	Art. 6º, VIII, LGPD Art. 4º, II, Decreto nº 59.767/202	O órgão deve realizar as atividades de identificação, avaliação e tratamento dos riscos associados aos processos que realizam tratamento de dados pessoais. Isto é importante para a compreensão da probabilidade e do impacto de cada risco, possibilitando a priorização de ações e também o gerenciamento dos controles que devem ser implantados para se manter um nível de risco adequado à Política de Riscos do órgão.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
19. O órgão elaborou e/ou atualizou no período a sua **Política de Gestão de Riscos em Segurança da Informação, Privacidade e Proteção de Dados Pessoais** (documento que contém diretrizes gerais relacionadas à gestão de riscos, a definição do apetite e da tolerância ao risco, além de estabelecer os objetivos e comunicar o comprometimento da unidade em relação à gestão de riscos)?	Art. 6º, VIII, Art. 50, LGPD Art. 4º, II, Decreto nº 59.767/2020 Art. 4º e 14, V, h, IN/CGM nº 01/2022	O órgão deve estabelecer Política de Gestão de Riscos (ou documento similar) em Segurança da Informação, Privacidade e Proteção de Dados Pessoais, de modo a orientar os seus agentes públicos sobre os riscos existentes em sua atuação. Essa avaliação auxilia a organização a compreender as consequências e as probabilidades dos riscos para direcionar a definição de quais processos devem ser priorizados na iniciativa de adequação à LGPD.
20. O órgão adequou e/ou revisou, conforme a necessidade, **seus processos e atividades** relacionadas ao tratamento de dados pessoais às legislações/normativos vigentes, implementando o conceito de ***Privacy by Design e Privacy by Default***, de modo que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD?	Art. 6º, VIII, Art. 46, § 2º, Art. 50, § 2º, I, a, LGPD	O órgão deve assegurar que os processos e sistemas internos sejam projetados de forma que os tratamentos de dados pessoais estejam alinhados aos princípios e valores da LGPD, desde a fase de concepção do produto ou do serviço até a sua execução. É importante que o órgão revise seus processos e atividades atuais, adotando medidas que visem implementar a proteção de dados pessoais.
21. O órgão tem definido um **fluxo de atendimento** das demandas dos titulares de dados pessoais?	Art. 6º, X, Art. 50, LGPD Art. 13, III, IN/CGM nº 01/2022	É importante que o órgão esteja preparado para responder as demandas dos titulares de dados pessoais. Assim, é uma boa prática definir as responsabilidades e estruturar os procedimentos de atendimento, evitando possíveis ruídos e o descumprimento dos prazos.
22. O órgão **responde às solicitações** dos titulares quanto aos seus dados pessoais, observando os seus direitos, conforme disposto pela LGPD?	Art. 6º, IV, Art. 19, II, Art. 23, § 3º, LGPD	Quando aplicável, a organização deve atender aos direitos dos titulares assegurados pela LGPD (Arts. 17 a 20), como, por exemplo: confirmação da existência de tratamento; acesso aos dados; e correção de dados.
23. O órgão tem definido um **fluxo de comunicação às autoridades e aos titulares de dados pessoais a respeito dos incidentes e violações** que possam acarretar risco ou danos?	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	É importante que o órgão estabeleça responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação que envolvem violação de dados pessoais. Entre os procedimentos necessários, destaca-se a definição de fluxo de comunicação às autoridades competentes e ao titular dos dados a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
24. O órgão **comunica as autoridades e os titulares de dados** sobre os incidentes e violações que possam acarretar risco ou danos, fornecendo todas as informações pertinentes, quando solicitado pelas autoridades competentes?	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	O órgão deve comunicar, em prazo razoável, às autoridades competentes e ao titular de dados pessoais, a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante. Ademais, deve fornecer, quando solicitado por instituição competente, informações relativas a violações de privacidade, juntamente com as ações adotadas para mitigar os riscos decorrentes da violação.
25. O órgão adequou e/ou revisou o seu **Portal da Transparência**, conforme a necessidade, de modo a se ajustar às exigências da LGPD com relação aos dados pessoais publicizados (análise de necessidade e adequação)?	Art. 6º, I, II, III, IV, VI, LGPD	Pelo princípio do livre acesso e da transparência, garante-se aos titulares de dados pessoais, a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Desta forma, espera-se que o Portal da Transparência esteja ajustado às exigências da LGPD com relação aos dados pessoais publicizados.
26. Foram estabelecidas **arquitetura e infraestrutura de redes seguras**, com a manutenção de **rede corporativa** segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD, OT nº 002 e 013 do Decreto nº 57.653/2017	A gestão do controle de acesso às informações é necessária a fim de se ofertar o acesso aos dados pessoais exclusivamente àqueles que detenham propósitos legítimos e específicos. O controle de acesso lógico é utilizado em espaços digitais, como aplicações utilizadas pela organização. No caso da rede corporativa, é importante que haja segmentação em domínios lógicos, limitando-se o acesso às redes e aos serviços especificamente para aqueles autorizados à utilizá-los.
27. O órgão mantém **softwares antimalware**, incluindo proteções para servidor de e-mail, navegador web e outras defesas contra malware?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD, OT nº 013 do Decreto nº 57.653/2017	É considerada uma boa prática de Segurança de Informação implantar e manter proteção antimalware de servidores de e-mail, como varredura de anexos e/ou sandbox. É importante instalar e manter atualizado um software antimalware em todos os ativos cibernéticos da organização.
28. Existem e são executados processos periódicos de **cópias de segurança** dos servidores, roteadores, infraestrutura da rede corporativa, e das configurações e sistemas operacionais?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD, OT nº 007 e 013 do Decreto nº 57.653/2017	Entre as boas práticas para garantia da disponibilidade da informação está a realização de processos periódicos de cópias de segurança (backup), a fim de se garantir o acesso aos dados em caso de ameaças de perdas e destruição.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
29. O órgão adequou e/ou revisou, conforme a necessidade, os **instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres**, a fim de manter a sua conformidade à LGPD?	Art. 6º, X, Art. 33, II, b, LGPD	O controlador deve firmar contrato com terceiros (operadores, co-controladores e fornecedores, entre outros) com quem compartilha dados pessoais, para assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles. É importante que os contratos, instrumentos convocatórios e instrumentos congêneres estejam alinhados à LGPD.
30. O órgão adequou e/ou revisou, conforme a necessidade, os **compartilhamentos e as transferências internacionais** de dados pessoais, a fim de manter a sua **conformidade** com os critérios estabelecidos na LGPD?	Art. 6º, VIII, LGPD Art. 13, II, IN/CGM nº 01/2022	Os compartilhamentos e as transferências internacionais de dados pessoais devem respeitar os critérios estabelecidos na LGPD. Assim, deve-se revisar, conforme a necessidade, os compartilhamentos realizados para ajustá-los à legislação.
31. As **funções e responsabilidades** dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas (em normativo, política, procedimento ou documento similar)?	Art. 6º, VIII, LGPD Art. 13, II, IN/CGM nº 01/2022	Os recursos humanos envolvidos em atividades relacionadas ao tratamento de dados pessoais devem ter as suas funções e responsabilidades determinadas em normativo, política, procedimento ou documento similar, sendo comunicadas de maneira clara.
