

**SECRETARIA DE ESTADO DE DESENVOLVIMENTO
ECONÔMICO - SEDES**

CARTILHA DE INTRODUÇÃO À CULTURA DE PROTEÇÃO DE DADOS PESSOAIS

Lei Geral de Proteção de Dados – LGPD

Uma responsabilidade de todos nós

APRESENTAÇÃO

A proteção de dados pessoais é uma responsabilidade de todos que trabalham na Administração Pública.

Mesmo que a Secretaria não preste, em regra, serviços diretamente ao cidadão, suas atividades envolvem diariamente o tratamento de dados pessoais de servidores, colaboradores, fornecedores, representantes de empresas, participantes de eventos, palestrantes, parceiros e demais pessoas que tenham algum relacionamento com a Administração Pública.

Por isso, conhecer os princípios da **Lei Geral de Proteção de Dados Pessoais – LGPD** e adotar cuidados no dia a dia são atitudes fundamentais para proteger a privacidade das pessoas e contribuir para a segurança das informações sob responsabilidade da Secretaria.

Esta cartilha foi elaborada como uma introdução à cultura de proteção de dados e tem como objetivo apresentar, de forma simples e prática, os principais conceitos da LGPD e os cuidados que devem fazer parte da rotina de trabalho.

Proteção de dados não é responsabilidade apenas da área de Tecnologia da Informação, do Encarregado ou da área jurídica. É responsabilidade de todos nós.

1. O QUE É A LGPD?

A **Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº 13.709/2018)** estabelece regras para o tratamento de dados pessoais de pessoas naturais, realizado por meios físicos ou digitais.

A Lei busca proteger direitos fundamentais relacionados à liberdade, à privacidade e ao livre desenvolvimento da personalidade.

Na prática, a LGPD estabelece regras para que os dados pessoais sejam utilizados de maneira **responsável, adequada, segura e transparente**.

A adequação à LGPD não depende apenas de sistemas de tecnologia. Ela também envolve:

- capacitação dos servidores;
- mudança de cultura;

- revisão de processos e procedimentos;
- definição de responsabilidades;
- segurança da informação;
- documentos e instrumentos jurídicos;
- controle de acesso às informações;
- prevenção e tratamento de incidentes.

Em outras palavras: a LGPD exige cuidado com a informação desde o momento em que ela é coletada até o momento em que deixa de ser necessária.

2. O QUE SÃO DADOS PESSOAIS?

Dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável.

São exemplos:

- nome;
- CPF;
- RG;
- data de nascimento;
- endereço;
- telefone;
- endereço de e-mail;
- fotografia;
- informações cadastrais;
- dados funcionais;
- endereço IP;
- cookies;
- informações de localização;
- números de documentos.

Importante: um dado aparentemente simples pode ser considerado dado pessoal quando puder ser relacionado a uma pessoa.

3. O QUE É TRATAMENTO DE DADOS PESSOAIS?

Na LGPD, o conceito de **tratamento** é bastante amplo.

Tratamento é toda operação realizada com dados pessoais, como:

- coletar;
- acessar;
- consultar;
- utilizar;
- organizar;
- armazenar;
- compartilhar;
- transmitir;
- arquivar;
- alterar;
- eliminar.

Portanto, **não é necessário modificar ou divulgar um dado para que exista tratamento.**

Por exemplo: se um servidor apenas visualiza uma planilha contendo nomes, CPF ou outras informações pessoais, já está realizando uma operação de tratamento de dados.

4. QUEM É O TITULAR DOS DADOS?

O titular é a **pessoa natural a quem os dados pessoais se referem.**

Podem ser titulares, por exemplo:

- servidores públicos;
- ocupantes de cargos em comissão;
- empregados públicos;
- trabalhadores temporários;
- colaboradores;
- fornecedores;
- representantes de empresas;
- participantes de eventos;
- palestrantes;
- cidadãos que mantenham relacionamento com a Administração Pública.

O dado pessoal pertence à esfera de proteção da pessoa a quem ele se refere.

5. QUEM SÃO OS PRINCIPAIS PERSONAGENS DA LGPD?

5.1 Titular

É a pessoa natural a quem os dados pessoais se referem.

5.2 Controlador

É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

No âmbito da Administração Pública Direta, o Estado do Rio de Janeiro o controlador, sendo suas funções exercidas pela autoridade superior de cada órgão, nos limites de suas competências e atribuições. As entidades da Administração Indireta, por sua vez, são controladoras de seus próprios dados, conforme os arts. 29 e 30 do Decreto Estadual nº 48.891/2024.

5.3 Operador

É a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Um exemplo é uma empresa contratada pelo Poder Público para executar determinado serviço que envolva o tratamento de dados pessoais.

