GUIA ORIENTATIVO

Modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPP)



Portaria CGM/SP nº 27/2026

Programa de Governança em Privacidade e Proteção de Dados Pessoais

PREFEITURA DE SÃO PAULO

FICHA

Prefeitura do Município de São Paulo

Prefeito

Ricardo Nunes

Controladoria Geral do Município

Controlador Geral do Município

Daniel Falcão

Chefe de Gabinete

Marcos Augusto Carboni

Equipe da Coordenadoria de Proteção de Dados Pessoais

Coordenador

Edson Joaquim Raimundo de Araujo Júnior

Elaboração

Fábio Fernandes Libonati

Thiago Ryuichi Hirata

Revisão

Alana Leite Catuzzati

João Francisco Resende

Arte e Diagramação

Marília Miquelin de Oliveira

Versão 02

Outubro de 2026

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

Controlador Geral do Município

Daniel Falcão

VERSÃO

Versão	Descrição	Data
1.0	Versão inicial	02/2025
2.0	Atualização pós alteração do Decreto Municipal nº 59.767/2020	10/2026

Sumário

1. Apresentação 5
2. Considerações iniciais 7
3. Modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais 10
3.1. Do agrupamento dos controles por temas 11
3.2. Das fases para verificação dos controles 13
3.3. Resumo da estruturação dos controles 14
3.4. Acompanhamento do PGPP 15
Apêndice 1 – Lista dos controles por fase de verificação 17
Apêndice 2 – Quadro resumo dos controles 22
Referências 23

1. Apresentação

Este manual foi elaborado com o objetivo de auxiliar os agentes públicos responsáveis por implementar os controles previstos na Portaria CGM nº 27/2026, que regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPP) da Administração Pública Municipal. O foco deste manual é a explicação do modelo de PGPP.

Os órgãos e entidades possuem autonomia técnica e devem considerar o contexto, o volume e o risco dos tratamentos de dados pessoais realizados na implementação do modelo de PGPP. Assim, o modelo apresentado neste manual não é de uso obrigatório, possui natureza orientativa e poderá ser adaptado para diferentes realidades, desde que justificado.

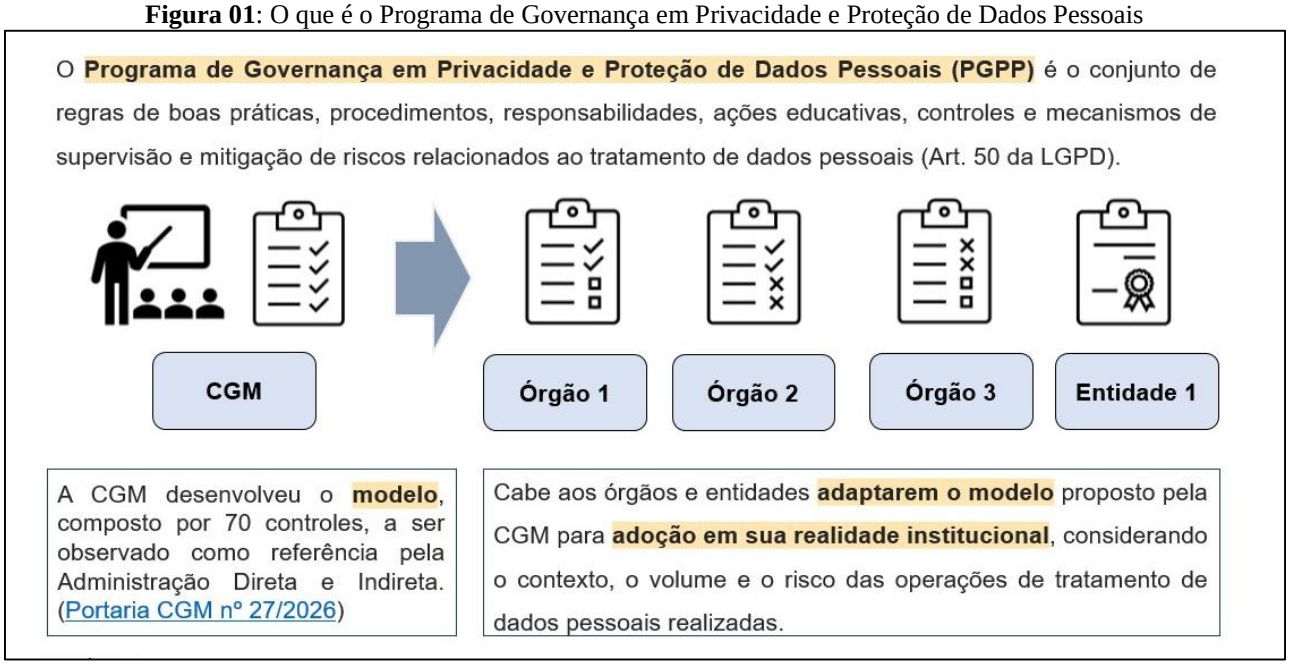
A elaboração do modelo de PGPP utilizou metodologia que teve como base (i) a análise da legislação vigente e identificação dos principais requisitos de conformidade aplicáveis aos órgãos e entidades da Prefeitura do Município de São Paulo (PMSP)[1]; (ii) a análise de normas técnicas e de referências 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 (alterado pelo Decreto Municipal nº 65.117/2026) e Instrução Normativa CGM nº 01/2022 (revogada pela Portaria CGM nº 27/2026).

