



LGPD

Cartilha Simplificada de Proteção de Dados



PER NAM BUCO

Secretaria de Justiça,
Direitos Humanos
e Prevenção à Violência





**PER
NAM
BUCO**

SUMÁRIO



<u>INTRODUÇÃO À LGPD</u>	4
<u>CONCEITOS ESSENCIAIS LGPD</u>	5
<u>AGENTES NA PROTEÇÃO DE DADOS LGPD</u>	6
<u>RESUMO DAS ATRIBUIÇÕES NA PROTEÇÃO DE DADOS</u>	8
<u>PRINCÍPIOS BÁSICOS DA LGPD</u>	9
<u>IMPORTÂNCIA DO MAPEAMENTO DE DADOS</u>	10
<u>PONTOS PRINCIPAIS DO MAPEAMENTO</u>	11
<u>PROCEDIMENTOS RECOMENDADOS NA ETAPA DEMAPEAMENTO</u>	14
<u>POR QUE É CRUCIAL PARA A EQUIPE?</u>	15
<u>LGPD X SERVIÇO PÚBLICO</u>	16
<u>RESTRIÇÕES QUANTO AO TRATAMENTO DE DADOS PESSOAIS</u>	18
<u>ORIENTAÇÕES FINAIS E AÇÕES DE IMPLEMENTAÇÃO</u>	20
<u>REFERÊNCIAS</u>	21

INTRODUÇÃO À LGPD

O QUE É A LGPD?

A Lei Geral de Proteção de Dados (LGPD) é uma normativa brasileira que regula o uso, tratamento e armazenamento de dados pessoais, garantindo a privacidade e segurança dos cidadãos. Complementada por mecanismos de fiscalização e punições, ela entrou em vigor em 2020.



POR QUE ELA É IMPORTANTE PARA O SETOR PÚBLICO?



1. Protege os direitos dos cidadãos sobre seus dados pessoais.
2. Assegura que os órgãos públicos tratem os dados com responsabilidade e transparência.
3. Previne riscos de vazamentos, acessos não autorizados e uso indevido de informações.

OBJETIVO DESTA CARTILHA

Orientar os responsáveis na Secretaria para um entendimento básico da LGPD e orientar sobre o mapeamento e proteção de dados.



CONCEITOS ESSENCIAIS DA LGPD

DADOS PESSOAIS

Qualquer informação que identifique uma pessoa, como nome, CPF, endereço, telefone, informações de saúde, e-mail, etc.



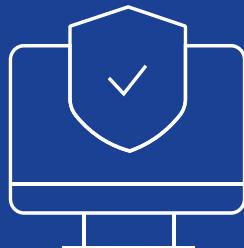
DADOS SENSÍVEIS

Informações que incluem origem étnica, saúde, religião, orientação sexual, opinião política, entre outros. Exigem cuidados adicionais.



DIREITOS DOS TITULARES

- Confirmar quais dados possuem sobre ele.
- Pedir a correção ou exclusão dos dados.
- Saber como seus dados estão sendo usados.
- Requisitar a eliminação de dados quando não mais necessários.



AGENTES NA PROTEÇÃO DE DADOS NA LGPD

1. CONTROLADOR

Definição:

Pessoa natural ou jurídica, de direito público ou privado, a quem cabe as decisões referentes ao tratamento de dados pessoais.

Atribuições principais:

- Definir as finalidades do tratamento de dados pessoais.
- Estabelecer as bases legais para o tratamento.
- Colaborar na elaboração de políticas internas de proteção de dados.
- Garantir a transparência e a segurança dos dados tratados.
- Responder pelos danos causados por violações à legislação ou à própria política de proteção de dados.

Na prática:

No setor público, o controlador geralmente é a própria entidade ou órgão responsável pelo tratamento dos dados.