5.4 Encarregado pelo Tratamento de Dados Pessoais

O Encarregado atua como canal de comunicação entre o órgão ou entidade, em articulação com o Encarregado Central, os titulares dos dados e a **Agência Nacional de Proteção de Dados – ANPD**, além de exercer outras atribuições relacionadas à proteção de dados.

Importante: o Encarregado não é o único responsável pela proteção de dados. A adequação à LGPD depende da participação de toda a organização.

5.5 Agência Nacional de Proteção de Dados – ANPD

A ANPD é a entidade responsável por zelar pela proteção de dados pessoais e por fiscalizar o cumprimento da LGPD, dentro de suas competências legais.

6. POR QUE A LGPD É IMPORTANTE PARA O SERVIDOR PÚBLICO?

A Administração Pública trata diariamente uma grande quantidade de informações pessoais.

Mesmo quando o servidor não atende diretamente ao cidadão, ele pode ter acesso a dados pessoais durante atividades como:

- gestão de pessoas;
- elaboração de documentos;
- processos administrativos;
- contratos;
- compras e licitações;
- eventos;
- comunicação;
- atendimento de solicitações;
- gestão financeira;
- utilização de sistemas;
- armazenamento de documentos físicos e digitais.

Por isso, **cada servidor deve compreender que o acesso a um dado pessoal representa também uma responsabilidade sobre aquele dado.**

7. O QUE SÃO DADOS PESSOAIS SENSÍVEIS?

Alguns dados pessoais recebem proteção especial pela LGPD.

São considerados dados pessoais sensíveis aqueles relacionados, entre outros, a:

- origem racial ou étnica;
- convicção religiosa;
- opinião política;
- filiação a sindicato ou organização de caráter religioso, filosófico ou político;
- saúde;
- vida sexual;
- dado genético;
- dado biométrico, quando vinculado a uma pessoa natural.

Essas informações exigem cuidados especiais porque seu uso inadequado pode causar prejuízos, constrangimentos ou discriminação.

Regra prática: quanto maior o potencial de dano ao titular, maior deve ser o cuidado no tratamento da informação.

8. EXISTEM DADOS QUE EXIGEM CUIDADOS ESPECIAIS?

Sim.

Além dos dados pessoais sensíveis, a LGPD estabelece cuidados específicos em determinadas situações, incluindo o tratamento de dados pessoais de **crianças e adolescentes**.

Por isso, sempre que houver dúvida sobre a necessidade, finalidade ou forma de utilização de determinado dado, o servidor deve procurar orientação da área responsável.

9. A LGPD PROÍBE O USO DE DADOS PESSOAIS?

Não.

A LGPD não proíbe o tratamento de dados pessoais.

O que a Lei estabelece são regras e condições para que o tratamento seja realizado de forma legítima, adequada, necessária e segura.

O tratamento deve estar fundamentado em uma das hipóteses legais previstas na LGPD.

Na hipótese legal depende da natureza dos dados e das circunstâncias de cada tratamento.

Na Administração Pública estadual, o tratamento deve estar relacionado à finalidade e ao interesse público previstos em lei. O consentimento deve ser utilizado excepcionalmente, quando for possível assegurar uma manifestação efetivamente livre, informada e inequívoca. O legítimo interesse também exige avaliação específica e não deve ser empregado quando o tratamento for compulsório ou necessário ao cumprimento de obrigações e atribuições legais do Estado, conforme os arts. 7º e 8º do Decreto Estadual nº 48.891/2024.

Entre elas estão:

Consentimento

Quando o titular manifesta sua vontade de forma livre, informada e inequívoca, nas situações em que essa hipótese for adequada.

Cumprimento de obrigação legal ou regulatória

Quando o tratamento é necessário para cumprir uma obrigação prevista em lei ou regulamento.

Exemplo: divulgação de informações exigidas pela legislação de transparência.

Execução de políticas públicas

Quando o tratamento é realizado para a execução de políticas públicas previstas em leis e regulamentos.

Estudos por órgãos de pesquisa

Nas situações previstas pela legislação para realização de estudos e pesquisas.

Execução de contrato

Quando o tratamento é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato.

Exercício regular de direitos

Quando o tratamento é necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Proteção da vida

Quando o tratamento é indispensável para proteger a vida ou a integridade física de uma pessoa.

Tutela da saúde

Nas situações previstas pela LGPD para procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Proteção do crédito

Nas hipóteses previstas na legislação.

Prevenção à fraude e segurança

Em situações previstas pela LGPD, especialmente para procedimentos de identificação e autenticação.

Legítimo interesse

Nas situações em que essa hipótese puder ser legalmente utilizada e forem observados os requisitos e princípios previstos na LGPD.

Atenção: não basta existir uma hipótese legal. O tratamento também precisa respeitar os princípios da LGPD.