[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.

Figura 01: O que é o Programa de Governança em Privacidade e Proteção de Dados Pessoais



Fonte: CGM/CPD

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 e entidades de se adequarem a outras determinações legais existentes na própria Lei Geral de Proteção de Dados Pessoais (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 e entidades 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[4].

c) Os aspectos verificados podem ser adaptados pelos órgãos e entidades para o seu contexto e realidade. A abordagem proposta à PMSP oferece uma sugestão de implementação de controles, porém é importante que cada unidade 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 unidade.

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 sobre a implementação de controles relacionados a requisitos da LGPD 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 e entidades de suas obrigações e responsabilidades. Salienta-se que é dever do agente público ter sua conduta permeada pelos valores da ética, devendo ainda observar o princípio da responsabilização e prestação de contas (Art. 6º, X, LGPD).

f) Os resultados obtidos na mensuração não devem ser interpretados como um "selo" de garantia de cumprimento à LGPD, uma vez que a própria Agência Nacional de Proteção de Dados (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 e entidades devem adotar práticas de revisões e de melhoria contínua em um processo de constante monitoramento.

[4] Disponível em: <https://tecnologia.prefeitura.sp.gov.br/?page_id=1155> Acesso em: 28/08/2026

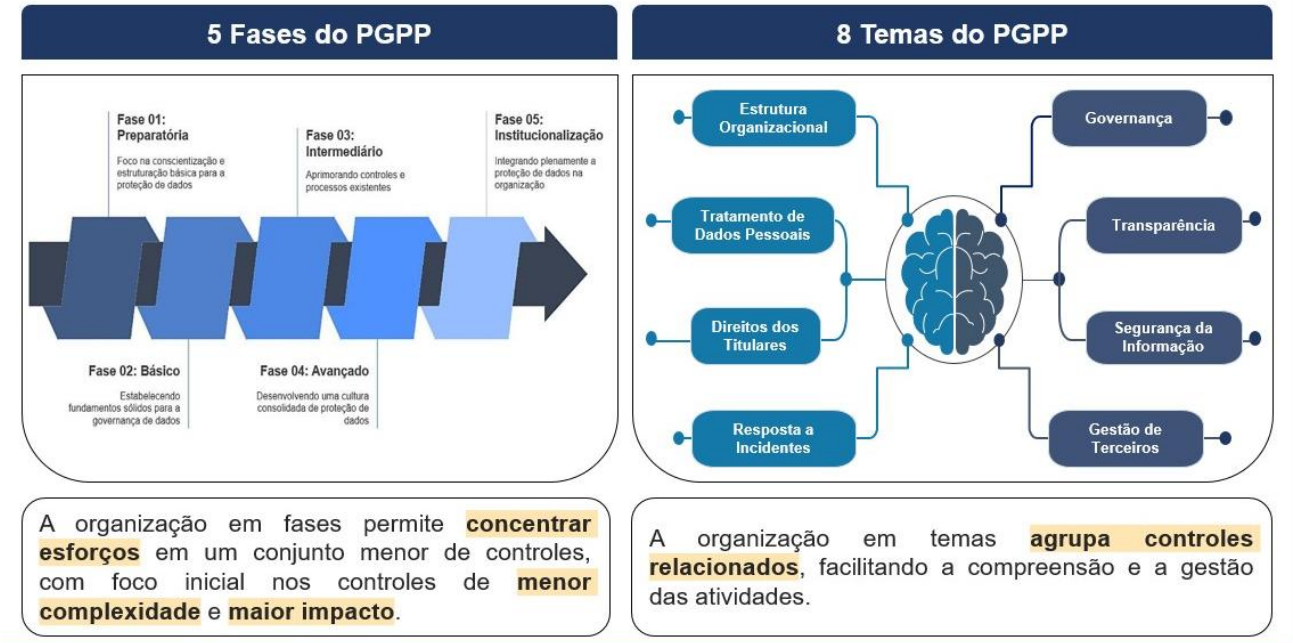
g) A metodologia desenvolvida não representa ou se manifesta em nome de nenhuma das referências de normas técnicas e/ou boas práticas utilizadas. Sugere-se que os órgãos e entidades que desejarem se aprofundar no estudo a respeito dos controles e práticas adotadas pelas referências analisadas consultem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

3. Modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais

A metodologia desenvolvida pela CGM-SP na elaboração do modelo do PGPP consiste na verificação da implementação de controles relacionados a requisitos da LGPD e boas práticas no tema pelos órgãos e entidades 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 e entidades, 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.

Figura 02: Divisão em Fases e Temas do PGPP



Fonte: CGM/CPD

3.1. Do agrupamento dos controles por temas

A fim de se promover melhor organização dos controles, foi realizado agrupamento por temas, totalizando os oito temas descritos a seguir:

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 ou entidade 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 ou entidade 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**: Conforme 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. É importante estabelecer uma estrutura

adequada para executar esta função e implementar procedimentos de identificação do titular de dados pessoais, registro e processamento das requisições.

5. **Resposta a incidentes**: De acordo com o Art. 50, § 2º, I, g, LGPD, o órgão ou entidade 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, clara e visível, 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 ou entidade.

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 ou entidade 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 busca 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 mapeamento de dados pessoais, que depende do prévio mapeamento de processos da unidade.

Foram definidas cinco fases de verificação, descritas a seguir (o detalhamento dos controles por fase encontra-se no Apêndice 1):

a) **Fase 01 - Preparatório**: todos os órgãos e entidades 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 já haja execução das principais atividades relacionadas à privacidade e à proteção de dados pessoais, com processos de negócio mapeados. Contudo, a 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 e entidades 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, os processos de negócio devem estar formalizados em procedimentos e fluxos, havendo documentação que demonstre como o trabalho deve ser realizado. Espera-se que os principais processos e atividades relacionados à privacidade e à proteção de dados pessoais tenham sido revisados.

c) **Fase 03 - Intermediário**: os órgãos e entidades 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, os processos de negócio devem estar definidos em regulamento próprio, havendo políticas e normas disciplinando os procedimentos. Espera-se que haja controle e documentação sobre os principais processos e atividades relacionados à privacidade e à proteção de dados pessoais. Após a conclusão da Fase 03, considera-se que os órgãos e entidades 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 e entidades 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, deve haver gerenciamento de processos através de indicadores de desempenho, com o monitoramento da implementação dos controles com maior profundidade. Espera-se que os órgãos e entidades realizem o acompanhamento periódico sobre os planos elaborados anteriormente (ex.: capacitação, implementação de controles, vulnerabilidades técnicas, entre outros).

e) **Fase 05 – Institucionalização**: os órgãos e entidades 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[5].

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 2):

[5] Método de melhoria contínua que consiste em Planejar (*Plan*), Executar (*Do*), Verificar (*Check*) e Agir (*Act*) para aperfeiçoar processos e alcançar resultados de forma sistemática.

Tabela 01 – Estrutura de temas e fases dos controles (quantidade de controles)

Tema	Fase 01 – Prepara-tório	Fase 02 - Básico	Fase 03 – Interme-diário	Fase 04 – Avançado	Fase 05 – Institucio-nalização	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 controles por fase	**15**	**15**	**14**	**11**	**15**	**70**

Fonte: CGM/CPD

3.4. Acompanhamento do Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPP)

O acompanhamento da implementação do PGPP pelos órgãos e entidades é realizado, anualmente, por meio do Diagnóstico de Maturidade em Proteção de Dados Pessoais, conduzido pela Coordenadoria de Proteção de Dados (CPD). O diagnóstico consiste em um processo de autoavaliação dos órgãos e entidades municipais, destinado a aferir o estágio de maturidade da governança em privacidade por meio da verificação da implementação dos controles.