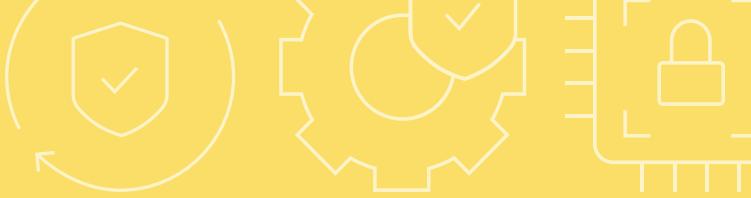
2. ENCARREGADO (DPO - DATA PROTECTION OFFICER)

Definição: Pessoa indicada pelo controlador ou operador para atuar como canal de comunicação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Atribuições principais:

- Encaminhar as demandas dos titulares de dados.
- Cooperar com a autoridade reguladora.
- Orientar a organização sobre boas práticas de proteção de dados.
- Monitorar o cumprimento da LGPD e das políticas internas.
- Auxiliar na elaboração de relatórios e na implementação de medidas de proteção.





3. OPERADOR

Definição: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Atribuições principais:

- Seguir as instruções do controlador.
- Manter sigilo e confidencialidade.
- Implementar as medidas de segurança estabelecidas.
- Comunicar ao controlador qualquer incidente de segurança ou vazamento de dados.

Importante: Responsabilidade pelo tratamento dos dados de acordo com o controlador e a legislação, podendo ser responsabilizado por danos ou violações.

4. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Definição: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Atribuições principais (com base na Lei):

- Elaborar diretrizes e regulamentos.
- Fiscalizar o cumprimento da LGPD.
- Requerer informações às organizações públicas e privadas.
- Emissão de pareceres técnicos.
- Aplicar sanções em caso de infrações.
- Orientar e capacitar os agentes envolvidos na proteção de dados.
- Solicitar relatórios de impacto ou auditorias.



RESUMO DAS ATRIBUIÇÕES NA PROTEÇÃO DE DADOS

AGENTE	FUNÇÃO PRINCIPAL	ATRIBUIÇÕES
CONTROLADOR	Decisor do tratamento	Definir finalidades, bases legais, políticas de privacidade, responder por violações.
ENCARREGADO (DPO)	Canal de comunicação	Atuar como ponte entre titulares, órgãos reguladores e a organização, orientando e monitorando o cumprimento da LGPD.
OPERADOR	Executor do tratamento	Seguir as instruções do controlador, garantir sigilo, aplicar medidas de segurança.
AUTORIDADE (ANPD)	Órgão regulador	Fiscalizar, emitir diretrizes, aplicar sanções, orientar o setor público e privado.



PRINCÍPIOS BÁSICOS DA LGPD

PRINCIPAIS PILARES PARA O TRATAMENTO DE DADOS:

Finalidade: Os dados só podem ser usados para o que foi informado ao cidadão.

Necessidade: Apenas os dados essenciais para o objetivo devem ser coletados.

Transparência: Os titulares devem ser claramente informados sobre o uso de seus dados.

Segurança: Os dados devem ser protegidos contra acessos indevidos, vazamentos e ataques.

Exclusão: Após o uso, os dados devem ser apagados ou anonimizados.

IMPORTÂNCIA DO MAPEAMENTO DE DADOS

O mapeamento de dados é o primeiro passo essencial para entender completamente as operações de tratamento de informações pessoais dentro de um órgão ou entidade pública.

Permite identificar:

- Quais dados são coletados.
- Onde esses dados estão armazenados.
- Como são tratados, utilizados ou compartilhados.
- Quem tem acesso a esses dados.
- Quais pontos de vulnerabilidade podem existir.

Esse processo é a base para estabelecer controles efetivos, reduzir riscos, cumprir regulamentações e elaborar a política interna de proteção de dados.



PONTOS PRINCIPAIS DO MAPEAMENTO

1. Tipos de Dados Sensíveis e Não Sensíveis

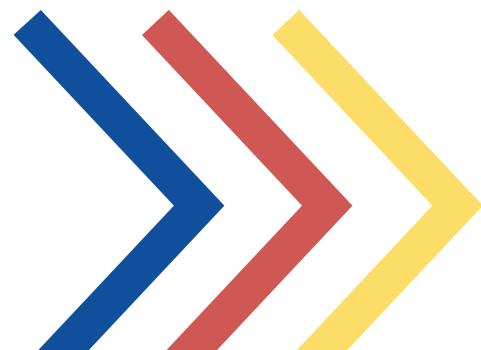
Identifique quais dados pessoais e sensíveis estão presentes nos processos. Por exemplo, dados sensíveis incluem informações sobre origem racial, religiosa, saúde, orientação sexual, entre outros. A classificação ajuda a definir medidas específicas de proteção.

