GUIA ORIENTATIVO

FASE 1: PREPARATÓRIO

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

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

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

Guia Orientativo - Fase 01: Preparatório

Instrução Normativa CGM/SP nº 02/2024

Diagnóstico de Maturidade em Proteção de Dados Pessoais

FICHA TÉCNICA

Prefeitura do Município de São Paulo
Prefeito
Ricardo Nunes

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

Chefe de Gabinete
Thalita Abdala Aris

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

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

Arte e Diagramação
Marília Miquelin de Oliveira

Versão 01
Janeiro de 2025

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

Controlador Geral do Município

Daniel Falcão

VERSÃO

Versão	Descrição	Data
1.0	Versão inicial	02/2025

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

ABNT	*Associação Brasileira de Normas Técnicas*
ANPD	*Autoridade Nacional de Proteção de Dados*
CGM-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*
IEC	*International Electrotechnical Commission*
IN	*Instrução Normativa*
ISO	*International Organization of Standardization*
LGPD	*Lei Geral de Proteção de Dados Pessoais*
MGI	*Ministério da Gestão e da Inovação em Serviços Públicos*
NBR	*Normas Brasileiras Regulamentadoras*
NIST	*National Institute of Standards and Technology*
OT	*Orientação Técnica*
PEPDP	*Política Estadual de Proteção de Dados Pessoais*
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*
TCU	*Tribunal de Contas da União*
TI	*Tecnologia da Informação*

SUMÁRIO

INTRODUÇÃO

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

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

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

A elaboração da metodologia teve como base:

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

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

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

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

O presente Guia Orientativo detalha os controles da **Fase 01 – Preparatório**. Todos os órgãos serão 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 os órgãos já executem as primeiras atividades relacionadas à privacidade e à proteção

[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.

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.

CONTROLE 01. O órgão possui a indicação formal de um Encarregado da proteção de dados pessoais?

- **Referência**:
    - Art. 6º, inc. X; Art. 23, inc. III, LGPD.
- **Descrição resumida**:
    - O órgão deve designar oficialmente o Encarregado, mediante nomeação por meio de Portaria publicada no Diário Oficial da Cidade.
- **Para saber mais**:
    - A indicação do Encarregado é essencial e obrigatória para o processo de adequação do órgão à LGPD, cabendo a ele exercer diversas funções importantes, a exemplo da atuação como canal de comunicação entre o controlador de dados, os titulares e a ANPD, além da orientação dos funcionários e contratados a respeito de práticas relacionadas à proteção de dados pessoais.
    - A indicação do Encarregado deve ser realizada por ato formal (documento escrito, datado e assinado), no qual deve constar as suas formas de atuação e as atividades a serem desempenhadas. A indicação deve ser publicada no Diário Oficial da Cidade.
    - A indicação do Encarregado deve recair, preferencialmente, sobre servidores ou empregados públicos detentores de reputação ilibada. Ressalta-se que o Encarregado deve atuar com ética, integridade e autonomia técnica, evitando situações que possam configurar conflito de interesse, conforme Arts. 18 a 21 da Resolução CD/ANPD nº 18, de 16 de julho de 2024, que aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.
    - Conforme dispõe o Guia Orientativo da ANPD sobre a "*Atuação do encarregado pelo tratamento de dados pessoais*", a indicação formal do Encarregado titular deve ser acompanhada de designação de seu substituto (para os casos de ausências, impedimentos e vacâncias), para que não haja prejuízo ao exercício dos direitos dos titulares de dados pessoais.
    - Cabe ao órgão definir as qualificações profissionais necessárias para o desempenho das atribuições do Encarregado, considerando seus conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto operacional, o volume e o risco das operações de tratamento realizadas.
    - Para o exercício da função de Encarregado, espera-se que o agente público designado cumpra com os requisitos elencados no Decreto Municipal nº 59.767/2020, na Resolução CD/ANPD nº 18, de 16 de julho de 2024 e no Guia Orientativo da ANPD sobre a "*Atuação do encarregado pelo tratamento de dados pessoais*".
- **Requisitos**:
    - Designação de Encarregado e seu substituto mediante publicação de portaria.
- **Respostas esperadas**:

- **Sim**: O órgão já realizou a indicação formal de um Encarregado mediante publicação de portaria.
- **Não**: O órgão não realizou indicação formal de um Encarregado mediante publicação de portaria.
- **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Modelo de ato formal de designação de Encarregado:
    - Anexo I do Guia Orientativo da ANPD sobre a "*Atuação do encarregado pelo tratamento de dados pessoais*". "*Modelo de Ato Formal para Indicação de Encarregado Pessoa Natural*". Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf> Acesso em: 06/02/2025
  - Exemplo de portaria de designação publicada:
    - PORTARIA AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DO MUNICÍPIO DE SÃO PAULO – SP REGULA Nº 30 DE 27 DE DEZEMBRO DE 2022. Designação do encarregado de proteção de dados pessoais da Agência Reguladora de Serviços Públicos do Município de São Paulo – SP REGULA. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-agencia-reguladora-de-servicos-publicos-do-municipio-de-sao-paulo-sp-regula-30-de-27-de-dezembro-de-2022> Acesso em: 17/06/2024

- **Observação**:

  - Considerando o atual estágio de normatização na PMSP a respeito deste tema, os órgãos não precisarão analisar este controle neste ciclo de avaliação. Assim, todos os órgãos terão considerada a resposta "Sim", com a evidência cumprida pela própria CGM-SP, conforme Art. 5º do Decreto Municipal nº 59.767, de 2020. Caso haja alteração normativa que exija a implementação deste controle pelos órgãos da PMSP, este controle poderá ser reavaliado.

CONTROLE 02. O órgão possui um Grupo de Trabalho, ou estrutura equivalente, para apoiar na adequação à LGPD?

- **Referência**:
    - Art. 6º, inc. X; Art. 50, LGPD.
- **Descrição resumida**:
    - 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.
- **Para saber mais**:
    - O Grupo de Trabalho é importante para se garantir que a implementação da LGPD no órgão ocorra de maneira coordenada. Espera-se que o Grupo de Trabalho coordene a implementação dos controles previstos na Metodologia de Diagnóstico de Maturidade em Proteção de Dados Pessoais no respectivo órgão, aprofundando seus conhecimentos no tema e planejando os trabalhos de maneira estruturada.
    - A composição do grupo deve ser proporcional ao tamanho do órgão e à complexidade do tratamento de dados. Ademais, espera-se que os integrantes do grupo tenham competências multidisciplinares, envolvendo a área Jurídica, de Tecnologia, de Segurança da Informação, de Recursos Humanos / Gestão de Pessoas, entre outros.
    - Após a definição do grupo, é boa prática atribuir funções a seus membros e formalizar a sua instituição através da publicação de ato normativo.
    - É importante que o grupo tenha apoio e/ou participação da alta administração, como também tenha acesso a áreas-chave relacionadas com a implementação da LGPD, tais como o setor de TI, a Segurança da Informação, a Ouvidoria, o Controle Interno, o Departamento Jurídico, entre outros.
- **Requisitos**:
    - Designação de Grupo de Trabalho por meio da publicação de portaria.
- **Respostas esperadas**:
    - **Sim**: Houve formalização de grupo de trabalho ou estrutura equivalente para apoiar na adequação à LGPD, por meio de ato normativo devidamente publicado.
    - **Não**: Não houve formalização ou criação de grupo de trabalho ou estrutura equivalente para apoiar o órgão na adequação à LGPD.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.
- **Exemplos de evidências**:
    - Exemplos de portaria de designação publicada:

- PORTARIA SECRETARIA MUNICIPAL DE HABITAÇÃO - SEHAB Nº 101 DE 31 DE DEZEMBRO DE 2021. Cria o “Grupo de Trabalho para implantar o Programa de Adequação à Lei Geral de Proteção a Dados Pessoais" (GT-LGPD) na Secretaria Municipal da Habitação. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-da-habitacao-e-desenvolvimento-urbano-sehab-101-de-31-de-dezembro-de-2021> Acesso em: 14/06/2024
- PORTARIA SECRETARIA MUNICIPAL DE ASSISTÊNCIA E DESENVOLVIMENTO SOCIAL - SMADS Nº 71 DE 24 DE NOVEMBRO DE 2021. Institui grupo de trabalho para a regulamentação e implementação da Lei Geral de Proteção de Dados Pessoais no âmbito da Secretaria Municipal de Assistência e Desenvolvimento Social. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-de-assistencia-e-desenvolvimento-social-smads-71-de-24-de-novembro-de-2121> Acesso em: 17/06/2024
- PORTARIA SECRETARIA MUNICIPAL DE HABITAÇÃO - SEHAB/COHAB Nº 18 DE 14 DE DEZEMBRO DE 2020. Cria Equipe Multidisciplinar, em atendimento à aplicação da Lei Federal nº 13.709 de 14 de agosto de 2018, - Lei Geral de Proteção de Dados Pessoais - LGPD, regulamentada no âmbito municipal, pelo Decreto nº 59.767 de 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-de-habitacao-sehab-cohab-18-de-14-de-dezembro-de-2020> Acesso em: 17/06/2024
- PORTARIA SECRETARIA MUNICIPAL DA FAZENDA - SF Nº 331 de 13 de Dezembro de 2019. Constitui Grupo de Trabalho para implantar o Programa de Proteção à Privacidade na Secretaria Municipal da Fazenda aderente à Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais. Disponível em: < https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-da-fazenda-sf-331-de-13-de-dezembro-de-2019 > Acesso em: 17/06/2024
- PORTARIA SECRETARIA MUNICIPAL DE MOBILIDADE E TRÂNSITO – SMT Nº 3 DE 13 DE JANEIRO DE 2023. Institui o Grupo de Trabalho da SMT com o objetivo de discutir, propor e implementar um Plano de Adequação da Pasta à Lei Geral de Proteção de Dados - LGPD. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-de-mobilidade-e-transito-smt-3-de-13-de-janeiro-de-2023> Acesso em: 17/06/2024

CONTROLE 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?

- **Referência**:
    - Art. 6º, inc. X; Art. 50, LGPD.
    - Art. 14, inc. VI, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - 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 e visam promover mudanças no comportamento dos indivíduos, demonstrando a importância de cada um dos colaboradores para uma mudança na cultura organizacional. Exemplos de ações de sensibilização: 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.

- **Para saber mais**:
    - A adequação do órgão à LGPD exige um esforço coletivo de todos os envolvidos, sendo imprescindível promover um reforço na cultura organizacional de proteção de dados pessoais. Desta forma, espera-se que as ações de sensibilização atinjam todo o órgão e, inclusive, parceiros e a sociedade civil.
    - O conteúdo das ações de sensibilização pode estar relacionado com boas práticas de segurança da informação, aspectos conceituais básicos da LGPD, conceitos de privacidade e proteção de dados pessoais e aspectos procedimentais do órgão, entre outros.
    - Espera-se que as ações de sensibilização sejam personalizadas ao contexto e características do órgão, para que os colaboradores assimilem os conceitos de modo mais próximo à realidade em que atuam.

- **Requisitos**:
    - Realização de no mínimo uma ação de sensibilização com envolvimento de todo o órgão, não sendo necessária a participação de todos os funcionários.

- **Respostas esperadas**:

- **Sim**: o órgão realizou uma ou mais ações de sensibilização sobre a LGPD que envolveu toda a organização de forma sistêmica, isto é, atingiu todos os colaboradores, ainda que nem todos tenham participado diretamente da ação.
- **Não**: o órgão não realizou evento de sensibilização sobre LGPD com envolvimento de toda a organização.
- **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Exemplos de evidências que podem ser armazenadas:
    - Campanhas institucionais;
    - Materiais educativos (apresentações, vídeos, guias, cartilhas, etc.);
    - Comunicação com os colaboradores (e-mails, cartazes, etc.);
    - Atividades (desafios, questionários, atividades interativas, etc.);
    - Avaliações de conhecimento (testes, dinâmicas, avaliações, etc.);
    - Ata de presença dos cursos oferecidos e programa ofertado;
    - Resultado de avaliação de entendimento dos colaboradores.
  - Exemplo de curso realizado:
    - 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 em: <https://capital.sp.gov.br/web/controladoria_geral/cursos> Acesso em: 13/12/2024

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

- **Referência**:
    - Art. 6º, inc. VIII, LGPD.
    - Art. 4º, inc. III; Art. 15, Decreto nº 59.767/2020.

- **Descrição resumida**:
    - 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.

- **Para saber mais**:
    - O planejamento das ações para a adequação do órgão à LGPD é importante para que todo o processo ocorra de forma coordenada.
    - O documento de planejamento é importante para registrar as ações que já foram realizadas, e também as ações que estão previstas para implementação futura, assim como os respectivos responsáveis e prazos.

- **Requisitos**:
    - Documento com a descrição das atividades necessárias e respectivos responsáveis e prazos.

- **Respostas esperadas**:
    - **Sim**: O órgão elaborou Planejamento para elaboração de seu Programa de Governança em Privacidade e Proteção de Dados Pessoais.
    - **Não**: O órgão não elaborou Planejamento para elaboração de seu Programa de Governança em Privacidade e Proteção de Dados Pessoais.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:
    - Modelo de documento (uso não obrigatório):
        - **Modelo de Planejamento da IN CGM nº 02/2024**. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/instru%C3%A7%C3%A3o-normativa-cgm-n-02-2024> Acesso em: 11/02/2025

CONTROLE 05. O órgão realizou, revisou ou atualizou, no período, o mapeamento de processos que tratam dados pessoais?

- **Referência**:
    - Art. 6º, inc. VIII, LGPD.
    - Art. 4º, inc. I, Decreto nº 59.767/2020.
    - Art. 2º; Art. 14, inc. IV, alínea *b*, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - O mapeamento de processos é etapa preliminar importante para se realizar o inventário de dados pessoais do órgão. É por meio do mapeamento de processos que se pode ter uma visão geral das atividades realizadas e em quais etapas se concentram o tratamento de dados pessoais.

- **Para saber mais**:
    - O mapeamento de processos precede a realização do mapeamento de dados pessoais, porque é necessária a identificação de todas as ações existentes no órgão a fim de que possam ser identificadas as operações de tratamento de dados pessoais havidas em cada processo.

- **Requisitos**:
    - O mapeamento de processos resulta em uma lista contendo o repositório de todos os processos do órgão. O nível de detalhamento pode variar de acordo com as suas necessidades;

- **Respostas esperadas**:
    - **Sim**: O órgão realizou o mapeamento de todos os processos que tratam dados pessoais.
    - **Não**: O órgão não realizou o mapeamento dos processos que tratam dados pessoais.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:
    - Modelos de documento (uso não obrigatório):
        - **Modelo de Mapeamento de Processos da IN CGM nº 02/2024**. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/instru%C3%A7%C3%A3o-normativa-cgm-n-02-2024> Acesso em: 11/02/2025
        - **Modelo de Mapeamento de Processos da IN CGM nº 01/2022.**
            - Anexo I – Mapeamento de Dados Pessoais, da IN CGM nº 01/2022 <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controlado

ria_geral/Anexo%20I%20-%20Mapeamento%20de%20Dados%20Pessoais.xlsx> Acesso: 17/06/2024

- Capítulo I – Mapeamento de Processos, do Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022. 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: 13/12/2024

CONTROLE 06. O órgão realizou, revisou ou atualizou, no período, o mapeamento de dados pessoais dos processos mapeados?

- **Referência**:
    - Art. 6º, inc. VIII; Art. 37, LGPD.
    - Art. 4º, inc. I, Decreto nº 59.767/2020.
    - Art. 2º; Art. 14, inc. IV, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - O mapeamento de dados pessoais deve conter as informações, de forma clara, adequada e ostensiva, sobre todo o ciclo de vida dos dados pessoais do titular (com a identificação dos dados pessoais utilizados em cada processo). A elaboração do mapeamento é importante para entender como os dados pessoais são coletados e como se movem pelo órgão, facilitando a rápida localização de um dado mapeado em caso de ocorrer algum incidente, assim como o rápido atendimento a uma requisição do titular de dados pessoais.

- **Para saber mais**:
    - Realizado o mapeamento de processos do órgão, é possível iniciar o mapeamento de dados pessoais.
    - O mapeamento de dados pessoais é um procedimento que serve para verificar as atividades que utilizam dados pessoais e se a realização de tais atividades se encontra em conformidade com a LGPD. Trata-se de um documento que identifica todos os processos que tratam dados pessoais.
    - O mapeamento de dados pessoais consiste no registro das operações de tratamento dos dados pessoais realizados pelo órgão (Art. 37 da LGPD).

- **Requisitos**:
    - O mapeamento de dados pessoais resulta em uma lista contendo o repositório de todos os dados pessoais tratados pelo órgão. O nível de detalhamento pode variar de acordo com as suas necessidades;

- **Respostas esperadas**:
    - **Sim**: O órgão realizou o mapeamento de dados pessoais dos processos mapeados.
    - **Não**: O órgão não realizou o mapeamento de dados pessoais dos processos mapeados.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:
    - Modelos de documento (uso não obrigatório):
        - **Modelo de Mapeamento de Dados Pessoais da IN CGM nº 02/2024**. Disponível em:

<https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/instru%C3%A7%C3%A3o-normativa-cgm-n-02-2024> Acesso em: 11/02/2025

- **Modelo de Mapeamento de Dados Pessoais da IN CGM nº 01/2022.**
  - Anexo I – Mapeamento de Dados Pessoais, da IN CGM nº 01/2022 <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/Anexo%20I%20-%20Mapeamento%20de%20Dados%20Pessoais.xlsx> Acesso: 17/06/2024
  - Capítulo II – Mapeamento de Dados Pessoais, do Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022. 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: 13/12/2024

CONTROLE 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?

- **Referência**:
    - Art. 6º, inc. I, II, III; Art. 23, inc. I, LGPD.
    - Art. 10; Art. 14, inc. IV, alínea *f*, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - A identificação das finalidades e das hipóteses legais para o tratamento de dados pessoais envolve o levantamento dos fundamentos que autorizam o tratamento de dados pessoais pelo órgão. Como exemplo, pode ser citada a identificação de obrigações legais e regulatórias, execução de políticas públicas, contratos e normas específicas relativas às atividades do órgão. Nota-se que, além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser respeitados. As atividades de tratamento de dados pessoais devem ter propósitos legítimos e específicos, os quais devem ser devidamente informados ao titular.

- **Para saber mais**:
    - O tratamento de dados pessoais deve ter propósitos legítimos, específicos e explícitos, os quais devem ser informados ao titular, sendo que não poderá haver tratamento posterior de forma incompatível com as finalidades anteriormente informadas ao titular.
    - Adicionalmente à finalidade, deve-se relacionar o tratamento de dados pessoais com as respectivas hipóteses legais que fundamentam a operação, previstas nos arts. 7º ou 11 da LGPD. A análise das hipóteses legais também inclui o levantamento de outras normas relativas às atividades do órgão, como leis, decretos, regimentos, resoluções e portarias que também fundamentam o tratamento de dados pessoais.
    - Espera-se que o órgão seja devidamente orientado pelo respectivo Encarregado quanto à identificação das finalidades e hipóteses legais. Ações de conscientização para a correta identificação são importantes para que o tratamento de dados pessoais ocorra em conformidade com a LGPD.
    - A partir do mapeamento de processos e do mapeamento de dados pessoais (controles também avaliados nesta Fase 01 do Diagnóstico), o órgão poderá consolidar a identificação das finalidades e das hipóteses legais referentes às operações de tratamento de dados pessoais em documento resumido.

- **Requisitos**:
    - Documento consolidado com lista de todos as operações de tratamento de dados pessoais realizadas pelo órgão, com a indicação da respectiva finalidade e hipótese legal.

- **Respostas esperadas**:

- **Sim**: O órgão realizou análise das finalidades e das hipóteses legais que foram consideradas para o tratamento de dados pessoais.
- **Não**: O órgão não realizou análise das finalidades e das hipóteses legais que foram consideradas para o tratamento de dados pessoais.
- **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Modelos de documento (uso não obrigatório):
    - **Modelo de documento sobre finalidades e hipóteses legais da IN CGM nº 02/2024**. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/instru%C3%A7%C3%A3o-normativa-cgm-n-02-2024> Acesso em: 11/02/2025

CONTROLE 08. O órgão disponibiliza canal específico para recebimento de demandas de atendimento aos direitos dos titulares referentes à LGPD?

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

- **Descrição resumida**:
    - É importante e obrigatório disponibilizar um canal específico para recebimento de demandas referentes à LGPD, como o atendimento dos direitos dos titulares, uma vez que a definição dessa estrutura possibilita que o procedimento de resposta ao titular de dados pessoais seja mais organizado e célere.

- **Para saber mais**:
    - De acordo com o Art. 41 da LGPD, a identidade e as informações de contato com o Encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do órgão.
    - Nesse sentido, o canal de comunicação para assuntos relacionados à LGPD é importante para o recebimento de demandas relacionadas ao atendimento aos direitos dos titulares.

- **Requisitos**:
    - Indicação de meios de contato no sítio eletrônico do órgão para assuntos relacionados à LGPD.

- **Respostas esperadas**:
    - **Sim**: O órgão disponibilizou canal específico para recebimento de demandas referentes à LGPD.
    - **Não**: O órgão não disponibilizou canal para recebimento de demandas referentes à LGPD.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:
    - Exemplo do site da CGM:
        - Link para canal de recebimento de demandas dos titulares de dados pessoais. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/w/encarregado-pelo-tratamento-de-dados-pessoais> Acesso em 06/02/2025

- **Observação**:

- Todos os órgãos deverão ter seção própria em seus sítios eletrônicos para assuntos relacionados à proteção de dados pessoais. Considerando o atual estágio de normatização na PMSP, para o atendimento do presente controle, os órgãos deverão indicar em seus sítios eletrônicos o canal da CGM-SP para recebimento de demandas dos titulares de dados pessoais (<https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/w/encarregado-pelo-tratamento-de-dados-pessoais>, acesso em 10/06/2024). Isto porque no atual estágio de normatização da PMSP, o Controlador Geral do Município é o encarregado pelo tratamento de dados pessoais na PMSP, sendo sua atribuição manter o canal para recebimento das demandas dos titulares de dados pessoais, conforme Art. 5º e 6º do Decreto Municipal nº 59.767 de 2020. Caso haja alteração normativa que modifique a implementação deste controle pelos órgãos da PMSP, este controle poderá ser reavaliado.

CONTROLE 09. Existe um canal apropriado para o recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação?

- **Referência**:
    - Art. 6º, inc. X; Art. 48; Art. 50, § 2º, inc. I, alínea *g*, LGPD.
- **Descrição resumida**:
    - É importante que o órgão disponibilize canal apropriado para o recebimento de denúncias e encaminhamento de soluções a respeito dos incidentes envolvendo o tratamento de dados pessoais.
- **Para saber mais**:
    - De acordo com a ANPD, incidente de segurança é qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade dos dados pessoais.
    - O Art. 48 da LGPD, por sua vez, estabelece a obrigação de comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Tal comunicação deve ocorrer nos prazos previstos pela ANPD.
    - Considerando a importância do registro dos incidentes de segurança e os prazos exíguos para comunicação, entende-se como boa prática a utilização de um canal para recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação, para que o tratamento desses casos ocorra de forma coordenada e eficiente. O canal deve ser divulgado a todos os colaboradores do órgão público.
    - Para mais informações, consulte a Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.
- **Requisitos**:
    - Existência de canal para recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação.
    - Divulgação do canal nos meios de comunicação adequados para o público interno e externo.
- **Respostas esperadas**:
    - **Sim**: O órgão disponibilizou canal específico para recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação.
    - **Não**: O órgão não disponibilizou canal específico para recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.
- **Exemplos de evidências**:

- Link para canal de recebimento de denúncias e/ou notificações de incidentes de Segurança da Informação.

    - Para o recebimento de notificações provenientes de colaboradores internos, o órgão pode se utilizar do sistema CITI (<http://citi.pmsp/>), sendo considerada como evidência a indicação do link e informações explicativas aos colaboradores no site da instituição.

    - Para o recebimento de notificações provenientes de público externo, a unidade pode adotar a menção, em seu site, das informações para contato do encarregado pelo tratamento de dados pessoais (com o respectivo link), ou canal específico, caso exista. Exemplo do site da CGM: Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/w/encarregado-pelo-tratamento-de-dados-pessoais> Acesso em 06/02/2025

CONTROLE 10. O órgão divulga a identidade e as informações de contato do Encarregado de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?

- **Referência**:
    - Art. 6º, inc. VI; Art. 41, § 1º, LGPD.
    - Art. 5º, parágrafo único, Decreto nº 59.767/2020.

- **Descrição resumida**:
    - A identidade e as informações de contato (ex.: e-mail, telefone) com o Encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico do órgão.

- **Para saber mais**:
    - O Art. 41 da LGPD define que a identidade e as informações de contato com o Encarregado devem ser divulgadas publicamente, de forma objetiva e clara, em local de destaque e de fácil acesso, preferencialmente no sítio eletrônico do órgão.
    - As informações de contato devem conter dados referentes aos meios de comunicação que viabilizem o exercício dos direitos dos titulares e possibilitem o recebimento de comunicações da ANPD.
    - A divulgação de tais informações é importante para a garantia dos princípios de livre acesso e de transparência, além de viabilizar ao titular de dados a possibilidade de exercer seus direitos.
    - Conforme o Guia Orientativo da ANPD sobre a "*Atuação do encarregado pelo tratamento de dados pessoais*" também deve haver divulgação da identidade e formas de contato do substituto do Encarregado titular.
    - Para mais informações, vide Resolução CD/ANPD nº 18, de 16 de julho de 2024.

- **Requisitos**:
    - Divulgação do nome completo e contato do Encarregado e seu substituto no sítio eletrônico.

- **Respostas esperadas**:
    - **Sim**: O órgão divulgou a identidade e as informações de contato do Encarregado de forma pública no sítio eletrônico do Órgão.
    - **Não**: O órgão não divulgou devidamente a identidade e as informações de contato do Encarregado de forma pública no sítio eletrônico do Órgão.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:
    - Exemplo do site da CGM:

- Link para transparência com as informações de contato do Encarregado. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/w/encarregado-pelo-tratamento-de-dados-pessoais> Acesso em 06/02/2025

- **Observação**:

  - Todos os órgãos deverão ter seção própria em seus sítios eletrônicos para assuntos relacionados a proteção de dados pessoais. Considerando o atual estágio de normatização na PMSP, para o atendimento do presente controle, os órgãos deverão indicar em seus sítios eletrônicos a identidade e as informações de contato do Encarregado conforme divulgado no sítio eletrônico da CGM-SP (<https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/w/encarregado-pelo-tratamento-de-dados-pessoais>, acesso em 10/06/2024). Isto porque no atual estágio de normatização da PMSP, o Controlador Geral do Município é o Encarregado pelo tratamento de dados pessoais da PMSP, conforme Art. 5º do Decreto Municipal nº 59.767 de 2020. Caso haja alteração normativa que modifique a implementação deste controle pelos órgãos da PMSP, este controle poderá ser reavaliado.

CONTROLE 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?

- **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.
    - Art. 10, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - Conforme dispõe o Art. 9º, inc. I, II e V da LGPD, o titular de dados pessoais 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. Nesse sentido, deve ser concedido acesso a informações sobre: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; e informações acerca do uso compartilhado de dados pelo controlador e a sua finalidade.

- **Para saber mais**:
    - De acordo com o disposto no Art. 23, inc. I da LGPD, o tratamento de dados pessoais pelo Poder Público exige que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, devendo ser fornecidas informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.
    - A divulgação de tais informações é importante para garantir o livre acesso e a transparência, além de assegurar ao titular de dados pessoais a possibilidade de exercer seus direitos.

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

- **Respostas esperadas**:
    - **Sim**: O órgão fornece em seu sítio eletrônico informações sobre previsão legal, finalidade, compartilhamentos, transferências, procedimentos e práticas utilizadas.

- **Não**: O órgão não fornece em seu sítio eletrônico informações sobre previsão legal, finalidade, compartilhamentos, transferências, procedimentos e práticas utilizadas.
- **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Modelos de documento (uso não obrigatório):
    - **Modelo de documento sobre transparência do tratamento de dados pessoais da IN CGM nº 02/2024**. Disponível em: <https://capital.sp.gov.br/web/controladoria_geral/w/coordenadoria_de_protecao_de_dados_pessoais/instru%C3%A7%C3%A3o-normativa-cgm-n-02-2024> Acesso em: 11/02/2025

CONTROLE 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?

- **Referência**:
    - Art. 6º, inc. VI; Art. 9º; Art. 18, LGPD.
    - Art. 10, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - 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 pessoais, 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.

- **Para saber mais**:
    - Os Banners de Cookies reforçam os princípios da transparência e do livre acesso, uma vez que apresentam, de maneira resumida e simplificada, informações essenciais para a tomada de decisão consciente pelo titular, além de fomentar o controle sobre seus dados pessoais.
    - Uma boa prática na elaboração do Banner de Cookies é a separação em duas camadas, sendo que a primeira oferece as opções de "aceitar todos os cookies", "rejeitar cookies não necessários" e "selecionar cookies".
    - Por sua vez, a segunda camada deve classificar os cookies em categorias, de acordo com seus usos e finalidades, permitindo a obtenção do consentimento pelo titular para cada finalidade específica. Deve-se desativar os cookies baseados no consentimento por padrão.
    - É importante apresentar informações simples, claras e precisas, além de disponibilizar informações sobre como realizar o bloqueio de cookies pelas configurações do navegador.

- **Requisitos**:
    - Banner de Cookies de primeiro nível:[4]
        - Disponibilizar botão que permita rejeitar todos os cookies não necessários, de fácil visualização;

[4] ANPD, Brasil. Guia Orientativo – Cookies e proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 12/07/2024. Pgs. 30 e 31.

        - Fornecer um link de fácil acesso para que o titular possa exercer os seus direitos.
    - Banner de Cookies de segundo nível:[5]
        - Classificar os cookies em categorias, com a descrição de acordo com seus usos e finalidades, de forma simples, clara e precisa;
        - Permitir a obtenção do consentimento para cada finalidade específica, quando couber;
        - Desativar cookies baseados no consentimento por padrão;
        - Disponibilizar informações sobre como realizar o bloqueio de cookies pelas configurações do navegador.

- **Respostas esperadas**:

    - **Sim**: O órgão realiza a coleta de cookies em camadas, utilizando-se de informações simples e acessíveis, havendo opção para o usuário gerenciar o seu consentimento no banner da segunda camada sobre a possibilidade de ativação ou desativação de categorias de cookies quando estes não forem estritamente necessários.
    - **Não**: O órgão não realiza a coleta de cookies em camadas, não informa o usuário de maneira simples e acessível ou não permite que ele realize a gestão de seu consentimento.
    - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

    - Link para site contendo banner de cookies.

[5] Idem, pgs. 31 e 32.

CONTROLE 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?

- **Referência**:
    - Art. 6º, inc. VII; Art. 46; Art. 47; Art. 49, LGPD.
    - OT nº 004 e 013 do Decreto nº 57.653/2017.

- **Descrição resumida**:
    - É uma boa prática manter 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 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).

- **Para saber mais**:
    - A realização de inventário físico corresponde ao levantamento de todos os bens em uma determinada data, com detalhamento de quantidades e estado de cada item. Entre as vantagens da realização de inventário está a visão geral obtida quanto a situação dos bens, incluindo o fornecimento de informações para tomada de decisão quando da ocorrência de sinistro sobre algum ativo que contenha dados pessoais. Recomenda-se que os ativos físicos estejam identificados com número de patrimônio e possuam um gestor responsável associado.
    - É essencial que os órgãos estabeleçam controle das licenças de software que possuam, para que exerçam uma gestão efetiva dos custos de TI e possam planejar suas demandas relacionadas à manutenção das licenças. Recomenda-se que os comprovantes de aquisição sejam armazenados e que as licenças sejam contratadas do tipo "corporativa", não permitindo a instalação de softwares com licenças pessoais ou que não tenham sido adquiridos pela PMSP.
    - Para a realização do inventário é importante considerar as disposições da legislação:
        - 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;
        - 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;
        - 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.

- Orientação Técnica nº 004 – Inventário de Ativos e Licenças de Software e Orientação Técnica nº 013 – Diretrizes Básicas de Segurança da Informação, previstas pelo Decreto Municipal 57.653, de 07 de abril de 2017, o qual define a Política Municipal de Tecnologia da Informação e Comunicação.

- **Requisitos**:

  - Possuir um inventário de ativos de Tecnologia da Informação (físico e de software), atualizado periodicamente.

- **Respostas esperadas**:

  - **Sim**: O órgão realizou o inventário de software e de ativos de tecnologia da informação e também executou uma configuração segura nos ativos.
  - **Não**: O órgão não realizou o inventário de software e de ativos de tecnologia da informação ou não executou uma configuração segura nos ativos.
  - **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Documento contendo inventário de software e ativos de tecnologia da informação.

CONTROLE 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?

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

- **Descrição resumida**:
    - Uma boa prática de tratamento de dados pessoais envolve o estabelecimento de um procedimento de gestão de contratações de terceiros. Nesse sentido, é importante definir as disposições específicas para cada modalidade de contratação, criar cláusulas contratuais padrão, instituir procedimentos de fiscalização, entre outras ações pertinentes.

- **Para saber mais**:
    - A permissão para o tratamento de dados pessoais constantes das bases de dados detidas pelo Poder Público com respaldo em contrato de prestação de serviços tem fundamento no art. 26, §1º, inc. IV, da LGPD.
    - Nesse contexto, cabe ao órgão público decidir sobre as formas e limites do tratamento, assim como instruir e fiscalizar o contratado. É importante que os instrumentos que estabeleçam relação com terceiros para o tratamento de dados pessoais contenham cláusulas que protejam o interesse público.
    - A utilização de cláusulas padrão é uma boa prática que acelera as contratações públicas, devendo haver avaliação das assessorias jurídicas das unidades sobre a sua utilização.
    - É importante ressaltar que as cláusulas podem variar de acordo com o contexto das contratações. Assim, é possível que sejam elaboradas cláusulas padrão para a contratação de determinados serviços que diferem das cláusulas padrão elaboradas para a contratação de outros (ex. utilização de cláusulas padrão específicas para contratos que prevejam o tratamento de dados pessoais de crianças e adolescentes). Ademais, é possível que contratações que não sejam frequentes não necessitem de cláusulas padrão específicas. Cabe a cada órgão avaliar a necessidade de tais instrumentos.
    - Para os casos de transferências internacionais de dados pessoais, consulte mais informações sobre cláusulas contratuais padrão aplicáveis no Capítulo V da Resolução CD/ANPD nº 19/2024.

- **Requisitos**:
    - Lista com os tipos mais frequentes de instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres com os seus respectivos requisitos mínimos relativos ao tratamento de dados pessoais.

- **Respostas esperadas**:
    - **Sim**: O órgão adotou minutas padrão para todos os casos em que entendeu ser necessário.
    - **Não**: O órgão não adotou minutas padrão com requisitos mínimos relativos ao tratamento de dados pessoais.
    - **Não se aplica**: Caso o órgão entenda que não seja necessário a adoção de minutas padrão em razão de alguma especificidade de sua atuação, justifique.

- **Exemplos de evidências**:
    - Documento com as minutas padrão para instrumentos convocatórios, contratos administrativos, termos de cooperação e instrumentos congêneres.

CONTROLE 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?

- **Referência**:
    - Art. 6º, inc. VIII; Art. 26; Art. 27; Art. 37; Art. 39, LGPD.
    - Art. 14, inc. IV, alíneas *j*, *k*, *l*, IN/CGM nº 01/2022.

- **Descrição resumida**:
    - É importante que o órgão identifique os terceiros que possuem responsabilidades associadas ao tratamento de dados pessoais, mapeando os contratos firmados com operadores, controladores conjuntos e fornecedores, entre outros. É importante que o órgão tenha registro dos compartilhamentos e das transferências internacionais de dados pessoais realizados.

- **Para saber mais**:
    - O levantamento de informações sobre terceiros (operadores, co-controladores, etc.) é uma ação importante para se garantir o processo de adequação dos instrumentos contratuais. Ademais, tal atividade também permite a identificação dos requisitos aplicáveis a esses terceiros para posterior monitoramento.
    - O levantamento de informações sobre compartilhamentos e transferências internacionais de dados pessoais é importante para que o órgão possa realizar o controle e monitoramento do tratamento desses dados. Assim, em caso de incidente de segurança da informação, o órgão estará capacitado para agir com maior celeridade e eficiência.

- **Requisitos**:
    - Documento com o mapeamento de contratos firmados com terceiros, com informações mínimas acerca das condições de tratamento de dados pessoais realizados.
    - Documento com o mapeamento de compartilhamentos e transferências de dados pessoais, com informações mínimas acerca dos dados pessoais tratados, prazos, mecanismos de segurança, etc.

- **Respostas esperadas**:
    - **Sim**: O órgão realizou o mapeamento de contratos com terceiros e também o mapeamento de compartilhamentos e transferências de dados pessoais.
    - **Não**: O órgão realizou o mapeamento de contratos com terceiros ou o mapeamento de compartilhamentos e transferências de dados pessoais.

- **Não se aplica**: Este controle é aplicável a todos os órgãos.

- **Exemplos de evidências**:

  - Documento com relação/lista de contratos com terceiros que envolvam tratamento de dados pessoais; e
  - Documento com relação/lista de compartilhamentos e transferências de dados pessoais.

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). 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 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/arquivos/ot-volumes/OT_vol3.pdf#page=35> 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.

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO