GUIA PRÁTICO
PROTEÇÃO DE DADOS

NA ADMINISTRAÇÃO PÚBLICA

BOAS-PRÁTICAS, ALERTAS E DICAS PARA AGENTES PÚBLICOS

neogov

POR QUE ISSO IMPORTA?

Se você trabalha em uma Entidade Pública — prefeitura, câmara, autarquia, fundação, escola, unidade de saúde, assistência social — você lida todos os dias com dados pessoais de cidadãos, servidores, fornecedores, pacientes, estudantes e beneficiários. Essas informações precisam ser tratadas com responsabilidade.

A Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018) trouxe regras claras para como esses dados devem ser coletados, armazenados, usados, compartilhados e divulgados. Ela não veio para impedir o serviço público, mas para garantir que o Estado trate os dados de forma adequada, proporcional e respeitosa.

Ao mesmo tempo, a Lei de Acesso à Informação (LAI — Lei nº 12.527/2011) exige transparência, publicidade e controle social. O equilíbrio entre essas duas normas é o que garante uma gestão moderna, ética e juridicamente segura da informação pública.

Este guia foi criado para você utilizar no dia a dia, como referência rápida e prática.

CONCEITOS ESSENCIAIS

LGPD - Norma federal que regulamenta o tratamento de dados pessoais e garante direitos fundamentais relacionados à privacidade, liberdade e dignidade humana.

Dado pessoal - Qualquer informação que identifique ou possa identificar uma pessoa.
Exemplos: Nome, CPF, RG, e-mail, matrícula funcional, endereço residencial, telefone, etc.

Dado pessoal sensível - Informação que pode gerar discriminação, exigindo maior proteção.
Exemplos: Dados de saúde, religião, biometria, orientação sexual, origem racial/étnica, filiação sindical.

Controlador - A Entidade Pública responsável pelas decisões referentes ao tratamento dos dados (ex.: Prefeitura, Câmara, Autarquia).

Operador - Quem trata dados em nome do controlador (ex.: empresa fornecedora de produto/serviço, terceiro conveniado).

Titular - A pessoa a quem o dado pertence — cidadão, estudante, paciente, servidor, representante do fornecedor.

Encarregado de Dados (DPO) - A pessoa que atua como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

BASES LEGAIS DO TRATAMENTO NO SETOR PÚBLICO

Diferente da iniciativa privada, o setor público não depende, como regra, do consentimento do cidadão para tratar dados pessoais. O tratamento normalmente é baseado em fundamentos legais específicos, como:

Cumprimento de obrigação legal

Ex.: folha de pagamento, declarações fiscais, cadastro escolar.

Execução de políticas públicas

Ex.: Cadastro Único, vacinação, assistência social, educação.

Tratamento compartilhado entre entes públicos

Ex.: compartilhamento de dados com Ministério Público, TCE, tribunais, consórcios públicos.

Processo administrativo, judicial ou disciplinar

Ex.: PAD, auditorias, sindicâncias, processos judiciais.

Proteção da vida e integridade

Ex.: dados médicos, SAMU, situações emergenciais.

Execução de contratos e convênios públicos

Ex.: contratações via licitação, serviços terceirizados, estágios.

Pergunta-guia:

"Se eu não tivesse obrigação legal ou política pública definida, eu precisaria tratar esse dado?"

Se a resposta for não, o tratamento é possivelmente excessivo.

PERGUNTAS FREQUENTES 04

O que é tratar dados pessoais?

Não é só quando você coleta um dado. Toda ação realizada com um dado pessoal como coletar, armazenar, usar, compartilhar, alterar ou eliminar é um tratamento. Mesmo que não tenha sido você que coletou esse dado do cidadão, o simples fato de você ter o recebido por ofício, requerimento, sistema, e-mail e armazená-lo ou enviar para outro setor já faz de você alguém que está tratando dados pessoais.

Quais direitos o cidadão pode exercer de acordo com a LGPD?

O cidadão pode pedir acesso, correção, confirmar se há tratamento, exclusão ou anonimização quanto a dados desnecessário, revogar consentimento quando este tiver sido necessário. Exemplo: se alguém quiser sabe se seus dados estão no sistema da Entidade, tem esse direito! Mas apenas se for o próprio titular. Não permita um cidadão acesse dados de outro cidadão. E nunca corrija, exclua ou anonimize dados sem antes falar com o Encarregado de Dados.

Alguém pediu um documento com dados pessoais de um cidadão. Permito o acesso?

Como regra não, salvo se for o próprio titular destes dados pessoais. Antes de dar acesso, verifique se a pessoa é o próprio titular, se está autorizada pelo titular ou se há justificativa legal. Em caso de dúvidas, procure o Encarregado de Dados.

PERGUNTAS FREQUENTES

Quem é o Encarregado de Dados?

É a pessoa formalmente nomeada para orientar os servidores, responder aos pedidos dos cidadãos e atuar como ponte com a Agência Nacional de Proteção de Dados (ANPD), Ministério Público e Tribunal de Contas. Ele é seu aliado no dia a dia da privacidade!

Qual o papel do servidor público nisso tudo?

Você, servidor, atua como um braço da própria Entidade Controladora de Dados no exercício de suas funções. Isso significa que suas decisões no dia a dia influenciam como os dados dos cidadãos são tratados. E se ficar sabendo de algum vazamento, comunique imediatamente o Encarregado de Dados, pois a Entidade tem somente 03 (três) dias úteis para comunicar a ANPD sobre esse tipo de incidente. Por isso, é fundamental agir com responsabilidade e seguir as boas práticas.

E quanto aos fornecedores e prestadores de serviço?

Quando contratamos empresas para lidar com dados pessoais, elas atuam como operadores (não tomam decisões, mas operam os dados em nome da Entidade). Mesmo assim, o cuidado com os dados continua sendo da Entidade Pública! Exemplo: se um sistema ou serviço terceirizado trata dados dos cidadãos, o servidor público deve buscar garantir que a empresa também siga a LGPD.

PERGUNTAS FREQUENTES

06

Estou usando um formulário para coletar dados do cidadão. Posso pedir qualquer dado?

Não. Peça apenas dados que forem realmente necessários para a atividade. Dados em excesso ou sem utilidade clara devem ser evitados. Devemos minimizar o máximo possível a quantidade de dados pessoais sendo tratados. Quando não tiver certeza, consulte o Encarregado.

Outro órgão público ou empresa contratada está solicitando documentos ou arquivos com dados pessoais. Entrego?

Compartilhar dados exige muito cuidado. Só é permitido quando houver base legal e proteção adequada. Nunca repasse informações sem ter certeza. Formalize e registre sempre. E o mais importante, verifique a finalidade, se é legal, se é de interesse público. Aquilo que não for, não forneça ou anonimize.

Posso enviar dados por WhatsApp/Telegram/Instagram ou e-mail pessoal?

Como regra, não compartilhe dados por essas plataformas. Essas ferramentas não são seguras do ponto de vista de controle de compartilhamentos. Opte sempre pelos canais institucionais e autorizados, que garantem mais proteção e podem ser verificados/auditados.

PERGUNTAS FREQUENTES

07

Devo impedir que outra Secretaria/Departamento tenha acesso a dados pessoais quando solicitado?

Unidades internas como secretarias, setores, departamentos fazem parte de uma só Entidade Controladora. Por isso, o compartilhamento interno não deve ser impedido como regra geral que possa atrapalhar o funcionamento das atividades. Mas, lembre-se, o compartilhamento deve sempre ser justificado com uma finalidade pública legal.

Exemplo:

a) Controladoria Interna solicita informações de outra Secretaria/Departamento para prestar informações ao Tribunal de Contas/Ministério Público. Há finalidade e obrigação legal envolvida! Portanto, deve haver o fornecimento das informações.

b) Secretaria/Departamento de Obras/Infraestrutura solicita dados pessoais da Secretaria de Saúde (prontuário médico de cidadão) sem demonstrar efetiva justificativa. Não deve haver o fornecimento, sob pena de violação à LGPD.

Ficou com dúvida sobre a LGPD?

Na dúvida, fale com o Encarregado de Dados. É melhor perguntar do que correr o risco de expor um dado pessoal de forma indevida.

LAI E LGPD: COMPLEMENTARES E NÃO RIVAIS

Uma das grandes dúvidas da Administração Pública é: a LGPD impede a aplicação da LAI ou vice-versa? A resposta é não!

A LAI garante transparência da gestão pública, permitindo que a sociedade fiscalize o uso do dinheiro público, o funcionamento de políticas públicas e as decisões administrativas.

A LGPD protege a privacidade e a dignidade do cidadão, limitando a exposição indevida de informações pessoais. Ao contrário do que muitos pensam, a LGPD existe para permitir - e não impedir - o fluxo de informações, mas da forma adequada.

Ambas leis se complementam:

Princípio	LGPD garante	LAI garante
Transparência	Tratamento correto, seguro e proporcional de dados pessoais	Acesso à informação de interesse público
Privacidade	Proteção da vida privada e dos dados pessoais	Não se aplica à informação pessoal, exceto quando publicizada por dever legal
Publicidade qualificada	Divulgação sem exposição desnecessária	Divulgação obrigatória de atos públicos

LAI E LGPD: COMPLEMENTARES E NÃO RIVAIS

Regra prática:

Publica-se o fato administrativo. Protege-se o dado pessoal.

O que significa isso na prática?

Contratos Administrativos ou outros atos administrativos devem ser publicados, mas não com informações excessivas como endereço pessoal, CPF ou outros dados pessoais irrelevantes para a finalidade de transparência pública.

Processos administrativos podem ser públicos, mas documentos com dados pessoais, principalmente os sensíveis devem ser restritos ou anonimizados.

Informações funcionais do servidor são públicas; dados privados do servidor não são.

A LGPD foi construída com base em um grande princípio chamado de **MINIMIZAÇÃO DE DADOS PESSOAIS**, ou seja, deve-se tratar apenas os dados pessoais estritamente necessários e sempre com uma finalidade legal.

Sempre for publicar um dado pessoal, você deve se perguntar: 1) Qual a finalidade legal estou atendendo publicando este dado (**finalidade**)? 2) Eu preciso realmente publicar todos esses dados pessoais (**necessidade**)? 3) Eu estou fazendo a publicação de forma adequada (**adequação**)?

EXEMPLO PRÁTICO DE BALIZA ENTRE LAI E LGPD

1) Para atender (finalidade) essa obrigação legal/regulatória eu preciso, necessariamente (necessidade), divulgar esse dado pessoal?

2) Essa divulgação está sendo realizada de forma adequada (alinhamento entre necessidade e finalidade) e com mitigação de riscos ao titular (anonimização, pseudoanonimização)?

CASO PRÁTICO - DIVULGAÇÃO DADOS REMUNERATÓRIOS DE SERVIDORES PÚBLICOS

1) Qual a **finalidade**? R: Atender o princípio da publicidade e da transparência quanto a gastos públicos na Administração (art. 8º, LAI e art. 4º, do Decreto Estadual (MG) nº 45.969/2012).

2) Quais dados são **necessários (mínimo possível)**? R: Nome, cargo, lotação, remuneração bruta com adicionais e descontos legais. NÃO É JUIZO DE "SERIA BOM..."

3) A forma de divulgação está **adequada**? Estão sendo divulgados somente aqueles dados necessários à finalidade sem dados como descontos pessoais (empréstimo consignado, pensões alimentícias), telefone, endereço pessoal, e-mail, CPF completo, estado civil, etc. Estou usando matrícula ao invés de CPF ou divulgando CPF de forma mascarada como XX5.XX4.X3X-X3?

SEGURANÇA DA INFORMAÇÃO: O QUE PRECISO SABER?

Segurança da Informação pode parecer algo técnico demais ou "coisa da TI", mas na prática ela diz respeito a uma regra simples:

Informação certa, disponível para as pessoas certas, no momento certo e protegida de quem não deveria vê-la.

No setor público, isso significa garantir que dados pessoais, documentos administrativos, atas, processos e sistemas sejam protegidos contra acessos indevidos, alteração, perda ou divulgação acidental.

A Segurança da Informação tem quatro fundamentos principais (fácil de lembrar usando a sigla CIDAR):

Letra	Significado	Explicação simples
C	Confidencialidade	Só quem pode, acessa
I	Integridade	A informação não pode ser alterada sem autorização
D	Disponibilidade	A informação deve estar acessível quando necessária
A	Autenticidade	A informação deve ter fonte confiável
R	Rastreabilidade	Deve ser possível saber quem acessou e o que fez

ESSES PRINCÍPIOS PROTEGEM NÃO APENAS DADOS PESSOAIS (LGPD), MAS TAMBÉM A QUALIDADE E CONFIABILIDADE DA GESTÃO PÚBLICA.

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Embora muita gente confunda os termos, eles não são sinônimos, mas estão conectados:

Tema	Foco principal	Exemplo
Privacidade / LGPD	Proteger direitos do cidadão sobre seus dados pessoais	Não divulgar CPF, histórico médico, dados socioassistenciais
Segurança da Informação	Proteger as informações (públicas e pessoais) contra ataques, erros ou acessos indevidos	Senha forte, backups, bloqueio de tela, controle de acesso

Ou seja:

> ***Sem Segurança da Informação, não existe proteção de dados pessoais.***
>
> ***E sem proteção de dados, o serviço público não está em conformidade com a LGPD.***

Segurança da Informação não é apenas tecnologia — **é comportamento, cultura e cuidado coletivo**.

No setor público, cada servidor é ***guardião das informações da sociedade***.

A proteção dos dados começa com atitudes simples e termina com um serviço público mais confiável, eficiente e ético.

PRINCIPAIS AMEAÇAS

Atualmente, com os avanços tecnológicos, inúmeras ameaças cibernéticas estão presentes em nosso dia a dia. Mas em grande parte, elas precisam que tenhamos alguma atitude para que possam realmente nos causar prejuízos. Por isso, é muito importante estar atento e ter uma conduta de "**duvidar de tudo que é simples, fácil ou bom demais**". As principais são:

Ameaça	Explicação	Exemplo real
Phishing	O golpe do "clique aqui, preencha seus dados, você foi contemplado". Alguém tenta te enganar para clicar num link ou informar senhas	E-mails falsos pedindo atualização de senha bancária
Malware/Vírus	"Bichos digitais" que entram no computador e estragam tudo	Pen drives infectados ou downloads piratas
Ransomware	Sequestro digital: o sistema é bloqueado e só libera os dados mediante pagamento	Ataques a prefeituras e câmaras onde dados ficaram criptografados e inacessíveis
Engenharia social	Quando o ataque acontece usando conversa, confiança e manipulação	Alguém dizendo ser técnico de TI e pedindo sua senha
Descuido humano	O erro mais comum — sem intenção, mas com efeitos graves	Documento publicado com dados pessoais sem revisão

Sempre que receber algum contato estranho, duvidoso, um e-mail, uma mensagem, um telefonema, algum pedido incomum ou de desconhecido - duvide, não clique, não forneça informação e reporte imediatamente ao Setor de T.I.

BOAS PRÁTICAS PARA SEU DIA A DIA

Senhas e acessos

- Use senhas fortes: mistura de letras, números e símbolos
- Nunca reutilize a mesma senha em sistemas diferentes e troque sua senha a cada 90 dias.
- Ative autenticação em duas etapas quando possível
- Jamais compartilhe senha ou as anote em post-it (adesivos) visíveis — nem com colegas, TI ou chefia

Computadores e sistemas

- Bloqueie a tela ao se afastar (Windows + L)
- Não instale programas sem autorização da TI
- Não use computadores pessoais para armazenar arquivos institucionais

Arquivos e documentos

- Revise documentos antes de publicar (ex.: portais e Diário Oficial)
- Evite salvar dados pessoais em pen drives sem senha
- Use ferramentas autorizadas e sistemas oficiais
- Armazene documentos impressos em locais seguros e trancados

Comunicação

- Desconfie de links inesperados ou urgentes
- Confirme identidade antes de enviar documentos pessoais
- Use sempre e-mails/canais institucionais, nunca e-mails/canais pessoais

Internet e redes

- Não use Wi-Fi público para acessar sistemas ou arquivos institucionais
- Evite baixar arquivos desconhecidos ou piratas

CONSEQUÊNCIAS E CULTURA DE PROTEÇÃO

Ignorar boas práticas pode causar:

- Determinações corretivas da ANPD
- Questionamentos de Tribunais de Contas
- Representações no Ministério Público
- Ações civis públicas (improbidade administrativa)
- Ações judiciais por danos morais
- Indisponibilidade de sistemas
- Vazamentos com danos à imagem da Entidade
- Riscos pessoais de responsabilização funcional (processo disciplinar)

Construir uma cultura de proteção de dados é um processo contínuo. Não exige perfeição imediata, mas exige responsabilidade.

Ao tratar dados com cuidado, tratamos a população com respeito.

Lembre-se:

> ***Transparência fortalece o setor público.***
> ***Privacidade protege as pessoas.***
> ***Segurança da informação garante os dois.***

COMPROMISSO

A proteção de dados pessoais e a segurança da informação no setor público não são tarefas isoladas ou restritas à área de tecnologia: são responsabilidades compartilhadas. Cada servidor, independentemente de função ou setor, participa da proteção das informações que pertencem aos cidadãos e não ao órgão.

Ao aplicar os conceitos apresentados (como minimização de dados, transparência responsável, revisão antes da publicação, senha forte, cuidado com links suspeitos e uso correto de arquivos e documentos), o serviço público se torna mais seguro, mais confiável e mais alinhado à legislação vigente, especialmente à **LGPD** e à **Lei de Acesso à Informação**.

Mais do que cumprir uma lei, este material convida à mudança de cultura: ***sair da lógica do "sempre fiz assim" e avançar para a lógica do "estou fazendo da forma correta, segura e proporcional"***.

Caso tenha dúvidas sobre como aplicar essas orientações no dia a dia, procure:

- Encarregado da LGPD (DPO) do órgão;
- A equipe de Tecnologia da Informação; ou
- Durante todo o processo de implementação da LGPD e Segurança da Informação, você pode tirar suas dúvidas enviando um e-mail para juridico@neogov.com.br.