2. Local de Armazenamento

Verificar onde esses dados ficam guardados: sistemas informatizados, arquivos físicos, dispositivos móveis, servidores internos, nuvem, etc.

3. Forma de Tratamento

Compreender os procedimentos realizados com esses dados: coleta, armazenamento, uso, comunicação, transmissão, conservação ou exclusão.



1 coleta

Recebimento ou obtenção de dados pessoais, por qualquer meio (físico ou digital), com ou sem o conhecimento do titular.

2 armazenamento

Armazenamento dos dados pessoais pelo tempo necessário para atender à finalidade específica, conforme previsto na LGPD.

3 uso

Utilização dos dados pessoais para cumprir a finalidade legítima informada ao titular, respeitando os princípios da LGPD (como finalidade, necessidade e transparência).

4 comunicação

Disponibilização dos dados pessoais a agentes internos ou terceiros, dentro do mesmo controlador, para fins legítimos, com base legal e transparência.

5 transmissão

Transferência dos dados pessoais a terceiros externos, inclusive fora do país, exigindo base legal adequada, medidas de segurança e garantias ao titular.

6 conservação ou exclusão

Os dados pessoais devem ser conservados apenas pelo tempo necessário para cumprir a finalidade que justificou sua coleta ou conforme exigido por obrigações legais e regulatórias. Após esse período, os dados devem ser excluídos, salvo se houver base legal que justifique sua retenção, como defesa em processos, cumprimento de obrigações legais ou exercício regular de direitos.

4. Fluxo de Dados e Trafego

Mapear por onde esses dados trafegam dentro da organização, incluindo transferências internas e externas, bem como acessos e partilhas de informações.

5. Profissionais com Acesso

Listar os profissionais com acesso a esses dados e o nível de permissão de cada um, garantindo que apenas pessoas autorizadas tenham acesso às informações sensíveis.

6. Controle de Acesso e Segurança

Analistar os mecanismos de controle existentes: senhas, logs, autorização por níveis, criptografia, etc.

7. Capacitação e Equipe

Identificar profissionais responsáveis pela análise e atualização de políticas de proteção de dados. Manter capacitação contínua dos agentes de tratamento de dados pessoais, como palestra, cursos, oficinas, manuais, cartilhas, workshop e outros.



8. Pontos Fracos e Estratégias de Mitigação

Identificar vulnerabilidades, como sistemas desatualizados ou procedimentos inadequados, e propor ações correctivas.

9. Avaliação da Classificação dos Dados

Verificar se os dados foram classificados adequadamente, considerando os critérios atuais da LGPD.

PROCEDIMENTOS RECOMENDADOS NA ETAPA DE MAPEAMENTO

Criar um inventário detalhado de todos os sistemas e bancos de dados de tratamento de dados pessoais.

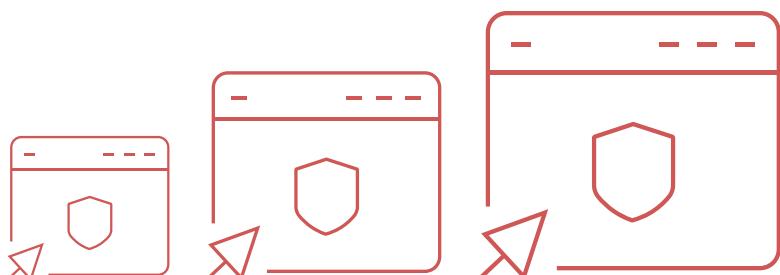
- **Constituir uma equipe multidisciplinar** envolvendo TI, jurídico, gestão de riscos, entre outros, para garantir uma análise completa.
- **Documentar todo o processo**, incluindo mapas, fluogramas, responsáveis, descrições e justificativas.



POR QUE É CRUCIAL PARA A EQUIPE?

