GUIA ORIENTATIVO

Fase 02 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

João Francisco Resende

Thiago Ryuichi Hirata

Revisão

Alana Leite Catuzzati

Arte e Diagramação

Marília Miquelin de Oliveira

Versão 01

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	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 do Diagnóstico de Maturidade.

O presente manual detalha os controles da Fase 02. Os órgãos e entidades devem completar a implementação de todos os controles previstos (ou justificar sua não aplicabilidade) na fase anterior (Fase 01) para progredir à Fase 02. Após a implementação dos controles exigidos nesta fase, as unidades devem ter seus processos de negócios formalizados em procedimentos e fluxos, havendo documentação que demonstre como o trabalho deve ser realizado. Espera-se que o órgão ou a entidade tenha revisado seus principais processos e atividades relacionados à privacidade e à proteção de dados pessoais.

Controle 16. Capacitação do Encarregado

Fase: 02. Básico	**Tema:** 01. Estrutura Organizacional

O Encarregado pelo tratamento de dados pessoais participou, no período, de alguma capacitação específica direcionada à sua função?

Referência

- Art. 6º, inc. X; Art. 50, LGPD;
- Art. 2º, inc. XIII, Decreto nº 59.767/2020;
- Resolução CD/ANPD nº 18/2024.

Descrição

Participação do Encarregado pelo tratamento de dados pessoais da unidade em, ao menos, uma capacitação sobre tema relacionado com as suas atribuições.

Justificativa

A atuação do Encarregado envolve conhecimentos multidisciplinares e assuntos objeto de constante regulamentação por parte da Agência Nacional de Proteção de Dados (ANPD). Dessa forma, é importante que o Encarregado aprimore os seus conhecimentos sobre a legislação vigente e normas técnicas aplicáveis, com foco nos temas referentes a riscos, segurança da informação, tratamento de dados pessoais e privacidade, bem como acompanhe as atualizações e orientações da ANPD (atos normativos, notas técnicas, guias orientativos, entre outros) a respeito de temas que impactem a sua atuação. Diminui-se o risco de lentidão ou não adequação da unidade à LGPD e às boas práticas em privacidade e proteção de dados pessoais.

Áreas envolvidas

Encarregado.

Momento de implementação

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

Principais requisitos e diretrizes de implantação

- Participação em capacitação no período, independentemente de carga horária;
- Conteúdo da capacitação deve abordar conceitos mais aprofundados acerca da atuação do encarregado em temas como atendimento aos direitos do titular, segurança da informação, gestão de riscos, privacidade e proteção de dados pessoais, entre outros;
- A capacitação consiste em atividade contínua e periódica, de modo que somente será aceito certificado de curso realizado ao longo do ciclo anual de avaliação da Fase 02 do Diagnóstico.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Certificado de participação em capacitação.

Controle 17. Capacitação do Grupo de Trabalho

Fase: 02. Básico	**Tema:** 01. Estrutura Organizacional

O Grupo de Trabalho de apoio à adequação à LGPD participou no período de algum treinamento relacionado com a temática de proteção de dados pessoais?

Referência

- Art. 6º, inc. X; Art. 50, LGPD;
- Art. 2º, inc. XIII, Decreto nº 59.767/2020.

Descrição

Participação dos integrantes do Grupo de Trabalho do órgão ou da entidade em, ao menos, uma capacitação sobre tema relacionado com as suas atribuições.

Justificativa

O Grupo de Trabalho terá papel de destaque na implementação de atividades relacionadas à adequação do órgão à LGPD. Investir na capacitação dos agentes públicos integrantes do grupo torna-se tarefa importante para conferir à equipe os conhecimentos necessários para implantar o programa de governança do órgão, bem como auxiliar e orientar os demais agentes públicos da unidade sobre os requisitos e as melhores práticas em termos de proteção de dados pessoais. Diminui-se o risco de lentidão ou não adequação da unidade à LGPD e às boas práticas em privacidade e proteção de dados pessoais.

Áreas envolvidas

Grupo de Trabalho.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 02 – Grupo de Trabalho.

Principais requisitos e diretrizes de implantação

- Participação dos agentes públicos integrantes do grupo de trabalho em capacitação no período, independentemente de carga horária;
- Conteúdo da capacitação deve abordar conceitos mais aprofundados em temas como atendimento aos direitos do titular, segurança da informação, gestão de riscos, privacidade e proteção de dados pessoais, entre outros;
- A capacitação consiste em atividade contínua e periódica, de modo que somente será aceito certificado de curso realizado ao longo do ciclo anual de avaliação da Fase 02 do Diagnóstico.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Certificado de participação em capacitação.

Controle 18. Plano de Gestão de Riscos em Privacidade

Fase: 02. Básico	**Tema:** 02. Governança

A unidade elaborou e/ou atualizou, no período, o seu Plano de Gestão de Riscos em Privacidade (contemplando as atividades de Identificação, Análise, Avaliação e Tratamento de Riscos)?

Referência

- Art. 6º, inc. VIII; Art. 50, LGPD;
- Art. 2º, inc. XIII, Decreto nº 59.767/2020.

Descrição

O órgão ou a entidade deve realizar as atividades de identificação, análise, avaliação e tratamento dos riscos de privacidade associados aos processos que realizam tratamento de dados pessoais.

Justificativa

A elaboração de plano de gestão de riscos em privacidade envolve a identificação e a compreensão da probabilidade e do impacto de cada risco, a partir da qual é possível priorizar ações e gerenciar as medidas necessárias para manter o risco em um nível aceitável para o gestor. Diminui-se o risco de concretização de ameaças relacionadas ao tratamento de dados pessoais.

Áreas envolvidas

Encarregado, grupo de trabalho, alta administração da unidade e demais unidades a critério do gestor.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 05 – Mapeamento de processos, 06 – Mapeamento de dados pessoais, 07 – Finalidades e hipóteses legais e 19 – Política de Gestão de Riscos.

Principais requisitos e diretrizes de implantação

- O plano de gestão de riscos da unidade deve conter as etapas de identificação, análise, avaliação e tratamento dos riscos;
- Metodologia deve incluir aspectos relacionados à privacidade;
- Documento deve ser ratificado pela alta administração e revisado periodicamente.

Material de apoio para documentação de evidências

- **Tipo de evidência**: documento com o Plano de Gestão de Riscos da unidade, contemplando o tema da Privacidade.
- **Modelo**: Planilha com modelo de gestão de riscos, em conjunto ao Manual sobre Gestão de Riscos em Privacidade para a Administração Pública do Município de São Paulo (Controle 18), disponível no sítio eletrônico da CGM-SP.

Controle 19. Política de Gestão de Riscos em Privacidade

Fase: 02. Básico	**Tema:** 02. Governança

A unidade elaborou e/ou atualizou, no período, a sua Política de Gestão de Riscos em Privacidade?

Referência

- Art. 6º, inc. VIII; Art. 50, LGPD;
- Art. 2º, inc. XIII, Decreto nº 59.767/2020.

Descrição

A unidade deve estabelecer Política de Gestão de Riscos em Privacidade, de modo a orientar os seus agentes públicos sobre os procedimentos a serem adotados frente aos riscos existentes em sua atuação.

Justificativa

A elaboração de uma Política de Gestão de Riscos em Privacidade permite a criação de processos estruturados e contínuos de gerenciamento de riscos. Trata-se de documento que estabelece o compromisso da unidade com a gestão de riscos, incluindo-se o tema da privacidade, com a definição de princípios, diretrizes, objetivos e responsabilidades pelo gerenciamento de riscos no respectivo órgão ou entidade. Diminui-se o risco de concretização de ameaças relacionadas ao tratamento de dados pessoais.

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 05 – Mapeamento de processos, 06 – Mapeamento de dados pessoais e 07 – Finalidades e hipóteses legais.

Principais requisitos e diretrizes de implantação

- Publicação de ato normativo instituindo a Política de Gestão de Riscos da unidade;
- Metodologia deve incluir aspectos relacionados à privacidade;
- Documento deve ser ratificado pela alta administração e revisado periodicamente.

Material de apoio para documentação de evidências

- **Tipo de evidência**: ato normativo que institui a Política de Gestão de Riscos da unidade, contemplando o tema da Privacidade.
- **Exemplo de evidência implementada**: Política de Gestão de Riscos da CGM (Portaria CGM nº 49/2023).
- **Modelo**: Manual Política de Gestão de Riscos no contexto da privacidade para a Administração Pública do Município de São Paulo (Controle 19), disponível no sítio eletrônico da CGM-SP.

Controle 20. Adequação de processos e atividades

Fase: 02. Básico	**Tema:** 03. Tratamento de dados pessoais

A unidade adequou e/ou revisou, conforme a necessidade, seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos vigentes, de modo que processos e sistemas sejam projetados em conformidade com a LGPD?

Referência

- Art. 6º, inc. VIII; Art. 46, §2º; Art. 50, §2º, inc. I, alínea "a" LGPD;
- Art. 2º, inc. XIII, Decreto nº 59.767/2020.

Descrição

Revisão dos processos e atividades para adoção de medidas de privacidade e proteção de dados pessoais, garantindo que os procedimentos administrativos, ferramentas e sistemas utilizados pelo órgão ou entidade estejam alinhados aos princípios e valores da LGPD, desde a fase de concepção das políticas e serviços públicos até a sua implementação e execução.

Justificativa

O mapeamento de processos caracteriza-se como atividade dinâmica e, portanto, deve estar em constante atualização pela unidade. Com base no mapeamento realizado, é importante que o órgão avalie a necessidade de adequação dos processos sob a perspectiva da privacidade e proteção de dados pessoais. Diminui-se o risco de falha na gestão do tratamento de 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 05 – Mapeamento de processos, 06 – Mapeamento de dados pessoais, 07 – Finalidades e hipóteses legais e 18 – Plano de Gestão de Riscos.

Principais requisitos e diretrizes de implantação

- Indicação, para os processos de maior relevância, se eles foram revisados sob a perspectiva da privacidade e proteção de dados pessoais e, caso necessário, as medidas necessárias para sua adequação;
- Cabe à unidade avaliar a necessidade de ajuste dos processos.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento consolidado com a lista dos processos da unidade, após a revisão de processos e atividades;
- **Modelo**: Planilha com modelo de adequação dos processos e atividades, em conjunto ao Manual sobre Adequação de Processos no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 20), disponível no sítio eletrônico da CGM-SP.

Controle 21. Fluxo de atendimento

Fase: 02. Básico	**Tema:** 04. Direitos dos titulares

A unidade tem definido um fluxo de atendimento das requisições dos titulares de dados pessoais?

Referência

- Art. 6º, inc. IV; Art. 18; Art. 23, §3º, LGPD;
- Art. 6º, inc. I, Decreto nº 59.767/2020.

Descrição

Definição de responsabilidades e estruturação dos procedimentos de atendimento às requisições dos titulares de dados pessoais. O fluxo deve prever etapas claras desde o recebimento do pedido até a sua resposta final, incluindo registro, confirmação de identidade do titular ou representante legal, análise de legitimidade, encaminhamento às áreas responsáveis e resposta ao titular dentro dos prazos legais.

Justificativa

A definição do fluxo contribui para a padronização do atendimento, promove a rastreabilidade e o atendimento aos prazos. Diminui-se o risco de não atendimento aos direitos do titular, reduzindo-se respostas inadequadas, atrasos e falhas de comunicação interna à unidade, que podem comprometer a confiança do titular.

Áreas envolvidas

Alta Administração, encarregado e eventuais áreas relacionadas, a critério do gestor.

Momento de implementação

Recomenda-se que este controle seja elaborado após a implementação do Controle 08 – Canal de atendimento aos direitos dos titulares.

Principais requisitos e diretrizes de implantação

- Estruturação do procedimento de atendimento aos direitos do titular de dados pessoais;
- Aprovação pelo gestor do processo.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento formalizado e aprovado pelo gestor do processo com a estruturação do atendimento aos direitos do titular de dados pessoais.

Controle 22. Resposta às requisições dos titulares

Fase: 02. Básico	**Tema:** 04. Direitos dos titulares

A unidade responde às requisições dos titulares quanto aos seus dados pessoais, observando os seus direitos, conforme disposto pela LGPD?

Referência

- Art. 6º, IV, Art. 19, II, Art. 23, § 3º, LGPD;
- Art. 6º, inc. I, Decreto nº 59.767/2020.

Descrição

Verificação se a unidade atende, de fato, às requisições relacionadas aos direitos do titular de dados pessoais, de forma adequada, tempestiva e completa. Isso inclui o atendimento às requisições dos titulares, conforme previsto pela LGPD, e também os casos de negativa de atendimento, quando aplicável, com a devida fundamentação.

Justificativa

Trata-se de verificação sobre o atendimento adequado às demandas, pois a resposta eficaz às solicitações concretiza o exercício dos direitos do titular. Diminui-se o risco de não atendimento aos direitos do titular, verificando-se a existência de respostas incompletas, imprecisas ou fora do prazo e as respectivas ações de melhoria contínua.

Áreas envolvidas

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

Momento de implementação

Recomenda-se que este controle seja elaborado após a implementação do Controle 08 – Canal de atendimento aos direitos dos titulares.

Principais requisitos e diretrizes de implantação

- A resposta deve estar formalizada em meio de comunicação institucional (SEI, e-mail institucional, etc);
- Controle não aplicável caso o órgão não tenha recebido nenhuma requisição de titular de dados pessoais no período de avaliação.

Material de apoio para documentação de evidências

- **Tipo de evidência:** Cópia de 01 (uma) resposta ao titular de dados pessoais no período (de preferência, a mais recente), bem como formalização da resposta pelos canais institucionais.

Controle 23. Fluxo de comunicação de incidentes

Fase: 02. Básico	**Tema:** 05. Resposta a incidentes

A unidade tem definido um fluxo de comunicação às autoridades e aos titulares de dados pessoais a respeito dos incidentes e violações que possam acarretar risco ou danos?

Referência

- Art. 6º, X; Art. 48; Art. 50, § 2º, inc. I, alínea "g", LGPD;
- Art. 6º, § 1º, inc. I, Decreto nº 59.767, de 2020;
- Resolução CD/ANPD nº 15/2024.

Descrição

Estruturação de resposta específica a incidentes de segurança, com definição de fluxo de comunicação ao encarregado, que avaliará a necessidade de comunicação à ANPD e ao titular dos dados pessoais. O fluxo deve estabelecer procedimentos para identificação, registro e avaliação de incidentes, além de papéis e responsabilidades das áreas envolvidas e prazos aplicáveis. Tal fluxo não se confunde com o atendimento às requisições dos titulares de dados pessoais (ou seja, difere do Fluxo de Atendimento do Controle 21).

Justificativa

Importante para comunicação adequada e tempestiva dos incidentes de segurança às autoridades competentes e aos titulares de dados pessoais, quando necessário. Diminui-se o risco de resposta intempestiva ou ineficiente aos incidentes de segurança, minimizando-se eventuais danos (financeiros, reputacionais, morais) aos titulares e à unidade.

Áreas envolvidas

Alta administração, encarregado, área de tecnologia e/ou segurança da informação, assessoria de comunicação e assessoria jurídica.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 09 – Canal de denúncias e/ou notificações de incidentes.

Principais requisitos e diretrizes de implantação

- Estruturação de procedimento de comunicação ao encarregado, que avaliará a necessidade de comunicação à ANPD e ao titular dos dados pessoais a respeito dos incidentes de segurança;
- Aprovação pelo gestor do processo.

Material de apoio para documentação de evidências

- **Tipo de evidência**: documento que contenha a definição de fluxo de comunicação às autoridades e aos titulares de dados pessoais.

Controle 24. Resposta aos incidentes

Fase: 02. Básico	**Tema:** 05. Resposta a incidentes

A unidade comunica as autoridades e os titulares de dados pessoais sobre os incidentes e violações que possam acarretar risco ou danos?

Referência

- Art. 6º, inc. X; Art. 48; Art. 50, § 2º, inc. I, alínea "g", LGPD;
- Art. 6º, § 1º, inc. I, Decreto nº 59.767, de 2020;
- Resolução CD/ANPD nº 15/2024.

Descrição

Comunicação às autoridades competentes e ao titular de dados pessoais sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. Isso inclui a adoção de medidas para conter e mitigar os efeitos do incidente, a investigação de suas causas, o registro de evidências e a implementação de ações corretivas para evitar recorrências (vide requisitos da Resolução CD/ANPD nº 15/2024).

Justificativa

Importante para comunicação adequada dos incidentes aos titulares e às autoridades competentes. Diminui-se o risco de resposta intempestiva ou ineficiente aos incidentes de segurança, minimizando-se os impactos aos titulares, além de se preservar a integridade e a confiabilidade da Administração Pública.

Áreas envolvidas

Alta administração, encarregado, área de tecnologia e/ou segurança da informação, assessoria jurídica e assessoria de comunicação.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação do Controle 09 – Canal de denúncias e/ou notificações de incidentes.

Principais requisitos e diretrizes de implantação

- Comprovação da comunicação de incidente de segurança, quando for o caso, ao encarregado, bem como, por este, à ANPD e aos titulares dos dados pessoais;
- Controle não aplicável caso o órgão não possua registro de incidente de segurança no período da avaliação.

Material de apoio para documentação de evidências

- **Tipo de evidência**: cópia de 01 (uma) comunicação enviada ao encarregado, bem como, por este, à ANPD e aos titulares dos dados pessoais, no período (de preferência, a mais recente), se houver; alternativamente, relatório sobre o incidente de segurança.

Controle 25. Adequação de sítios eletrônicos

Fase: 02. Básico	**Tema:** 06. Transparência

A unidade adequou e/ou revisou os seus sítios eletrônicos, conforme a necessidade, de modo a se ajustar às exigências da LGPD com relação aos dados pessoais publicizados?

Referência

- Art. 6º, incisos. I, II, III, IV, VI, LGPD;
- Art. 3º, incisos I, II, III, IV, VI, do Decreto nº 59.767, de 2020.

Descrição

Adequação das páginas da internet da unidade com relação aos dados pessoais publicizados.

Justificativa

Necessidade de analisar as informações e documentos publicados nas páginas da internet da unidade, parte tornada pública em momento anterior à vigência da LGPD, e implementar as adequações necessárias para refletir a preocupação com os direitos fundamentais da privacidade e da proteção de dados pessoais, sem prejuízo ao exercício do direito à transparência e ao controle social. Diminui-se o risco de divulgação inadequada de dados pessoais.

Áreas envolvidas

Encarregado, grupo de trabalho, assessora jurídica e assessoria de comunicação.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 11 – Informações do tratamento de dados e 12 – Aviso de privacidade e *cookies.*

Principais requisitos e diretrizes de implantação

- Identificação dos portais com os respectivos documentos publicizados e avaliação da necessidade de ajustes.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Nota técnica, Relatório, Estudo, Justificativa, Parecer ou documento similar que ateste que foi realizada revisão sobre as páginas da internet da unidade e adequação da publicidade dada aos documentos.

Controle 26. Arquitetura e infra de redes

Fase: 02. Básico	**Tema:** 07. Segurança da informação

Foram estabelecidas arquitetura e infraestrutura de redes seguras, com a manutenção de rede corporativa segmentada em domínios lógicos?

Referência

- Art. 6º, inc. VII; Art. 46; Art. 48; Art. 49, LGPD;
- Art. 3º, inc. VII, do Decreto nº 59.767, de 2020;
- OT nº 002 e 013 do Decreto nº 57.653/2017.

Descrição

Gestão do controle de acesso utilizado em espaços digitais, como aplicações utilizadas pela organização e acesso às redes e aos serviços para aqueles autorizados a utilizá-los.

Justificativa

A gestão do controle de acesso às informações pessoais é necessária para limitar o acesso aos dados pessoais àqueles que detenham propósitos legítimos e específicos. Diminui-se risco de incidente de segurança relacionado à violação de dados pessoais e aos princípios da confidencialidade, integridade e disponibilidade.

Áreas envolvidas

Encarregado, grupo de trabalho e área de tecnologia da informação e/ou segurança da informação.

Momento de implementação

Recomenda-se que este controle seja elaborado após a implementação do Controle 13 – Inventário de software e de ativos de tecnologia da informação.

Principais requisitos e diretrizes de implantação

- Espera-se que o responsável técnico de tecnologia da informação da unidade adote medidas de segurança física e lógica sobre a arquitetura da rede corporativa.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento formalizado pelo responsável técnico de Tecnologia da Informação da unidade que evidencie a existência de medidas de segurança física, como documentação da infraestrutura e medidas de proteção física da rede, e lógica, como procedimento de gestão de acessos corporativos e política de senhas.

Controle 27. Softwares *antimalware*

Fase: 02. Básico	**Tema:** 07. Segurança da informação

A unidade mantém softwares *antimalware*, incluindo proteções para servidor de e-mail, navegador web e outras defesas contra malware?

Referência

- Art. 6º, inc. VII; Art. 46; Art. 47; Art. 49, LGPD;
- Art. 3º, inc. VII, do Decreto nº 59.767, de 2020;
- OT nº 013 do Decreto nº 57.653/2017.

Descrição

Manutenção de proteção *antimalware* de servidores de e-mail e ativos de tecnologia de informação de toda a rede interna do órgão.

Justificativa

Necessidade de prevenção a ameaças provenientes de ataques externos aos dispositivos de tecnologia da informação. Diminui-se o risco de incidente de segurança relacionado à violação de dados pessoais e aos princípios da confidencialidade, integridade e disponibilidade.

Áreas envolvidas

Encarregado, grupo de trabalho e área de tecnologia e/ou segurança da informação da unidade.

Momento de implementação

Recomenda-se que este controle seja elaborado após a implementação do Controle 13 – Inventário de software e de ativos de tecnologia da informação.

Principais requisitos e diretrizes de implantação

- Adoção, por parte do responsável técnico de tecnologia da informação da unidade, de medidas de segurança adotadas sobre os *endpoints* (qualquer dispositivo que se conecte a uma rede) e dispositivos móveis, como por exemplo instalação e atualização contínua de soluções *antimalware*, varreduras periódicas (diárias ou semanais) e sob demanda etc.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento formalizado pelo responsável técnico de Tecnologia da Informação da unidade sobre a contratação de conjunto de soluções de proteção contra ameaças externas sobre *endpoints* (qualquer dispositivo que se conecte a uma rede) e dispositivos móveis.

Controle 28. Cópias de segurança

Fase: 02. Básico	**Tema:** 07. Segurança da Informação

Existem e são executados processos periódicos de cópias de segurança dos servidores, roteadores, infraestrutura da rede corporativa, e das configurações e sistemas operacionais?

Referência

- Art. 6º, inc. VII; Art. 46; Art. 47; Art. 49, LGPD;
- Art. 3º, inc. VII, do Decreto nº 59.767, de 2020;
- OT nº 007 e 013 do Decreto nº 57.653/2017.

Descrição

Realização de processos periódicos de cópias de segurança (*backup*), a fim de se garantir o acesso aos dados em caso de ameaças de perdas e destruição.

Justificativa

Controle necessário para garantia da disponibilidade da informação, por meio do qual é possível o acesso aos dados em caso de ameaças de perdas e destruição. Diminui-se o risco de incidente de segurança relacionado à violação de dados pessoais e aos princípios da confidencialidade, integridade e disponibilidade.

Áreas envolvidas

Encarregado, grupo de trabalho, área de tecnologia e/ou segurança da informação da unidade.

Momento de implementação

Recomenda-se que este controle seja elaborado após a implementação do Controle 13 – Inventário de software e de ativos de tecnologia da informação.

Principais requisitos e diretrizes de implantação

- Elaboração e execução da política de cópias de segurança (*backup*).

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento formalizado pelo responsável técnico de Tecnologia da Informação da unidade com o registro dos procedimentos adotados com relação às cópias de segurança.

Controle 29. Decisões administrativas sobre uso compartilhado

Fase: 02. Básico	**Tema:** 08. Gestão de terceiros

As decisões administrativas que envolvam o uso compartilhado de dados pessoais consideram requisitos relativos ao tratamento de dados pessoais?

Referência

- Art. 6º, inc. VIII; Art. 26; Art. 27; LGPD;
- Art. 3º, inc. VIII, Art. 12; Art. 13; Art. 14; do Decreto nº 59.767, de 2020;
- Art. 2º, Resolução SGM/CCGD nº 2, de 2022.

Descrição

Trata-se de controle na formalização de compartilhamento de dados pessoais com outros órgãos da Administração Pública Municipal Direta ou com outros agentes de tratamento, seja no âmbito da Administração Pública Municipal Indireta, seja para agentes externos, conforme o caso. Espera-se que a decisão administrativa que formalize o compartilhamento de dados pessoais indique requisitos mínimos para o tratamento.

Justificativa

A adoção de padrão de decisões administrativas visa estabelecer mecanismo de controle prévio para formalização de compartilhamento de dados pessoais a outros agentes de tratamento. Diminui-se o risco de descumprimento de obrigações legais por meio do compartilhamento com terceiros.

Áreas envolvidas

Alta administração, encarregado, grupo de trabalho e assessoria jurídica.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 14 - Modelos de cláusulas contratuais e 15 - Relação/lista de contratos.

Principais requisitos e diretrizes de implantação

- Espera-se que as decisões administrativas que envolvam o compartilhamento de dados pessoais contenham requisitos de privacidade.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento aprovado pela unidade com modelo ou instruções para a disciplina de compartilhamento de dados pessoais; alternativamente, relação/lista exemplificativa de decisões administrativas que considerem requisitos para o compartilhamento de dados pessoais.

Controle 30. Avaliação de Compatibilidade das Finalidades

Fase: 02. Básico	**Tema:** 08. Gestão de terceiros

O uso compartilhado de dados pessoais é precedido de avaliação sobre a compatibilidade entre a finalidade original e a do uso compartilhado?

Referência

- Art. 6º, inc. X; Art. 26; Art. 27; LGPD;
- Art. 3º, inc. X, Art. 12; Art. 13; Art. 14; do Decreto nº 59.767, de 2020.

Descrição

Trata-se de controle na formalização do uso compartilhado de dados pessoais pela Administração Pública Municipal. Espera-se que seja realizada avaliação prévia sobre a compatibilidade entre a finalidade original e a do uso compartilhado. Dessa forma, busca-se assegurar que o compartilhamento seja justificado, proporcional, alinhado ao interesse público e não gere violações aos direitos dos titulares.

Justificativa

A adoção de padrão de avaliação da compatibilidade entre a finalidade original e a do uso compartilhado visa garantir que o tratamento posterior dos dados respeite os princípios da LGPD. Diminui-se o risco de descumprimento de obrigações legais por meio do compartilhamento com terceiros.

Áreas envolvidas

Alta administração, encarregado e assessoria jurídica.

Momento de implementação

Recomenda-se que o controle seja elaborado após a implementação dos Controles 14 - Modelos de cláusulas contratuais, 15 - Relação/lista de contratos e 29 - Decisões administrativas sobre uso compartilhado.

Principais requisitos e diretrizes de implantação

- Espera-se que o uso compartilhado de dados pessoais seja precedido da avaliação de compatibilidade e que esta seja formalizada e documentada.

Material de apoio para documentação de evidências

- **Tipo de evidência**: Documento aprovado pela unidade com modelo de avaliação de compatibilidade entre a finalidade original e a do uso compartilhado; alternativamente, relação/lista exemplificativa de avaliações realizadas.

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. 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 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União, 26 de abril de 2024.

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 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 002 – Interconectividade de Rede. Disponível em: <https://tecnologia.prefeitura.sp.gov.br/wp-content/uploads/2023/03/Brochura_OT_Vol1_v19.pdf#page=30> Acesso em: 26/11/2025

SÃO PAULO (Cidade). Orientação Técnica nº 007 – Backup e armazenamento de dados. Disponível em: <https://tecnologia.prefeitura.sp.gov.br/wp-content/uploads/2023/03/Brochura_OT_Vol2_v7.pdf#page=37> Acesso em: 26/11/2025

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: 26/11/2025

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.

São Paulo (Cidade). Resolução Secretaria de Governo Municipal – SGM/CCGS nº 2 de 22 de maio de 2022. Dispõe sobre as regras e os parâmetros para o compartilhamento e a categorização de dados no âmbito da administração pública municipal. São Paulo, Diário Oficial da Cidade, 23 de agosto de 2022.

PREFEITURA DE
SÃO PAULO