MANUAL

IMPLEMENTAÇÃO DA LGPD

CGE

CONTROLADORIA GERAL DO ESTADO DO PARANÁ

GOVERNO DO ESTADO DO PARANÁ

Governador do Estado do Paraná
Carlos Massa Ratinho Junior

Controladora-Geral do Estado do Paraná
Louise da Costa e Silva Garnica

Elaboração
Assessora Técnica
Mineia Lückfett de Oliveira

Contato:
lgpd@cge.pr.gov.br
mineial@cge.pr.gov.br
(41) 3883-4047

SUMÁRIO

1 APRESENTAÇÃO

A proteção de dados pessoais constitui um dos principais desafios da Administração Pública atual, especialmente diante da crescente digitalização dos serviços públicos, da ampliação do uso de tecnologias da informação e do aumento exponencial do compartilhamento de dados entre órgãos e entidades.

Nesse contexto, a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)** inaugura um novo paradigma na atuação estatal, ao estabelecer regras, princípios e responsabilidades para o tratamento de dados pessoais, com o objetivo de **proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural,** sem comprometer o atendimento ao interesse público.

A adequação à LGPD não se resume ao cumprimento formal de exigências legais. Trata-se de um **processo estruturante**, contínuo e transversal, que demanda mudanças organizacionais, revisão de práticas administrativas, fortalecimento da governança, capacitação de servidores e consolidação de uma cultura institucional orientada à proteção de dados pessoais.

Nesse sentido, o presente **Manual de Implementação da Lei Geral de Proteção de Dados Pessoais** foi elaborado com a finalidade de **orientar gestores, servidores e colaboradores** quanto às medidas necessárias para a conformidade com a LGPD, considerando as especificidades da Administração Pública e a necessária harmonização com outras normas aplicáveis, em especial a **Lei de Acesso à Informação (Lei nº 12.527/2011)**, e as orientações da **Agência Nacional de Proteção de Dados (ANPD)**.

O Manual adota uma abordagem **prática, sistematizada e fundamentada**, abordando, entre outros temas:

- o mapeamento e inventário de dados pessoais;
- a elaboração do mapa de riscos e do Relatório de Impacto à Proteção de Dados (RIPD);
- a estrutura organizacional de governança, com a designação do encarregado, a criação de comitês e a instituição de programas de governança;
- a elaboração de políticas de proteção de dados;
- a adequação de documentos e a gestão de terceiros;
- a garantia dos direitos dos titulares;
- a relação entre LGPD e transparência pública;
- a resposta a incidentes de segurança; e
- as ações de treinamento, aculturamento e comunicação interna.

Portanto, o material apresentado pretende auxiliar **à tomada de decisão**, à padronização de procedimentos e ao fortalecimento da **accountability (conformidade com as normas de proteção)**, contribuindo para uma atuação administrativa mais segura, transparente, responsável e alinhada aos princípios constitucionais.

A implementação efetiva da LGPD depende do engajamento institucional e do compromisso de todos os agentes públicos.

Ao adotar as diretrizes aqui apresentadas, a Administração Pública reafirma seu compromisso com a proteção de dados pessoais, a segurança da informação e o respeito aos direitos fundamentais dos cidadãos.

2 MAPEAMENTO INVENTÁRIO DE DADOS

O **mapeamento ou inventário de dados pessoais** é o processo de **identificação, registro, organização e documentação** de todas as operações de tratamento de dados pessoais realizadas por uma organização, desde a **coleta até a eliminação**, abrangendo:

- Quais dados são tratados;
- De quem são os dados (titulares);
- Para que finalidades;
- Com base em quais fundamentos legais;
- Quem acessa e com quem os dados são compartilhados;
- Onde os dados são armazenados;
- Por quanto tempo são mantidos;
- Quais medidas de segurança são adotadas.

Na prática, o inventário **materializa o "ciclo de vida do dado pessoal"** na organização. O inventário de dados é a base estrutural da governança em proteção de dados, visto que sem ele, não há LGPD efetiva.

PRINCIPAIS RAZÕES PARA SUA IMPORTÂNCIA:

Conformidade legal
- Atende diretamente ao art. 37 da LGPD;
- Permite demonstrar accountability.

Transparência e controle
- Viabiliza respostas adequadas aos titulares (art. 18);
- Dá suporte à política de privacidade e aos avisos de tratamento.

Gestão de riscos
- Identifica tratamentos excessivos, desnecessários ou irregulares;
- Permite avaliar riscos e definir prioridades de adequação.

Base para decisões
- Subsidia o RIPD;
- Fundamenta cláusulas contratuais, políticas internas e decisões de compartilhamento.

Segurança da informação
- Facilita a identificação de dados críticos e sensíveis;
- Direciona controles de acesso e medidas de segurança.

Integração LGPD–LAI
- Permite classificar corretamente informações pessoais, protegidas ou passíveis de acesso público.

Um inventário minimamente adequado deve conter, por operação de tratamento:

a. Identificação do órgão/unidade responsável
b. Nome do processo ou atividade
c. Finalidade do tratamento
d. Categoria dos titulares
e. Tipos de dados pessoais tratados
f. Indicação de dados sensíveis (se houver)
g. Base legal do tratamento
h. Forma de coleta
i. Compartilhamentos internos e externos
j. Transferências (inclusive internacionais, se houver)
k. Sistemas ou repositórios utilizados
l. Prazo de retenção e critérios de descarte
m. Medidas de segurança adotadas
n. Grau de risco (baixo, médio, alto)
o. Necessidade de RIPD
p. Responsável pelo tratamento (área/função)

O inventário **não é documento estático**, deve ser atualizado periodicamente e possui relação com outros instrumentos da LGPD, tais com:

Instrumento	Relação com o inventário
Política de Privacidade	Base de informação
RIPD	Depende do inventário
Atendimento ao titular	Fundamentado no inventário
Contratos e convênios	Identificação de compartilhamentos
Gestão de incidentes	Identificação rápida dos dados afetados

Portanto, é possível depreender que sem inventário, a LGPD tende a se tornar meramente formal; com inventário bem estruturado, ela se transforma em **política pública efetiva de proteção de dados.**

3 MAPA DE RISCOS E RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O **levantamento de riscos em proteção de dados pessoais** é o processo sistemático de **identificação, análise e avaliação** dos riscos que as operações de tratamento de dados pessoais podem gerar aos **direitos dos titulares**, considerando:

- A natureza dos dados tratados;
- As finalidades do tratamento;
- Os agentes envolvidos;
- Os meios utilizados;
- As vulnerabilidades técnicas e organizacionais.

Feito o levantamento, será elaborado o **mapa de riscos, que é a representação estruturada e sistematizada** dos riscos identificados nos tratamentos de dados, normalmente organizada em uma matriz que cruza a **probabilidade** de ocorrência do evento de risco e o **impacto** potencial aos titulares de dados.
O mapa de riscos permite **visualizar, priorizar e tratar riscos**, orientando a tomada de decisão administrativa.

3.1 ETAPAS DA ELABORAÇÃO DO MAPA DE RISCOS

3.1.1 IDENTIFICAÇÃO DOS RISCOS

A partir do inventário de dados, identificar eventos como:

- Coleta excessiva de dados;
- Acesso indevido;
- Compartilhamento não autorizado;
- Armazenamento inseguro;
- Retenção além do prazo necessário;
- Ausência de base legal adequada;
- Falhas em contratos com operadores.

3.1.2 ANÁLISE DE PROBABILIDADE

Avaliar a chance de ocorrência do risco, considerando:

- Frequência do tratamento;
- Quantidade de titulares afetados;
- Grau de exposição do sistema;
- Histórico de incidentes.

3.1.3. ANÁLISE DE IMPACTO

Avaliar os possíveis danos aos titulares, como:

- Discriminação;
- Fraude;
- Exposição indevida;
- Danos morais, patrimoniais ou reputacionais;
- Violação de direitos fundamentais.

3.1.4.
CLASSIFICAÇÃO DO RISCO

Combinação entre probabilidade e impacto, resultando em:
- Risco baixo;
- Risco médio;
- Risco alto ou crítico.

3.2
O QUE DEVE CONTER NO MAPA DE RISCOS

Um mapa de riscos deve conter, no mínimo:

1. Processo ou atividade de tratamento;
2. Descrição do risco identificado;
3. Dados pessoais envolvidos;
4. Categoria dos titulares;
5. Probabilidade do risco;
6. Impacto aos titulares;
7. Nível de risco (inicial);
8. Controles existentes;
9. Medidas mitigadoras propostas;
10. Nível de risco residual;
11. Responsável pelo tratamento;
12. Prazo para implementação das medidas.

3.3
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o documento técnico que descreve e avalia os impactos de uma ou mais operações de tratamento de dados pessoais que possam gerar riscos relevantes aos direitos e liberdades dos titulares, bem como as medidas adotadas para mitigá-los.

O RIPD é recomendado, especialmente, quando o tratamento envolver:
- Dados pessoais sensíveis;
- Dados de crianças e adolescentes;
- Uso de novas tecnologias;
- Monitoramento sistemático de titulares;
- Tratamento em larga escala;
- Compartilhamento amplo de dados;
- Decisões automatizadas;
- Risco identificado no mapa de riscos.

A estruturação do RIPD requer as seguintes informações:

a) Identificação do controlador
Órgão/entidade;
Unidade responsável;
Encarregado pelo tratamento de dados.

b) Descrição do tratamento
Finalidades;
Fluxo do tratamento;
Categorias de dados e titulares;
Sistemas utilizados;
Compartilhamentos e operadores.

c) Fundamentação legal
Bases legais aplicáveis;
Conformidade com os princípios da LGPD.

d) Avaliação da necessidade e proporcionalidade
Adequação do tratamento à finalidade;
Minimização dos dados;
Alternativas menos invasivas.

e) Identificação e análise dos riscos
Riscos aos direitos e liberdades dos titulares;
Classificação dos riscos (com base no mapa de riscos).

f) Medidas de mitigação
Medidas técnicas;
Medidas administrativas;
Salvaguardas contratuais;
Capacitação e governança.

g) Avaliação do risco residual
Risco após adoção das medidas;
Aceitação ou necessidade de ajustes adicionais.

h) Conclusão e recomendações
Viabilidade do tratamento;
Condicionantes para continuidade;
Plano de ação.

Mais do que exigências formais, esses instrumentos permitem **antecipar riscos, prevenir danos e demonstrar conformidade,** especialmente em contextos de alta complexidade e sensibilidade, típicos da Administração Pública.

4 ESTRUTURA ORGANIZACIONAL

A estrutura organizacional em proteção de dados consiste no conjunto de papéis, instâncias decisórias, fluxos de comunicação e instrumentos normativos destinados a assegurar que o tratamento de dados pessoais ocorra de forma lícita, segura, transparente e responsável, em conformidade com a LGPD e demais normas aplicáveis.

4.1 DESIGNAÇÃO DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

O Encarregado pelo Tratamento de Dados Pessoais é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Agência Nacional de Proteção de Dados (ANPD).

A designação do Encarregado tem por finalidade assegurar a conformidade do tratamento com a LGPD, facilitar o exercício dos direitos dos titulares, centralizar comunicações com a ANPD e orientar servidores e gestores quanto às boas práticas.

Para o desempenho das atribuições elencadas na legislação, é recomendável que este profissional possua conhecimento jurídico-institucional e técnico, autonomia funcional, acesso à alta administração, estrutura de apoio compatível com a complexidade do órgão e não esteja sujeito a conflito de interesses.

4.2 COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS - CGPD

O Comitê Gestor de Proteção de Dados Pessoais – CGPD é instância colegiada e estratégica, responsável por articular, deliberar e supervisionar as ações institucionais relacionadas à proteção de dados pessoais.

O CGPD tem por finalidade promover a governança institucional em proteção de dados, harmonizar decisões entre áreas finalísticas e de apoio, definir diretrizes estratégicas de conformidade, apoiar o encarregado no exercício de suas funções.

Recomenda-se que seja composto de representantes da alta administração, área jurídica, tecnologia da informação, controle interno, ouvidoria, gestão de pessoas e encarregado de dados.

São competências típicas do Comitê:
- Aprovar políticas e normativos internos de proteção de dados;
- Deliberar sobre riscos elevados e RIPDs;
- Definir diretrizes para compartilhamento de dados;
- Acompanhar incidentes relevantes;
- Propor planos de ação e capacitação;
- Monitorar a maturidade institucional em LGPD.

O Regimento Interno do Comitê deve disciplinar, no mínimo:

a. Natureza e finalidade do Comitê;
b. Composição e critérios de designação;
c. Competências;
d. Funcionamento (quórum, reuniões, deliberações);
e. Papel do encarregado;
f. Fluxos decisórios e de comunicação;
g. Registro e publicidade dos atos;
h. Revisão e atualização do regimento.

4.3 PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS PESSOAIS

O Programa de Governança em Proteção de Dados Pessoais é o conjunto estruturado e contínuo de políticas, processos, controles e mecanismos institucionais voltados à conformidade com a LGPD e à proteção dos direitos fundamentais dos titulares.

Não se trata de ação pontual, mas de política institucional permanente.
O Programa tem por finalidade estruturar a conformidade contínua com a LGPD, prevenir riscos e incidentes, integrar proteção de dados à gestão pública, demonstrar accountability à ANPD e aos órgãos de controle e à sociedade.

Os objetivos do Programa de Governança são:

- Garantir tratamento lícito e proporcional de dados pessoais;
- Proteger os direitos dos titulares;
- Estabelecer cultura organizacional de proteção de dados;
- Padronizar processos e decisões;
- Fortalecer a segurança da informação.

Um Programa de Governança deve conter, ao menos:

a) Base normativa
Política de Privacidade;
Política de Segurança da Informação;

b) Estrutura organizacional
Encarregado;
Comitê Gestor;
Pontos focais nas unidades;
c) Instrumentos operacionais
Inventário de dados;
Mapa de riscos;
RIPD;
Procedimentos para atendimento ao titular;
Plano de resposta a incidentes;

d) Capacitação e cultura
Treinamentos periódicos;
Comunicação institucional;

e) Monitoramento e revisão
Indicadores de maturidade;
Auditorias internas;
Atualização contínua.

Esses elementos não se sobrepõem, mas se complementam, formando a espinha dorsal da governança em proteção de dados.

A estrutura organizacional em proteção de dados pessoais é condição indispensável para a efetividade da LGPD no setor público. A adequada designação do encarregado, a instituição de um Comitê Gestor com regimento interno e a implementação de um Programa de Governança asseguram:

- Segurança jurídica;
- Eficiência administrativa;
- Proteção dos direitos fundamentais;
- Conformidade sustentável e auditável

5 POLÍTICAS DE PROTEÇÃO DE DADOS PESSOAIS

As Políticas de Proteção de Dados são instrumentos normativos institucionais que estabelecem diretrizes, regras, responsabilidades e procedimentos para o tratamento de dados pessoais, assegurando a conformidade com a LGPD, a transparência aos titulares, a padronização de condutas internas e a demonstração de accountability.

5.1 POLÍTICA DE PRIVACIDADE

A Política de Privacidade é o documento público que informa de forma clara, acessível e transparente como a instituição trata os dados pessoais dos titulares, descrevendo quais dados são coletados; para qual finalidades, quais os fundamentos legais aplicáveis; como são protegidos e quais direitos assistem aos titulares.

Uma Política de Privacidade deve conter, no mínimo:

a) Identificação do controlador
Órgão/entidade responsável;
Base legal da atuação pública.

b) Finalidades do tratamento
Descrição clara das finalidades institucionais;
Vinculação às políticas públicas ou competências legais.

c) Dados pessoais tratados
Categorias de dados pessoais;
Indicação de dados sensíveis (quando houver).

d) Fundamentos legais
Bases legais aplicáveis (art. 7º e art. 23 da LGPD);
Hipóteses específicas para dados sensíveis (art.11 da LGPD).

e) Compartilhamento de dados
Com outros órgãos;
Com operadores e terceiros;
Critérios e salvaguardas.

f) Direitos dos titulares
Lista dos direitos previstos no art. 18 da LGPD;
Procedimentos para exercício desses direitos.

g) Medidas de segurança
Referência às práticas de segurança adotadas.

h) Prazo de retenção
Critérios de guarda e eliminação dos dados.

i) Canal de comunicação
Contato do encarregado de dados.

j) Atualizações
Forma de comunicação de alterações na política.

5.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A Política de Segurança da Informação é o instrumento normativo que define as diretrizes, responsabilidades e controles destinados a proteger informações e dados pessoais contra acesso não autorizado, incidentes de segurança, vazamentos e perda, alteração ou destruição indevida.

A PSI tem por finalidades:

- Proteger a confidencialidade, integridade e disponibilidade da informação;
- Previnir incidentes e violações de dados pessoais;
- Atender exigências legais e normativas;
- Orientar condutas de servidores e terceiros; e
- Reduzir impactos jurídicos, financeiros e reputacionais.

Deve conter:

a) Objetivo e escopo
Abrangência da política;
Tipos de informações protegidas.

b) Princípios de segurança
Confidencialidade;
Integridade;
Disponibilidade;
Autenticidade.

c) Papéis e responsabilidades
Alta administração;
TI;
Encarregado;
Usuários/servidores;
Terceiros.

d) Controles de acesso
Perfis de usuários;
Gestão de credenciais.

e) Uso aceitável dos recursos
Sistemas, redes, e-mails, dispositivos.

f) Gestão de incidentes
Identificação;
Comunicação;
Resposta e mitigação.

g) Classificação da informação
Pública, restrita, sigilosa;
Integração com a LAI.

h)Responsabilização
Consequências pelo descumprimento.

5.3 POLÍTICA DE COOKIES

A Política de Cookies é o documento que informa ao usuário sobre a utilização de cookies e tecnologias similares em sítios eletrônicos e sistemas digitais, explicando que tipos de cookies são utilizados, para quais finalidades e como o usuário pode gerenciá-los.

A Política de Cookies deve conter ao menos o seguinte conteúdo:

a) O que são cookies
Conceito acessível ao cidadão.

b) Tipos de cookies utilizados
Necessários;
Funcionais;
Analíticos;
De terceiros.

c) Finalidades
Funcionamento do site;
Melhoria de serviços;
Estatísticas.

d) Base legal
Consentimento (quando aplicável);
Legítimo interesse / execução de políticas públicas (quando cabível).

e) Gerenciamento pelo usuário
Como aceitar, recusar ou excluir cookies.

f) Tempo de armazenamento
Cookies de sessão;
Cookies persistentes.

g) Atualizações
Comunicação de alterações na política.

A criação e implementação das **Políticas de Privacidade, Segurança da Informação e Cookies** constituem **pilares normativos da governança em proteção de dados**, especialmente no setor público. Elas transformam os princípios da LGPD em **regras claras, operacionais e auditáveis,** fortalecendo a proteção de direitos fundamentais e a segurança jurídica institucional.

6 ADEQUAÇÕES DE CONTRATOS E RELAÇÃO COM TERCEIROS

A adequação contratual em proteção de dados pessoais consiste na revisão, atualização e padronização dos instrumentos jurídicos firmados pela instituição — contratos, convênios, termos de cooperação, ajustes, formulários, editais e documentos correlatos — para assegurar que o tratamento de dados pessoais realizado direta ou indiretamente esteja em conformidade com a LGPD.

A adequação de terceiros refere-se ao processo de avaliação, classificação e monitoramento da conformidade dos fornecedores, prestadores de serviços, parceiros e operadores que tratam dados pessoais em nome do controlador.

6.1 IMPORTÂNCIA DA ADEQUAÇÃO CONTRATUAL E DA GESTÃO DE TERCEIROS

A ausência de cláusulas adequadas ou de controle sobre terceiros é uma das fontes de risco em LGPD. Por este motivo, são razões centrais da importância:

a) Responsabilização solidária
O controlador pode ser responsabilizado por falhas do operador (art. 42).

b) Segurança jurídica
Define papéis, limites e responsabilidades;
Reduz litígios e apontamentos de órgãos de controle.

c) Proteção dos titulares
Garante que terceiros adotem medidas equivalentes de segurança.

d) Accountability
Demonstra diligência e governança ativa.

e) Conformidade com contratações públicas
Atendimento à Lei nº 14.133/2021 (gestão de riscos, cláusulas obrigatórias).

6.2 REVISÃO DE CONTRATOS E DOCUMENTOS PARA ATENDIMENTO À LGPD

A revisão deve contemplar:

- Contratos administrativos;
- Convênios, termos de cooperação e parcerias;
- Editais de licitação;
- Termos de referência e projetos básicos;
- Acordos de compartilhamento de dados;
- Formulários físicos e digitais;
- Políticas internas e manuais operacionais;
- Sistemas e plataformas digitais.

6.3 ELEMENTOS ESSENCIAIS A SEREM REVISADOS OU INCLUÍDOS

a) Definição clara dos papéis
Identificação do controlador e do operador;
Limitação do tratamento às finalidades contratadas.

b) Finalidade e base legal do tratamento
Vinculação às competências legais e à política pública;
Vedação a usos incompatíveis.

c) Obrigações do operador
Tratar dados apenas conforme instruções do controlador;
Garantir confidencialidade;
Adotar medidas técnicas e administrativas de segurança;
Restringir subcontratações.

d) Segurança da informação
Adoção de padrões mínimos de segurança;
Gestão de acessos;
Registro de operações relevantes.

e) Incidentes de segurança
Comunicação imediata ao controlador;
Cooperação na resposta ao incidente;
Apoio na comunicação à ANPD e aos titulares.

f) Direitos dos titulares
Apoio ao controlador no atendimento das requisições;
Fluxos e prazos definidos.

g) Auditoria e fiscalização
Direito de auditoria ou comprovação de conformidade;
Prestação de informações sempre que solicitado.

h) Encerramento do contrato
Devolução, eliminação ou anonimização dos dados;
Comprovação formal das providências adotadas.

A adequação não se limita aos contratos formais. Devem ser revisados:

- Fichas cadastrais;
- Formulários de inscrição;
- Sistemas eletrônicos;
- Termos de consentimento (quando aplicável);
- Avisos de privacidade e textos informativos.

O objetivo é assegurar clareza, necessidade, proporcionalidade e segurança.

6.4 DIAGNÓSTICO DE ADEQUAÇÃODE TERCEIROS (FORNECEDORES E PARCEIROS)

O diagnóstico de adequação de terceiros em LGPD é o processo de avaliação estruturada do nível de conformidade dos fornecedores, operadores e parceiros que realizam tratamento de dados pessoais em nome da instituição.

A finalidade deste diagnóstico é:
- Identificar riscos jurídicos e operacionais;
- Classificar terceiros por nível de risco;
- Definir exigências proporcionais;
- Subsidiar decisões de contratação e renovação;
- Fortalecer a governança e a segurança da informação.

Etapas que devem ser observadas:
a) Identificação dos terceiros relevantes
Quais tratam dados pessoais;
Quais tratam dados sensíveis ou em larga escala.

b) Classificação do risco do terceiro
Critérios usuais:
Tipo e volume de dados;
Categoria de titulares;
Acesso direto ou indireto;
Uso de tecnologia ou nuvem;
Histórico de incidentes.

c) Avaliação de conformidade
Por meio de:
Questionários de adequação;
Análise documental;
Evidências técnicas e organizacionais.

d) Definição de medidas
Ajustes contratuais;
Exigência de políticas e controles;
Capacitação;
Monitoramento contínuo.

O diagnóstico deve avaliar, ao menos:
- Governança em proteção de dados;
- Existência de encarregado ou responsável;
- Políticas de privacidade e segurança;
- Medidas técnicas adotadas;
- Gestão de incidentes;
- Controle de acessos;
- Subcontratações;
- Treinamento de colaboradores;
- Conformidade contratual;
- Mecanismos de prestação de contas.

A adequação de contratos e a gestão da relação com terceiros são pilares da conformidade com a LGPD. No setor público, tais medidas asseguram proteção efetiva dos dados pessoais, segurança jurídica, eficiência administrativa e responsabilidade institucional, mitigando riscos que frequentemente extrapolam os limites do próprio órgão.

7 DIREITOS DOS TITULARES DE DADOS PESSOAIS

Os direitos dos titulares de dados pessoais constituem o núcleo de proteção da LGPD, garantindo às pessoas naturais controle, informação e autodeterminação sobre o tratamento de seus dados, inclusive quando realizado pelo Poder Público.

O titular tem direito a obter do controlador, em relação aos seus dados pessoais:

- **Confirmação da existência de tratamento;**
- **Acesso aos dados;**
- **Correção de dados incompletos, inexatos ou desatualizados;**
- **Anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade;
- **Portabilidade dos dados,** quando aplicável;
- **Eliminação dos dados tratados com consentimento,** ressalvadas as hipóteses legais;
- **Informação sobre compartilhamentos;**
- **Informação sobre a possibilidade de não consentir** e as consequências;
- **Revogação do consentimento;**
- **Revisão de decisões automatizadas**, quando houver.

Importa mencionar que no setor público nem todos os direitos são absolutos (ex.: eliminação pode ser limitada por obrigação legal), a portabilidade e o consentimento tem aplicação restrita e deve haver compatibilização com a guarda obrigatória, o interesse público, as políticas públicas e a proteção de terceiros.

7.1 GESTÃO DE DOCUMENTOS E RELAÇÃO COM OS DIREITOS DOS TITULARES

A gestão documental é condição para o atendimento efetivo dos direitos dos titulares, observados os aspectos relevantes, tais como:

- Localização dos dados;
- Controle de versões;
- Classificação da informação (LAI);
- Prazos de guarda e descarte;
- Registro das respostas fornecidas.

A falta de gestão documental adequada pode ocasionar que o atendimento ao titular seja incompleto ou inviável.

7.2
FLUXO INSTITUCIONAL DE RESPOSTA AOS TITULARES

O **fluxo de resposta aos titulares** define **como, por quem e em que prazo** a Administração Pública deve tratar as solicitações relativas aos direitos previstos na LGPD, garantindo padronização, rastreabilidade, segurança jurídica e transparência, e deve conter as seguintes etapas:

a) Recebimento da solicitação
Canal oficial (formulário eletrônico, ouvidoria, protocolo);
Identificação do solicitante;
Registro do pedido.

b) Análise preliminar
Verificação da identidade do titular ou representante legal;
Classificação do tipo de direito solicitado;
Avaliação de competência do órgão.

c) Encaminhamento interno
À unidade responsável pelo tratamento;
À área jurídica, quando necessário;
Ao encarregado de dados.

d) Análise técnica e jurídica
Verificação da existência do dado;
Avaliação de base legal;
Conciliação com LAI, sigilo e interesse público.

e) Elaboração da resposta
Fundamentação clara;
Linguagem acessível;
Indicação de limites legais, se houver.

f) Resposta ao titular
Dentro do prazo legal (LGPD e LAI);
Pelo canal adequado;
Com registro e arquivamento.

7.3 PROTOCOLOS DE RESPOSTA AOS TITULARES

Os Protocolos de Resposta aos Titulares são documentos internos que padronizam o tratamento das solicitações, definindo procedimentos, responsáveis, critérios de análise e modelos de respostas.
Desta forma, evitam respostas divergentes, reduzem riscos jurídicos, facilitam capacitação de servidores e demonstram accountability.

Cada protocolo deve conter:
- Tipo de direito exercido;
- Descrição do procedimento;
- Documentos necessários;
- Área responsável;
- Prazos;
- Hipóteses de deferimento, parcial ou indeferimento;
- Fundamentação legal;
- Modelo de resposta.

São exemplos de protocolos específicos:
- Protocolo de acesso a dados pessoais;
- Protocolo de correção de dados;
- Protocolo de eliminação/anonimização;
- Protocolo de revogação de consentimento;
- Protocolo de revisão de decisão automatizada.

7.4 FORMULÁRIOS DE COLETA DE CONSENTIMENTO (QUANDO APLICÁVEL)

O consentimento é base legal residual no setor público, devendo ser utilizado quando não houver obrigação legal, não se tratar de política pública e/ou o tratamento for facultativo ao cidadão.

Nos termos da LGPD, o consentimento deve ser livre, informado, inequívoco, para finalidades específicas e com a possibilidade de revogação.

Um formulário adequado deve ter linguagem clara e acessível, consentimento destacado, registro de manifestação, facilidade de revogação e compatibilidade com meios físicos e digitais. Portanto, em sua estrutura devem estar presentes os seguintes elementos:

- Identificação do controlador;
- Finalidade específica do tratamento;
- Tipos de dados coletados;
- Base legal (consentimento);
- Prazo de retenção;

- Compartilhamentos;
- Direitos do titular;
- Informação sobre revogação;
- Canal de contato com o encarregado;
- Manifestação expressa de concordância.

A gestão dos direitos dos titulares, aliada a fluxos bem definidos, protocolos padronizados e formulários adequados, concretiza a LGPD no cotidiano da Administração Pública.

8 SISTEMA DE TRANSPARÊNCIA NA ADMINISTRAÇÃO PÚBLICA

O Sistema de Transparência consiste no conjunto de normas, processos, instâncias decisórias e controles destinados a assegurar o direito fundamental de acesso à informação pública, a proteção de dados pessoais e da intimidade dos titulares e a conformidade simultânea com a Lei nº 12.527/2011 - Lei de Acesso à Informação e a LGPD. Não se trata de optar entre transparência ou privacidade, mas de compatibilizar direitos fundamentais, conforme o caso concreto.

A relação entre LGPD e LAI é de complementaridade, não de hierarquia, considerando que a primeira não revogou a segunda. Assim, a LAI regula o acesso à informação, enquanto a LGPD regula o tratamento de dados pessoais, devendo estas serem aplicadas de forma harmônica e complementar.
Neste contexto, o Enunciado nº 04/2022 – CGU apresenta o seguinte entendimento:

ENUNCIADO Nº 4, DE 10 DE MARÇO DE 2022

Nos pedidos de acesso à informação e respectivo recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), vez que:

A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e

A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos.

WAGNER DE CAMPOS ROSARIO
Ministro

Sendo assim, a LGPD não constitui fundamento, por si só, para negativa de acesso à informação pública, devendo haver ponderação entre a transparência e a privacidade, visto que dado pessoal não é, por si só, informação sigilosa. Quando houver necessidade, conforme o caso concreto, a informação solicitada pode ser fornecida com supressão dos dados pessoais.

Portanto, para que haja um fluxo integrado entre LGPD e LAI na análise dos pedidos de acesso à informação, recomenda-se sejam observadas as seguintes etapas:

a) Identificação da natureza da informação
Informação pública?
Informação com dado pessoal?
Dado pessoal sensível?

b) Análise jurídica e técnica
Finalidade do pedido;
Interesse público envolvido;
Risco aos direitos do titular;
Necessidade/Possibilidade de anonimização.

c) Aplicação dos princípios da LGPD
Finalidade;
Necessidade;
Proporcionalidade;
Transparência.

d) Decisão fundamentada
Concessão integral;
Concessão parcial (com ocultação/anonimização);
Negativa fundamentada.

e) Resposta ao solicitante
Clareza;
Fundamentação legal;
Indicação de recurso, se cabível.

O Sistema de Transparência, quando estruturado à luz da LAI e da LGPD, permite à Administração Pública conciliar publicidade e proteção de dados, evitando tanto a opacidade indevida quanto a exposição excessiva de informações pessoais.

9 RESPOSTAS A INCIDENTES DE SEGURANÇA

Incidente de segurança é qualquer evento adverso que resulte, de forma acidental ou ilícita, em acesso não autorizado; destruição; perda; alteração; vazamento; e divulgação indevida de dados pessoais.
O foco da LGPD está nos incidentes que possam acarretar risco ou dano relevante aos titulares de dados.

9.1 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA (PRI)

O Plano de Resposta a Incidentes de Segurança é o documento institucional que define fluxos, papéis, responsabilidades, procedimentos e prazos para identificação, contenção, análise, mitigação e encerramento de incidentes de segurança que envolvam dados pessoais.

Trata-se de instrumento preventivo e reativo, essencial ao Programa de Governança em Proteção de Dados, tendo por finalidades:

- Minimizar impactos aos titulares;
- Garantir resposta rápida e coordenada;
- Atender às exigências do art. 48 da LGPD;
- Padronizar decisões e comunicações;
- Preservar evidências e registros;
- Demonstrar accountability.

O PRI deve conter, no mínimo:
a) Escopo e definições
Conceito de incidente;
Tipos de incidentes cobertos;
Critérios de classificação (baixo, médio, alto impacto).

b) Estrutura organizacional de resposta
Equipe de Resposta a Incidentes;
Papéis da TI, área jurídica, encarregado, comunicação e alta gestão;
Responsáveis por decisão.

O fluxo de resposta a incidentes está sujeito as seguintes etapas:

- Detecção e identificação
- Registro do incidente
- Análise preliminar
- Contenção imediata
- Avaliação de impacto
- Mitigação e correção
- Comunicação (quando aplicável)
- Encerramento e lições aprendidas

Os riscos devem ser avaliados de acordo com os seguintes critérios:

- Tipo de dados afetados;
- Volume de dados;
- Categoria dos titulares;
- Possibilidade de dano;
- Facilidade de identificação do titular.

9.2
PROTOCOLOS DE COMUNICAÇÃO DE INCIDENTES

O art. 48 da LGPD estabelece que o controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.
A comunicação deve ser feita de forma tempestiva, clara e fundamentada.

9.2.1.
PROTOCOLO DE COMUNICAÇÃO INTERNA

Antes da comunicação externa, deve haver fluxo interno, prevendo:
a. Notificação imediata à TI;
b. Comunicação ao encarregado de dados;
c. Acionamento da área jurídica;
d. Informação à alta administração;
e. Avaliação colegiada (Cômite - quando necessário).

9.2.2.
PROTOCOLO DE COMUNICAÇÃO À ANPD

A comunicação de incidentes deve ser realizada à ANPD quando houver risco ou dano relevante aos titulares, devendo conter no mínimo as seguintes informações:

a. Descrição da natureza dos dados afetados;
b. Informações sobre os titulares envolvidos;
c. Indicação das medidas técnicas e de segurança utilizadas;
d. Riscos relacionados ao incidente;
e. Medidas adotadas ou propostas para mitigar os efeitos;
f. Motivo da demora, se houver;
g. Contato do encarregado.

A ANPD disponibiliza o passo a passo para promover a informação em pauta por meio o processo de Comunicação de Incidente de Segurança (CIS), disponível no seguinte endereço eletrônico: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

9.2.3.
PROTOCOLO DE COMUNICAÇÃO AOS TITULARES

Os incidentes de segurança devem ser comunicados ao titular de dados quando ocasionarem dano relevante, contendo ao menos as seguintes informações, utilizando linguagem clara e acessível:

- Descrição objetiva do ocorrido;
- Dados potencialmente afetados;
- Riscos envolvidos;
- Medidas adotadas pela instituição;
- Recomendações ao titular;
- Canal de atendimento e contato do encarregado.

9.2.4.
COMUNICAÇÃO ENTRE CONTROLADOR E OPERADOR

Nos contratos com terceiros é importante que conste a obrigatoriedade de comunicação imediata do incidente ao controlador; de cooperação técnica e jurídica; de fornecimento de informações completas; e de apoio à comunicação à ANPD e aos titulares.

9.2.5.
REGISTRO E DOCUMENTAÇÃO DO INCIDENTE

Todo incidente de segurança, independente da gravidade, deve gerar um registro formal, por meio de um relatório técnico, avaliando os impactos, estabelecendo quais as medidas corretivas serão aplicadas e atualizando o mapa de riscos.
Esse registro é essencial para fins de auditorias, fiscalizações, defesas institucionais e aprendizado organizacional.
A resposta a incidentes de segurança é elemento indispensável da governança em proteção de dados. A criação de um Plano de Resposta a Incidentes, aliada a Protocolos claros de Comunicação, permite à Administração Pública agir com rapidez, responsabilidade e transparência.

10 TREINAMENTO E COMUNICAÇÃO INTERNA

A LGPD exige não apenas medidas técnicas e jurídicas, mas também medidas organizacionais e comportamentais. A maioria dos incidentes de segurança decorre de falhas humanas, desconhecimento ou práticas inadequadas no uso de dados pessoais.

Estes erros se manifestam por meio de situações, tais como:

- Abertura de anexos infectados ou fornecimento de credenciais em páginas falsas.
- Uso de senhas fracas ou repetidas, comprometendo múltiplos acessos com um único vazamento.
- Configuração incorreta de sistemas, concedendo permissões excessivas, falta de segmentação e ambientes expostos.
- Uso de dispositivos pessoais, que dificultam o controle e o monitoramento da superfície de ataque.

Desta forma, a promoção de ações de aculturamento, capacitação e comunicação interna é essencial para prevenir incidentes de segurança; assegurar o respeito aos direitos dos titulares; padronizar condutas dos agentes públicos; garantir a efetividade das políticas institucionais; e demonstrar accountability perante a ANPD e órgãos de controle.

O aculturamento é o processo contínuo de internalização dos valores, princípios e boas práticas da proteção de dados por todos os agentes públicos, independentemente da função exercida, superando o treinamento formal, envolvendo mudança de mentalidade e de comportamento organizacional.
As ações de conscientização visam a criação de um senso de responsabilidade coletiva, reduzindo práticas informais e inseguras, fortalecendo a cultura de proteção de dados e integrando a LGPD às rotinas administrativas.

Estas ações podem ser promovidas através dos seguintes instrumentos, utilizando linguagem simples, exemplos práticos e foco na prevenção:

- Campanhas institucionais periódicas;
- Cartilhas e guias práticos;
- Vídeos curtos e informativos;
- Semana ou mês da proteção de dados;
- Divulgação de casos práticos (anonimizados);
- Inserção do tema em eventos internos;
- Comunicação sobre boas práticas.

10.2 COMUNICAÇÃO INTERNA SOBRE A IMPLANTAÇÃO DA LGPD

A comunicação interna é o conjunto de estratégias institucionais destinadas a informar, orientar e engajar os agentes públicos sobre a implantação, evolução e responsabilidades relacionadas à LGPD.

É um instrumento importante para tornar a implantação da LGPD transparente, esclarecer papéis e responsabilidades, divulgar normas internas e políticas, orientar sobre canais de denúncia e reforçar mensagens de prevenção.

Pode ser realizada por canais de comunicação institucionais como e-mails, murais físicos e digitais, portais internos, newsletters, entre outros.

O treinamento e a comunicação interna são elementos essenciais para a efetividade da LGPD na Administração Pública. Sem servidores conscientes, capacitados e bem informados, não há governança possível em proteção de dados.

A adoção de ações contínuas de aculturamento, capacitações estruturadas e comunicação institucional transparente fortalece a prevenção de riscos, a proteção dos titulares e a legitimidade da atuação estatal.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 janeiro 2026.

GOVERNO FEDERAL. **Guias operacionais para adequação à LGPD.** 11 abr. 2019. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em: 20 janeiro 2026.

GOVERNO FEDERAL. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). 10 abr. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 20 janeiro 2026.

PARANÁ. Decreto nº 6.474, de 14 de dezembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná. Disponível em: <https://www.legislacao.pr.gov.br/legislacao/pesquisarAto.do?action=exibir&codAto=244066&indice=1&totalRegistros=7&dt=18.4.2021.10.54.41.988>. Acesso em: 20 janeiro 2026.

CGE

CONTROLADORIA GERAL
DO ESTADO DO PARANÁ