Para os servidores responsáveis pelo mapeamento, entender esses pontos é fundamental porque:

- Garantem a legalidade do tratamento de dados.
- Facilitam a identificação de pontos de risco e vulnerabilidades.
- Auxiliam na elaboração de políticas internas de proteção de dados.
- São essenciais para que órgãos públicos possam atender a eventuais solicitações da Autoridade Nacional de Proteção de Dados (ANPD).
- Contribuem para a transparência e responsabilidade na gestão de informações pessoais, fortalecendo a confiança dos cidadãos.



LGPD X SERVIÇO PÚBLICO

PRINCÍPIO FUNDAMENTAL DO TRATAMENTO DE DADOS NO SETOR PÚBLICO

Os órgãos públicos, ao tratar dados pessoais, devem seguir o princípio de que essa atividade seja realizada **apenas para fins de interesses públicos legítimos**. Ou seja, qualquer coleta, processamento ou armazenamento de informações deve estar alinhado às finalidades institucionais, como fornecer serviços, garantir direitos ou cumprir deveres legais.

FINALIDADE E LEGALIDADE

O tratamento de dados no setor público deve estar respaldado por uma base legal clara, como uma lei, regulamento ou decisão administrativa. Assim, as atividades de tratamento são legítimas somente quando atendem a uma finalidade pública específica, definida previamente e de conhecimento do titular dos dados.





No âmbito do Estado de Pernambuco, os normativos que estabelecem a política de Proteção de Dados e suas diretrizes são:

- Lei Estadual nº 17.117, de 23 de setembro de 2020, que dispõe sobre a proteção de dados pessoais no âmbito da Administração Pública estadual.
- Decreto Estadual nº 50.384, de 16 de março de 2021, que regulamenta a implementação da Lei Estadual nº 17.117/2020, trata da governança, designação de encarregados (DPOs) e das responsabilidades de cada órgão para a proteção de dados.
- Estadual de Proteção aos Defensores dos Direitos Humanos - PEPDDH/PE, no âmbito do Estado de Pernambuco, e dá outras providências.
- LEI N° 16.559, DE 15 DE JANEIRO DE 2019. Código Estadual de Defesa do Consumidor de Pernambuco.
- LEI N° 13.371, DE 19 DE DEZEMBRO DE 2007. Política Estadual de Assistência e Proteção a Vítimas e Colaboradores da Justiça, o PROVITA/PE e o seu Conselho Deliberativo.
- LEI N° 15.188, DE 12 DE DEZEMBRO DE 2013. Institui o Programa de Proteção a Crianças e Adolescentes Ameaçados de Morte no Estado de Pernambuco - PPCAAM/PE.

No âmbito da atuação da Secretaria de Justiça, Direitos Humanos e Prevenção à Violência, são as bases legais que justificam o tratamento:

- LEI N° 14.912, DE 27 DE DEZEMBRO DE 2012. Cria o Programa

RESTRIÇÕES QUANTO AO TRATAMENTO DE DADOS PESSOrais

Respeito à privacidade e aos direitos do titular:

os dados não podem ser utilizados para finalidades secundárias ou diferentes do objetivo original, sem autorização ou justificativa legal.

Necessidade:

somente os dados imprescindíveis para o cumprimento da finalidade devem ser coletados e tratados. No âmbito da Secretaria de Justiça, Direitos Humanos e Prevenção à Violência, a coleta de dados pessoais sensíveis é, por vezes, necessária para fins de indicadores sociais e participação ativa de grupos sociais específicos.

Transparência:

os cidadãos devem ser informados sobre as operações de tratamento de seus dados, incluindo quais dados são utilizados, com qual finalidade e por quanto tempo serão armazenados.

IMPLICAÇÕES PRÁTICAS PARA OS ÓRGÃOS PÚBLICOS

- É necessário mapear todas as atividades de tratamento para garantir que estejam alinhadas às finalidades públicas.





- Deve-se garantir que o tratamento seja realizado com medidas de segurança adequadas, evitando vazamentos, acessos não autorizados ou uso indevido das informações.
- A cobrança pela transparência exige que os cidadãos tenham acesso às informações relevantes sobre o uso de seus dados.

EXEMPLOS DE APLICAÇÕES RELEVANTES NA ADMINISTRAÇÃO PÚBLICA

- Gestão de cadastro de cidadãos para o fornecimento de serviços públicos.
- Processamento de informações para fiscalização, licitações ou contratos administrativos.
- Compartilhamento de dados entre entidades públicas, desde que autorizado e justificado pelo interesse público.
- Compartilhamento de dados com Organizações da Sociedade Civil para execução de políticas públicas descentralizadas, executadas a partir de parcerias.

RESPONSABILIDADE DA ADMINISTRAÇÃO PÚBLICA

A administração pública tem o dever de adotar uma postura proativa na proteção de dados, implementando controles, treinamentos, auditorias e políticas internas, além de assegurar que qualquer procedimento de tratamento seja documentado, justificável e minimize riscos à privacidade dos titulares.

ORIENTAÇÕES FINAIS E AÇÕES DE IMPLÉMENTAÇÃO

QUEM DEVE SE ENVOLVER?

Responsáveis de cada setor, com apoio da Comissão de Conformidade à Lei Geral de Proteção de Dados, juntamente com a/o encarregado (DPO).

PRINCIPAIS AÇÕES PARA GARANTIR A CONFORMIDADE:

- **Mapear todos os dados:**
Conhecer o que você possui.
- **Criar uma política interna de proteção de dados:**
Normas, procedimentos e treinamentos.
- **Controlar acessos:**
Garantir que apenas pessoas autorizadas possam acessar os dados sensíveis.
- **Implementar medidas de segurança:**
Tecnológicas e administrativas.
- **Preparar-se para fiscalizações:**
Documentar ações, políticas e treinamentos.

CONTATO PARA ORIENTAÇÃO

Procure Comissão de Conformidade à Lei Geral de Proteção de Dados e o(a) encarregado(a).

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

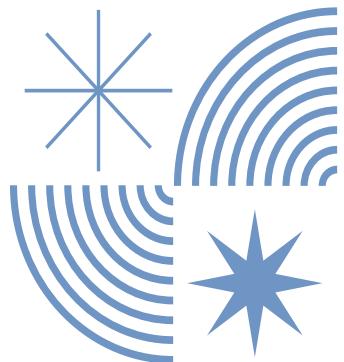
Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

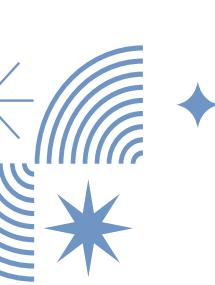
CONTROLADORIA GERAL DO ESTADO (CGE). Cartilha LGPD: Lei Geral de Proteção de Dados. Brasília: CGE, 2020. Disponível em: https://www.cge.pr.gov.br/cartilha_LGPD.pdf.

Acesso em: 5 abril. 2025.

PERNAMBUCO. Controladoria Geral do Estado. Manual de orientação à Lei Geral de Proteção de Dados Pessoais (LGPD) para o poder executivo estadual de Pernambuco: versão 3.2. Recife: SCGE, 2021.

Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2021/11/ManualLGPDv3-2.pdf>. Acesso em: 5 abril. 2025.





Expediente:

Raquel Teixeira Lyra Lucena

Governadora do Estado de Pernambuco

Priscila Krause Branco

Vice-Governadora do Estado de Pernambuco

Joana D'Arc da Silva Figueiredo

Secretária de Justiça, Direitos Humanos
e Prevenção à Violência

Cecília Souto Maior

Diretora de Controle Interno

Daniel Sylas

Assessor Jurídico

Diógenes Veras Brasileiro

Gerência de Planejamento e Monitoramento de Projetos

Natália Maria Martins Oliveira

Designer - Comunicação

Poliana Caroliny dos Santos Nascimento

Chefe de Gabinete

Maria Tayne Bezerra Cavalcanti

Superintendente Jurídica

Thamires Lívia Lima da Silva

Consultora Técnica

Thyago Amorim

ATI

Victoria Freire

Assessora de Controle Interno

Ficha Técnica:

**Organização: Secretaria de Justiça Direitos Humanos e
Prevenção a Violência de Pernambuco**

Texto/Redação:

**Victoria Fernanda Freire Muniz
e Poliana Caroliny dos Santos Nascimento**

Diagramação e design gráfico

Natália Maria Martins Oliveira



PER
NAM
BUCO

PER
NAM
BUCO

