Cartilha de
Proteção de Dados Pessoais

LGPD: o que todo Servidor precisa saber

GOVERNO DA PARAÍBA

Governador

João Azevêdo Lins Filho

Vice-Governador

Lucas Ribeiro Novais de Araújo

Conselho Gestor de Proteção de Dados Pessoais do Estado da Paraíba

Fábio Brito Ferreira (Procurador Geral do Estado e Presidente do CGPDP)

Carlos Tibério Limeira Santos Fernandes (Secretário de Estado da Administração)

Antônio Roberto de Sousa Paulino (Secretário Chefe do Governo)

Marialvo Laureano dos Santos Filho (Secretário de Estado da Fazenda)

Letácio Tenório Guedes Júnior (Secretário Chefe da Controladoria Geral do Estado)

Comitê Executivo de Proteção de Dados Pessoais do Estado da Paraíba

Ana Carolina Domingos Matias de Araújo
(representante da Secretaria de Estado da Administração - SEAD)

Severino Gilson Peixoto de Oliveira Júnior
(representante da Controladoria Geral do Estado - CGE)

Júlia Monteiro Lucena Agra
(representante da CODATA)

João Bosco Germano Júnior
(representante da Secretaria de Estado da Fazenda - SEFAZ)

Leonardo Ventura Maciel
(representante da Procuradoria Geral do Estado - PGE)

Laís Dantas de Araújo
(representante da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPLAG)

Histórico de versões:

Data	Versão	Descrição	Autor
xx/xx/2025	1.0	Primeira versão da cartilha LGPD	Comitê Executivo de Proteção de Dados Pessoais do Estado da Paraíba

Sumário

Apresentação e Objetivos da Cartilha

A presente Cartilha de Proteção de Dados Pessoais foi elaborada pelo **Comitê Executivo de Proteção de Dados Pessoais do Estado da Paraíba**, com o objetivo de orientar e sensibilizar os(as) servidores(as) quanto à aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito da Administração Pública estadual.

O tratamento de dados pessoais no setor público deve ocorrer de forma transparente, ética e em conformidade com a legislação vigente, assegurando direitos fundamentais de liberdade, privacidade e proteção das informações dos cidadãos. Essa responsabilidade recai sobre todos os agentes públicos, uma vez que o Estado lida diariamente com um grande volume de informações sensíveis e estratégicas.

Assim, esta cartilha busca oferecer informações práticas e diretas, funcionando como um guia para o correto tratamento de dados pessoais nas atividades administrativas. **Mais do que cumprir uma exigência legal, a proteção de dados representa o fortalecimento da confiança da sociedade na gestão pública, promovendo maior segurança jurídica, eficiência e respeito aos direitos dos cidadãos paraibanos.**

Glossário: Conceitos Básicos

Agentes de tratamento: o controlador e o operador.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Agência Nacional de Proteção de Dados (ANPD): Antiga Autoridade Nacional de Proteção de Dados. É o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional". Cabe à ANPD, por exemplo, receber denúncias e determinar multas e outras sanções administrativas a quem não cumprir a LGPD.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Cidadão: nesta cartilha o termo cidadão será considerado em sentido amplo como sinônimo de habitante, usuário de serviços públicos, pessoa ou indivíduo titular de dados pessoais.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

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

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dado pessoal de criança e de adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Dado pessoal anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Glossário: Conceitos Básicos

Encarregado(a) pelo Tratamento dos Dados Pessoais (DPO): pessoa indicada pelo controlador e operador corporativo para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). A LGPD utiliza o termo encarregado(a), no entanto muitas pessoas conhecem como DPO (Data Protection Officer).

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

Pseudonimização: o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Ou seja, é uma espécie de anonimização reversível.

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Servidor público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Violação de dados pessoais: é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Conhecendo a LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a norma brasileira que define como os dados pessoais dos titulares devem ser coletados, usados, armazenados e compartilhados. Seu objetivo é proteger os direitos fundamentais de liberdade, privacidade e segurança das pessoas.

Na prática, a LGPD estabelece regras claras para que órgãos públicos, empresas e pessoas naturais tratem informações de forma transparente, justa e responsável.

Os principais pilares da LGPD são:

Transparência: o cidadão tem o direito de saber como seus dados estão sendo utilizados.

Finalidade: os dados só podem ser usados para objetivos legítimos, específicos e informados ao titular.

Segurança: os dados devem ser protegidos contra acessos não autorizados, perdas ou vazamentos.

Necessidade: só devem ser coletados os dados realmente indispensáveis para a atividade.

Responsabilização: quem trata os dados deve demonstrar que adota medidas para cumprir a lei.

Direitos do titular: toda pessoa pode acessar, corrigir ou solicitar a exclusão de seus dados, entre outros direitos previstos.

Com a LGPD, o setor público reforça seu compromisso com a ética, a confiança da sociedade e a proteção dos cidadãos, garantindo que cada dado pessoal seja tratado com respeito.

Afinal, o que são Dados Pessoais?

Dados pessoais são todas as informações que permitem identificar uma pessoa, de forma direta ou indireta. Ou seja, qualquer dado que, sozinho ou em conjunto com outras informações, revele a identidade de uma pessoa natural — seja ela beneficiária de políticas públicas, servidora pública, cliente, entre outros.

No serviço público, lidamos com dados pessoais diariamente, muitas vezes sem perceber. Por isso, é fundamental reconhecer que essas informações precisam de cuidado e proteção.

Exemplos de dados pessoais no dia a dia do serviço público:

- Nome completo
- CPF
- RG
- Endereço e número de telefone descritos em diversos tipos de documentos, como em comprovantes de residência, contratos e outros
- E-mail institucional ou pessoal
- Data de nascimento
- Matrícula funcional
- Prontuário médico ou informações de saúde
- Dados bancários para pagamento de salários ou benefícios
- Histórico escolar ou acadêmico
- Fotos e imagens em sistemas de segurança

Esses dados, quando usados de forma inadequada ou expostos sem autorização, podem gerar riscos para o cidadão e responsabilidade para o órgão público.

Lembre-se: proteger dados pessoais é proteger pessoas.

Funções e responsabilidades no tratamento de dados pessoais

A Lei Geral de Proteção de Dados (LGPD) estabelece papéis específicos para quem lida com dados pessoais. Esses papéis são denominados agentes de tratamento e possuem responsabilidades distintas e complementares, a saber:

Controlador:
quem toma as decisões sobre o tratamento dos dados pessoais.

Operador:
quem realiza o tratamento em nome do controlador, seguindo suas instruções.

1. O Controlador no Setor Público

De acordo com o art. 5º, VI, da LGPD, o controlador é a pessoa jurídica de direito público — no caso do Estado da Paraíba, o **Governo do Estado.** Isso significa que, em uma eventual ação judicial, é o Estado da Paraíba quem figura como responsável legal pelo tratamento de dados pessoais realizado por seus órgãos da administração direta.

No entanto, por força do princípio da desconcentração administrativa, **as Secretarias e os demais órgãos estaduais exercem funções típicas de controlador.** Na prática, isso quer dizer que cada órgão:

- deve indicar um **Encarregado(a) pelo Tratamento dos Dados Pessoais (DPO), considerando as deliberações do Conselho Gestor de Proteção de Dados Pessoais da Paraíba;**
- precisa atender diretamente às solicitações dos titulares de dados pessoais e às determinações da ANPD;
- deve manter estruturas adequadas para receber requerimentos e gerenciar incidentes de segurança;
- responde administrativamente pelas suas próprias decisões sobre tratamento de dados pessoais.

→ Portanto, ainda que juridicamente o controlador seja o Governo do Estado da Paraíba, cada Secretaria deve atuar como controlador em suas funções, sem se eximir de suas obrigações.

Importante destacar que essa lógica se aplica apenas à **administração direta do Estado da Paraíba,** formada pelas Secretarias de Estado e demais órgãos sem personalidade jurídica própria (como a Procuradoria Geral do Estado, a Polícia Civil, a Controladoria Geral do Estado, entre outros). Já os componentes da **administração indireta** — autarquias, fundações públicas, empresas públicas e sociedades de economia mista — possuem personalidade jurídica própria, razão pela qual cada uma dessas entidades será considerada **controladora independente**, responsável por suas próprias decisões e obrigações perante a LGPD.

Exemplo prático – Estado da Paraíba:

A Secretaria de Saúde da Paraíba contrata uma empresa para implantar um sistema eletrônico de prontuários médicos.

O controlador é o **Estado da Paraíba,** mas a **Secretaria de Estado da Saúde**, na prática, exerce funções típicas de controlador: decide quais dados serão coletados, como serão armazenados e quem terá acesso.	Cabe à Secretaria, portanto, designar o Encarregado pelo Tratamento dos Dados Pessoais, responder às demandas da ANPD e comunicar incidentes de segurança.	Caso um titular questione judicialmente o tratamento realizado, a ação será contra o **Estado da Paraíba,** mas administrativamente é a Secretaria que deve prestar contas e adotar as medidas necessárias.

2. O Operador no Setor Público

O operador é a pessoa física ou jurídica que realiza o tratamento de dados em nome do controlador, sempre de acordo com suas instruções.

No Estado da Paraíba, os operadores podem ser tanto empresas contratadas quanto órgãos ou entidades que prestam apoio técnico especializado.

Exemplo prático 1 – CODATA:

A CODATA, quando contratada para desenvolver e hospedar um sistema de gestão escolar para a Secretaria de Educação, atua como operadora. Ela trata os dados pessoais conforme instruções da Secretaria, que é a responsável por definir as regras e finalidades do tratamento.

Exemplo prático 2 – Empresa contratada:

Uma empresa terceirizada de call center contratada pela Secretaria da Fazenda para realizar atendimento ao contribuinte.

- A Secretaria da Fazenda (em nome do Estado) é a **controladora,** pois define quais dados serão tratados e com qual finalidade.
- A empresa de call center é a operador, pois apenas executa as atividades seguindo orientações da Secretaria.

3. Encarregado(a) pelo Tratamento dos Dados Pessoais (ou Data Protection Officer - DPO)

O(A) Encarregado(a) pelo Tratamento dos Dados Pessoais (DPO), também chamado de DPO (Data Protection Officer), é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o órgão, os cidadãos (titulares dos dados) e a Agência Nacional de Proteção de Dados (ANPD).

No Estado da Paraíba, a nomeação do(a) Encarregado(a) e de seu(sua) suplente está prevista no **Decreto Estadual nº 41.238/2021** e regulamentada pela **Resolução do Conselho Gestor de Proteção de Dados Pessoais – CGPDP nº 01/2024.**

Funções do(a) Encarregado(a)

- **Receber e responder demandas dos cidadãos:** aceitar reclamações, esclarecer dúvidas e adotar providências relacionadas ao tratamento de dados pessoais.
- **Atuar como canal com a ANPD:** receber comunicações da Agência e coordenar a resposta do órgão.
- **Orientar e sensibilizar servidores e contratados:** difundir boas práticas e procedimentos seguros no tratamento de dados pessoais.
- **Coordenar a adequação à LGPD:** acompanhar a execução do Programa de Governança em Privacidade, políticas e rotinas internas sobre proteção de dados.
- **Mapear e avaliar processos de tratamento:** identificar como os dados são coletados, utilizados e compartilhados dentro do órgão.
- **Gerenciar incidentes de segurança:** executar e acompanhar medidas de resposta em casos de vazamento ou uso indevido de dados.
- **Garantir transparência:** manter divulgadas, no site institucional, informações de contato para atendimento dos titulares.

Exemplo prático:

Na **Secretaria de Estado da Saúde da Paraíba,** o(a) Encarregado(a) pelo Tratamento dos Dados Pessoais recebe solicitações de cidadãos sobre acesso e correção de informações nos prontuários eletrônicos da rede pública. Caso ocorra um incidente de segurança envolvendo dados de pacientes, caberá a esse(a) Encarregado(a) comunicar à ANPD e orientar a Secretaria sobre as medidas a adotar.

Tratamento de Dados Pessoais no Serviço Público

No setor público, o tratamento de dados pessoais é uma atividade constante: cadastros de servidores, emissão de documentos, execução de políticas sociais, registros de saúde, educação, segurança, entre muitos outros.

Mas afinal, quando e por que o Estado pode tratar dados pessoais?

A LGPD estabelece fundamentos específicos que permitem o tratamento de dados pela Administração Pública, sempre em respeito ao interesse público e aos direitos do cidadão.

Principais fundamentos legais no serviço público:

- Execução de políticas públicas

O Estado pode tratar dados para planejar, implementar e avaliar políticas públicas. Exemplo: Cadastro Único para programas sociais.

- Cumprimento de obrigação legal ou regulatória

Quando há uma lei que exige a coleta e uso de determinados dados. Exemplo: Órgãos de trânsito, como o DETRAN, que registram dados pessoais de motoristas para emissão de CNH.

- Execução de contratos, convênios e parcerias

Dados podem ser tratados quando o cidadão mantém uma relação contratual com o Estado. Exemplo: Bolsistas de pesquisa que assinam termo de compromisso com universidades públicas.

- Proteção da vida e da incolumidade física

Quando o tratamento é necessário para proteger a vida ou a saúde. Exemplo: Hospitais públicos utilizando dados pessoais de pacientes em situações de urgência.

- Tutela da saúde

Específico para ações realizadas por órgãos ou entidades públicas da área da saúde. Exemplo: Campanhas de vacinação que utilizam dados de pacientes para acompanhamento.

- Execução de competências legais

Sempre que um órgão precisa de dados pessoais para exercer as atribuições que a lei lhe conferiu. Exemplo: Secretaria da Fazenda usando dados de contribuintes para arrecadação de tributos.

O Estado precisa do consentimento do cidadão para tratar dados pessoais nessas e outras situações?

Em regra, não. Basta que o caso concreto se enquadre em uma das bases legais previstas na LGPD para que o consentimento seja desnecessário. **Excepcionalmente, quando não houver base legal aplicável, poderá ser solicitado o consentimento do cidadão.** Em todos os casos, deve-se agir com transparência, segurança e responsabilidade, utilizando apenas os dados pessoais necessários para cumprir sua finalidade.

Quais são os direitos do cidadão sobre seus dados?

A LGPD garante a todo titular de dados pessoais um conjunto de direitos para proteger sua privacidade e dar mais controle sobre suas informações pessoais.

No setor público, respeitar esses direitos é essencial para fortalecer a confiança da sociedade na Administração e demonstrar transparência.

Quais são os principais direitos do titular?

Confirmação da existência de tratamento:

O cidadão pode perguntar se seus dados pessoais estão sendo usados pelo órgão público.

Acesso aos dados:

O titular pode solicitar cópia ou consulta de seus dados pessoais em posse do Estado.

Correção de dados pessoais:

Se houver erro (como nome digitado errado ou endereço desatualizado), o cidadão pode pedir a retificação.

Portabilidade dos dados pessoais:

O cidadão pode pedir que seus dados pessoais sejam transferidos do órgão público para outro serviço ou entidade, quando houver essa possibilidade, de forma segura e estruturada.
A aplicação da portabilidade depende de regulamentação específica pela ANPD.

Eliminação dos dados pessoais:

O cidadão pode solicitar que seus dados sejam apagados quando não houver mais motivo legal ou necessidade para o órgão público continuar guardando essas informações.

Anonimização, bloqueio ou eliminação:

Em alguns casos, o titular pode pedir que seus dados sejam bloqueados, tornados anônimos ou eliminados — exceto quando o tratamento é necessário para cumprir obrigação legal ou política pública.

Informação sobre o compartilhamento e possibilidade de não fornecer o consentimento:

O titular tem direito de saber com quais órgãos ou entidades seus dados foram compartilhados. Além disso, tem direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Revisão de decisões automatizadas:

Quando decisões que afetam o cidadão forem tomadas com base apenas em sistemas automatizados (como algoritmos), ele pode solicitar revisão por uma pessoa.

Revogação do Consentimento:

O cidadão tem o direito de retirar a autorização que deu para o uso de seus dados pessoais, sempre que o tratamento depender do seu consentimento.

Explicação sobre o uso dos dados:

O titular pode solicitar informações claras sobre a finalidade do tratamento e a forma como seus dados estão sendo utilizados.

Exemplo prático no setor público:

- Um servidor aposentado pode solicitar à PBPREV a correção de seus dados bancários para garantir o pagamento correto de sua aposentadoria.
- Um cidadão pode pedir à Secretaria de Estado de Saúde acesso ao seu histórico de vacinação registrado no sistema.

Boas práticas para o servidor público

O servidor público é peça-chave na proteção dos dados pessoais na administração pública. A forma como cada um lida com as informações de cidadãos e colegas faz toda a diferença para garantir a confiança, a segurança e a transparência da Administração Pública.

A seguir, algumas boas práticas que devem ser seguidas no dia a dia:

Confidencialidade no atendimento ao público

- ✅ Atenda com discrição, garantindo que só pessoas autorizadas tenham acesso às informações pessoais.
- ✅ Fale de dados pessoais apenas em locais adequados.
- ❌ Não revele informações por telefone ou pessoalmente sem confirmar a identidade de quem pede.

Exemplo: Se alguém ligar pedindo informações sobre o cadastro de outro cidadão, não repasse dados sem confirmar a identidade e a finalidade.

Cuidado com e-mails e documentos

- ✅ Confira o destinatário antes de enviar dados pessoais.
- ✅ Guarde documentos em locais seguros (armários trancados).
- ✅ Descarte papéis com fragmentadora ou procedimento adequado.
- ❌ Nunca mande dados pessoais no corpo do e-mail sem proteção.
- ❌ Não jogue documentos com dados pessoais no lixo comum.

Exemplo: Antes de enviar um contracheque por e-mail, confira se o endereço eletrônico do servidor está correto.

Compartilhamento com outros órgãos

- ✅ Compartilhe dados apenas quando houver previsão legal e finalidade legítima e específica.
- ✅ Registre o motivo e para quem os dados foram enviados.
- ✅ Em caso de dúvida, consulte o setor responsável ou o(a) encarregado(a) pelo Tratamento dos Dados Pessoais (DPO).
- ❌ Não repasse dados "por favor" ou "para ajudar" sem base legal.

Exemplo: A Secretaria de Educação só deve repassar dados de alunos à Secretaria de Saúde quando houver previsão legal ou necessidade comprovada para execução de políticas públicas conjuntas em benefício da população.

Uso seguro de sistemas e senhas

- ✅ Crie senhas fortes (letras, números e símbolos) e troque-as regularmente.
- ✅ Bloqueie o computador sempre que se afastar.
- ✅ Use apenas redes seguras para acessar sistemas do órgão.
- ❌ Não compartilhe sua senha com colegas.
- ❌ Não anote senhas em papéis deixados sobre a mesa.

Exemplo: Ao sair para o almoço, bloqueie o computador para que ninguém acesse informações de cidadãos em seu nome.

O que o servidor não deve fazer com dados pessoais

Assim como existem boas práticas para proteger dados, também é importante saber o que não pode ser feito. Certos comportamentos podem gerar riscos para os cidadãos e responsabilidade para o órgão público.

Dados pessoais não são "do órgão" nem "do servidor": pertencem ao cidadão e devem ser protegidos.

Confira alguns exemplos do que o servidor **não deve fazer** no dia a dia:

⊘ Exemplos práticos de condutas inadequadas:

✗ Enviar dados pessoais ou documentos sensíveis por **WhatsApp** ou redes sociais.

✗ Deixar fichas, prontuários ou pastas **abertos em balcões ou mesas de atendimento.**

✗ Usar e-mail pessoal para enviar informações de trabalho.

✗ Compartilhar senhas de acesso a sistemas com colegas.

✗ Guardar dados em pen drives ou HDs externos sem proteção.

✗ Falar informações pessoais de cidadãos em locais públicos ou sem privacidade.

✗ Imprimir documentos desnecessariamente e deixá-los sem controle.

✗ Jogar papéis com dados pessoais no lixo comum.

✗ Repassar dados pessoais "para ajudar alguém" sem verificar se há base legal.

✗ Utilizar os dados de cidadãos para fins pessoais ou fora da finalidade do serviço público.

ANPD e Sanções à administração pública

A **Agência Nacional de Proteção de Dados (ANPD)** é o órgão responsável por fiscalizar e orientar o cumprimento da LGPD em todo o país.

Quando a Administração Pública descumpre a LGPD, podem ser aplicadas sanções como:

Advertência: comunicação formal para corrigir falhas.

Publicização da infração: divulgação da irregularidade cometida pelo órgão.

Bloqueio dos dados pessoais: suspensão temporária do uso dos dados até regularização.

Eliminação dos dados pessoais: exclusão definitiva de informações tratadas de forma irregular.

Além disso, gestores e servidores podem responder por **improbidade administrativa,** se houver uso indevido, vazamento ou descuido no tratamento de dados pessoais.

Dados pessoais sensíveis e dados de saúde, crianças e adolescentes

Nem todos os dados pessoais são iguais: alguns exigem **maior cuidado** por revelarem informações íntimas e que podem gerar discriminação ou exposição indevida.

O que são dados pessoais sensíveis?

São dados que dizem respeito à esfera mais íntima do cidadão, como:

- Origem racial ou étnica
- Convicção religiosa
- Opinião política
- Filiação sindical
- Dados sobre saúde
- Vida sexual
- Dados genéticos ou biométricos

Dados relativos à saúde

No setor público, esses dados são tratados principalmente em hospitais, postos de saúde e programas sociais.

- Devem ser **protegidos com sigilo absoluto**.
- Só podem ser usados para **finalidades específicas** ligada à saúde pública ou tutela da vida.
- Vazamentos ou usos indevidos podem causar danos graves ao cidadão.

Exemplo: prontuários médicos em hospitais públicos devem ser acessados apenas por profissionais autorizados e para atendimento ao paciente.

Dados de crianças e adolescentes

A LGPD dá proteção especial a dados de menores de 18 anos.

- O tratamento deve ser feito sempre em seu **melhor interesse**.
- Exige **consentimento específico dos pais ou responsáveis,** salvo exceções ligadas a políticas públicas ou proteção da criança/adolescente.
- O acesso a esses dados deve ser restrito e controlado.

Exemplo: cadastros escolares só podem ser usados para fins educacionais, não podendo ser compartilhados para outros propósitos sem previsão legal.

Atenção redobrada:

- Use somente os dados necessários.
- Restrinja o acesso apenas a pessoas autorizadas.
- Registre o motivo do uso.
- Mantenha sigilo absoluto.

Em resumo: dados sensíveis, de saúde e de crianças/adolescentes exigem cuidado especial, pois envolvem direitos fundamentais e proteção reforçada pela lei.

só use os dados necessários, com sigilo e restrição de acesso.

Incidentes de Segurança da Informação: O que fazer se ocorrerem vazamentos ou acessos indevidos?

Incidentes de segurança da informação, como vazamentos de dados ou acessos não autorizados, podem comprometer informações pessoais e institucionais, causando danos graves. É fundamental saber como agir rapidamente para minimizar esses impactos.

Passos a seguir se houver vazamento ou acesso indevido:

1 **Identifique o incidente:**
verifique qual tipo de dado foi exposto ou acessado indevidamente, quando e como o incidente ocorreu, para entender a gravidade e o alcance do problema.

2 **Troque as senhas imediatamente:**
Caso sejam afetadas informações de acesso, altere todas as senhas relacionadas com urgência, evitando usar a mesma senha em diferentes serviços. Ative a autenticação de dois fatores disponíveis para aumentar a segurança.

3 **Monitore contas e sistemas:**
Fique atento às movimentações suspeitas em contas bancárias, sistemas institucionais e outras plataformas. Registrar e relatar qualquer atividade anormal.

4 **Informe as autoridades competentes:**
Comunique o(a) Encarregado(a) pelo Tratamento de Dados Pessoais e a equipe de segurança da informação do seu órgão.

5 **Comunicação transparente:**
Caso tenha sido vítima de vazamento, procure confirmar a veracidade das informações por meio dos canais oficiais e evite acessar sites suspeitos ou abrir links que possam ser armadilhas para golpes.

6 **Siga as orientações institucionais:**
atenda todas as recomendações do(a) Encarregado(a) e da área de TI e segurança da informação do seu órgão para mitigar o problema.

7 **Não compartilhe dados confidenciais:**
Evite divulgar documentos ou informações pessoais em redes públicas para não ampliar os riscos.

Medidas para evitar futuros incidentes:

- Use senhas fortes e variadas.
- Atualize regularmente seus dispositivos e sistemas.
- Não compartilhe suas credenciais.
- Esteja atento a e-mails e mensagens suspeitas (phishing).
- Participe de treinamentos de conscientização em segurança da informação.

Seguindo essas orientações, os servidores podem contribuir para proteger informações sensíveis do estado da Paraíba e evitar prejuízos maiores em caso de incidentes de segurança.

Canais de apoio e denúncias internas

Para dúvidas, denúncias ou sugestões relacionadas à segurança da informação e proteção de dados pessoais, os servidores do estado da Paraíba podem recorrer aos canais internos oficiais do governo estadual, que oferecem atendimento transparente e seguro.

Principais canais para contato:

ENCARREGADOS(AS) PELO TRATAMENTO DE DADOS PESSOAIS DE CADA ÓRGÃO:

A lista com os nomes e contatos dos(as) encarregados(as) (DPOs) está disponível na página da LGPD no portal do Governo do Estado:

http://paraiba.pb.gov.br

OUVIDORIA GERAL DO ESTADO DA PARAÍBA:

Canal para registrar manifestações, reclamações, denúncias, sugestões ou elogios sobre os serviços públicos estaduais, com atendimento por telefone, e-mail e sistema informatizado:

0800.021.2310

ouvidoriageral@casacivil.pb.gov.br

https://ouvidoria.pb.gov.br

PÁGINA DA ANPD (AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS):

Disponibiliza orientações, canais de denúncia e acompanhamento para situações ligadas à LGPD no âmbito nacional:

https://www.gov.br/anpd/

Esses canais são fundamentais para garantir o suporte necessário aos servidores na proteção de dados pessoais e na condução correta das ações e investigações internas.

Em caso de dúvida, nunca hesite em procurar os canais oficiais.

Referências normativas

Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)
Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Decreto Estadual nº 41.238/2021 (PB)
Dispõe sobre a implementação da LGPD no âmbito do Poder Executivo do Estado da Paraíba e dá outras providências.

Resolução CGPDP nº 01/2024
Dispõe sobre as nomeações dos Encarregados pelo Tratamento de Dados Pessoais no âmbito do Poder Executivo do Estado da Paraíba, com base na LGPD e no Decreto Estadual nº 41.238/2021.

Agência Nacional de Proteção de Dados (ANPD)
Mais informações: https://www.gov.br/anpd/pt-br

Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado – ANPD
Disponível em:
https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

GOVERNO
DA PARAÍBA