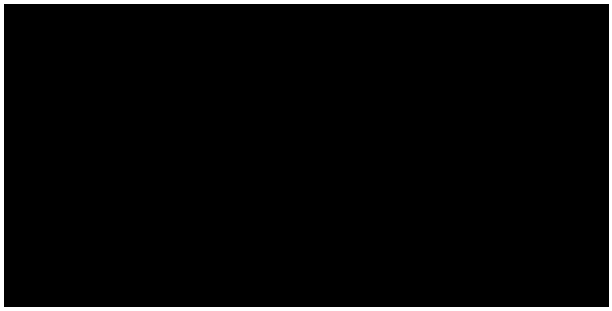
Guia de Boas Práticas para Tratamento de Dados Públicos e Sensíveis

Manual para Servidores Públicos de Florianópolis e São José



24 de abril de 2025

Conteúdo

1 Introdução

1.1 Objetivo do Guia

Este guia foi desenvolvido para fornecer orientações práticas aos servidores públicos das prefeituras de Florianópolis e São José sobre como lidar adequadamente com dados públicos e sensíveis. Seu objetivo é garantir que todas as informações sob responsabilidade da administração municipal sejam tratadas com o devido cuidado, respeito à legislação e aos direitos dos cidadãos.

1.2 Importância do Tratamento Adequado de Dados

O tratamento adequado de dados é fundamental para:

- Preservar a confiança da população na administração pública
- Garantir o cumprimento das leis de proteção de dados (LGPD)
- Prevenir vazamentos e incidentes de segurança
- Assegurar a precisão das informações utilizadas para tomada de decisões
- Promover a transparência e eficiência nos serviços públicos

1.3 Para Quem é Este Guia

Este material é direcionado a todos os servidores públicos que, em suas funções diárias, lidam com informações de cidadãos ou dados da administração pública. Isso inclui, mas não se limita a:

- Atendentes em postos de serviço ao cidadão
- Profissionais da saúde em postos e hospitais municipais
- Servidores da educação municipal
- Funcionários administrativos de todas as secretarias
- Gestores públicos e tomadores de decisão
- Equipes de assistência social

Lembre-se

Este guia não substitui treinamentos específicos para sistemas ou procedimentos de cada setor. Consulte sempre os manuais e normas específicas de sua área de atuação.

2 Fundamentos da Proteção de Dados

2.1 Conceitos Básicos

2.1.1 O que são Dados Pessoais

Dados pessoais são quaisquer informações relacionadas a uma pessoa natural identificada ou identificável. Exemplos incluem:

- Nome completo
- CPF, RG ou outros documentos de identificação
- Endereço residencial ou comercial
- E-mail pessoal
- Números de telefone
- Data de nascimento
- Registros de atendimentos médicos
- Informações bancárias

2.1.2 Dados Pessoais Sensíveis

São dados que merecem proteção especial por seu potencial discriminatório ou por revelarem aspectos íntimos da vida do cidadão:

- Origem racial ou étnica
- Convicção religiosa
- Opinião política
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político
- Dados referentes à saúde ou à vida sexual
- Dados genéticos ou biométricos

Atenção!

Dados sensíveis requerem proteções adicionais e não devem ser compartilhados sem autorização específica, mesmo entre departamentos da prefeitura.

2.1.3 Dados Públicos

São informações que podem ser acessadas por qualquer cidadão sem restrições significativas:

- Dados orçamentários municipais
- Informações sobre licitações e contratos
- Salários e cargos de servidores públicos (respeitando a privacidade)
- Dados estatísticos agregados sobre a população
- Informações sobre serviços públicos oferecidos

2.2 Legislação Aplicável

2.2.1 Lei Geral de Proteção de Dados (LGPD)

A LGPD (Lei nº 13.709/2018) estabelece regras sobre como os dados pessoais devem ser coletados, processados, armazenados e compartilhados. Principais pontos:

- Necessidade de base legal para tratamento de dados
- Princípios de finalidade, adequação e necessidade
- Direitos dos titulares de dados (cidadãos)
- Obrigações dos controladores de dados (prefeituras)
- Sanções por descumprimento

2.2.2 Lei de Acesso à Informação (LAI)

A LAI (Lei nº 12.527/2011) garante o acesso a informações públicas. Principais aspectos:

- Transparência ativa e passiva
- Prazo para respostas a pedidos de informação
- Limitações de acesso para informações pessoais e sigilosas
- Procedimentos para classificação de informações sigilosas

Equilíbrio Necessário

A administração pública deve buscar o equilíbrio entre transparência (LAI) e proteção de dados pessoais (LGPD). Nem todos os dados sob posse das prefeituras podem ou devem ser divulgados.

2.3 Princípios Éticos no Tratamento de Dados

- **Transparência:** Seja claro com o cidadão sobre quais dados são coletados e por quê
- **Finalidade:** Utilize os dados apenas para as finalidades informadas ao cidadão
- **Necessidade:** Colete apenas os dados realmente necessários para o serviço
- **Segurança:** Proteja as informações sob sua responsabilidade
- **Responsabilidade:** Assume seu papel na proteção dos dados dos cidadãos

3 Ciclo de Vida dos Dados na Administração Pública

3.1 Coleta de Dados

3.1.1 Boas Práticas na Coleta

1. **Planejamento Prévio:** Antes de criar formulários ou iniciar coletas de dados, identifique:
   - Quais dados são realmente necessários
   - Qual a finalidade específica de cada campo solicitado
   - Se há bases legais para a coleta (especialmente dados sensíveis)
   - Como os dados serão armazenados e protegidos
2. **Transparência com o Cidadão:**
   - Informe claramente por que cada informação está sendo solicitada
   - Explique como os dados serão utilizados
   - Disponibilize canais para dúvidas sobre o tratamento dos dados
   - Obtenha consentimento quando necessário (especialmente para dados sensíveis)
3. **Minimização de Dados:**
   - Colete apenas o necessário para a finalidade declarada
   - Evite cópias desnecessárias de documentos
   - Questione campos em formulários que pareçam excessivos

Exemplo Prático

Antes: Formulário de inscrição para vacinação solicitando nome completo, CPF, RG, data de nascimento, endereço completo, telefone, e-mail, profissão, local de trabalho, histórico completo de doenças.
Depois: Formulário simplificado pedindo apenas nome, CPF, data de nascimento, grupo prioritário (se aplicável) e contato para confirmação.

3.1.2 Documentação da Coleta

Para cada processo de coleta de dados, mantenha um registro que contenha:

- Data e local da coleta
- Finalidade específica
- Base legal para o tratamento
- Servidor responsável pela coleta
- Prazo previsto de armazenamento
- Medidas de segurança adotadas

3.2 Armazenamento de Dados

3.2.1 Segurança Física de Documentos

- Mantenha arquivos físicos em armários com chave
- Limite o acesso apenas a pessoas autorizadas
- Nunca deixe documentos sensíveis sobre a mesa ao se ausentar
- Utilize trituradoras para descartar documentos confidenciais
- Mantenha registro de quem acessou determinados documentos

3.2.2 Segurança Digital

- Utilize sempre senha forte em seu computador e sistemas
- Nunca compartilhe suas credenciais de acesso
- Bloqueie a tela ao se ausentar (Tecla Windows + L)
- Salve arquivos sensíveis apenas em locais autorizados pela TI
- Evite armazenar dados em dispositivos pessoais ou pen drives
- Nunca envie dados sensíveis por e-mail pessoal ou aplicativos de mensagem

Atenção!

O uso de pen drives, e-mails pessoais ou aplicativos como WhatsApp para transferir dados de cidadãos é expressamente proibido. Utilize apenas os canais oficiais disponibilizados pela prefeitura.

3.3 Organização e Classificação

3.3.1 Estrutura Organizada

Mantenha os dados organizados seguindo os padrões de sua secretaria ou departamento:

- Utilize pastas e subpastas com nomes claros
- Padronize a nomenclatura de arquivos
- Separe claramente documentos por tipo de acesso (público, restrito, sigiloso)
- Mantenha índices ou catálogos dos documentos arquivados

3.3.2 Classificação de Acesso

Classifique os documentos e dados de acordo com seu nível de confidencialidade:

- **Público:** Acessível a qualquer cidadão
- **Acesso Restrito:** Acessível apenas a servidores autorizados
- **Sigiloso:** Acesso limitado e controlado, com registro de acesso

3.4 Uso e Compartilhamento

3.4.1 Uso Responsável

- Utilize os dados apenas para a finalidade para a qual foram coletados
- Verifique a precisão e integridade antes de utilizar para tomada de decisões
- Documente as análises e relatórios produzidos a partir dos dados
- Sempre identifique a fonte dos dados em relatórios e apresentações

3.4.2 Compartilhamento Interno

Ao compartilhar dados com outros departamentos ou secretarias:

- Confirme se o compartilhamento é realmente necessário
- Verifique se há base legal para o compartilhamento
- Compartilhe apenas os dados mínimos necessários
- Utilize ferramentas e protocolos seguros autorizados pela prefeitura
- Registre formalmente o compartilhamento

3.4.3 Compartilhamento Externo

Dados só devem ser compartilhados com outras instituições quando:

- Houver obrigação legal (ex: requisição judicial)
- Existir convênio formal que preveja o compartilhamento
- Houver consentimento específico do titular dos dados
- Forem dados públicos, já divulgados em portais de transparência

Como Proceder

Em caso de dúvida sobre compartilhamento de dados, consulte sempre:

1. A chefia imediata
2. A área jurídica da prefeitura
3. O encarregado de proteção de dados (DPO) do município

4 Tratamento de Dados em Setores Específicos

4.1 Saúde

4.1.1 Cuidados Especiais

Os dados de saúde são considerados sensíveis e requerem proteções adicionais:

- Prontuários médicos devem ser mantidos em locais seguros
- O acesso digital a sistemas de saúde deve ser estritamente controlado
- Informações de saúde só devem ser compartilhadas com profissionais diretamente envolvidos no tratamento
- Dados estatísticos devem ser anonimizados antes de compartilhamento

4.1.2 Orientações Práticas

- Nunca discuta casos de pacientes em áreas públicas
- Evite deixar telas com informações visíveis a terceiros
- Utilize senhas fortes nos sistemas de saúde
- Descaracterize dados para fins estatísticos
- Obtenha consentimento específico para uso de dados em pesquisas

4.2 Educação

4.2.1 Dados de Alunos

- Boletins e históricos escolares devem ser entregues apenas aos pais ou responsáveis
- Fotografias de alunos só devem ser utilizadas com autorização
- Informações sobre desempenho escolar são confidenciais
- Dados de alunos com necessidades especiais requerem proteção adicional

4.2.2 Orientações Práticas

- Mantenha documentos escolares em armários seguros
- Proteja as senhas de acesso aos sistemas educacionais
- Obtenha autorização para uso de imagem no início do ano letivo
- Limpe quadros e lousas que contenham informações sensíveis após o uso

4.3 Assistência Social

4.3.1 Sensibilidade dos Dados

A assistência social lida com dados extremamente sensíveis e pessoais:

- Situação familiar e socioeconômica
- Violência doméstica e vulnerabilidades
- Benefícios sociais e assistenciais
- Histórico de atendimentos

4.3.2 Orientações Práticas

- Realize atendimentos em locais que garantam privacidade
- Mantenha sigilo absoluto sobre casos atendidos
- Compartilhe informações apenas com profissionais diretamente envolvidos
- Obtenha consentimento para encaminhamento a outros serviços
- Proteja documentos e relatórios de visitas domiciliares

4.4 Atendimento ao Cidadão

4.4.1 Balcões de Atendimento

- Organize o espaço para evitar que um cidadão veja os documentos de outro
- Não deixe documentos de identidade ou comprovantes expostos
- Mantenha a tela do computador posicionada de forma que apenas você possa ver
- Evite chamar cidadãos pelo nome completo em salas de espera

4.4.2 Orientações Práticas

- Confirme a identidade antes de fornecer informações pessoais
- Nunca deixe documentos de cidadãos sobre o balcão ao se ausentar
- Bloqueie o computador sempre que se afastar do posto de atendimento
- Oriente cidadãos sobre como proteger seus próprios dados

Situação Comum

Um cidadão solicita informações sobre outra pessoa (familiar, amigo, etc.).
Como proceder: Explique educadamente que informações pessoais só podem ser fornecidas ao próprio titular ou mediante procuração. Sugira que a pessoa interessada compareça pessoalmente ou autorize formalmente o acesso.

5 Qualidade dos Dados

5.1 Importância da Precisão dos Dados

Dados imprecisos ou desatualizados podem levar a:

- Decisões administrativas equivocadas
- Negação indevida de benefícios ou serviços
- Duplicação desnecessária de processos
- Desperdício de recursos públicos
- Perda de credibilidade da administração

5.2 Práticas para Garantir Qualidade

5.2.1 Na Coleta

- Confirme a grafia correta de nomes
- Verifique números de documentos (utilizando dígitos verificadores)
- Utilize formatos padronizados para datas, endereços e telefones
- Solicite confirmação de informações críticas
- Evite abreviações desnecessárias

5.2.2 Na Manutenção

- Realize atualização periódica de cadastros
- Estabeleça datas de verificação para dados críticos
- Corrija inconsistências assim que identificadas
- Unifique cadastros duplicados
- Documente as correções realizadas

Boas Práticas

- Solicite ao cidadão a confirmação dos dados a cada novo atendimento
- Pergunte periodicamente se houve mudanças nos dados de contato
- Implemente sistema de verificação de endereços retornados (correio)
- Utilize a expressão "Confere com o original"após verificar documentos

5.3 Lidando com Erros de Dados

Quando identificar erros em dados:

- Registre a inconsistência de forma clara
- Identifique a fonte ou causa do erro
- Corrija os registros em todos os sistemas afetados
- Comunique as áreas que possam ter utilizado os dados incorretos
- Implemente medidas para evitar repetição do erro

6 Incidentes de Segurança

6.1 O que é um Incidente de Segurança

Considera-se incidente de segurança qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade dos dados, como:

- Perda ou roubo de documentos físicos
- Acesso não autorizado a sistemas ou arquivos
- Compartilhamento indevido de informações
- Envio de dados ao destinatário errado
- Vazamento de informações confidenciais
- Mau funcionamento de sistemas que exponham dados

6.2 Como Proceder em Caso de Incidente

6.2.1 Passos Imediatos

1. **Contenção:** Adote medidas para interromper ou minimizar o incidente
2. **Comunicação:** Informe imediatamente sua chefia imediata
3. **Registro:** Documente detalhadamente o ocorrido (data, hora, local, dados afetados)
4. **Preservação:** Mantenha as evidências do incidente

6.2.2 Processo de Notificação

1. A chefia imediata deverá acionar o responsável pela segurança da informação
2. O encarregado de proteção de dados (DPO) da prefeitura deve ser informado
3. Dependendo da gravidade, a Autoridade Nacional de Proteção de Dados (ANPD) deverá ser notificada
4. Cidadãos afetados podem precisar ser informados, seguindo orientação jurídica

Atenção!

Ocultar ou deixar de reportar um incidente de segurança pode configurar infração administrativa e até mesmo penal, dependendo das circunstâncias e consequências.

6.3 Prevenção de Incidentes

- Mantenha-se atualizado sobre as políticas de segurança da informação
- Participe de treinamentos sobre proteção de dados
- Esteja atento a tentativas de phishing ou engenharia social
- Reporte vulnerabilidades ou situações de risco
- Adote uma postura preventiva no dia a dia

7 Transparência e Dados Abertos

7.1 Princípios da Transparência Pública

A transparência na administração pública é um dever constitucional e implica em:

- Disponibilização proativa de informações de interesse público
- Simplificação do acesso às informações
- Linguagem clara e acessível
- Dados em formatos abertos e compreensíveis
- Ferramentas que facilitem a análise pelos cidadãos

7.2 Dados que Devem Ser Públicos

- Orçamento municipal e execução financeira
- Licitações, contratos e convênios
- Estrutura organizacional e remuneração de servidores (sem CPF e outros dados pessoais)
- Programas, ações e projetos em andamento
- Indicadores de desempenho e resultados alcançados
- Agenda de autoridades

7.3 Equilíbrio entre Transparência e Proteção de Dados

7.3.1 Anonimização para Publicação

Antes de publicar dados, garanta que informações pessoais identificáveis sejam removidas:

- Substitua nomes por códigos ou identificadores
- Remova CPF, RG e outros documentos identificadores
- Generalize endereços para bairros ou regiões
- Agrupe dados sensíveis em categorias mais amplas
- Verifique se a combinação de dados não permite reidentificação

Exemplo Prático

Dado Original: "Maria da Silva, CPF 123.456.789-00, residente na Rua das Flores, 123, foi atendida pelo programa de assistência social em 15/03/2023 para receber cesta básica por ser mãe solteira com 3 filhos."
Dado Anonimizado para Estatística: "Em março/2023, foram concedidas 85 cestas básicas no bairro Centro, sendo 42% para famílias monoparentais."

7.3.2 Tratamento de Pedidos de Acesso à Informação

Ao receber um pedido pela Lei de Acesso à Informação:

- Verifique se a informação é pública ou contém dados protegidos
- Em caso de dados pessoais, avalie a possibilidade de anonimização
- Caso seja necessário negar acesso, fundamente com base legal
- Encaminhe ao setor responsável pelo e-SIC quando necessário
- Cumpra os prazos estabelecidos na lei

8 Capacitação Continuada

8.1 Importância da Atualização

A proteção de dados é uma área em constante evolução:

- Novas tecnologias trazem novos riscos e desafios
- Atualizações legislativas ocorrem regularmente
- Procedimentos internos são aperfeiçoados com o tempo
- Incidentes revelam vulnerabilidades que precisam ser endereçadas

8.2 Recursos para Capacitação

- Cursos oferecidos pelas prefeituras
- Materiais disponibilizados pela ANPD (Autoridade Nacional de Proteção de Dados)
- Treinamentos da ENAP (Escola Nacional de Administração Pública)
- Grupos de discussão internos sobre proteção de dados
- Cartilhas e guias elaborados pelo Ministério Público

Treinamentos Recomendados

- Curso Básico da LGPD para Servidores Públicos
- Oficina prática de anonimização de dados
- Seminário de segurança da informação no setor público
- Webinários sobre transparência e acesso à informação

8.3 Multiplicadores de Conhecimento

Cada setor deve contar com servidores capacitados para:

- Tirar dúvidas cotidianas sobre proteção de dados
- Orientar colegas sobre procedimentos corretos
- Identificar precocemente riscos e vulnerabilidades
- Fazer a ponte com a equipe de proteção de dados da prefeitura

9 Checklist para o Dia a Dia

9.1 Ao Iniciar o Expediente

- Verifique se documentos sensíveis estão guardados adequadamente
- Faça login em sistemas utilizando apenas suas credenciais
- Confira se há orientações novas sobre proteção de dados
- Prepare seu espaço de trabalho para garantir a privacidade

9.2 Durante o Atendimento

- Confirme a identidade da pessoa antes de fornecer informações
- Colete apenas os dados necessários para o serviço solicitado
- Explique por que determinadas informações são solicitadas
- Guarde documentos apresentados em local seguro
- Posicione a tela do computador de modo que apenas você possa ver

9.3 Ao Manusear Documentos

- Não deixe documentos expostos desnecessariamente
- Transporte documentos em pastas fechadas ou envelopes
- Utilize carimbos de "CONFIDENCIAL"quando apropriado
- Faça cópias apenas quando estritamente necessário
- Descarte documentos sensíveis utilizando fragmentadoras
- Registre a movimentação de documentos importantes

9.4 Ao Utilizar Sistemas Informatizados

- Bloqueie sua estação de trabalho sempre que se ausentar (Windows + L)
- Não compartilhe senhas sob nenhuma circunstância
- Utilize senhas fortes e diferentes para cada sistema
- Evite acessar sites não relacionados ao trabalho
- Não instale programas não autorizados no computador de trabalho
- Tenha cuidado ao abrir e-mails, especialmente com anexos

9.5 Ao Finalizar o Expediente

- Guarde todos os documentos sensíveis em gavetas ou armários com chave
- Desligue-se de todos os sistemas utilizados
- Bloqueie ou desligue seu computador
- Verifique se impressoras e copiadoras não contêm documentos esquecidos
- Certifique-se de que gavetas e armários com documentos sensíveis estão trancados
- Recolha anotações ou rascunhos com informações confidenciais

Lembre-se

Uma simples verificação de poucos minutos antes de sair pode prevenir incidentes graves de segurança da informação. Desenvolva o hábito de fazer uma rápida inspeção em sua estação de trabalho antes de encerrar o expediente.

10 Direitos dos Titulares de Dados

10.1 Principais Direitos dos Cidadãos

De acordo com a LGPD, os cidadãos têm direito a:

- **Confirmação:** Saber se seus dados são tratados pela prefeitura
- **Acesso:** Obter cópia dos dados pessoais armazenados
- **Correção:** Solicitar atualização de dados incorretos ou desatualizados
- **Anonimização:** Pedir que dados sejam anonimizados quando possível
- **Portabilidade:** Receber seus dados em formato que permita transferência
- **Eliminação:** Solicitar exclusão de dados tratados com consentimento
- **Informação:** Conhecer com quem seus dados foram compartilhados
- **Revogação:** Retirar consentimento previamente fornecido

10.2 Como Atender Solicitações dos Titulares

10.2.1 Procedimento Padrão

1. Receba a solicitação e registre formalmente
2. Confirme a identidade do solicitante (evite fraudes)
3. Encaminhe ao setor responsável pela proteção de dados
4. Acompanhe o prazo de resposta (até 15 dias, conforme LGPD)
5. Forneça resposta clara e completa
6. Mantenha registro de todo o processo

10.2.2 Casos Específicos

- **Pedido de Acesso:** Forneça cópia dos dados em formato compreensível
- **Pedido de Correção:** Atualize os dados em todos os sistemas
- **Pedido de Exclusão:** Analise se há outras bases legais para manutenção
- **Contestação de Dados:** Suspenda o uso até verificação completa

Importante

Sempre consulte a área jurídica ou o Encarregado de Proteção de Dados em casos complexos ou que envolvam possíveis exceções legais ao atendimento de solicitações.

11 Boas Práticas para Situações Específicas

11.1 Reuniões e Apresentações

- Ao preparar apresentações, evite incluir dados pessoais identificáveis
- Utilize dados agregados ou anonimizados em gráficos e tabelas
- Não deixe documentos confidenciais na sala após reuniões
- Tenha cuidado com projeções que possam expor informações sensíveis
- Desconecte-se de sistemas ao fazer apresentações públicas

11.2 Trabalho Remoto

Quando autorizado a trabalhar remotamente:

- Utilize apenas equipamentos e conexões autorizados pela prefeitura
- Evite imprimir documentos em casa
- Não permita que familiares visualizem informações de trabalho
- Utilize VPN quando disponível
- Não salve arquivos de trabalho em dispositivos pessoais
- Mantenha seu ambiente de trabalho seguro e privado

11.3 Uso de E-mail

- Utilize apenas e-mail institucional para assuntos de trabalho
- Verifique os destinatários antes de enviar
- Tenha cuidado com a função "Responder a todos"
- Evite encaminhar longas cadeias de e-mails
- Não envie dados sensíveis por e-mail sem proteção adequada
- Desconfie de e-mails solicitando informações confidenciais

Nunca Faça Isso

- Enviar listas com dados pessoais de cidadãos por e-mail
- Encaminhar documentos sensíveis para seu e-mail pessoal
- Compartilhar informações confidenciais em grupos de WhatsApp
- Utilizar serviços de armazenamento em nuvem pessoais (Dropbox, Google Drive pessoal)
- Tirar fotos de documentos de cidadãos com seu celular pessoal

11.4 Interação com a Imprensa

- Encaminhe solicitações da imprensa para a assessoria de comunicação
- Não forneça informações sobre casos específicos sem autorização
- Utilize apenas dados estatísticos e agregados em declarações
- Evite mencionar situações que possam identificar cidadãos específicos
- Consulte a área jurídica em caso de dúvidas

12 Estudo de Casos

12.1 Caso 1: Atendimento em Unidade de Saúde

12.1.1 Situação

Um cidadão comparece a uma unidade de saúde para consulta. Na recepção, a atendente solicita atualização de dados cadastrais e, em seguida, uma pessoa na sala de espera, que é vizinha do paciente, pergunta sobre o diagnóstico de um atendimento anterior.

12.1.2 Boas Práticas

- **Correto:** Solicitar atualização de dados em local que garanta privacidade
- **Correto:** Explicar à vizinha que informações de saúde são sigilosas
- **Correto:** Orientar o paciente sobre a importância da privacidade
- **Incorreto:** Atualizar cadastro com voz alta, expondo dados pessoais
- **Incorreto:** Entregar resultados de exames à vizinha, mesmo a pedido do paciente, sem autorização formal

12.2 Caso 2: Secretaria de Educação

12.2.1 Situação

Uma escola municipal precisa enviar boletim escolar aos pais de alunos. A coordenadora sugere criar um grupo de WhatsApp para agilizar o processo, enviando todos os boletins de uma vez para os representantes de turma distribuírem.

12.2.2 Boas Práticas

- **Correto:** Disponibilizar boletins individualmente para cada responsável
- **Correto:** Utilizar sistema oficial da secretaria de educação para comunicação
- **Correto:** Entregar boletins impressos em reunião de pais ou em envelope lacrado
- **Incorreto:** Criar grupo de WhatsApp para compartilhar documentos oficiais
- **Incorreto:** Permitir que terceiros (representantes) tenham acesso aos boletins de todos os alunos

12.3 Caso 3: Assistência Social

12.3.1 Situação

Uma assistente social atende família em situação de vulnerabilidade. Durante visita domiciliar, tira fotos da residência para compor relatório e, por ter limite de armazenamento no celular de trabalho, envia as imagens para seu WhatsApp pessoal.

12.3.2 Boas Práticas

- **Correto:** Solicitar autorização para registro fotográfico
- **Correto:** Utilizar apenas equipamento institucional para registros
- **Correto:** Transferir imagens diretamente para sistema oficial
- **Incorreto:** Enviar dados de trabalho para dispositivos pessoais
- **Incorreto:** Manter registros de visitas em aplicativos não oficiais

Solução Adequada

Solicitar à coordenação dispositivo com maior capacidade ou procedimento para transferência direta das imagens para os sistemas oficiais, sem uso de canais não autorizados.

12.4 Caso 4: Setor de Protocolo

12.4.1 Situação

Um cidadão solicita cópia de processo administrativo que contém dados pessoais de terceiros. O servidor responsável pelo atendimento tem dúvidas sobre como proceder.

12.4.2 Boas Práticas

- **Correto:** Verificar se o solicitante é parte no processo
- **Correto:** Consultar setor jurídico em caso de dúvida
- **Correto:** Fornecer cópia com tarjas em dados pessoais de terceiros
- **Incorreto:** Negar acesso completo sem análise prévia
- **Incorreto:** Fornecer cópia integral com dados sensíveis de terceiros

13 Perguntas Frequentes

13.1 Dúvidas Comuns sobre Proteção de Dados

13.1.1 Posso usar meu celular pessoal para fotografar documentos no trabalho?

Resposta: Não é recomendado. Documentos oficiais e dados de cidadãos devem ser manipulados apenas em equipamentos institucionais, com as devidas medidas de segurança. O uso de dispositivos pessoais pode comprometer a segurança das informações e configurar violação às políticas de proteção de dados.

13.1.2 Preciso obter consentimento para todos os dados que coletamos?

Resposta: Nem sempre. A administração pública pode tratar dados pessoais com base em outras hipóteses legais, como o cumprimento de obrigação legal ou execução de políticas públicas. No entanto, para dados sensíveis ou usos que fujam da finalidade original, o consentimento específico pode ser necessário. Consulte sempre o setor jurídico em caso de dúvidas.

13.1.3 Como proceder quando um cidadão solicita exclusão de seus dados?

Resposta: Registre formalmente o pedido e encaminhe ao encarregado de proteção de dados. Nem todos os dados podem ser excluídos, especialmente aqueles necessários para cumprimento de obrigações legais ou interesse público. O cidadão deve receber resposta fundamentada, explicando se o pedido pode ser atendido e, em caso negativo, qual a base legal para manutenção dos dados.

13.1.4 Posso compartilhar informações entre secretarias sem autorização?

Resposta: O compartilhamento entre órgãos da mesma entidade (prefeitura) é permitido quando necessário para execução de políticas públicas, mas deve seguir princípios como necessidade e finalidade. Compartilhe apenas os dados mínimos necessários, utilize canais seguros e registre formalmente o compartilhamento.

13.1.5 O que devo fazer se perceber que dados foram acessados indevidamente?

Resposta: Comunique imediatamente sua chefia e o encarregado de proteção de dados. Registre detalhadamente o ocorrido e coopere com a investigação interna. Incidentes de segurança devem ser tratados com rapidez para minimizar possíveis danos.

Canais de Suporte

Em caso de dúvidas sobre proteção de dados, entre em contato com:

- Encarregado de Proteção de Dados: [email/ramal]
- Comitê de Privacidade e Proteção de Dados: [email/ramal]
- Suporte Técnico de Segurança da Informação: [email/ramal]

14 Glossário

- **ANPD:** Autoridade Nacional de Proteção de Dados, órgão responsável por zelar pela proteção dos dados pessoais e fiscalizar o cumprimento da LGPD.
- **Anonimização:** Processo pelo qual dados perdem a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais.
- **Controlador:** Pessoa natural ou jurídica que toma as decisões sobre o tratamento de dados pessoais (no caso, a prefeitura).
- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** Dado sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos ou biométricos.
- **DPO (Data Protection Officer):** Encarregado de proteção de dados, pessoa indicada pelo controlador para atuar como canal de comunicação entre a instituição, os titulares e a ANPD.
- **Incidente de Segurança:** Qualquer evento adverso que comprometa a segurança dos dados pessoais.
- **LGPD:** Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que regula o tratamento de dados pessoais no Brasil.
- **LAI:** Lei de Acesso à Informação (Lei nº 12.527/2011), que regula o acesso a informações públicas.
- **Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.
- **Pseudonimização:** Tratamento que remove a possibilidade de associação direta ou indireta dos dados ao titular, exceto pelo uso de informação adicional mantida separadamente.
- **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento:** Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, armazenamento, eliminação, entre outras.

15 Apêndices

15.1 Legislação Relacionada

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)
- Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI)
- Lei nº 12.965/2014 - Marco Civil da Internet
- Decreto Municipal [inserir número] - Regulamenta a aplicação da LGPD no município
- Normas e Procedimentos Internos [inserir referências locais]

15.2 Modelos de Documentos

15.2.1 Termo de Responsabilidade

TERMO DE RESPONSABILIDADE NO TRATAMENTO DE DADOS
Eu, [NOME COMPLETO], matrícula [NÚMERO], declaro estar ciente das normas e políticas de proteção de dados do município de [NOME DO MUNICÍPIO] e assumo o compromisso de:
1. Tratar os dados pessoais aos quais tenho acesso apenas para finalidades legítimas e autorizadas; 2. Manter sigilo sobre informações confidenciais e dados pessoais; 3. Adotar as medidas de segurança necessárias para proteção dos dados; 4. Comunicar imediatamente qualquer incidente de segurança; 5. Respeitar os direitos dos titulares de dados.
Estou ciente de que o descumprimento destes compromissos pode acarretar responsabilização administrativa, civil e criminal.
[LOCAL], [DATA]
_____ Assinatura do Servidor

15.2.2 Formulário para Registro de Incidente

REGISTRO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO
Data e hora do incidente: _____
Data e hora da descoberta: _____
Local/sistema afetado: _____
Descrição detalhada do ocorrido: _____
Dados afetados: _____
Possíveis causas: _____
Medidas imediatas tomadas: _____
Pessoas notificadas: _____
Nome do servidor que registrou: _____
Assinatura: _____

15.3 Contatos Úteis

- Encarregado de Proteção de Dados (DPO): [NOME] - [CONTATO]
- Comitê de Proteção de Dados: [CONTATO]
- Suporte Técnico: [CONTATO]
- Ouvidoria: [CONTATO]
- Canal de Denúncias: [CONTATO]

16 Considerações Finais

A proteção de dados não é apenas uma exigência legal, mas um compromisso ético com os cidadãos que confiam seus dados à administração pública. Cada servidor tem papel fundamental na construção de uma cultura de privacidade e segurança da informação.

Este guia fornece diretrizes gerais, mas situações específicas podem exigir análise caso a caso. Em caso de dúvidas, sempre consulte sua chefia imediata, o setor jurídico ou o encarregado de proteção de dados.

Lembre-se: proteger dados é proteger pessoas. Ao tratar adequadamente as informações sob sua responsabilidade, você contribui para uma administração pública mais eficiente, transparente e respeitosa com os direitos fundamentais dos cidadãos.

Contamos com seu compromisso e dedicação nessa importante missão!