10. QUAIS SÃO OS PRINCÍPIOS DA LGPD?

Os principais princípios que devem orientar o tratamento de dados pessoais são:

- **Finalidade** – utilizar os dados para propósitos legítimos e informados;
- **Adequação** – utilizar os dados de acordo com a finalidade informada;
- **Necessidade** – utilizar apenas os dados necessários;
- **Livre acesso** – garantir ao titular informações sobre o tratamento de seus dados;
- **Qualidade dos dados** – manter os dados corretos e atualizados;
- **Transparência** – fornecer informações claras sobre o tratamento;
- **Segurança** – adotar medidas para proteger os dados;
- **Prevenção** – agir para evitar danos;
- **Não discriminação** – não utilizar os dados para fins discriminatórios, ilícitos ou abusivos;
- **Responsabilização e prestação de contas** – demonstrar a adoção de medidas eficazes para cumprir a legislação.

Uma pergunta simples pode ajudar no dia a dia:

“Eu realmente preciso acessar, utilizar ou compartilhar este dado para realizar minha atividade?”

Se a resposta for não, o acesso ou compartilhamento deve ser evitado.

11. QUAIS SÃO OS DIREITOS DO TITULAR?

A LGPD assegura diversos direitos às pessoas em relação aos seus dados pessoais.

Entre eles estão:

1. Confirmar se seus dados pessoais estão sendo tratados;
2. Acessar seus dados pessoais;
3. Solicitar a correção de dados incompletos, inexatos ou desatualizados;
4. Solicitar informações sobre o compartilhamento de seus dados;
5. Solicitar informações sobre o tratamento realizado;
6. Revogar o consentimento, quando o tratamento estiver baseado nessa hipótese;
7. Solicitar a eliminação dos dados nas situações previstas na LGPD;
8. Solicitar a portabilidade dos dados, quando aplicável;
9. Opor-se ao tratamento realizado em determinadas situações;
10. Não ser submetido a tratamento discriminatório, ilícito ou abusivo;
11. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação;
12. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, quando cabível;
13. Revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem os interesses do titular.

Importante: nem todo pedido de eliminação ou interrupção do tratamento poderá ser atendido. Existem situações em que a Administração Pública precisa manter ou tratar determinados dados para cumprir uma obrigação legal, exercer suas competências ou atender a outras hipóteses previstas na legislação.

12. ONDE ESTÃO OS RISCOS NO NOSSO DIA A DIA?

A proteção de dados começa com atitudes simples.

Algumas situações que merecem atenção:

Sobre a mesa

Não deixe expostos:

- documentos;
- processos;
- listas;
- planilhas;
- fotografias;
- cópias de documentos;
- anotações contendo dados pessoais.

Computador

- Bloqueie a estação de trabalho ao se afastar;
- Não deixe sistemas abertos sem supervisão;
- Não compartilhe sua senha;
- Não anote senhas em locais de fácil acesso.

E-mail

- Confira o destinatário antes de enviar;
- Verifique os anexos antes do envio;
- Não utilize e-mail pessoal para atividades institucionais;
- Tenha cuidado com arquivos e links recebidos de remetentes desconhecidos.

WhatsApp e aplicativos de mensagens

Evite utilizar contas ou dispositivos pessoais para compartilhar documentos institucionais, especialmente quando contiverem dados pessoais.

Sempre que houver uma ferramenta institucional disponível, dê preferência aos canais oficiais.

Pendrives e mídias removíveis

Não utilize mídias pessoais em equipamentos institucionais sem autorização.

Planilhas e arquivos

Evite armazenar dados pessoais em sistemas, planilhas ou ferramentas que não sejam autorizados ou monitorados pela instituição.

Documentos físicos

Documentos que contenham dados pessoais devem permanecer em locais protegidos e com acesso restrito às pessoas que realmente necessitem dessas informações.

13. O PRINCÍPIO DO “PRECISO SABER”

Uma das atitudes mais importantes para a proteção de dados é limitar o acesso às informações.

O fato de o servidor conseguir acessar determinado dado **não significa que ele possa utilizá-lo livremente.**

O acesso deve ocorrer somente quando for necessário para o desempenho das atividades funcionais.

Pergunte sempre:

Eu preciso dessa informação para realizar meu trabalho?

Se não precisar, não acesse.

Se precisar, utilize somente o necessário.

14. EXEMPLOS PRÁTICOS

Situação 1 – Lista de presença

Uma lista de presença contém nome, telefone e e-mail dos participantes de um evento.

Cuidado: não compartilhe ou publique essas informações sem verificar a finalidade e a necessidade do tratamento.

Situação 2 – E-mail

Você precisa enviar uma planilha contendo dados pessoais.

Cuidado: confira o destinatário, o conteúdo do arquivo e se o envio é realmente necessário.