32. O órgão realizou no período campanha institucional de **conscientização** (transmissão de conhecimentos teóricos e práticos com vistas a capacitação técnica para atuação profissional) sobre a LGPD voltada para seus agentes públicos, por meio de ações como cursos, treinamentos ou oficinas, entre outros?	Art. 6º, X, Art. 50, LGPD Art. 14, VI, IN/CGM nº 01/2022	A conscientização 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 conscientização envolvem a organização de forma sistêmica, disponibilizadas para todos os colaboradores, ainda que nem todos tenham participado. O objetivo da conscientização é de transmitir conhecimento aos indivíduos, promovendo a interiorização e a apreensão de informações (dados, estatísticas, conceitos, etc) que auxiliem os indivíduos no entendimento do contexto. Podem ocorrer na forma de campanhas institucionais, disponibilização de materiais educacionais (apresentações, vídeos, guias, cartilhas, etc.), comunicação contínua com os colaboradores (e-mails, cartazes, etc.), elaboração de atividades (desafios, programas de incentivos, quizzes, atividades interativas, etc.), avaliações de conhecimento (testes, dinâmicas, avaliações, etc.), entre outros.
33. O órgão elaborou e/ou atualizou no período o **Relatório de Impacto à Proteção de Dados Pessoais?**	Art. 4º, § 3º, Art. 6º, VIII, Art. 10, § 3º, Art. 32, Art. 38, Art. 50, LGPD Art. 4º, IV, Decreto nº 59.767/2020 Art. 3º, IN/CGM nº 01/2022	O Relatório de Impacto à Proteção de Dados Pessoais é um documento que contém a identificação dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares e também a descrição das medidas adotadas para tratamento desses riscos. É importante que o documento seja anualmente atualizado.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
34. O órgão elaborou e/ou atualizou no período o seu **Programa de Governança em Privacidade e Proteção de Dados Pessoais?**	Art. 6º, VIII, LGPD Art. 4º, III, Art. 15, Decreto nº 59.767/2020 Art. 13, I, Art. 14, I, IN/CGM nº 01/2022	O Programa de Governança em Privacidade e Proteção de Dados Pessoais é o principal documento que reúne as ações do órgão com relação à privacidade e à proteção de dados pessoais.
35. A organização possui **Política de Classificação da Informação** ou instrumento similar, abrangendo diretrizes para a classificação de dados pessoais?	Art. 6º, III, LGPD Art. 12, II, Decreto nº 57.783/2017 - Política Municipal de Gestão Documental (PGDOC) Art. 11 a 18, Portaria SGM/SEGES/CGDOC nº 01/2021	Considerando o ciclo do tratamento de dados pessoais, verifica-se que há possibilidade de eliminação dos dados pessoais: (i) a pedido do titular, caso não sejam necessários à consecução de interesse público; (ii) após a utilização, por desnecessidade de armazenamento; ou (iii) por temporalidade. Nesse sentido, o órgão deve consultar a Tabela de Temporalidade de Documentos e os parâmetros relativos ao tempo de guarda e eliminação dos dados de que tem posse.
36. O Órgão possui uma **Tabela de Temporalidade de Documentos** (ou documento similar) ou adota parâmetros e controles relativos ao tempo de guarda e eliminação dos dados de que tem posse?	Art. 6º, III, LGPD Art. 12, II, Decreto nº 57.783/2017 - Política Municipal de Gestão Documental (PGDOC) Art. 11 a 18, Portaria SGM/SEGES/CGDOC nº 01/2021	Considerando o ciclo do tratamento de dados pessoais, verifica-se que há possibilidade de eliminação dos dados pessoais: (i) a pedido do titular, caso não sejam necessários à consecução de interesse público; (ii) após a utilização, por desnecessidade de armazenamento; ou (iii) por temporalidade. Nesse sentido, o órgão deve consultar a Tabela de Temporalidade de Documentos e os parâmetros relativos ao tempo de guarda e eliminação dos dados de que tem posse.
37. O órgão possui uma **Política de Atendimento** (ou documento similar) aos direitos dos titulares?	Art. 6º, IV, Art. 18, Art. 23, § 3º, LGPD	É importante que o órgão esteja preparado para responder às demandas dos titulares de dados pessoais. Assim, é uma boa prática definir as responsabilidades e estruturar os procedimentos de atendimento, evitando possíveis ruídos e o descumprimento dos prazos.
38. O órgão realiza o controle de recebimento e resposta das **petições** recebidas dos titulares de dados pessoais?	Art. 6º, IV, Art. 18, Art. 19, LGPD	Convém que o órgão possua um procedimento para gestão de recebimento e de resposta às petições recebidas dos titulares de dados pessoais.
39. O órgão possui uma **Política de Resposta a Incidentes** (ou documento similar) para tratar violações relativas à privacidade dos titulares de dados pessoais?	Art. 6º, X, Art. 50, § 2º, I, g, LGPD	É importante que o órgão estabeleça responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de Segurança da Informação que envolvem violação de dados pessoais.
40. Todas as violações de dados pessoais são **documentadas para fins de rastreabilidade**, em atendimento ao princípio da responsabilização e da prestação de contas?	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	Convém que o órgão possua um procedimento de registro e gestão de incidentes de Segurança da Informação, que viabilize o tratamento de casos que envolvem violação de dados pessoais com organização e celeridade.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
41. O órgão possui e divulga a **Política de Privacidade e Proteção de Dados Pessoais** em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?	Art. 6º, IV, VI, VIII, Art. 9º, VII, Art. 23, 50, LGPD	A Política de Privacidade deve ser publicada em local facilmente acessível pelos titulares de dados pessoais. A Política de Privacidade e Proteção de Dados Pessoais é importante para institucionalizar no órgão o comprometimento para alcançar a conformidade com os normativos de proteção de dados pessoais.
42. O órgão possui uma **Política de Segurança da Informação** (ou documento similar) contendo diretrizes e procedimentos sobre controle de acesso, uso de senhas, rotina de backup, uso de cookies, entre outros?	Art. 6º, VII, LGPD, OT nº 013 do Decreto nº 57.653/2017	A Política de Segurança da Informação é um documento oficial que inclui informações, regras e práticas com o objetivo de proteger a propriedade, a confidencialidade, a disponibilidade e a integridade da informação de diversas ameaças existentes, tais como invasões e outros tipos de ataques.
43. O órgão possui uma **Política de Contratações de Terceiros** (Gerenciamento de Fornecedores, Due Dilligence, ou documento similar) adequada às exigências da LGDP, contendo disposições específicas para cada modalidade de contratação, informando os documentos e requisitos necessários que devem instruir cada procedimento?	Art. 6º, VIII, Art. 33, II, b, Art. 39, LGPD	Uma boa prática de tratamento de dados pessoais envolve o estabelecimento de um procedimento de gestão de contratações de terceiros. É importante definir as disposições específicas para cada modalidade de contratação, criar cláusulas contratuais padrão, instituir procedimentos de fiscalização, entre outras ações pertinentes.
44. O órgão, ao compartilhar ou transferir dados pessoais, adota um processo de **formalização e registro, incluindo a comunicação à CGM-SP no caso de compartilhamento a pessoa de direito privado**, identificando objeto e finalidade, responsabilidades, nível de serviço, base legal, duração e outras condições do tratamento?	Art. 6º, VI, Art. 25, Art. 26, Art. 27, Art. 30, LGPD Art. 14, I, Decreto nº 59.767/2020 Art. 12, IN/CGM nº 01/2022	É conveniente que a organização tenha registros sobre os dados que passam por compartilhamento ou transferência internacional. Ademais, é necessário que o órgão informe a autoridade competente no caso de compartilhamento a pessoa de direito privado (Conforme Art. 14 do Decreto nº 59.767/2020, os órgãos e entidades da Administração Pública Municipal podem efetuar a comunicação ou o uso compartilhado de dados pessoais a pessoa de direito privado, desde que o Controlador Geral do Município informe a Autoridade Nacional de Proteção de Dados, na forma do regulamento federal correspondente).

