GUIA ORIENTATIVO

Fase 01 do 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 (PGPP)

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

Marcus 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

Junho 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 nº 59.767/2020	06/2026

Sumário

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 da Administração Pública Municipal (PGPP).

A metodologia desenvolvida pela CGM estabelece cinco fases de maturidade para classificação dos órgãos e entidades da PMSP, cada uma prevendo a verificação da implementação de diferentes controles relacionados a requisitos da Lei Geral de Proteção de dados (LGPD) e boas práticas no tema. Para auxiliar os gestores públicos na implementação dos controles em suas unidades, foram criados guias e manuais para detalhar os controles de cada fase da metodologia.

O presente manual detalha os controles da Fase 01. Todas as unidades serão inicialmente classificadas 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 unidades já executem as primeiras atividades relacionadas à privacidade e à proteção de dados pessoais, possuindo seus processos de negócio mapeados.

Controle 01. Encarregado

Fase: 01. Preparatório	**Tema:** 01. Estrutura Organizacional

A unidade possui a indicação formal de um encarregado pelo tratamento de dados pessoais?

Referência

- Art. 6º, inc. X; Art. 23, inc. III; Art. 41, LGPD;
- Art. 5º, Decreto nº 59.767/2020;
- Resolução CD/ANPD nº 18, de 16 de julho de 2024.

Descrição

O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a ANPD, entre outras atribuições. O órgão ou entidade deve designar oficialmente o encarregado, bem como respectivo substituto, mediante nomeação por meio de Portaria publicada no Diário Oficial da Cidade.

Justificativa

A indicação do encarregado é essencial e obrigatória para o processo de adequação da unidade à LGPD. Cabe ao encarregado o exercício de funções importantes, a exemplo da atuação como canal de comunicação entre o controlador, os titulares e a ANPD, além da orientação dos funcionários e contratados a respeito do tema. Diminui-se o risco de lentidão ou não adequação da unidade à LGPD e às boas práticas em privacidade e proteção de dados pessoais, bem como do risco de não institucionalização das políticas de implementação da LGPD na unidade.

Áreas envolvidas

Alta administração da unidade.

Momento de implementação

Não há controles prévios à implementação deste.

Principais requisitos e diretrizes de implantação

- Designação de encarregado e seu substituto mediante publicação de ato normativo, que deve contemplar a forma de atuação e as atribuições que serão desenvolvidas;
- A indicação do encarregado deve recair, preferencialmente, sobre servidores ou empregados públicos detentores de reputação ilibada, evitando situações que possam configurar conflito de interesses;
- Cabe ao órgão ou entidade definir as qualificações profissionais necessárias para o desempenho das atribuições do encarregado, considerando seus conhecimentos sobre a legislação de proteção de dados pessoais, o contexto operacional, volume e risco das operações de tratamento realizadas.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para ato normativo de designação de encarregado
- **Exemplo de evidência implementada**: Portaria ADE SAMPA nº 1, de 2025.

Controle 02. Grupo de Trabalho

Fase: 01. Preparatório	**Tema:** 01. Estrutura Organizacional

A unidade possui um Grupo de Trabalho, ou estrutura equivalente, para apoiar na adequação à LGPD?

Referência

- Art. 6º, inc. X; Art. 50, LGPD;
- Art. 4º, § 3º, Decreto nº 59.767/2020.

Descrição

O grupo de trabalho tem como objetivo coordenar a implementação da LGPD no seu contexto. Tal grupo não é subordinado e não se confunde com a figura do encarregado.

Justificativa

O grupo de trabalho é importante para se garantir a implementação da LGPD na unidade de maneira coordenada e estruturada. Diminui-se o risco de lentidão ou não adequação da unidade à LGPD e às boas práticas em privacidade e proteção de dados pessoais, bem como do risco de não institucionalização das políticas de implementação da LGPD na unidade.

Áreas envolvidas

Alta Administração, assessoria jurídica, setor de TI, segurança da informação, ouvidoria, controle interno, e outros setores a critério do gestor da unidade.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 01.