Situação 3 – Mesa de trabalho

Você precisa sair por alguns minutos e deixou um processo aberto sobre a mesa.

Cuidado: documentos contendo dados pessoais não devem ficar expostos desnecessariamente.

Situação 4 – Computador

Você saiu para tomar café e deixou seu computador desbloqueado.

Cuidado: sempre bloqueie a estação de trabalho ao se afastar.

Situação 5 – WhatsApp

Um colega pede que você envie pelo seu WhatsApp pessoal uma planilha contendo informações de servidores.

Cuidado: utilize os meios institucionais autorizados e evite o uso de ferramentas pessoais para documentos de trabalho.

15. E SE OCORRER UM INCIDENTE?

Um incidente pode ocorrer mesmo quando não existe intenção de causar dano.

Exemplos:

- envio de documento para destinatário errado;
- perda de equipamento;
- acesso indevido;
- compartilhamento acidental;
- exposição de documento;
- perda de pendrive;
- abertura de arquivo suspeito;
- divulgação indevida de informação.

O mais importante é comunicar rapidamente. Todo incidente envolvendo dados pessoais, confirmado ou ainda sob suspeita, deve ser comunicado

imediatamente ao Encarregado Setorial. Caberá a ele dar seguimento ao Plano de Resposta a Incidentes e informar o Encarregado Central, conforme os arts. 26 e 27 do Decreto Estadual nº 48.891/2024.

Não tente esconder um erro.

Quanto mais rapidamente um incidente for comunicado à área responsável, maiores serão as possibilidades de reduzir seus impactos e adotar as medidas necessárias.

Em caso de dúvida, procure a área responsável pela proteção de dados ou pelos procedimentos de segurança da informação da Secretaria.

16. RESPONSABILIDADE DE TODOS

A proteção de dados não é uma tarefa exclusiva:

- da área de Tecnologia da Informação;
- do Encarregado;
- da área jurídica;
- da Ouvidoria;
- da área de segurança da informação.

Todos os servidores participam, direta ou indiretamente, do tratamento de dados pessoais.

Cada acesso, cada compartilhamento, cada documento enviado e cada arquivo armazenado representa uma oportunidade de proteger — ou colocar em risco — os dados de uma pessoa.

17. PENALIDADES E CONSEQUÊNCIAS

A LGPD prevê sanções administrativas aplicáveis em caso de infrações, observadas as condições previstas na legislação.

Entre as sanções estão:

- advertência;
- publicização da infração;
- bloqueio dos dados pessoais;

- eliminação dos dados pessoais;
- suspensão de determinadas atividades de tratamento;
- proibição parcial ou total de atividades relacionadas ao tratamento de dados.

No caso do Poder Público, existem regras específicas sobre a aplicação das sanções administrativas.

Além das sanções administrativas, o tratamento inadequado de dados pode gerar outras consequências jurídicas, administrativas e funcionais, conforme o caso.

18. A LGPD NA NOSSA SECRETARIA

A adequação à LGPD é um processo contínuo.

Não se trata de uma ação isolada ou de uma responsabilidade atribuída a apenas uma unidade administrativa.

A participação dos servidores é fundamental para a construção de uma verdadeira **cultura de proteção de dados**.

Esta cartilha representa um primeiro passo para:

- conscientizar os servidores;
- disseminar conceitos básicos;
- identificar riscos;
- estimular boas práticas;
- fortalecer a segurança das informações;
- contribuir para a adequação dos processos internos à LGPD.

Novas orientações, capacitações e procedimentos poderão ser desenvolvidos e divulgados conforme o avanço do processo de adequação da Secretaria.

19. CHECKLIST DO SERVIDOR

Antes de acessar, utilizar ou compartilhar um dado pessoal, pergunte:

- Eu realmente preciso desse dado?
- O acesso é necessário para o meu trabalho?
- Estou utilizando um canal institucional adequado?

- O destinatário realmente precisa receber essa informação?
- Estou compartilhando somente o necessário?
- O documento está protegido contra acesso indevido?
- Minha estação de trabalho está bloqueada quando estou ausente?
- Estou protegendo minhas senhas?
- Estou evitando ferramentas pessoais para atividades institucionais?
- Sei a quem comunicar caso ocorra um incidente?

20. MENSAGEM FINAL

PROTEGER DADOS É PROTEGER PESSOAS

A LGPD não deve ser vista apenas como uma obrigação legal.

Ela representa uma mudança de cultura.

Proteger dados pessoais significa respeitar a privacidade, a dignidade e os direitos das pessoas que confiam suas informações à Administração Pública.

Cada servidor tem um papel nessa construção.

Antes de acessar, compartilhar, armazenar ou enviar um dado pessoal, pare e pense:

É necessário? É adequado? É seguro?

Se houver dúvida, procure orientação.

A proteção de dados começa com cada um de nós.