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
45. O órgão executa e monitora o seu **Plano de Capacitação em Privacidade e Proteção de Dados Pessoais** (processo permanente aprendizagem com o objetivo de desenvolver competências individuais) para seus colaboradores, contemplando atividades de conscientização periódicas, incluindo ações especializadas para os colaboradores que exercem funções com responsabilidades relacionadas à proteção de dados pessoais?	Art. 6º, X, Art. 50, LGPD Art. 13, III, Art. 14, VI, IN/CGM nº 01/2022	É importante que o órgão elabore um Plano de Capacitação de seus agentes públicos que contemple treinamento a respeito de privacidade e proteção de dados pessoais. É necessário que todos os colaboradores do órgão estejam cientes da importância do tema na sua área de atuação, sendo importante a sua participação em treinamentos periódicos sobre aspectos gerais de privacidade e de proteção de dados pessoais. Espera-se que os recursos humanos envolvidos em atividades relacionadas ao tratamento de dados pessoais recebam treinamento além do nível básico fornecido aos demais colaboradores.
46. O órgão executa e monitora o seu **Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais** (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?	Art. 6º, VIII, LGPD Art. 4º, II, Decreto nº 59.767/2020	O órgão deve executar e monitorar o seu Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, de modo a manter os riscos em nível aceitável pela Política de Riscos do órgão.
47. O Órgão conta com processo formal e documentado de gestão do **Consentimento do Titular de Dados** (quando utiliza esta hipótese legal), fornecendo instrumentos adequados para que o titular de dados pessoais manifeste o seu consentimento, quando necessário, de forma livre, informada e inequívoca?	Art. 6º, IV, Art. 8º, § 5º, LGPD Art. 10, IN/CGM nº 01/2022	O processo de gestão de consentimento necessita de um controle detalhado de quais consentimentos o titular de dados pessoais concedeu, proibiu, suspendeu ou cancelou. Fornecer meios práticos para os titulares gerenciarem seus dados pessoais de forma simples, rápida e eficiente é importante para a garantia do direito à transparência e ao acesso à informação.
48. A organização mantém o controle se os dados pessoais são retidos (armazenados) durante o **tempo estritamente** necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas (em observância à Tabela de Temporalidade de Documentos)?	Art. 6º, I, III, LGPD	A organização não deve reter dados pessoais por tempo maior do que o estritamente necessário para cumprir com as finalidades de tratamento de dados que foram determinadas.
49. O órgão monitora **Indicadores de Desempenho** com relação ao atendimento aos Direitos dos Titulares?	Art. 19, II, Art. 23, § 3º, LGPD	O monitoramento da perspectiva de desempenho dos órgãos deve ser realizado a partir da definição de indicadores. Exemplos de indicadores de atendimento aos direitos dos titulares são: total de consultas; total de reclamações; total de respostas fora do prazo; total de atendimentos automatizados.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
50. O órgão monitora **Indicadores de Desempenho** com relação às respostas aos incidentes de segurança?	Art. 48, § 1º, LGPD	O monitoramento da perspectiva de desempenho dos órgãos deve ser realizado a partir da definição de indicadores. Exemplos de indicadores de respostas aos incidentes de segurança são: quantidade de incidentes de segurança; tipos de incidentes; tempo de respostas.
51. O órgão implementa meios práticos para permitir que os **titulares gerenciem os seus dados pessoais**, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular?	Art. 6º, IV, Art. 18, § 5º, LGPD	O processo de gestão de consentimento necessita de um controle detalhado de quais consentimentos o titular de dados pessoais concedeu, proibiu, suspendeu ou cancelou. Fornecer meios práticos para os titulares gerenciarem seus dados pessoais de forma simples, rápida e eficiente é importante para a garantia do direito à transparência e ao acesso à informação.
52. O órgão realiza o monitoramento das **vulnerabilidades técnicas** nos tratamentos de dados pessoais, incluindo o monitoramento e **defesa da rede** (sistemas de detecção e alerta para eventos de segurança)?	Art. 6º, VII, LGPD Art. 4º, IN/CGM nº 01/2022, OT nº 013 do Decreto nº 57.653/2017	Considera-se uma boa prática realizar o monitoramento de vulnerabilidades técnicas nos tratamentos de dados pessoais, bem como gerir medidas de segurança, técnicas e administrativas, aptas à proteção de dados pessoais contra ameaças e vulnerabilidades, considerados os riscos inerentes e residuais ao processo ou atividade.
53. A instituição realiza a **gestão do controle de contas e acessos (físicos e lógicos)** centralizada, considerando o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais, em que deve ser dado **acesso apenas aos dados pessoais** necessários para o desempenho das funções dos colaboradores?	AArt. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD , OT nº 013 do Decreto nº 57.653/2017	A ANPD recomenda a aplicação do princípio do menor privilégio (need to know), segundo o qual os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades.
54. O órgão **monitora e inspeciona** a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores e terceiros?	Art. 6º, VIII, Art. 33, II, b, Art. 47, LGPD	O órgão deve ter contrato firmado com terceiros com quem compartilhe dados pessoais, sendo uma boa prática monitorar e inspecionar a implementação dos requisitos estabelecidos nas cláusulas contratuais, a fim de assegurar a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles.
55. O órgão monitora e comunica qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados?	Art. 6º, V, Art. 18, § 6º, Art. 39, LGPD	Com o objetivo de implementar o princípio da qualidade dos dados, espera-se que o órgão possua processo estruturado para comunicar qualquer alteração, correção ou remoção dos dados pessoais para terceiros com quem os dados foram compartilhados.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
56. O órgão estabelece e mantém contato com as **autoridades relevantes, grupos de interesse especial ou fóruns especializados**, buscando-se atualização e conhecimento das melhores práticas na área?	Art. 6º, X, Art. 50, LGPD	Convém que o órgão busque comunicação com as autoridades relevantes, grupos de interesse especial ou fóruns especializados. Trata-se de um meio para melhorar o conhecimento sobre as melhores práticas no tema e manter constante atualização, compartilhando informações e recebendo avisos, alertas, entre outros.
57. O órgão submete o seu **Programa de Governança em Privacidade e Proteção de Dados Pessoais** a revisão e reavaliação periódicas em um processo contínuo de gerenciamento de riscos de segurança?	Art. 6º, VIII, LGPD Art. 4º, III, Art. 15, Decreto nº 59.767/2020 Art. 13, I, Art. 14, I, IN/CGM nº 01/2022	O Programa de Governança em Privacidade e Proteção de Dados Pessoais é o principal documento que reúne as ações do órgão com relação à privacidade e à proteção de dados pessoais, devendo ser atualizado periodicamente, com vistas à melhoria contínua.
58. O órgão, ao realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, mantém controles para restringir o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária?	Art. 6º, III, Art. 11, II, f, LGPD	De acordo com o Art. 11 da LGPD, o tratamento de dados pessoais sensíveis poderá ocorrer sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
59. O órgão mantém controles para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais?	Art. 6º, VII, Art. 13, § 1º, LGPD	De acordo com o Art. 13 § 1º da LGPD, a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais.
60. O órgão mantém controles sobre os dados pessoais que necessitam ser **anonimizados** de acordo com o tratamento e exigências estabelecidas por leis aplicáveis?	Art. 6º, I, III, Art. 12, Art. 13, Art. 18, IV, LGPD	De acordo com o Art. 5º, III da LGPD, dado anonimizado é dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
61. O órgão mantém controles sobre a manutenção dos dados em formato **interoperável e estruturado** para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?	Art. 6º, V, Art. 25, LGPD Art. 14, III, IN/CGM nº 01/2022	De acordo com o Art. 25 da LGPD, os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
62. O órgão mantém controles sobre o tratamento de dados pessoais de **crianças e adolescentes**, com o objetivo de verificar o atendimento ao seu melhor interesse, conforme preconizado pelo art. 14 da LGPD?	Art. 6º, I, Art. 14, LGPD	O tratamento de dados pessoais de crianças deverá ser realizado no seu melhor interesse com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
63. O órgão mantém controles sobre as técnicas ou métodos apropriados para garantir **exclusão ou destruição segura de dados pessoais** (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD	Dentre as boas práticas da Segurança da Informação, destaca-se o procedimento de descarte seguro dos dados pessoais que estejam em sua posse, ao encerrar a execução do contrato ou após a satisfação da finalidade pretendida.
64. O órgão mantém controles sobre as decisões relacionadas ao titular de dados pessoais que são baseadas em **tratamento automatizado** e fornece, sempre que solicitada, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados?	Art. 20, § 1º, LGPD	O órgão deve mapear as decisões que são realizadas com base em tratamento automatizado, informando os critérios e procedimentos utilizados para a decisão.
65. O órgão mantém controles que o permitam **otimizar as respostas aos titulares** (ex. análise estatística das demandas, uso de modelos de respostas, análise de gargalos, pesquisa de satisfação, etc.)?	Art. 6º, VI, LGPD	É importante que o órgão estabeleça procedimentos de melhoria contínua no atendimento aos direitos dos titulares. Como exemplo, podem-se citar a análise estatística das demandas, uso de modelos de respostas, análise de gargalos, pesquisa de satisfação, etc.
66. O órgão executa as atividades de **documentação e de avaliação pós-incidente**, promovendo uma análise detalhada dos incidentes para identificar as suas causas, as lições aprendidas e as recomendações para prevenir futuros incidentes similares, buscando implementar os pontos de melhoria e revisar políticas e procedimentos?	Art. 6º, X, Art. 50, § 2º, I, g, LGPD	Os conhecimentos adquiridos com os incidentes de segurança da informação devem ser utilizados para reforçar e melhorar os controles de segurança da informação.
67. O órgão mantém controles sobre os níveis de acesso dos processos que utilizam dados pessoais, quando tramitados pelo Sistema Eletrônico de Informação - SEI, a fim de monitorar o cumprimento às regras de classificação de acesso adequadas à LGPD (em observância à Política de Classificação da Informação)?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD	A gestão do controle de acesso às informações é necessária a fim de se ofertar o acesso aos dados pessoais exclusivamente àqueles que detenham propósitos legítimos e específicos. O controle de acesso lógico é utilizado em espaços digitais, como aplicações utilizadas pela organização. No caso do SEI, é importante que os processos que utilizam dados pessoais tenham as regras de classificação de acesso respeitadas.