O procedimento é regulamentado pela Portaria CGM nº 27/2026, e tem como finalidade fornecer aos gestores um panorama da implementação do PGPP em seus respectivos órgãos ou entidades, permitindo a identificação de pontos de melhoria, a priorização de ações e o acompanhamento da evolução da maturidade institucional ao longo do tempo.

Apêndice 1 – Lista dos controles por fase de verificação

Fase 01 - Preparatório

Tema	Controle
01. Estrutura organizacional	01. A unidade possui a indicação formal de um encarregado pelo tratamento de dados pessoais?
01. Estrutura organizacional	02. A unidade possui um Grupo de Trabalho ou estrutura equivalente, para apoiar na adequação à LGPD?
01. Estrutura organizacional	03. A unidade realizou no período atividade de sensibilização sobre a importância da LGPD e seu impacto nas atividades exercidas pelos respectivos agentes públicos?
02. Governança	04. A unidade elaborou e/ou atualizou no período o seu Planejamento para implementação do Programa de Governança em Privacidade e Proteção de Dados Pessoais?
03. Tratamento de dados pessoais	05. A unidade realizou, revisou ou atualizou no período o mapeamento de processos que tratam dados pessoais?
03. Tratamento de dados pessoais	06. A unidade realizou, revisou ou atualizou no período o mapeamento de dados pessoais dos processos mapeados?
03. Tratamento de dados pessoais	07. A unidade 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. A unidade 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?
06. Transparência	10. A unidade divulga a identidade e as informações de contato do encarregado pelo tratamento de dados pessoais de forma clara e objetiva, nos seus sítios eletrônicos?
06. Transparência	11. A unidade informa a respeito do tratamento de dados pessoais realizado no âmbito de suas competências em seus sítios eletrônicos?
06. Transparência	12. A unidade mantém aviso de privacidade e banners de cookies em dois níveis em seus sítios eletrônicos, conferindo transparência e possibilitando a obtenção do consentimento dos usuários?
07. Segurança da Informação	13. A unidade mantém um inventário de software e de ativos de tecnologia da informação?
08. Gestão de terceiros	14. A unidade adota modelo de cláusulas contratuais para os instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres com requisitos relativos ao tratamento de dados pessoais?
08. Gestão de terceiros	15. A unidade realizou, revisou ou atualizou no período a relação/lista dos contratos, termos de parceria, acordos de cooperação ou instrumentos congêneres firmados com terceiros?

Fase 02 - Básico

Tema	Controle
01. Estrutura organizacional	16. O Encarregado pelo tratamento 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. A unidade elaborou e/ou atualizou no período o seu Plano de Gestão de Riscos em Privacidade (contemplando as atividades de Identificação, Análise, Avaliação e Tratamento de Riscos)?
02. Governança	19. A unidade elaborou e/ou atualizou no período a sua Política de Gestão de Riscos em Privacidade?
03. Tratamento de dados pessoais	20. A unidade adequou e/ou revisou, conforme a necessidade, seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos vigentes, de modo que processos e sistemas sejam projetados em conformidade com a LGPD?
04. Direitos dos titulares	21. A unidade tem definido um fluxo de atendimento das demandas dos titulares de dados pessoais?
04. Direitos dos titulares	22. A unidade responde às solicitações dos titulares quanto aos seus dados pessoais, observando os seus direitos, conforme disposto pela LGPD?
05. Resposta a incidentes	23. A unidade 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. A unidade comunica as autoridades e os titulares de dados pessoais sobre os incidentes e violações que possam acarretar risco ou danos?
06. Transparência	25. A unidade adequou e/ou revisou os seus sítios eletrônicos, conforme a necessidade, de modo a se ajustar às exigências da LGPD com relação aos dados pessoais publicizados?
07. Segurança da Informação	26. Foram estabelecidas arquitetura e infraestrutura de redes seguras, com a manutenção de rede corporativa segmentada em domínios lógicos?
07. Segurança da Informação	27. A unidade 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. As decisões administrativas que envolvam o uso compartilhado de dados pessoais consideram requisitos relativos ao tratamento de dados pessoais?
08. Gestão de terceiros	30. O uso compartilhado de dados pessoais é precedido de avaliação sobre a compatibilidade entre a finalidade original e a do uso compartilhado?

Fase 03 - Intermediário

Tema	Controle
01. Estrutura organizacional	31. As funções e responsabilidades dos agentes públicos envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas (em normativo, política, procedimento ou documento similar)?
01. Estrutura organizacional	32. A unidade realizou no período campanha institucional de conscientização para transmissão de conhecimentos teóricos e práticos sobre a LGPD e as responsabilidades envolvidas, voltada para seus agentes públicos?
02. Governança	33. A unidade elaborou e/ou atualizou no período o Relatório de Impacto à Proteção de Dados Pessoais?
02. Governança	34. A unidade 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 unidade possui Política de Classificação da Informação ou instrumento similar, abrangendo diretrizes para a classificação de dados pessoais?
03. Tratamento de dados pessoais	36. A unidade 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. A unidade possui uma Política de Atendimento (ou documento similar) aos direitos dos titulares?
04. Direitos dos titulares	38. A unidade realiza o controle de recebimento e resposta das petições recebidas dos titulares de dados pessoais?
05. Resposta a incidentes	39. A unidade 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. A unidade possui e divulga a Política de Privacidade e Proteção de Dados Pessoais em local de fácil acesso?
07. Segurança da Informação	42. A unidade 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. A unidade possui uma Política de Contratações de Terceiros (Gerenciamento de Fornecedores, *Due Dilligence*, ou documento similar) adequada às exigências da LGPD, contendo disposições específicas de acordo com a modalidade de contratação, informando os documentos e requisitos necessários que devem instruir cada procedimento?
08. Gestão de terceiros	44. A unidade, ao compartilhar ou transferir dados pessoais, adota um processo de formalização e registro, incluindo a comunicação ao encarregado no caso de uso compartilhado com terceiros, identificando objeto e finalidade, responsabilidades, nível de serviço, base legal, duração e outras condições do tratamento?

Fase 04 - Avançado

Tema	Controle
01. Estrutura organizacional	45. A unidade executa e monitora o seu Plano de Capacitação em Privacidade e Proteção de Dados Pessoais (processo permanente de aprendizagem com o objetivo de desenvolver competências individuais) para seus agentes públicos?
02. Governança	46. A unidade executa e monitora o seu Plano de Gestão de Riscos em Privacidade (contemplando as atividades de Identificação, Análise, Avaliação e Tratamento de Riscos)?
03. Tratamento de dados pessoais	47. A unidade 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 unidade 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. A unidade monitora Indicadores de Desempenho com relação ao atendimento aos Direitos dos Titulares?
05. Resposta a incidentes	50. A unidade monitora Indicadores de Desempenho com relação às respostas aos incidentes de segurança?
06. Transparência	51. A unidade implementa meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente?
07. Segurança da Informação	52. A unidade realiza o monitoramento das vulnerabilidades técnicas nos tratamentos de dados pessoais, incluindo o monitoramento e defesa da rede?
07. Segurança da Informação	53. A unidade 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 tratamento de dados pessoais, em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos agentes públicos?
08. Gestão de terceiros	54. A unidade monitora e inspeciona a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores e terceiros?
08. Gestão de terceiros	55. A unidade 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

Tema	Controle
01. Estrutura organizacional	56. A unidade 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. A unidade 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?
03. Tratamento de dados pessoais	58. A unidade, 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade 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. A unidade mantém controle de registros de eventos (logs), quando aplicável, 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. A unidade mantém controles sobre as medidas de proteção de dados pessoais adotadas por terceiros no caso de uso compartilhado de dados pessoais?
08. Gestão de terceiros	70. A unidade mantém controles sobre o uso compartilhado de dados pessoais e se é realizado por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança?

Apêndice 2 – Quadro resumo dos controles

<table>
<tr><td rowspan="5">05. Institucionalização</td><td rowspan="5">56. Participação em fóruns especializados</td><td rowspan="5">57. Atualização do Programa de Governança</td><td rowspan="5">Controles sobre:</td><td>64. Tratamento automatizado</td><td rowspan="5">65. Controles sobre a melhoria contínua no atendimento</td><td rowspan="5">66. Controles sobre a documentação e avaliação pós-incidente</td><td rowspan="5">67. Controles sobre os níveis de acesso no SEI</td><td rowspan="5">68. Controles sobre registros de eventos (logs)</td><td>70. Controles sobre a transferência de dados e criptografia</td></tr>
<tr><td>63.Exclusão ou destruição de dados</td><td rowspan="4">69. Controles sobre as medidas de proteção adotadas por terceiros</td></tr>
<tr><td>62. Dados de crianças e adolescentes</td></tr>
<tr><td>61. Formato interope-rável e estruturado</td></tr>
<tr><td>60. Dados anonimizados</td></tr>
<tr><td rowspan="2">04. Avançado</td><td rowspan="2">45. Monitoramento do Plano de Capacitação</td><td rowspan="2">46. Monitoramento do Plano de Gestão de Riscos</td><td colspan="2">48. Monitoramento do tempo de armazenamento dos dados pessoais</td><td rowspan="2">49. Monitoramento de Indicadores de Desempenho do atendimento aos titulares</td><td rowspan="2">50. Monitoramento de Indicadores de Desempenho de incidentes de segurança</td><td rowspan="2">51. Gerenciamento de dados pelo titular</td><td>53. Gestão do controle de contas e acessos</td><td>55. Monitoramento e comunicação de alterações a terceiros</td></tr>
<tr><td colspan="2">47. Gestão do Consentimento do Titular de Dados Pessoais</td><td>52. Monitoramento de vulnerabilidades técnicas</td><td>54. Monitoramento de requisitos de terceiros</td></tr>
<tr><td rowspan="2">03. Intermediário</td><td>32. Conscientização</td><td>34. Programa de Governança</td><td colspan="2">36. Tabela de Temporalidade de Documentos</td><td>38. Registro dos atendimentos</td><td>40. Registro dos incidentes</td><td rowspan="2">41. Política de Privacidade e Proteção de Dados Pessoais</td><td rowspan="2">42. Política de Segurança da Informação</td><td>44. Registro de uso compartilhado</td></tr>
<tr><td>31. Funções e responsabilidades</td><td>33. Relatório de Impacto à Proteção de Dados Pessoais</td><td colspan="2">35. Política de Classificação da Informação</td><td>37. Política de Atendimento</td><td>39. Política de Resposta a Incidentes</td><td>43. Política de Contratações de Terceiros</td></tr>
<tr><td rowspan="2">02. Básico</td><td>17. Capacitação do Grupo de Trabalho</td><td>19. Política de Gestão de Riscos</td><td colspan="2" rowspan="2">20. Adequação de processos e atividades</td><td>22. Resposta às solicitações dos titulares</td><td>24. Resposta aos incidentes</td><td rowspan="2">25. Adequação de sítios eletrônicos</td><td>28. Cópias de segurança</td><td rowspan="2">30. Avaliação de Compatibilidade das Finalidades</td></tr>
<tr><td>16. Capacitação do Encarregado</td><td>18. Plano de Gestão de Riscos</td><td>21. Fluxo de atendimento</td><td>23. Fluxo de comunicação de incidentes</td><td>27. Softwares antimalware</td></tr>
<tr><td rowspan="3">01. Preparatório</td><td>03. Sensibilização</td><td rowspan="3">04. Planejamento</td><td colspan="2">07. Finalidades e hipóteses legais</td><td rowspan="3">08. Canal de atendimento aos direitos dos titulares</td><td rowspan="3">09. Canal de denúncias e/ou notificações de incidentes</td><td>12. Aviso de privacidade e cookies</td><td rowspan="3">13. Inventário de software e de ativos de tecnologia da informação</td><td rowspan="3">15. Relação/lista dos contratos</td></tr>
<tr><td>02. Grupo de Trabalho</td><td colspan="2">06. Mapeamento de dados pessoais</td><td>11. Informações do tratamento de dados</td></tr>
<tr><td>01. Encarregado</td><td colspan="2">05. Mapeamento de processos</td><td>10. Informações do Encarregado</td></tr>
<tr><td>Fase / Tema</td><td>01. Estrutura organizacional</td><td>02. Governança</td><td colspan="2">03. Tratamento de dados pessoais</td><td>04. Direitos dos titulares</td><td>05. Resposta a incidentes</td><td>06. Transparência</td><td>07. Segurança da Informação</td><td>08. Gestão de terceiros</td></tr>
</table>

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

SÃO PAULO (Cidade). Orientação Técnica nº 013 – Diretrizes básicas de segurança da informação. Disponível em: <https://tecnologia.prefeitura.sp.gov.br/?page_id=1155>. Acesso em: 28/08/2026.

SÃO PAULO (Cidade). Portaria CGM/SP nº 27, de 22 de Junho de 2026. Regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP), assim como o procedimento do Diagnóstico de Maturidade em Proteção de Dados Pessoais. Disponível em: <https://legislacao.prefeitura.sp.gov.br/portaria-controladoria-geral-do-municipio-cgm-27-de-22-de-junho-de-2026>. Acesso em: 23/06/2026.



PREFEITURA DE
SÃO PAULO