Principais requisitos e diretrizes de implantação

- Designação de grupo de trabalho por meio de publicação de portaria;
- A composição do grupo deve ser proporcional ao tamanho do órgão e à complexidade do tratamento de dados;
- Espera-se que os integrantes do grupo tenham competências multidisciplinares.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para ato normativo de designação do grupo de trabalho
- **Exemplo de evidência implementada**: Portaria SF nº 131, de 2025; Portaria SEHAB/COHAB Nº 18, de 2020; Portaria SEHAB Nº 101, 2021; Portaria SMADS Nº 71, 2021; Portaria SMT Nº 3, de 2023.

Controle 03. Sensibilização

Fase: 01. Preparatório	**Tema:** 01. Estrutura Organizacional

A unidade realizou, no período, atividade de sensibilização sobre a importância da LGPD e seu impacto nas atividades exercidas pelos respectivos agentes públicos?

Referência

- Art. 6º, inc. X; Art. 50, LGPD.

Descrição

As ações de sensibilização visam a promoção de mudanças no comportamento dos agentes públicos e o fomento à cultura de privacidade na Administração Pública municipal.

Justificativa

A sensibilização dos agentes públicos do órgão ou da entidade é importante para a implantação e manutenção da cultura da privacidade e da proteção de dados pessoais na rotina dos agentes públicos. Diminui-se o risco de lentidão ou não adequação da unidade à LGPD e às boas práticas em privacidade e proteção de dados pessoais, bem como do risco de não institucionalização das políticas de implementação da LGPD na unidade.

Áreas envolvidas

Encarregado, assessoria de comunicação, controle interno e outros setores a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 01 e 02.

Principais requisitos e diretrizes de implantação

- Realização de, no mínimo, uma ação de sensibilização com envolvimento de todas as áreas de atuação do órgão ou entidade, não sendo obrigatória a participação de todos os funcionários;
- O conteúdo das ações de sensibilização pode estar relacionado com boas práticas de segurança da informação, conceitos básicos da LGPD, conceitos de privacidade e proteção de dados pessoais e aspectos procedimentais da unidade, entre outros;
- Recomenda-se que as ações de sensibilização sejam personalizadas ao contexto e características do órgão ou entidade, para que os agentes públicos assimilem os conceitos de modo mais próximo à realidade que atuam.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Campanhas institucionais; materiais educativos (apresentações, vídeos, guias, cartilhas); comunicação com os colaboradores (e-mails, cartazes); atividades (desafios, questionários, atividades interativas); avaliações de conhecimento (testes, dinâmicas, avaliações); ata de presença dos cursos oferecidos e programa ofertado; resultado de avaliação de entendimento dos colaboradores.
- **Exemplo de evidência implementada**: Curso sobre Privacidade e Proteção de Dados Pessoais disponibilizado pela CGM/CPD a servidores públicos e à sociedade civil através do Centro de Formação em Controle Interno (CFCI), disponível no sítio eletrônico da CGM-SP.

Controle 04. Planejamento

Fase: 01. Preparatório	**Tema:** 02. Governança

A unidade elaborou e/ou atualizou, no período, o seu Planejamento para implementação do Programa de Governança em Privacidade e Proteção de Dados Pessoais?

Referência

- Art. 6º, inc. VIII, LGPD;
- Art. 4º, Decreto nº 59.767/2020.

Descrição

O planejamento consiste na preparação para a implementação de um projeto, envolvendo a definição de objetivos, metas e ações necessárias para alcançá-los. O órgão ou entidade deve documentar o planejamento das ações e medidas necessárias para implementação do Programa de Governança em Privacidade e Proteção de Dados Pessoais, visando a sua adequação às melhores práticas na área.

Justificativa

O planejamento das ações para a adequação da unidade à LGPD é importante para que todo o processo ocorra de forma coordenada e consistente. Diminui-se o risco de implementação incompleta da adequação à LGPD e de concretização de ameaças relacionadas a riscos que poderiam ser tratados previamente.

Áreas envolvidas

Alta administração, encarregado, grupo de trabalho e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 01 e 02.

Principais requisitos e diretrizes de implantação

- O planejamento deve conter a descrição dos controles com os seus respectivos prazos de implementação;
- É importante também designar os respectivos responsáveis pela implementação das ações previstas.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Planilha, Cronograma, Plano de Ação ou outro documento que contemple os prazos e responsáveis pela implementação do Programa.
- **Modelo:** Planilha com modelo de Planejamento disponível no sítio eletrônico da CGM-SP.

Controle 05. Mapeamento de Processos

Fase: 01. Preparatório	**Tema:** 03. Tratamento de dados pessoais

A unidade realizou, revisou ou atualizou, no período, o mapeamento de processos que tratam dados pessoais?

Referência

- Art. 6º, inc. VIII, LGPD.

Descrição

O mapeamento de processos consiste no estudo do conjunto de etapas relacionadas e executadas pelas áreas do órgão ou entidade, com vistas a alcançar determinado resultado. Consiste em uma técnica para representar um fluxo de trabalho, com o detalhamento de suas etapas, permitindo a institucionalização de procedimentos e a compreensão por todos os envolvidos.

Justificativa

Trata-se de etapa preliminar importante para a implementação de diversos controles do Diagnóstico de Maturidade, em especial o mapeamento de dados pessoais do órgão ou entidade, por meio do qual será possível uma visão geral das atividades realizadas e em quais etapas ocorrem o tratamento de dados pessoais. Diminuem-se os riscos de falha na gestão do tratamento de dados pessoais, na realização de tratamento de dados pessoais em desacordo com a legislação e na impossibilidade de realização de gestão adequada dos dados pessoais.

Áreas envolvidas

Encarregado, grupo de trabalho e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos controles 01, 02, 03 e 04.

Principais requisitos e diretrizes de implantação

- O mapeamento de processos resulta em uma lista contendo o repositório de todos os processos do órgão ou da entidade;
- O nível de detalhamento pode variar de acordo com as necessidades da unidade, sendo recomendada a priorização dos processos mais relevantes para maior detalhamento.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento consolidado com a lista de todos os processos de negócio do órgão ou entidade
- **Modelo**: Planilha com modelo de mapeamento de processos, em conjunto ao Manual sobre mapeamento de processos no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 05), disponível no sítio eletrônico da CGM-SP.

Controle 06. Mapeamento de dados pessoais	
Fase: 01. Preparatório	**Tema:** 03. Tratamento de dados pessoais
A unidade realizou, revisou ou atualizou, no período, o mapeamento de dados pessoais dos processos mapeados?	
Referência	
• Art. 6º, inc. VIII; Art. 37, LGPD.	
Descrição	
Trata-se de um registro detalhado de todas as operações de tratamento de dados pessoais realizada no âmbito do órgão ou entidade. O mapeamento de dados pessoais deve conter informações claras sobre todo o ciclo de vida dos dados pessoais do titular, com a identificação dos dados pessoais utilizados em cada processo.	
Justificativa	
A elaboração do mapeamento é importante para entender como os dados pessoais são coletados e como se movem pelo órgão ou entidade, facilitando a rápida localização de um dado na ocorrência de algum incidente de segurança, assim como o rápido atendimento a uma requisição do titular de dados pessoais. Diminuem-se os riscos de falha na gestão do tratamento de dados pessoais, na realização de tratamento de dados pessoais em desacordo com a legislação e na impossibilidade de realização de gestão adequada dos dados pessoais.	
Áreas envolvidas	
Encarregado, grupo de trabalho e eventuais áreas relacionadas, a critério do gestor.	
Momento de implementação	
Recomenda-se que este controle seja elaborado por processo, após a implementação do Controle 05.	
Principais requisitos e diretrizes de implantação	
• O mapeamento de dados pessoais resulta em um repositório de todas as operações de tratamento de dados pessoais do órgão ou da entidade; • O nível de detalhamento pode variar de acordo com as necessidades da unidade, sendo recomendada a priorização dos processos mais relevantes para maior detalhamento.	
Material de apoio para documentação de evidências	
• **Tipo de evidência**: Documento consolidado com a lista de todas as operações de tratamento de dados pessoais realizadas pelo órgão ou entidade • **Exemplo de evidência implementada**: Inventário de Dados Pessoais atualizado em 18/04/2024 do Tribunal Regional do Trabalho da 15ª Região Campinas/SP; Tabela de Tratamento de dados pessoais atualizada em 24/11/2022 do Ministério Público de Pernambuco. • **Modelo**: Planilha com modelo de mapeamento de dados pessoais, em conjunto ao Manual sobre mapeamento de dados pessoais para a Administração Pública do Município de São Paulo (Controle 06), disponível no sítio eletrônico da CGM-SP.	

Controle 07. Finalidades e hipóteses legais

Fase: 01. Preparatório	**Tema:** 03. Tratamento de Dados Pessoais

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?

Referência

- Art. 6º, inc. I, II, III; Art. 7º; Art. 11; Art. 23, inc. I, LGPD.

Descrição

A identificação das finalidades e das hipóteses legais para o tratamento de dados pessoais envolve o levantamento dos fundamentos que autorizam o tratamento realizado pelo órgão ou entidade.

Justificativa

O tratamento de dados pessoais deve ter propósitos legítimos, específicos e explícitos, além de estar fundamentado nas hipóteses legais que justificam tais operações. Diminuem-se os riscos de falha na gestão do tratamento de dados pessoais, na realização de tratamento de dados pessoais em desacordo com a legislação e na impossibilidade de realização de gestão adequada dos dados pessoais.

Áreas envolvidas

Assessoria jurídica, encarregado, grupo de trabalho e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que este controle seja elaborado por processo, após a implementação dos Controles 05 e 06.

Principais requisitos e diretrizes de implantação

- Recomenda-se identificar as finalidades para todas as operações de tratamento de dados pessoais realizadas pelo órgão ou entidade;
- Ademais, as operações de tratamento devem estar fundamentadas com base na indicação da respectiva hipótese legal, prevista nos arts. 7º ou 11 da LGPD;
- Nota-se que, além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser considerados.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento consolidado com a lista de todas as operações de tratamento de dados pessoais realizadas pelo órgão ou entidade, com a indicação da respectiva finalidade e hipótese legal
- **Exemplo de evidência implementada**: Inventário de Dados Pessoais atualizado em 18/04/2024 do Tribunal Regional do Trabalho da 15ª Região Campinas/SP; Tabela de Tratamento de dados pessoais atualizada em 24/11/2022 do Ministério Público de Pernambuco.
- **Modelo**: Planilha com modelo para identificação de finalidades e hipóteses legais, em conjunto ao Manual sobre finalidades e hipóteses legais no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 07), disponível no sítio eletrônico da CGM-SP.

Controle 08. Canal de atendimento aos direitos dos titulares

Fase: 01. Preparatório	**Tema:** 04. Direitos dos titulares

A unidade disponibiliza canal específico para recebimento de requisições de atendimento aos direitos dos titulares referentes à LGPD?

Referência

- Art. 6º, inc. IV; Arts. 17 a 20; Art. 41, LGPD;
- Art. 6º, Decreto nº 59.767/2020.

Descrição

Disponibilização de um canal específico para recebimento de requisições referentes à LGPD. Os direitos dos titulares estão definidos nos Arts. 17 a 20 da LGPD e é necessário viabilizar o exercício desses direitos.

Justificativa

O canal de comunicação para assuntos relacionados à LGPD é imprescindível para o recebimento de requisições relacionadas ao atendimento dos direitos dos titulares, uma vez que a definição dessa estrutura possibilita que o procedimento seja mais organizado e tempestivo. Diminui-se o risco de não atendimento das requisições dos titulares.

Áreas envolvidas

Alta administração, encarregado, assessoria de comunicação e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 01.

Principais requisitos e diretrizes de implantação

- Indicação de meios de contato no sítio eletrônico do órgão ou da entidade para assuntos relacionados à LGPD;
- É importante esclarecer ao titular de dados pessoais quais são os seus direitos e a forma de exercê-los.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para sítio eletrônico da unidade com as informações pertinentes.
- **Exemplo de evidência implementada**: Página do Encarregado da CGM disponível no sítio eletrônico da CGM-SP.
- **Modelo**: Modelo de página web, constante no Apêndice I do Manual sobre Disponibilização de informações do encarregado, do canal de atendimento ao titular e do canal para comunicação de denúncias e incidentes de segurança (Controles 08, 09 e 10), disponível no sítio eletrônico da CGM-SP.

Controle 09. Canal de denúncias e/ou notificações de incidentes

Fase: 01. Preparatório	**Tema:** 05. Resposta a incidentes

Existe um canal apropriado para o recebimento de denúncias e/ou notificações de incidentes de segurança?

Referência

- Art. 6º, inc. X; Art. 48; Art. 50, § 2º, inc. I, alínea *g*, LGPD;
- Art. 6º, Decreto nº 59.767/2020;
- Resolução CD/ANPD nº 15, de 2024.

Descrição

Disponibilização de canal apropriado para recebimento de denúncias e notificações de incidentes de segurança envolvendo o tratamento de dados pessoais. De acordo com o glossário da ANPD, incidente de segurança se refere a "*qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais*". Por sua vez, o conceito de denúncia, envolve "*suposta infração cometida contra a legislação de proteção de dados pessoais do País, que não seja uma petição de titular".*

Justificativa

É importante que o órgão ou entidade disponibilize canal apropriado para o recebimento de denúncias e notificações de incidentes de segurança envolvendo o tratamento de dados pessoais, para que a resolução desses casos e as medidas necessárias possam ser realizadas de forma coordenada e tempestiva. Diminui-se o risco de resposta intempestiva ou ineficiente aos incidentes de segurança.

Áreas envolvidas

Alta administração, encarregado, controle interno, assessoria de comunicação e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 01.

Principais requisitos e diretrizes de implantação

- Existência de canal para recebimento de denúncias e/ou notificações de incidentes de segurança;
- Divulgação do canal nos meios de comunicação adequados para o público interno e externo.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para sítio eletrônico da unidade com as informações pertinentes.
- **Exemplo de evidência implementada**: Página do Encarregado da CGM disponível no sítio eletrônico da CGM-SP.
- **Modelo**: Modelo de página web, constante no Apêndice I do Manual sobre Disponibilização de informações do encarregado, do canal de atendimento ao titular e do canal para comunicação de denúncias e incidentes de segurança (Controles 08, 09 e 10), disponível no sítio eletrônico da CGM-SP.

Controle 10. Informações do Encarregado

Fase: 01. Preparatório	**Tema:** 06. Transparência

A unidade divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, nos seus sítios eletrônicos?

Referência

- Art. 6º, inc. VI; Art. 41, § 1º, LGPD;
- Art. 5º, §4º, Decreto nº 59.767/2020;
- Resolução CD/ANPD nº 18, de 2024.

Descrição

Disponibilização da identidade e das informações de contato (ex.: e-mail, telefone) do encarregado nos respectivos sítios eletrônicos.

Justificativa

Trata-se de medida de transparência para a garantia dos direitos dos titulares de dados pessoais. Diminui-se o risco de ausência de transparência, da impossibilidade de o titular gerir os próprios dados pessoais e de divulgação inadequada de dados pessoais.

Áreas envolvidas

Alta administração, encarregado, assessoria de comunicação e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 01.

Principais requisitos e diretrizes de implantação

- Divulgação do nome completo e contato do encarregado e seu substituto no sítio eletrônico do órgão ou da entidade, de forma clara e objetiva, em local de destaque e de fácil acesso.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para sítio eletrônico da unidade com as informações pertinentes
- **Exemplo de evidência implementada**: Página do Encarregado da CGM disponível no sítio eletrônico da CGM-SP.
- **Modelo**: Modelo de página web, constante no Apêndice I do Manual sobre Disponibilização de informações do encarregado, do canal de atendimento ao titular e do canal para comunicação de denúncias e incidentes de segurança (Controles 08, 09 e 10), disponível no sítio eletrônico da CGM-SP.

Controle 11. Informações do tratamento de dados

Fase: 01. Preparatório	**Tema:** 06. Transparência

A unidade informa a respeito do tratamento de dados pessoais realizado no âmbito de suas competências em seus sítios eletrônicos?

Referência

- Art. 6º, inc. IV e VI; Art. 9º, inc. I, II; Art. 23, inc. I LGPD;
- Art. 11, inc. II, Decreto nº 59.767/2020.

Descrição

O titular de dados pessoais tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva para o atendimento do princípio do livre acesso e da transparência. Relaciona-se com as informações do tratamento realizado pelo órgão ou entidade como um todo e não se confunde com o tratamento realizado no sítio eletrônico da unidade (ou seja, difere do Aviso de Privacidade do Controle 12).

Justificativa

O tratamento de dados pessoais exige que sejam informadas as hipóteses que fundamentam tais operações, de forma a se garantir os princípios do livre acesso e da transparência, além de assegurar ao titular de dados o exercício de seus direitos, bem como possibilitar o exercício do controle social. Diminui-se o risco de ausência de transparência, da impossibilidade de o titular gerir os próprios dados pessoais e de divulgação inadequada de dados pessoais.

Áreas envolvidas

Alta administração, encarregado, assessoria de comunicação e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que este controle seja implementado por processo, após a implementação dos Controles 05, 06 e 07.

Principais requisitos e diretrizes de implantação

- Informações no sítio eletrônico do órgão ou da entidade a respeito da previsão legal, da finalidade, dos compartilhamentos, das transferências, dos procedimentos e das práticas utilizadas no tratamento de dados pessoais.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para sítio eletrônico da unidade com as informações pertinentes
- **Exemplo de evidência implementada**: Inventário de Dados Pessoais atualizado em 18/04/2024 do Tribunal Regional do Trabalho da 15ª Região Campinas/SP; Tabela de Tratamento de dados pessoais atualizada em 24/11/2022 do Ministério Público de Pernambuco.
- **Modelo**: Planilha com modelo para publicação de informações sobre o tratamento de dados pessoais, em conjunto ao Manual sobre a transparência no tratamento de dados pessoais para a Administração Pública do Município de São Paulo (Controle 11), disponível no sítio eletrônico da CGM-SP.

Controle 12. Aviso de privacidade e *cookies*

Fase: 01. Preparatório	**Tema:** 06. Transparência

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?

Referência

- Art. 6º, inc. VI; Art. 9º; Art. 18, LGPD;
- ANPD. Guia Orientativo – *Cookies* e proteção de Dados Pessoais.

Descrição

Aviso de Privacidade: forma de comunicação com o titular de dados pessoais com o objetivo de informá-lo a respeito de como seus dados pessoais são tratados no âmbito do próprio sítio eletrônico a que se refere.

Política de Cookies: informe ao usuário do sítio eletrônico sobre arquivos instalados em seus dispositivos que permitem a coleta de determinadas informações, inclusive de dados pessoais, visando ao atendimento de finalidades diversas, tais como: a identificação de usuários, informações sobre o desempenho do sítio eletrônico, oferecimento de serviços solicitados pelo usuário, a personalização de anúncios de publicidade, entre outros.

Banner de Cookies: caracteriza-se como um recurso visual aplicado em sítios eletrônicos para informar o titular de dados pessoais sobre a utilização de tais arquivos e o modo de seu gerenciamento. São relevantes para a transparência e para a tomada de decisão informada pelo titular e deve conter *link* para a Política de *Cookies* e Aviso de Privacidade.

Botão de Cookies: trata-se de um botão ou ícone que, quando clicado, reabre o *Banner* de *Cookies*, permitindo que o usuário ajuste suas preferências.

Justificativa

O aviso de privacidade, a política, os *banners* e o botão de *cookies* permitem que o titular de dados possa ter maior controle sobre o tratamento de seus dados, permitindo consentir ou não com determinados tipos de tratamento e privilegiam, portanto, o direito à autodeterminação informativa. Diminui-se o risco de ausência de transparência, da impossibilidade de o titular gerir os próprios dados pessoais e de divulgação inadequada de dados pessoais.

Áreas envolvidas

Encarregado, setor de TI, assessoria de comunicação e eventuais áreas relacionadas.

Momento de implementação

Não há atividades prévias à implementação deste.

Principais requisitos e diretrizes de implantação

- Recomenda-se mapear os sítios eletrônicos pelos quais a unidade é responsável;
- Todos os sítios eletrônicos mapeados devem conter: Aviso de privacidade; Política de *cookies*; Botão de *cookies*; e *Banner* de *cookies* em dois níveis.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Link para sítio eletrônico contendo aviso de privacidade, política de cookies, botão e banner de cookies; Lista de todos os sítios eletrônicos mantidos pela unidade.
- **Exemplo de evidência implementada**: Aviso de Privacidade do Sítio eletrônico gov.br.
- **Modelo**: Referências aos sítios eletrônicos da Prefeitura, constantes no Manual sobre Aviso de Privacidade e *Cookies* no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 12), disponível no sítio eletrônico da CGM-SP.

Controle 13. Inventário de software e de ativos de tecnologia da informação

Fase: 01. Preparatório	**Tema:** 07. Segurança da Informação

A unidade mantém um inventário de software e de ativos de tecnologia da informação?

Referência

- Art. 6º, inc. VII; Art. 46; Art. 47; Art. 49, LGPD;
- Decreto nº 53.484, de 2012;
- Portaria SF nº 90, de 2022;
- Portaria SMIT nº 36, de 2018;
- OT nº 004 e 013 do Decreto nº 57.653/2017.

Descrição

Realização de um inventário preciso, detalhado e atualizado periodicamente de todos os ativos institucionais com potencial para armazenar ou processar dados, incluindo ativos que não estejam sob controle do órgão ou entidade, além dos softwares licenciados instalados nestes ativos.

Justificativa

Compreensão da situação dos bens relacionados ao tratamento de dados pessoais permite o monitoramento de vulnerabilidades e resposta eficiente a eventuais incidentes de segurança. Diminui-se risco de incidente de segurança relacionado ao tratamento de dados pessoais e de ofensa aos princípios da integridade, disponibilidade e confidencialidade.

Áreas envolvidas

Alta administração, encarregado, setor de TI e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Não há controles prévios à implementação deste.

Principais requisitos e diretrizes de implantação

- Possuir um inventário de ativos físicos de Tecnologia da Informação, atualizado periodicamente;
- Possuir controle das licenças de software, para uma gestão efetiva dos custos de TI e planejamento das demandas relacionadas à manutenção das licenças.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento contendo inventário de software e ativos de tecnologia da informação.

Controle 14. Modelo de cláusulas contratuais

Fase: 01. Preparatório	**Tema:** 08. Gestão de terceiros

A unidade adota modelo de cláusulas contratuais para os instrumentos convocatórios, contratos administrativos, termos de parceria, acordos de cooperação e instrumentos congêneres com requisitos relativos ao tratamento de dados pessoais?

Referência

- Art. 6º, inc. VIII; Art, 26, §1º, inc. IV; Art. 33, inc. II, alínea *b*; Art. 39, LGPD;
- Arts. 16 e 114, inc. III do Decreto nº 62.100/2022.

Descrição

Trata-se de controle no procedimento de contratação de terceiros, para definição de disposições específicas para determinados tipos de contratação.

Justificativa

A adoção de modelo de cláusulas contratuais caracteriza-se como etapa fundamental para a gestão de contratações de terceiros ao estabelecer formas e limites do tratamento de dados pessoais por parte do contratado. Diminui-se o risco de descumprimento de obrigações legais por meio de terceiros.

Áreas envolvidas

Alta administração, encarregado, assessoria jurídica, unidades de compras, licitações, e contratações e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que este controle seja implementado após o Controle 15.

Principais requisitos e diretrizes de implantação

- As cláusulas podem variar de acordo com o contexto das contratações que envolvam tratamento de dados pessoais. Assim, é possível que sejam elaboradas cláusulas para a contratação de bens e materiais que diferem das cláusulas para a contratação de serviços ou para a formalização de termos de parceria;
- É possível que contratações que não sejam frequentes não necessitem de modelo de cláusulas específicas;
- Necessária avaliação das assessorias jurídicas das unidades sobre o referido controle.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento com as cláusulas para instrumentos convocatórios, contratos administrativos, termos de parceria, acordos de cooperação e instrumentos congêneres.
- **Exemplo de evidência implementada**: Minutas Padrão de Mato Grosso do Sul; Minutas Padrão de Pernambuco; Minutas Padrão da Prefeitura de São Paulo.
- **Modelo**: Manual Modelos de cláusulas contratuais no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, disponível no sítio eletrônico da CGM-SP.

Controle 15. Relação/Lista dos contratos

Fase: 01. Preparatório	**Tema:** 08. Gestão de terceiros

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?

Referência

- Art. 6º, inc. VIII; Art. 26; Art. 27; Art. 37; Art. 39, LGPD.

Descrição

A relação/lista dos contratos e instrumentos congêneres visa identificar e monitorar os terceiros que possuem responsabilidades associadas ao tratamento de dados pessoais a partir de contratos e instrumentos congêneres firmados com operadores, controladores conjuntos e fornecedores, entre outros.

Justificativa

Compartilhar dados pessoais com terceiros traz riscos importantes, pois a proteção dos dados pessoais passa a depender deles. Por isso, é essencial adotar controles eficazes para garantir segurança e conformidade, evitando acessos indevidos, usos incorretos e violações de direitos dos titulares. Trata-se de ação importante para possibilitar o processo de adequação dos instrumentos contratuais que envolvam o tratamento de dados pessoais como objeto ou para execução deste. Diminui-se o risco de descumprimento de obrigações legais por meio de terceiros.

Áreas envolvidas

Encarregado, assessoria jurídica, setor de contratações, convênios e parcerias e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Não há controles prévios à implementação deste.

Principais requisitos e diretrizes de implantação

- Espera-se que seja produzido documento com relação de contratos e instrumentos congêneres firmados com terceiros que envolvam tratamento de dados pessoais;
- Recomenda-se que, durante a identificação dos contratos, seja feita análise prévia sobre a existência de tratamento de dados pessoais no âmbito do contrato ou instrumento congênere.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento com relação/lista de contratos e instrumentos congêneres, com terceiros que envolvam tratamento de dados pessoais;
- **Modelo:** Manual Relação/lista de contratos no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, disponível no sítio eletrônico da CGM-SP.

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 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. Resolução CD/ANPD nº 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União, 17 de julho de 2024.

BRASIL Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União, 23 de agosto de 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 53.484, de 19 de outubro de 2012 - Institui o Sistema de Bens Patrimoniais Móveis - SBPM no âmbito da Administração Direta do Município de São Paulo. São Paulo, Diário Oficial da Cidade, 20 de outubro de 2012.

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). 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.

SÃO PAULO (Cidade). Orientação Técnica nº 004 – Inventário de ativos e licenças de software. Disponível em: <https://tecnologia.prefeitura.sp.gov.br/wp-content/uploads/2023/03/Brochura_OT_Vol1_v19.pdf#page=82> Acesso em: 02/09/2024

SÃO PAULO (Cidade). Orientação Técnica nº 013 – Diretrizes básicas de segurança da informação. Disponível em: < https://tecnologia.prefeitura.sp.gov.br/wp-content/uploads/2023/03/Brochura_OT_Vol3_v8.pdf#page=41 > Acesso em: 21/03/2024

SÃO PAULO (Cidade). Portaria SF nº 90 de 20 de abril de 2022 – Estabelece normas complementares e procedimentos quanto ao registro e controle de bens móveis no Sistema de

Bens Patrimoniais Móveis – SBPM, regulamentado pelo Decreto nº 53.484, de 2012, com alterações introduzidas pelos Decretos nº 56.214, de 2015, e nº 59.822, de 2020, e dá outras providências. São Paulo, Diário Oficial da Cidade, 21 de abril de 2022.

SÃO PAULO (Cidade). Portaria SMIT nº 36 de 21 de junho de 2018 - Dispõe sobre a utilização do sistema Controle Integrado de Tecnologia da Informação - CITI como canal único de entrada para abertura de chamados de suporte, entre outras atividades inerentes à gestão da tecnologia da informação e comunicação, no âmbito da Secretaria de Inovação e Tecnologia. São Paulo, Diário Oficial da Cidade, 21 de junho de 2018.

PREFEITURA DE
SÃO PAULO