CONTROLE	REFERÊNCIA	TEXTO EXPLICATIVO CGM-SP
68. O órgão mantém controle de registros de eventos (logs), considerando o princípio de minimização de dados, gravando o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD, OT nº 013 do Decreto nº 57.653/2017	É importante que o órgão registre os eventos (logs) das atividades de tratamento de dados pessoais de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados ou tratados. Quando houver alterações nos dados, também deve ser registrada a ação realizada (ex: inclusão, alteração ou exclusão). Tal procedimento é importante para se garantir a rastreabilidade do tratamento de dados, garantindo-se a também os princípios da responsabilização e da prestação de contas.
69. O órgão mantém controles sobre as **medidas de proteção de dados pessoais adotadas pelas entidades** com quem compartilha dados pessoais?	Art. 6º, X, Art. 25, Art. 26, Art. 27, Art. 30, Art. 47, LGPD	Considera-se uma boa prática solicitar a descrição formal das medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais.
70. O órgão mantém controles sobre o compartilhamento ou transferência de dados pessoais e se tais atividades são realizadas por meio de um **canal criptografado** e de cifra recomendada pelos sítios especializados de segurança?	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD Art. 13, II, IN/CGM nº 01/2022	A utilização de criptografia reforça a proteção da confidencialidade, da autenticidade e da integridade da informação. A adoção de mecanismos de criptografia no trânsito e no armazenamento de dados pessoais pode mitigar riscos associados à violação dos dados.

APÊNDICE 2 – LISTA DOS CONTROLES POR TEMA

TEMA 01 - ESTRUTURA ORGANIZACIONAL

FASE	CONTROLE
1	01. O órgão possui a indicação formal de um Encarregado da proteção de dados pessoais?
1	02. O órgão possui um Grupo de Trabalho ou estrutura equivalente, para apoiar na adequação à LGPD?
1	03. O órgão realizou no período atividade de sensibilização (estímulo à reflexão sobre a importância da LGPD com vistas à mudança de comportamentos) dos seus agentes públicos acerca da LGPD por meio de ações como disponibilização de informativos, condução de workshops, realização de palestras ou seminários, entre outros?
2	16. O Encarregado da proteção de dados pessoais participou no período de alguma capacitação específica direcionada à sua função?
2	17. O Grupo de Trabalho de apoio à Adequação à LGPD participou no período de algum treinamento relacionado com a temática de proteção de dados pessoais?
3	31. As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas (em normativo, política, procedimento ou documento similar)?
3	32. O órgão realizou no período campanha institucional de conscientização (transmissão de conhecimentos teóricos e práticos com vistas a capacitação técnica para atuação profissional) sobre a LGPD voltada para seus agentes públicos, por meio de ações como cursos, treinamentos ou oficinas, entre outros?
4	45. O órgão executa e monitora o seu Plano de Capacitação em Privacidade e Proteção de Dados Pessoais (processo permanente aprendizagem com o objetivo de desenvolver competências individuais) para seus colaboradores, contemplando atividades de conscientização periódicas, incluindo ações especializadas para os colaboradores que exercem funções com responsabilidades relacionadas à proteção de dados pessoais?
5	56. O órgão estabelece e mantém contato com as autoridades relevantes, grupos de interesse especial ou fóruns especializados, buscando-se atualização e conhecimento das melhores práticas na área?

TEMA 02 - GOVERNANÇA

FASE	CONTROLE
1	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?
2	18. O Órgão elaborou e/ou atualizou no período o seu Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?
2	19. O órgão elaborou e/ou atualizou no período a sua Política de Gestão de Riscos em Segurança da Informação, Privacidade e Proteção de Dados Pessoais (documento que contém diretrizes gerais relacionadas à gestão de riscos, a definição do apetite e da tolerância ao risco, além de estabelecer os objetivos e comunicar o comprometimento da unidade em relação à gestão de riscos)?
3	33. O órgão elaborou e/ou atualizou no período o Relatório de Impacto à Proteção de Dados Pessoais?
3	34. O órgão elaborou e/ou atualizou no período o seu Programa de Governança em Privacidade e Proteção de Dados Pessoais?
4	31. As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas (em normativo, política, procedimento ou documento similar)?
5	32. O órgão realizou no período campanha institucional de conscientização (transmissão de conhecimentos teóricos e práticos com vistas a capacitação técnica para atuação profissional) sobre a LGPD voltada para seus agentes públicos, por meio de ações como cursos, treinamentos ou oficinas, entre outros?
4	46. O órgão executa e monitora o seu Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?
5	57. O órgão submete o seu Programa de Governança em Privacidade e Proteção de Dados Pessoais a revisão e reavaliação periódicas em um processo contínuo de gerenciamento de riscos de segurança?

TEMA 03 - TRATAMENTO DE DADOS PESSOAIS

FASE	CONTROLE
1	05. O órgão realizou, revisou ou atualizou no período o mapeamento de processos que tratam dados pessoais?
1	06. O órgão realizou, revisou ou atualizou no período o mapeamento de dados pessoais dos processos mapeados?
1	07. O órgão realizou, revisou ou atualizou no período a identificação das finalidades e das hipóteses legais que são consideradas para o tratamento de dados pessoais?
2	20. O órgão adequou e/ou revisou, conforme a necessidade, seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/ normativos vigentes, implementando o conceito de Privacy by Design e Privacy by Default, de modo que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD?
3	35. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo diretrizes para a classificação de dados pessoais?
3	36. O Órgão possui uma Tabela de Temporalidade de Documentos (ou documento similar) ou adota parâmetros e controles relativos ao tempo de guarda e eliminação dos dados de que tem posse?
4	47. O Órgão conta com processo formal e documentado de gestão do Consentimento do Titular de Dados (quando utiliza esta hipótese legal), fornecendo instrumentos adequados para que o titular de dados pessoais manifeste o seu consentimento, quando necessário, de forma livre, informada e inequívoca?
4	48. A organização monitora se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas (em observância à Tabela de Temporalidade de Documentos)?
5	58. O órgão, ao realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, mantém controles para restringir o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária?
5	59. O órgão mantém controles para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais?
5	60. O órgão mantém controles sobre os dados pessoais que necessitam ser anonimizados de acordo com o tratamento e exigências estabelecidas por leis aplicáveis?
5	61. O órgão mantém controles sobre a manutenção dos dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
5	62. O órgão mantém controles sobre o tratamento de dados pessoais de crianças e adolescentes, com o objetivo de verificar o atendimento ao seu melhor interesse, conforme preconizado pelo art. 14 da LGPD?
5	63. O órgão mantém controles sobre as técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?
5	64. O órgão mantém controles sobre as decisões relacionadas ao titular de dados pessoais que são baseadas em tratamento automatizado e fornece, sempre que solicitada, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados?

TEMA 04 - DIREITOS DOS TITULARES

FASE	CONTROLE
1	08. O órgão disponibiliza canal específico para recebimento de demandas de atendimento aos direitos dos titulares referentes à LGPD?
2	21. O órgão tem definido um fluxo de atendimento das demandas dos titulares de dados pessoais?
2	22. O órgão responde às solicitações dos titulares quanto aos seus dados pessoais, observando os seus direitos conforme disposto pela LGPD?
3	37. O órgão possui uma Política de Atendimento (ou documento similar) aos direitos dos titulares?
3	38. O órgão realiza o controle de recebimento e resposta das petições recebidas dos titulares de dados pessoais?
4	49. O órgão monitora Indicadores de Desempenho com relação ao atendimento aos Direitos dos Titulares?
5	65. O órgão mantém controles que o permitam otimizar as respostas aos titulares (ex. análise estatística das demandas, uso de modelos de respostas, análise de gargalos, pesquisa de satisfação, etc.)?

TEMA 05 - RESPOSTA A INCIDENTES

FASE	CONTROLE
1	09. Existe um canal apropriado para o recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação?
2	23. O órgão tem definido um fluxo de comunicação às autoridades e aos titulares de dados pessoais a respeito dos incidentes e violações que possam acarretar risco ou danos?
2	24. O órgão comunica as autoridades e os titulares de dados sobre os incidentes e violações que possam acarretar risco ou danos, fornecendo todas as informações pertinentes, quando solicitado pelas autoridades competentes?
3	39. O órgão possui uma Política de Resposta a Incidentes (ou documento similar) para tratar violações relativas à privacidade dos titulares de dados pessoais?
3	40. Todas as violações de dados pessoais são documentadas para fins de rastreabilidade, em atendimento ao princípio da responsabilização e da prestação de contas?
4	50. O órgão monitora Indicadores de Desempenho com relação às respostas aos incidentes de segurança?
5	66. O órgão executa as atividades de documentação e de avaliação pós-incidente, promovendo uma análise detalhada dos incidentes para identificar as suas causas, as lições aprendidas e as recomendações para prevenir futuros incidentes similares, buscando implementar os pontos de melhoria e revisar políticas e procedimentos?

TEMA 06 - TRANSPARÊNCIA

FASE	CONTROLE
1	10. O órgão divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?
1	11. O órgão informa a respeito do tratamento de dados pessoais realizado no âmbito de suas competências, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os compartilhamentos, as transferências, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos?
1	12. O órgão ao coletar cookies identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/ categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for o caso, no cumprimento de obrigações ou atribuições legais?
2	25. O órgão adequou e/ou revisou o seu Portal da Transparência, conforme a necessidade, de modo a se ajustar às exigências da LGPD com relação aos dados pessoais publicizados (análise de necessidade e adequação)?
3	41. O órgão possui e divulga a Política de Privacidade e Proteção de Dados Pessoais em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?
4	51. O órgão implementa meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular?
5	67. O órgão mantém controles sobre os níveis de acesso dos processos que utilizam dados pessoais, quando tramitados pelo Sistema Eletrônico de Informação - SEI, a fim de monitorar o cumprimento às regras de classificação de acesso adequadas à LGPD (em observância à Política de Classificação da Informação)?

TEMA 07 - SEGURANÇA DA INFORMAÇÃO

FASE	CONTROLE
1	13. O órgão mantém um inventário de software e de ativos de tecnologia da informação, executando também um processo de configuração segura de todos os ativos e softwares?
2	26. Foram estabelecidas arquitetura e infraestrutura de redes seguras, com a manutenção de rede corporativa segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
2	27. O órgão mantém softwares antimalware, incluindo proteções para servidor de e-mail, navegador web e outras defesas contra malware?
2	28. Existem e são executados processos periódicos de cópias de segurança dos servidores, roteadores, infraestrutura da rede corporativa, e das configurações e sistemas operacionais?
3	42. O órgão possui uma Política de Segurança da Informação (ou documento similar) contendo diretrizes e procedimentos sobre controle de acesso, uso de senhas, rotina de backup, uso de cookies, entre outros?
4	52. O órgão realiza o monitoramento das vulnerabilidades técnicas nos tratamentos de dados pessoais, incluindo o monitoramento e defesa da rede (sistemas de detecção e alerta para eventos de segurança)?
4	53. A instituição realiza a gestão do controle de contas e acessos (físicos e lógicos) centralizada, considerando o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais, em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos colaboradores?
5	68. O órgão mantém controle de registros de eventos (logs), considerando o princípio de minimização de dados, gravando o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento?

TEMA 08 - GESTÃO DE TERCEIROS

FASE	CONTROLE
1	14. 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?
1	15. O órgão realizou, revisou ou atualizou no período o mapeamento dos contratos firmados com terceiros (operadores, co-controladores, provedores de serviço de TI, fornecedores, etc), contemplando os registros de compartilhamentos e transferências internacionais de dados pessoais realizados, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?
2	29. O órgão adequou e/ou revisou, conforme a necessidade, os instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres, a fim de manter a sua conformidade à LGPD?
2	30. O órgão adequou e/ou revisou, conforme a necessidade, os compartilhamentos e as transferências internacionais de dados pessoais, a fim de manter a sua conformidade com os critérios estabelecidos na LGPD?
3	43. O órgão possui uma Política de Contratações de Terceiros (Gerenciamento de Fornecedores, Due Dilligence, ou documento similar) adequada às exigências da LGDP, contendo disposições específicas para cada modalidade de contratação, informando os documentos e requisitos necessários que devem instruir cada procedimento?
3	44. O órgão, ao compartilhar ou transferir dados pessoais, adota um processo de formalização e registro, incluindo a comunicação à CGM-SP no caso de compartilhamento a pessoa de direito privado, identificando objeto e finalidade, responsabilidades, nível de serviço, base legal, duração e outras condições do tratamento?
4	54. O órgão monitora e inspeciona a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores e terceiros?
4	55. O órgão monitora e comunica qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados?
5	69. O órgão mantém controles sobre as medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais?
5	70. O órgão mantém controles sobre o compartilhamento ou transferência de dados pessoais e se tais atividades são realizadas por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança?

APÊNDICE 3 – LISTA DOS CONTROLES POR FASE DE VERIFICAÇÃO

FASE 01 - PREPARATÓRIO

GRUPO	CONTROLE
01. Estrutura organizacional	01. O órgão possui a indicação formal de um Encarregado da proteção de dados pessoais?
01. Estrutura organizacional	02. O órgão possui um Grupo de Trabalho ou estrutura equivalente, para apoiar na adequação à LGPD?
01. Estrutura organizacional	03. O órgão realizou no período atividade de sensibilização (estímulo à reflexão sobre a importância da LGPD com vistas à mudança de comportamentos) dos seus agentes públicos acerca da LGPD por meio de ações como disponibilização de informativos, condução de workshops, realização de palestras ou seminários, entre outros?
02. Governança	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?
03. Tratamento de dados pessoais	05. O órgão realizou, revisou ou atualizou no período o mapeamento de processos que tratam dados pessoais?
03. Tratamento de dados pessoais	06. O órgão realizou, revisou ou atualizou no período o mapeamento de dados pessoais dos processos mapeados?
03. Tratamento de dados pessoais	07. O órgão realizou, revisou ou atualizou no período a identificação das finalidades e das hipóteses legais que são consideradas para o tratamento de dados pessoais?
04. Direitos dos titulares	08. O órgão disponibiliza canal específico para recebimento de demandas de atendimento aos direitos dos titulares referentes à LGPD?
05. Resposta a incidentes	09. Existe um canal apropriado para o recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação?
06. Transparência	10. O órgão divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?
06. Transparência	11. O órgão informa a respeito do tratamento de dados pessoais realizado no âmbito de suas competências, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os compartilhamentos, as transferências, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos?
06. Transparência	12. O órgão ao coletar cookies identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for o caso, no cumprimento de obrigações ou atribuições legais?
07. Segurança da Informação	13. O órgão mantém um inventário de software e de ativos de tecnologia da informação, executando também um processo de configuração segura de todos os ativos e softwares?
08. Gestão de terceiros	14. 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?
08. Gestão de terceiros	15. O órgão realizou, revisou ou atualizou no período o mapeamento dos contratos firmados com terceiros (operadores, co-controladores, provedores de serviço de TI, fornecedores, etc), contemplando os registros de compartilhamentos e transferências internacionais de dados pessoais realizados, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?

FASE 02 - BÁSICO

GRUPO	CONTROLE
01. Estrutura organizacional	16. O Encarregado da proteção de dados pessoais participou no período de alguma capacitação específica direcionada à sua função?
01. Estrutura organizacional	17. O Grupo de Trabalho de apoio à Adequação à LGPD participou no período de algum treinamento relacionado com a temática de proteção de dados pessoais?
02. Governança	18. O Órgão elaborou e/ou atualizou no período o seu Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?
02. Governança	19. O órgão elaborou e/ou atualizou no período a sua Política de Gestão de Riscos em Segurança da Informação, Privacidade e Proteção de Dados Pessoais (documento que contém diretrizes gerais relacionadas à gestão de riscos, a definição do apetite e da tolerância ao risco, além de estabelecer os objetivos e comunicar o comprometimento da unidade em relação à gestão de riscos)?
03. Tratamento de dados pessoais	20. O órgão adequou e/ou revisou, conforme a necessidade, seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos vigentes, implementando o conceito de Privacy by Design e Privacy by Default, de modo que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD?
04. Direitos dos titulares	21. O órgão tem definido um fluxo de atendimento das demandas dos titulares de dados pessoais?
04. Direitos dos titulares	22. O órgão responde às solicitações dos titulares quanto aos seus dados pessoais, observando os seus direitos conforme disposto pela LGPD?
05. Resposta a incidentes	23. O órgão tem definido um fluxo de comunicação às autoridades e aos titulares de dados pessoais a respeito dos incidentes e violações que possam acarretar risco ou danos?
05. Resposta a incidentes	24. O órgão comunica as autoridades e os titulares de dados sobre os incidentes e violações que possam acarretar risco ou danos, fornecendo todas as informações pertinentes, quando solicitado pelas autoridades competentes?
06. Transparência	25. O órgão adequou e/ou revisou o seu Portal da Transparência, conforme a necessidade, de modo a se ajustar às exigências da LGPD com relação aos dados pessoais publicizados (análise de necessidade e adequação)?
07. Segurança da Informação	26. Foram estabelecidas arquitetura e infraestrutura de redes seguras, com a manutenção de rede corporativa segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
07. Segurança da Informação	27. O órgão mantém softwares antimalware, incluindo proteções para servidor de e-mail, navegador web e outras defesas contra malware?
07. Segurança da Informação	28. Existem e são executados processos periódicos de cópias de segurança dos servidores, roteadores, infraestrutura da rede corporativa, e das configurações e sistemas operacionais?
08. Gestão de terceiros	29. O órgão adequou e/ou revisou, conforme a necessidade, os instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres, a fim de manter a sua conformidade à LGPD?
08. Gestão de terceiros	30. O órgão adequou e/ou revisou, conforme a necessidade, os compartilhamentos e as transferências internacionais de dados pessoais, a fim de manter a sua conformidade com os critérios estabelecidos na LGPD?

FASE 03 - INTERMEDIÁRIO

GRUPO	CONTROLE
01. Estrutura organizacional	31. As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas (em normativo, política, procedimento ou documento similar)?
01. Estrutura organizacional	32. O órgão realizou no período campanha institucional de conscientização (transmissão de conhecimentos teóricos e práticos com vistas a capacitação técnica para atuação profissional) sobre a LGPD voltada para seus agentes públicos, por meio de ações como cursos, treinamentos ou oficinas, entre outros?
02. Governança	33. O órgão elaborou e/ou atualizou no período o Relatório de Impacto à Proteção de Dados Pessoais?
02. Governança	34. O órgão elaborou e/ou atualizou no período o seu Programa de Governança em Privacidade e Proteção de Dados Pessoais?
03. Tratamento de dados pessoais	35. A organização possui Política de Classificação da Informação ou instrumento similar, abrangendo diretrizes para a classificação de dados pessoais?
03. Tratamento de dados pessoais	36. O Órgão possui uma Tabela de Temporalidade de Documentos (ou documento similar) ou adota parâmetros e controles relativos ao tempo de guarda e eliminação dos dados de que tem posse?
04. Direitos dos titulares	37. O órgão possui uma Política de Atendimento (ou documento similar) aos direitos dos titulares?
04. Direitos dos titulares	38. O órgão realiza o controle de recebimento e resposta das petições recebidas dos titulares de dados pessoais?
05. Resposta a incidentes	39. O órgão possui uma Política de Resposta a Incidentes (ou documento similar) para tratar violações relativas à privacidade dos titulares de dados pessoais?
05. Resposta a incidentes	40. Todas as violações de dados pessoais são documentadas para fins de rastreabilidade, em atendimento ao princípio da responsabilização e da prestação de contas?
06. Transparência	41. O órgão possui e divulga a Política de Privacidade e Proteção de Dados Pessoais em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?
07. Segurança da Informação	42. O órgão possui uma Política de Segurança da Informação (ou documento similar) contendo diretrizes e procedimentos sobre controle de acesso, uso de senhas, rotina de backup, uso de cookies, entre outros?
08. Gestão de terceiros	43. O órgão possui uma Política de Contratações de Terceiros (Gerenciamento de Fornecedores, Due Dilligence, ou documento similar) adequada às exigências da LGDP, contendo disposições específicas para cada modalidade de contratação, informando os documentos e requisitos necessários que devem instruir cada procedimento?
08. Gestão de terceiros	44. O órgão, ao compartilhar ou transferir dados pessoais, adota um processo de formalização e registro, incluindo a comunicação à CGM-SP no caso de compartilhamento a pessoa de direito privado, identificando objeto e finalidade, responsabilidades, nível de serviço, base legal, duração e outras condições do tratamento?

FASE 04 - AVANÇADO

GRUPO	CONTROLE
01. Estrutura organizacional	45. O órgão executa e monitora o seu Plano de Capacitação em Privacidade e Proteção de Dados Pessoais (processo permanente aprendizagem com o objetivo de desenvolver competências individuais) para seus colaboradores, contemplando atividades de conscientização periódicas, incluindo ações especializadas para os colaboradores que exercem funções com responsabilidades relacionadas à proteção de dados pessoais?
02. Governança	46. O órgão executa e monitora o seu Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais (contemplando as atividades de Identificação, Avaliação e Tratamento de Riscos)?
03. Tratamento de dados pessoais	47. O Órgão conta com processo formal e documentado de gestão do Consentimento do Titular de Dados (quando utiliza esta hipótese legal), fornecendo instrumentos adequados para que o titular de dados pessoais manifeste o seu consentimento, quando necessário, de forma livre, informada e inequívoca?
03. Tratamento de dados pessoais	48. A organização monitora se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas (em observância à Tabela de Temporalidade de Documentos)?
04. Direitos dos titulares	49. O órgão monitora Indicadores de Desempenho com relação ao atendimento aos Direitos dos Titulares?
05. Resposta a incidentes	50. O órgão monitora Indicadores de Desempenho com relação às respostas aos incidentes de segurança?
06. Transparência	51. O órgão implementa meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular?
07. Segurança da Informação	52. O órgão realiza o monitoramento das vulnerabilidades técnicas nos tratamentos de dados pessoais, incluindo o monitoramento e defesa da rede (sistemas de detecção e alerta para eventos de segurança)?
07. Segurança da Informação	53. A instituição realiza a gestão do controle de contas e acessos (físicos e lógicos) centralizada, considerando o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais, em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos colaboradores?
08. Gestão de terceiros	54. O órgão monitora e inspeciona a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores e terceiros?
08. Gestão de terceiros	55. O órgão monitora e comunica qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados?

FASE 05 – INSTITUCIONALIZAÇÃO

GRUPO	CONTROLE
01. Estrutura organizacional	56. O órgão estabelece e mantém contato com as autoridades relevantes, grupos de interesse especial ou fóruns especializados, buscando-se atualização e conhecimento das melhores práticas na área?
02. Governança	57. O órgão submete o seu Programa de Governança em Privacidade e Proteção de Dados Pessoais a revisão e reavaliação periódicas em um processo contínuo de gerenciamento de riscos de segurança?
03. Tratamento de dados pessoais	58. O órgão, ao realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, mantém controles para restringir o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária?
03. Tratamento de dados pessoais	59. O órgão mantém controles para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais?
03. Tratamento de dados pessoais	60. O órgão mantém controles sobre os dados pessoais que necessitam ser anonimizados de acordo com o tratamento e exigências estabelecidas por leis aplicáveis?
03. Tratamento de dados pessoais	61. O órgão mantém controles sobre a manutenção dos dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?
03. Tratamento de dados pessoais	62. O órgão mantém controles sobre o tratamento de dados pessoais de crianças e adolescentes, com o objetivo de verificar o atendimento ao seu melhor interesse, conforme preconizado pelo art. 14 da LGPD?
03. Tratamento de dados pessoais	63. O órgão mantém controles sobre as técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?
03. Tratamento de dados pessoais	64. O órgão mantém controles sobre as decisões relacionadas ao titular de dados pessoais que são baseadas em tratamento automatizado e fornece, sempre que solicitada, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados?
04. Direitos dos titulares	65. O órgão mantém controles que o permitam otimizar as respostas aos titulares (ex. análise estatística das demandas, uso de modelos de respostas, análise de gargalos, pesquisa de satisfação, etc.)?
05. Resposta a incidentes	66. O órgão executa as atividades de documentação e de avaliação pós-incidente, promovendo uma análise detalhada dos incidentes para identificar as suas causas, as lições aprendidas e as recomendações para prevenir futuros incidentes similares, buscando implementar os pontos de melhoria e revisar políticas e procedimentos?
06. Transparência	67. O órgão mantém controles sobre os níveis de acesso dos processos que utilizam dados pessoais, quando tramitados pelo Sistema Eletrônico de Informação - SEI, a fim de monitorar o cumprimento às regras de classificação de acesso adequadas à LGPD (em observância à Política de Classificação da Informação)?
07. Segurança da Informação	68. O órgão mantém controle de registros de eventos (logs), considerando o princípio de minimização de dados, gravando o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento?
08. Gestão de terceiros	69. O órgão mantém controles sobre as medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais?
08. Gestão de terceiros	70. O órgão mantém controles sobre o compartilhamento ou transferência de dados pessoais e se tais atividades são realizadas por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança?

APÊNDICE 4 – QUADRO RESUMO DOS CONTROLES

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
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 Desempe-nho 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 atendimento 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 compartilhamen-tos 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 ati-vos de tecnologia da informação	15. Mapeamento dos contratos e compartilhamentos 14. Minutas padrão

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. Cookies e proteção de dados pessoais. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: < https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf > Acesso em: 05/03/2024.

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. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Diário Oficial da União, 27 de fevereiro de 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 11, de 27 de dezembro de 2023. Altera a Agenda Regulatória para o biênio 2023-2024. Diário Oficial da União, 29 de dezembro de 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. ANPD esclarece dúvidas sobre a atuação do Encarregado e a emissão de selos de conformidade com a LGPD. Publicado em 31/03/2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esclarece-duvidas-sobre-a-atuacao-do-encarregado-e-a-emissao-de-selos-de-conformidade-com-a-lgpd> Acesso em: 29/02/2024.

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 57.653 DE 7 de abril de 2017. Dispõe sobre a Política Municipal de Governança de Tecnologia da Informação e Comunicação – PMGTIC, no âmbito da Administração Pública Municipal. São Paulo, Diário Oficial da Cidade, 7 de abril de 2017.

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). 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.

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
Kelvin Peroli dos Reis
Marcus Vinicius Marins
Maria Victoria Teodoro Raimundo
Mateus dos Santos Vieira

Arte e Diagramação
Marília Miquelin de Oliveira

Versão 01

Janeiro de 2025

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO