# Manual de Aplicação

# LGPD

## LEI GERAL DE PROTEÇÃO DE DADOS

INSTITUTO FEDERAL
Pernambuco

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco
Reitoria/Coordenação da Controladoria

# Manual de Aplicação da Lei Geral de Proteção de Dados (LGPD) no IFPE

Orientações práticas e procedimentos institucionais para o adequado tratamento de dados pessoais no âmbito do IFPE, em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

**Histórico de Atualizações**

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| 8/6/2026 | 1.0 | Primeira versão do Manual de Aplicação da LGPD no IFPE | Maria Dayana Lopes de Oliveira |
| 3/9/2026 | 1.1 | Segunda versão do Manual de Aplicação da LGPD no IFPE | Helena Cristina Rodrigues Alves |

Maria Dayana Lopes de Oliveira
Cargo/Função: Auditora/Coordenadora da Controladoria/Encarregada pelo Tratamento de Dados Pessoais do IFPE
Helena Cristina Rodrigues Alves
Cargo/Função: Auditora/Encarregada pelo Tratamento de Dados - Substituta

Designações: Portaria IFPE nº 233, de 21 de fevereiro de 2024
https://boletim.sigepe.gov.br/publicacao/detalhar/246573

**Sugestões de atualização e melhorias para o Manual devem ser encaminhadas por e-mail para controladoria@reitoria.ifpe.edu.br**

# SUMÁRIO

# 1 Conceitos Gerais

Seguem apresentados os principais conceitos relacionados à proteção de dados pessoais para facilitar a compreensão e a aplicação das orientações deste Manual:

1. Acesso: ato de ingressar, transitar, conhecer, consultar ou utilizar informação ou ativos de informação de órgão ou entidade, observada eventual restrição legal ou normativa aplicável;

2. Adolescente: pessoa entre doze e dezoito anos de idade, nos termos da Lei nº 8.069/1990;

3. Agentes de tratamento: o controlador e o operador de dados pessoais;

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

5. Armazenamento e/ou arquivamento: ação ou resultado de manter ou conservar dados em repositório físico ou eletrônico;

6. Ativos de informação: meios de armazenamento, transmissão e processamento de informações, sistemas de informação, infraestrutura tecnológica, ambientes físicos e demais recursos relacionados ao tratamento de dados;

7. Agência Nacional de Proteção de Dados – ANPD: órgão da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais;

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

9. Bases legais: hipóteses autorizativas previstas na LGPD que legitimam o tratamento de dados pessoais;

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

11. Classificação: processo de categorização dos dados conforme critérios estabelecidos pela legislação e pelas normas institucionais;

12. Coleta: recolhimento de dados pessoais para finalidade específica, explícita e legítima;
13. Comunicação: ato de transmitir, compartilhar ou disponibilizar informações ou dados;

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

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

16. Controle da informação: ação ou poder de regular, monitorar, supervisionar ou determinar operações relacionadas aos dados;

17. Criança: pessoa até doze anos de idade incompletos, nos termos da Lei nº 8.069/1990;

18. Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento;

19. Dado pessoal: informação relacionada à pessoa natural identificada ou identificável, inclusive dados de servidores, discentes, terceirizados, colaboradores e pessoas físicas externas vinculadas ao IFPE;

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

21. Difusão: ato de divulgação, propagação ou compartilhamento de dados pessoais;

22. Eliminação: exclusão ou destruição de dado pessoal armazenado em banco de dados, observadas as hipóteses legais de conservação;

23. Encarregado pelo Tratamento de Dados Pessoais: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Agência Nacional de Proteção de Dados;

24. Extração: ato de copiar, retirar ou reproduzir dados do repositório em que se encontravam armazenados;

25. Governança em privacidade e proteção de dados pessoais: conjunto de mecanismos, processos, políticas e medidas voltadas à conformidade com a LGPD e à proteção dos direitos dos titulares;

26. Idoso: pessoa com idade igual ou superior a 60 (sessenta) anos, nos termos da legislação vigente;

27. Incidente de segurança com dados pessoais: evento adverso confirmado ou sob suspeita relacionado à violação de dados pessoais, capaz de acarretar risco ou dano relevante aos titulares;

28. Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade, do Estado ou para a proteção de direitos individuais;

29. Modificação: ato ou efeito de alteração de dado pessoal;

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

31. Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

32. Processamento: operação ou conjunto de operações realizadas com dados pessoais visando à sua organização, tratamento ou utilização;

33. Produção: criação, obtenção ou geração de dados ou informações a partir de operações de tratamento;

34. Pseudonimização: tratamento por meio do qual o dado pessoal perde a possibilidade de associação direta a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro, observados os requisitos previstos na Lei Geral de Proteção de Dados Pessoais;

35. Recepção: ato de receber dados ao final de processo de transmissão ou compartilhamento;

36. Risco de reidentificação contextual: possibilidade de identificação de uma pessoa natural mediante a combinação ou correlação de dados que, isoladamente, não permitiriam sua identificação, mas que, em determinado contexto ou associados a outras informações, possam torná-la identificável;

37. Relatório de Impacto à Proteção de Dados Pessoais – RIPD: documentação elaborada pelo controlador contendo a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas de mitigação adotadas;

38. Reprodução: cópia de dado ou informação obtida por qualquer meio ou processo;

39. Serviço de Informação ao Cidadão – SIC: unidade responsável pelo atendimento dos pedidos de acesso à informação formulados com fundamento na Lei nº 12.527/2011;

40. Titular de dados pessoais: pessoa natural a quem se referem os dados pessoais objeto de tratamento;

41. Transferência: mudança de dados de uma área de armazenamento para outra ou para terceiros;

42. Transmissão: movimentação de dados entre sistemas, dispositivos, ambientes ou pontos distintos;

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

44. 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;

45. Usuário de dados: usuário autorizado a acessar dados pessoais para desempenho de suas atribuições institucionais;

46. Utilização: ato de uso, aproveitamento ou aplicação dos dados pessoais para finalidade legítima;

47. Violação de dados pessoais: incidente de segurança que resulte em destruição, perda, alteração, divulgação, acesso ou tratamento inadequado, ilícito ou não autorizado de dados pessoais, de forma acidental ou intencional.

Os conceitos apresentados neste Manual deverão ser interpretados em conformidade com a Lei Geral de Proteção de Dados Pessoais, normas complementares da Agência Nacional de Proteção de Dados e demais legislações aplicáveis à Administração Pública Federal.

## 2 Diferença entre dados pessoais comuns e dados pessoais sensíveis

Segue abaixo um quadro explicativo com os conceitos e as principais diferenças entre dados pessoais comuns e dados pessoais sensíveis, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD):

| **Dados Pessoais Comuns** | **Dados Pessoais Sensíveis** |
|---|---|
| LGPD, **art. 5º:**<br>**I -** dado pessoal: informação relacionada a pessoa natural identificada ou identificável. | LGPD, **art. 5º:**<br>**II -** dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a 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. |
| O art. 6º do Código Civil (Lei nº 10.406/2002) estabelece que "a existência da pessoa natural termina com a morte".<br><br>Nesse contexto, a LGPD destina-se, em regra, à proteção de dados pessoais de pessoas naturais vivas. Apesar disso, há corrente doutrinária que defende a necessidade de proteção dos dados de pessoas falecidas, especialmente em razão de possíveis impactos sobre a memória, a honra, a imagem e os direitos de familiares e terceiros relacionados. | Os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente **relacionados aos aspectos mais íntimos da personalidade de um indivíduo**[1]. Além disso, esses dados pessoais têm **potencial discriminatório** e, por isso, demandam maior proteção e cuidado em seu tratamento.<br><br>Portanto, o tratamento deve ser precedido de cautelas maiores, uma vez que eventual incidente de segurança com esse tipo de dado **pode trazer consequências mais gravosas aos direitos e às liberdades dos titulares**.[2] |
| **Pessoa natural identificada** é aquela que pode ser diretamente identificada por meio de dados pessoais, como nome, CPF, endereço, número de telefone, entre outros.<br>**Pessoa natural identificável** é aquela que, mesmo sem ter sido identificada diretamente, pode vir a ser identificada por meio de informações adicionais que estejam disponíveis ou que possam ser acessadas por quem esteja tratando esses dados.[3]<br>**Ex.:** O cruzamento e a combinação de diferentes dados, como a profissão e o local de trabalho (Auditora do IFPE - *Campus* Barreiros). | Embora a LGPD apresente um rol de dados pessoais sensíveis, um dado pessoal comum pode assumir caráter sensível dependendo do contexto em que é utilizado ou relacionado a outras informações. Dados pessoais comuns, como localização, podem permitir inferências sobre aspectos sensíveis, como convicção religiosa e estado de saúde.<br><br>Assim, parte da doutrina e da prática em proteção de dados entende que a análise da sensibilidade não deve considerar apenas a natureza isolada do dado, mas também o contexto de tratamento, a finalidade e o potencial discriminatório das informações. |

[1] Fonte: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes?activeAccordion=3e386dfb-319a-4656-ac85-4f4978a41168%2C42c9e3ca-bca6-4960-bb74-0ebdc1d6f2f0. Acesso em: 27 maio 2026.

[2] Fonte: https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis/. Acesso em: 28 ago. 2025.

[3] Fonte: https://lgpdnacional.com.br/ufaq/pessoa-identificada-ou-identificavel/. Acesso em: 28 ago. 2025.

| Dados Pessoais Comuns | Dados Pessoais Sensíveis |
|---|---|
| **Alguns exemplos práticos:**<br>**Dados de identificação civil -** Nome completo. Sobrenome. Apelido ou nome social. Data de nascimento. Estado civil. Sexo/gênero (quando informado apenas como dado cadastral, sem relação com vida sexual). Nacionalidade. Naturalidade.<br><br>**Documentos de identificação -** Número do RG, do CPF, da CNH e do passaporte. Título de eleitor (sem informação de voto). Número da identidade profissional (ex.: OAB, CRM, CREA).<br><br>**Dados de contato -** Endereço residencial. Endereço comercial. Telefone fixo/celular. E-mail pessoal ou institucional. Caixa postal.<br><br>**Dados profissionais e acadêmicos -**<br>Cargo ou função. Local de trabalho. Histórico escolar (disciplinas cursadas, notas, frequência). Diploma ou certificado de conclusão de curso. Currículo (experiências profissionais, qualificações). Carteira de trabalho (sem informações sobre saúde ou sindicato).<br><br>**Dados financeiros** - Conta bancária. Agência bancária. Dados de cartão de crédito (número, validade). Renda mensal. Histórico de pagamentos. Informações de compras em e-commerce.<br><br>**Dados digitais -** Endereço IP. Login de usuário. Senha (quando vinculada a uma pessoa). Cookies de navegação. Dados de geolocalização (GPS). Histórico de acesso a sites ou aplicativos.<br><br>**Outros exemplos -** Placa de veículo. Registro de imóveis em nome da pessoa. Fotos em que a pessoa possa ser identificada (mas não usadas para biometria). Vídeos em que a pessoa aparece (sem coleta biométrica). Assinatura manual ou digital. | **Alguns exemplos práticos:**<br>**Origem racial ou étnica -** Autodeclaração de raça/cor em formulários (branco, preto, pardo, indígena, amarelo). Informação sobre pertencimento a povo ou comunidade tradicional (ex.: quilombolas, indígenas).<br><br>**Convicção religiosa** - Religião declarada em formulário ou cadastro (ex.: católico, evangélico, espírita, umbandista, judeu, muçulmano, budista, hinduísta).<br><br>**Opinião política** - Opiniões manifestadas em pesquisas de intenção de voto ou em enquetes políticas.<br><br>**Filiação a sindicato ou a organização de caráter religioso, filosófico ou político -** Pagamento de contribuição sindical ou assistencial. Contribuições financeiras ou doações a instituições religiosas. Pertencer a uma sociedade filosófica ou escola de pensamento (ex.: sociedades esotéricas, grupos de filosofia clássica ou moderna). Registro de doações a organizações políticas.<br><br>**Dado referente à saúde** - Resultados de exames laboratoriais ou de imagem. Diagnósticos médicos ou psicológicos. Registros de vacinação. Informações sobre plano de saúde (cobertura, tratamentos realizados). Histórico de internações ou cirurgias.<br><br>**Dado referente à vida sexual** - Informação sobre orientação sexual (heterossexual, homossexual, bissexual, assexual etc.). Participação em pesquisas sobre comportamento sexual.<br><br>**Dado genético -** Perfil de DNA obtido em exames laboratoriais. Dados de exames de paternidade/maternidade. Resultados de testes de predisposição a doenças hereditárias<br><br>**Dado biométrico -** Impressão digital usada para autenticação em sistemas ou catracas. Reconhecimento facial (ex.: câmeras de segurança, desbloqueio de celular). Reconhecimento de voz para acesso a serviços. Geometria da mão ou da palma. |

## 3 Orientação sobre divulgação ou disponibilização de dados pessoais

- Quando não divulgar ou não disponibilizar o acesso a dados pessoais?

R. Quando ferir a vida privada, a honra e a imagem da pessoa, com o potencial de expor o titular dos dados a julgamento ou discriminação ou influenciar a forma como gostaria de ser visto por outros. Deve-se analisar cada caso para verificar se o fornecimento das informações pode comprometer as atividades desempenhadas pelo órgão (ex.: investigações em andamento) ou se representa risco concreto à privacidade, à honra e à imagem do indivíduo.

- O que podemos divulgar ou disponibilizar e o que precisamos tarjar, omitir ou descaracterizar em relação aos dados pessoais no IFPE?

Seguem os links das orientações da Controladoria-Geral da União (CGU) publicadas no "Boletim: Por dentro da LAI[4]", criado com o objetivo de desenvolver e disseminar orientações práticas sobre a aplicação da Lei de Acesso à Informação:

1. Dados de Agente Público: esclarece e exemplifica que, em regra, informações pessoais de agentes públicos, atuando em nome da Administração Pública, devem ser fornecidas diante de pedidos de informação, para possibilitar o exercício do controle social. Destaca, ainda, que pode haver exceções, caso o fornecimento das informações comprometa as atividades realizadas pelo órgão ou represente risco ao agente público.

2. Processos Administrativos com Dados Pessoais: trata da possibilidade de acesso a processos administrativos que contenham dados pessoais ou outras informações restritas, alertando para a necessidade de ocultação dessas informações antes da sua entrega. Esclarece como validar a identidade do solicitante pelo perfil Gov.BR e o que fazer diante de uma identidade não validada. Por fim, apresenta dicas sobre marcações de negativas de acesso no Fala.BR.

3. Informações Pessoais de Agentes Públicos por Terceiros: aborda a possibilidade de acesso a informações pessoais de agentes públicos por terceiros, mediante consentimento expresso do titular da informação. Destaca-se que o órgão deverá avaliar a conveniência e a oportunidade de solicitar esse consentimento ao agente público. Além disso, são apresentados critérios para análise e concessão da informação, em caso de interesse público geral e preponderante.

Para facilitar, apresentamos a seguir um quadro com as orientações:

[4] https://www.gov.br/acessoainformacao/pt-br/central-de-conteudo/boletim-por-dentro-da-lai. Acesso em: 27 maio 2026.

| Dado Pessoal | Pode divulgar/ disponibilizar o acesso? | Justificativa/Orientação |
|---|---|---|
| Nome completo de servidor | Sim | Trata-se de dado cadastral que não se refere à intimidade, à privacidade, à honra ou à imagem do servidor. |
| SIAPE | Sim | Pode ser fornecido, pois é considerado uma informação relativa ao exercício de cargo público. Não há necessidade de anonimização e tarjamento.<br><br>PARECER n. 00001/2021/CONJUR-CGU/CGU/AGU:<br>c) Na opção de se adotar o número do SIAPE para todos os servidores e demais funcionários, haveria afronta aos princípios e fundamentos elencados na LGPD e passível de questionamento futuro pelos respectivos titulares desse dado pessoal?<br>Conforme entendeu o item 78.9 do PARECER n. 00001/2021/CONJURCGU/CGU/AGU, "9. Com relação ao representante legal da pessoa jurídica de direito público (contratante), é possível a substituição do número do CPF pelo número de matrícula - que no âmbito federal é o número SIAPE – tanto na lavratura de contratos, termos aditivos e instrumentos congêneres, quanto em acordos de cooperação técnica, portarias de designação ou mesmo em relatórios e documentos relacionados às atividades finalísticas desta CGU, visto que se mostra suficiente para conseguir identificar o servidor responsável pelo ato (afastando-se os homônimos) e evitar o uso indevido do número de CPF por terceiros. O número SIAPE diz respeito à matrícula que identifica o servidor público no órgão em que desempenha suas atividades, e, embora se enquadre na definição de dado pessoal, à luz da LGPD, não possui repercussões para além da vida pública do servidor, não havendo razões para que esse dado tenha restrição de acesso." |
| CPF | Parcialmente (descaracterizar) | Trata-se de dado pessoal relativo à privacidade do agente público, portanto, quando houver necessidade de divulgação, ele deve ser anonimizado ou mascarado, recomendando-se o formato "***.999.999-**".<br><br>PARECER n. 00001/2021/CONJUR-CGU/CGU/AGU:<br>Reiterada jurisprudência administrativa da Controladoria-Geral da União, enquanto órgão julgador de recursos administrativos contra negativa de pedidos de acesso à informação, tem decidido de forma uníssona pela restrição de acesso ao CPF, mas que a sua descaracterização é medida que possibilita sua publicação em transparência ativa[2] |

| Dado Pessoal | Pode divulgar/ disponibilizar o acesso? | Justificativa/Orientação |
|---|---|---|
| | | A descaracterização do CPF, inclusive, é a forma utilizada no Portal da Transparência do Poder Executivo federal, para todas as consultas, tais como: “Auxílio Emergencial”, “Benefício ao Cidadão”, “Cartões de Pagamento”, “Convênios”, “Viagens a Serviço” e “Servidores e Pensionistas”. O formato de descaracterização também aparece explicitado no Guia de Transparência Ativa (GTA) para os órgãos e as entidades do Poder Executivo federal, material editado pela Controladoria-Geral da União[3] .<br>Em idêntico sentido ao do costume preponderante, de publicação descaracterizada do CPF, a LDO vem sucessivamente determinando que na execução de seus comandos de transparência a divulgação **"deverá ocultar os três primeiros dígitos e os dois dígitos verificadores do CPF"**[4]: Art. 149. A divulgação da informação de que tratam os arts. 146 e 148 deverá ocultar os três primeiros dígitos e os dois dígitos verificadores do CPF.<br><br>**Fórmulas, no Excel, conforme exemplos:**<br>A1 = 123.456.789-10<br>=CONCATENAR("***";(EXT.TEXTO(A1;5;7));"**")<br>***456.789**<br><br>A1 = 12345678910<br>=CONCATENAR("***";(EXT.TEXTO(A1;4;6));"**")<br>***456789** |
| E-mail institucional | A critério do órgão | Deve-se divulgar os e-mails de contato para atendimento ao público. Os e-mails funcionais não precisam ser divulgados. |
| Registros de entrada e saída de prédios públicos | Sim, com ressalva | Enunciado CGU nº 1/2023 - Registros de entrada e saída de prédios públicos:<br><br>Os registros de entrada e saída de pessoas em órgãos públicos do Poder Executivo federal, inclusive no Palácio do Planalto, são passíveis de acesso público, exceto quando as agendas sobre as quais eles se refiram estiverem enquadradas em hipótese legal de sigilo (art. 22), tiverem sido classificadas (art. 23) ou estiverem sob restrição temporária de acesso (art. 7º, § 3º), nos termos da Lei nº 12.527, de 18 de novembro de 2011. |
| Identificação do servidor que realizou um ato administrativo | Sim | Exemplos, não exaustivos, de atos praticados:<br>- Autoria de relatórios, notas técnicas, decisões administrativas etc.<br>- Servidor que acessou ou modificou informações em sistemas. |

| Dado Pessoal | Pode divulgar/ disponibilizar o acesso? | Justificativa/Orientação |
|---|---|---|
| Demais dados pessoais não citados anteriormente (ex.: endereço) | Não | Trata-se de dados relacionados à privacidade do titular. Caso um documento contenha tais dados pessoais, eles devem ser tarjados ou omitidos. |

- **Há exceções?**

Sim. Conforme orienta a CGU, deve-se analisar cada caso para verificar se o fornecimento das informações pode comprometer as atividades desempenhadas pelo órgão (ex.: investigações em andamento) ou se representa risco concreto à privacidade, à honra e à imagem do indivíduo.

# 4 Procedimento para o tratamento de dados pessoais por pesquisadores

Esse procedimento tem por objetivo estabelecer diretrizes para o adequado tratamento de dados pessoais no âmbito de estudos e pesquisas no Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco (IFPE), de forma a garantir a conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e assegurar os direitos dos titulares dos dados.

Para consultar o procedimento, acesse a Portaria IFPE nº 82, de 23 de janeiro de 2026, que aprovou o procedimento para o tratamento de dados pessoais por pesquisadores. Anexos I e II da Portaria (formato editável).

# 5 Procedimento para tarjar dados pessoais com a ferramenta PDF24 Creator

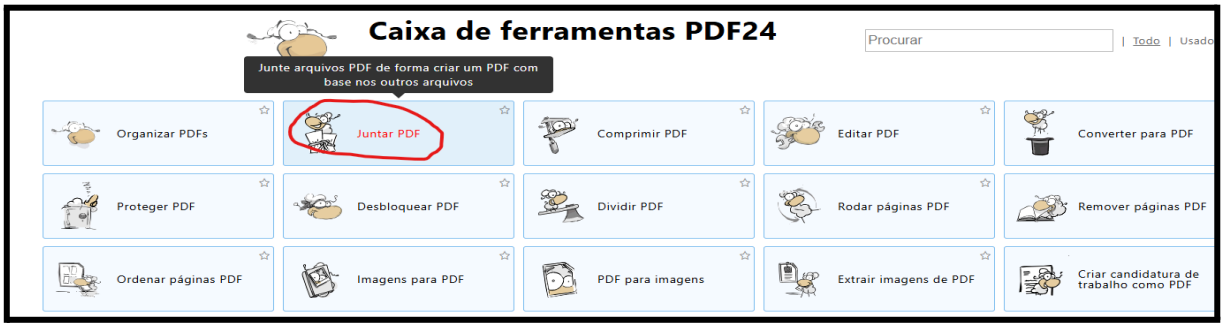
**Obs.:** Adaptação do Manual do Instituto Federal de São Paulo (IFSP) - Ferramentas para tarjamento de dados pessoais/sensíveis - Tarjando (anonimizando) dados pessoais/sensíveis - Ferramenta PDF24[5].

**TARJAR PARTES DO DOCUMENTO**

**Obs.:** O documento deve estar na **extensão PDF**.

**1.** Abra o programa PDF24 Creator (link para download gratuito da versão desktop).

**1.1** Caso os documentos baixados estejam separados, é possível, inicialmente, unificá-los utilizando a ferramenta PDF24 Creator. Para isso, abra o programa PDF24 Creator (versão desktop), disponível para download gratuito no link constante no subitem 4.1.




**Obs.:** Evite o uso de ferramentas online, como o site https://ilovepdf.com/, uma vez que essas plataformas podem armazenar, processar ou reutilizar dados em ambientes fora do controle institucional.

[5] https://manuais.ifsp.edu.br/books/ferramentas-para-tarjamento-de-dados-pessoaissensiveis. Acesso em: 25 jul. 2025.

**1.2** Na “Caixa de ferramentas PDF24”, escolha a opção "Censurar PDF":

**Figura 1**


**1.3** Escolha ou arraste o arquivo PDF a ser tarjado para a área indicada:

**Figura 2**


**1.4** Com o arquivo aberto, selecione “Desenho livre” ou “Adicionar forma” e tarje as áreas desejadas:

**Figura 3**

**Obs.:** O documento não aparece integralmente na tela. Dessa forma, selecione página a página do documento para tarjar as informações necessárias.

**1.5** Clique no **disquete** (primeiro ícone da Figura 3) e depois em **Salvar** (Salvar PDF), podendo editar o nome do arquivo

**Obs.:** O processo de tarjamento transforma a página em uma imagem, ou seja, um arquivo não pesquisável. As páginas em que não houve nenhum tarjamento permanecem pesquisáveis.

## TRANSFORMAR AS PÁGINAS TARJADAS EM PESQUISÁVEIS

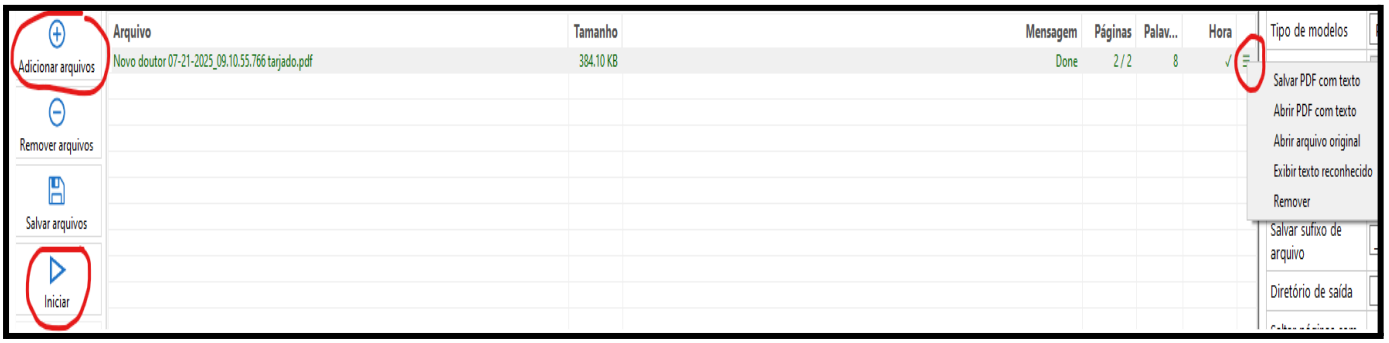
Para atribuir a todo o documento a condição de pesquisável, este deverá ser convertido em OCR, da seguinte forma:

**1.6** Na “Caixa de ferramentas PDF24”, escolha a opção "OCR PDF";

**Figura 4**


**1.7 Adicione** o arquivo tarjado com extensão PDF e clique em “**Iniciar”**. Espere ele fazer a conversão com o preenchimento das colunas, conforme a figura a seguir. Depois, clique no ícone com três traços no canto superior direito e selecione a opção “Salvar PDF como texto”:

**Figura 5**


Adicionar arquivos
Remover arquivos
Salvar arquivos
Iniciar
Arquivo
Tamanho
Mensagem
Páginas
Palav...
Hora
Novo doutor 07-21-2025_09.10.55.766 tarjado.pdf
384.10 KB
Done
2 / 2
8
Tipo de modelos
Salvar PDF com texto
Abrir PDF com texto
Abrir arquivo original
Exibir texto reconhecido
Remover
Salvar sufixo de arquivo
Diretório de saída

# 6 Orientação sobre a utilização da ferramenta de tarjamento do Fala.BR

As orientações sobre a utilização da ferramenta de tarjamento da plataforma Fala.BR encontram-se disponíveis na seção “Perguntas Frequentes – Ferramenta de Tarjamento” do site sobre a Lei de Acesso à Informação do governo federal.

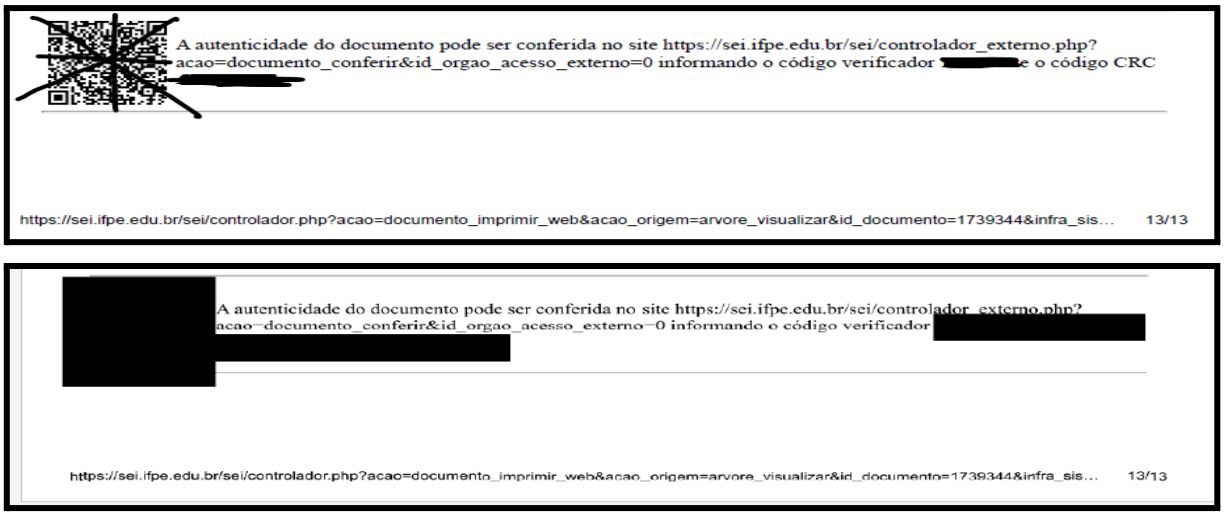
# 7 Orientação para tarjar documentos do SEI que contêm dados pessoais

**1.** Caso haja vários documentos, é possível realizar o download em PDF de todos eles em um único arquivo diretamente pelo SEI. Para isso, selecione o número do processo, clique no ícone de PDF e escolha os documentos que deseja incluir:


**2.** Identifique os dados pessoais e os dados pessoais sensíveis, observando as orientações constantes neste Manual, especialmente os itens "Diferença entre dados pessoais comuns e dados pessoais sensíveis" e "Orientação sobre divulgação ou disponibilização de dados pessoais".

**3.** Tarje os dados, conforme descrito no item "Procedimento para tarjar dados pessoais com a ferramenta PDF24 Creator" deste Manual.

**4.** Não se esqueça de **tarjar o QR Code, o código verificador e o código CRC** ao final de cada documento que contenha dados pessoais, uma vez que, por meio desses códigos, é possível acessar o documento original de forma integral.




**5.** Após o tarjamento, os documentos que contenham dados pessoais devem ser excluídos permanentemente do computador.

# 8 Orientações sobre o uso de dados pessoais em ferramentas de inteligência artificial

Ferramentas externas de inteligência artificial (IA), especialmente as gratuitas e disponíveis na internet, podem não oferecer garantias adequadas sobre como os dados inseridos serão utilizados, armazenados, compartilhados ou protegidos. Por esse motivo, não devem ser inseridos dados pessoais, dados pessoais sensíveis ou informações institucionais sigilosas em ferramentas de inteligência artificial externas que não tenham sido formalmente autorizadas pelo IFPE para essa finalidade.

Essa orientação tem como objetivo proteger a privacidade dos titulares dos dados, prevenir vazamentos de informações, garantir o cumprimento da Lei Geral de Proteção de Dados (LGPD) e reduzir riscos para o IFPE.

**Principais motivos para essa restrição**

**1.** O uso inadequado de dados pessoais pode expor informações dos titulares e violar seus direitos à privacidade e à proteção de dados.

**2.** O tratamento de dados sem controle institucional pode gerar responsabilidades administrativas e civis e danos à imagem da instituição.

**3.** Ao inserir dados em uma ferramenta externa de IA, pode ocorrer compartilhamento dessas informações com terceiros, o que exige fundamento legal adequado e compatível com a finalidade institucional.

**4.** A utilização de dados sem base legal ou sem consentimento válido, quando necessário, pode caracterizar tratamento irregular de dados pessoais.

**5.** Ferramentas externas de IA podem armazenar, processar ou reutilizar as informações fornecidas em ambientes que não estão sob controle do IFPE.

**6.** A divulgação indevida de informações institucionais ou sigilosas pode comprometer a segurança da instituição e a confiança da sociedade.

**7.** O uso inadequado de dados pessoais pode configurar descumprimento de normas institucionais e gerar responsabilização do agente envolvido.

**8.** Mesmo quando um dado parece não identificar uma pessoa diretamente, ele pode permitir sua identificação quando combinado com outras informações.

**9.** Ferramentas de IA podem relacionar, cruzar ou gerar novas informações a partir dos dados fornecidos, aumentando o risco de identificação indevida dos titulares.

# 9 Orientações para descarte de documentos com dados pessoais

**Descarte de Documentos Físicos**

1. Descarte seguro: utilize máquina fragmentadora/picotadora para destruir documentos que contenham dados pessoais.

2. Jamais descarte documentos em lixo comum ou locais sem controle, mesmo que aparentemente inofensivos (rasgados, amassados etc.).

3. O descarte deve garantir que as informações não possam ser recuperadas ou reconstruídas.

4. Registre o descarte de documentos sigilosos ou sensíveis, quando aplicável, como boa prática de conformidade e auditoria.

**Descarte de Documentos Digitais**

5. Ao eliminar arquivos digitais com dados pessoais, utilize métodos seguros de exclusão definitiva (“eliminação segura” ou “wipe”) para evitar recuperação.

6. Não reutilize mídias, como pen drives e HDs, sem antes realizar a eliminação completa dos dados anteriores.

7. Evite armazenar documentos pessoais em dispositivos pessoais ou não autorizados.

8. Em caso de uso de sistemas de armazenamento em nuvem, garanta que o provedor atenda aos requisitos da LGPD.

**Conduta e Responsabilidade**

9. Todo servidor, colaborador ou prestador de serviço é responsável pela proteção dos dados pessoais sob sua guarda.

10. Situações de risco, como extravio, descarte incorreto, impressões esquecidas ou acesso indevido, devem ser comunicadas imediatamente ao gestor da área e ao encarregado do IFPE.

# 10 Procedimento para permitir o acesso ao e-mail da unidade por servidores da equipe

O compartilhamento de senhas institucionais não deve ser realizado, pois pode comprometer a segurança da informação, dificultar a identificação de responsabilidades e aumentar o risco de uso indevido da conta. Por esse motivo, o acesso ao e-mail da unidade deve ser concedido por meio das funcionalidades próprias do sistema, que permitem autorizar outros usuários sem a necessidade de informar a senha.

Para permitir que outras pessoas da equipe tenham acesso ao e-mail da unidade sem a necessidade de compartilhar a senha, siga o passo a passo.

Esse procedimento orienta como conceder acesso de forma segura, preservando a confidencialidade da senha da conta institucional.

# 11 Orientação aos servidores quanto à inclusão de dados pessoais ou dados pessoais sensíveis em processos no SEI

A inserção de dados pessoais em processos administrativos deve observar os princípios da necessidade, finalidade e segurança, previstos na Lei Geral de Proteção de Dados (LGPD). Dessa forma, os servidores devem avaliar cuidadosamente a real necessidade de inclusão dessas informações nos processos do SEI, evitando exposição indevida.

**1. Não inclua dados pessoais ou dados pessoais sensíveis em processos com nível de acesso público.**
Sempre verifique o nível de acesso do processo antes de inserir documentos que contenham dados pessoais. Caso seja necessário incluir tais informações, o processo deve ser classificado com nível de acesso restrito ou o documento deve ser tratado adequadamente.

*Exemplo:* Não inclua atestado médico (dado pessoal sensível) em processo de jornada de trabalho.

**2. Avalie a possibilidade de abertura de processo relacionado (vinculado)** para a inclusão de documentos ou informações que contenham dados pessoais ou dados pessoais sensíveis, evitando, assim, a exposição indevida dessas informações em processos que necessitam permanecer públicos.

*Exemplo:* Processos podem permanecer públicos, enquanto documentos com dados pessoais ficam em processo restrito relacionado.

**3. Quando possível, tarje os dados pessoais**, conforme orientações do item 4 – Procedimento para tarjar dados pessoais com a ferramenta PDF24 Creator deste Manual, de modo a manter o máximo possível de transparência sem necessidade de restringir todo o processo.

**4. Evite a inserção de dados pessoais desnecessários nas solicitações.**
Insira apenas as informações estritamente necessárias para análise e decisão administrativa.

*Exemplo:* Nas solicitações de diárias, não é necessário incluir informações já registradas no Sistema de Concessão de Diárias e Passagens (SCDP).

**5. Evite anexar cópias de documentos pessoais quando não forem indispensáveis.**
Antes de anexar documentos como RG, CPF ou comprovante de residência, avalie se a informação já consta em sistemas institucionais ou se pode ser substituída por outro tipo de comprovação.

**6. Reduza a exposição de dados pessoais em despachos e manifestações.**

Nos textos de despachos, pareceres ou manifestações, evite repetir dados pessoais completos quando não for necessário.

*Exemplo:* Utilize apenas o nome do servidor ou o número de matrícula, evitando mencionar CPF ou endereço.

**7. Verifique se documentos de terceiros contêm dados pessoais antes da inclusão no processo.**

Documentos enviados por usuários externos ou por outras instituições podem conter dados pessoais que precisam ser tratados adequadamente antes de serem disponibilizados no processo.

**8. Em processos que envolvam estudantes, servidores ou usuários externos**, avalie se os dados apresentados são realmente necessários para a finalidade administrativa.

*Exemplo:* Em relatórios ou listas, utilize apenas o nome ou a matrícula, evitando incluir CPF, telefone ou endereço.

**9. Revise os documentos antes de disponibilizar o processo para acesso externo ou público.**

Sempre realize uma verificação final para identificar se há dados pessoais que precisam ser tarjados ou omitidos ou se o processo deve ter nível de acesso restrito.

# 12 Orientação sobre a coleta de dados pessoais por meio de formulários eletrônicos

1. **Colete apenas os dados necessários**

Antes de criar um formulário, verifique quais informações são realmente necessárias para alcançar a finalidade pretendida. Evite solicitar dados pessoais que não sejam necessários para a atividade, projeto, serviço ou procedimento administrativo.

**Exemplo:** Se o objetivo do formulário for realizar a inscrição em uma atividade institucional, não é necessário solicitar informações como CPF ou data de nascimento, a menos que esses dados sejam realmente necessários para a finalidade específica.

2. **Tenha atenção aos dados pessoais sensíveis**

Dados pessoais sobre saúde, raça ou etnia, religião, opinião política, entre outros, exigem cuidados especiais. Solicite esses dados somente quando forem necessários para a finalidade do formulário e houver fundamento legal que permita o seu tratamento.

3. **Inclua o link para o Termo de Uso e Aviso de Privacidade do IFPE, se necessário**

Sempre que um formulário eletrônico coletar dados pessoais, informe, em local de fácil visualização, que os dados serão tratados pelo IFPE. Recomenda-se que essa informação seja apresentada, preferencialmente, na descrição ou na seção inicial do formulário, acompanhada do link para o Termo de Uso e Aviso de Privacidade do IFPE.

**Exemplo:** Ao preencher este formulário, você declara estar ciente de que os dados pessoais coletados serão tratados de acordo com as diretrizes estabelecidas no Termo de Uso e Aviso de Privacidade do IFPE, disponível para consulta em: https://portal.ifpe.edu.br/wp-content/uploads/2024/11/Termo-de-Uso-e-Aviso-de-Privacidade.pdf

# 13 Documentos e publicações da ANPD

A Agência Nacional de Proteção de Dados (ANPD) é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Vinculada ao Ministério da Justiça e Segurança Pública, a ANPD atua na promoção da cultura de proteção de dados pessoais, na orientação dos agentes de tratamento e na edição de normas e diretrizes relacionadas ao tema.

Para apoiar a adequação à LGPD, a ANPD disponibiliza regulamentos, guias orientativos, manuais, perguntas frequentes e outros materiais educativos. A seguir, são apresentados os principais documentos e publicações elaborados pela ANPD que podem auxiliar a comunidade acadêmica no adequado tratamento de dados pessoais.

**Regulamentações da ANPD:**

1. Resolução CD/ANPD nº 18, de 16 de julho de 2024 – Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais;
2. Resolução CD/ANPD nº 15, de 24 de abril de 2024 – Aprova o Regulamento de Comunicação de Incidente de Segurança;
3. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 – Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas;
4. Enunciado CD/ANPD nº 1, de 22 de maio de 2023 – Sobre o tratamento de dados pessoais de crianças e adolescentes.

**Guias Orientativos:**

1. Atuação do Encarregado;
2. Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse;
3. Tratamento de Dados Pessoais pelo Poder Público;
4. Tratamento de Dados Pessoais para fins Acadêmicos e para a realização de estudos e pesquisas;
5. Cookies e Proteção de Dados;
6. Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

## 14 Agentes de tratamento no IFPE

| Papel | Quem exerce no IFPE |
|---|---|
| 1. Controlador | Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco (IFPE) |
| 2. Operadores | Empresas contratadas e terceiros que tratam dados em nome do IFPE |
| 3. Suboperadores | Empresas contratadas pelos operadores para auxiliar o tratamento |
| 4. Encarregado | Pessoa indicada pelo IFPE |

**1. Controlador**

O Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco (IFPE) é o controlador, pois é a instituição que define as finalidades e os meios do tratamento dos dados pessoais de estudantes, servidores, terceirizados, candidatos, fornecedores e demais titulares.

Na prática, a atuação do controlador se materializa por meio de seus dirigentes e unidades administrativas, tais como: Reitoria; Gabinete da Reitoria; pró-reitorias; Direções-Gerais dos *campi*; diretorias, coordenações e demais unidades que decidem sobre o tratamento de dados em seus processos de trabalho.

**2. Operadores**

São consideradas operadores as pessoas físicas ou jurídicas que realizam tratamento de dados pessoais em nome do IFPE e seguindo suas instruções.

Exemplos no contexto do IFPE: empresas terceirizadas de tecnologia da informação; empresas de hospedagem e manutenção de sistemas; empresas contratadas para concursos, seleções e eventos; empresas de vigilância, limpeza e apoio administrativo que tratem dados pessoais; prestadores de serviços de impressão, digitalização e gestão documental.

**3. Suboperadores**

São empresas ou organizações contratadas por um operador para auxiliar na execução do tratamento de dados pessoais, sempre vinculadas às instruções do controlador.

Exemplo: empresa contratada pelo fornecedor de sistema acadêmico para hospedar os dados em nuvem.

**4. Encarregado**

O encarregado pelo tratamento de dados pessoais é indicado pelo controlador para atuar como ponto de contato entre o IFPE, os titulares dos dados e a ANPD.

# 15 Bases legais para o tratamento de dados pessoais no IFPE

A LGPD estabelece que todo tratamento de dados pessoais deve estar fundamentado em uma hipótese legal específica.

No contexto da Administração Pública e, em especial, das atividades desenvolvidas pelo IFPE, as bases legais mais frequentemente utilizadas são:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas previstas em leis, regulamentos ou instrumentos congêneres;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Em situações específicas, quando não houver enquadramento nas hipóteses acima, poderão ser utilizadas outras bases legais previstas na LGPD, tais como o legítimo interesse do controlador ou o consentimento do titular, desde que observados os requisitos legais aplicáveis a cada caso.

É importante destacar que o tratamento de **dados pessoais sensíveis** está sujeito a requisitos mais rigorosos do que aqueles aplicáveis aos dados pessoais comuns. Da mesma forma, o tratamento de **dados de crianças e adolescentes** exige proteção especial, devendo sempre observar o princípio do seu melhor interesse.

Para facilitar a compreensão do tema, apresenta-se a seguir um quadro-resumo das hipóteses legais previstas na LGPD, organizado por categoria de dados e acompanhado de exemplos práticos relacionados à realidade do IFPE.

**1. Bases legais para o tratamento de dados pessoais comuns:**

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Consentimento do titular | Art. 7º, I | Servidor autoriza o uso de sua imagem em campanha institucional |
| Cumprimento de obrigação legal ou regulatória | Art. 7º, II | IFPE informa dados de servidores à Receita Federal |
| Execução de políticas públicas | Art. 7º, III | Compartilhamento de dados de estudantes com o MEC para programas educacionais |

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Estudos por órgão de pesquisa | Art. 7º, IV | Pesquisa acadêmica sobre evasão escolar com dados anonimizados |
| Execução de contrato ou procedimentos preliminares | Art. 7º, V | Tratamento dos dados de candidato aprovado para assinatura de contrato temporário |
| Exercício regular de direitos em processo judicial, administrativo ou arbitral | Art. 7º, VI | Uso de documentos funcionais em processo administrativo disciplinar |
| Proteção da vida ou da incolumidade física | Art. 7º, VII | Compartilhamento de informações para atendimento de emergência médica |
| Tutela da saúde | Art. 7º, VIII | Atendimento realizado pelo serviço médico institucional |
| Legítimo interesse do controlador ou de terceiro | Art. 7º, IX | Envio de pesquisa de satisfação para alunos e servidores |
| Proteção do crédito | Art. 7º, X | Não aplicável no IFPE |

**2. Bases legais para o tratamento de dados pessoais sensíveis:**

**Obs.:** Os dados pessoais sensíveis possuem um regime de proteção mais rigoroso na LGPD. Por esse motivo, não se aplicam aos dados pessoais sensíveis as seguintes bases legais previstas para os dados pessoais comuns: execução de contrato ou de procedimentos preliminares relacionados a contrato; legítimo interesse do controlador ou de terceiro; e proteção do crédito.

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Consentimento específico e destacado | Art. 11, I | Servidor autoriza a divulgação de sua condição de pessoa com deficiência para campanha institucional |
| Cumprimento de obrigação legal ou regulatória | Art. 11, II, “a” | Registro de afastamento por motivo de saúde exigido pela legislação |

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Execução de políticas públicas | Art. 11, II, “b” | Tratamento de dados sobre raça/cor para políticas de ações afirmativas |
| Estudos por órgão de pesquisa | Art. 11, II, “c” | Pesquisa sobre saúde mental de estudantes com anonimização dos dados |
| Exercício regular de direitos | Art. 11, II, “d” | Utilização de laudos médicos em processo judicial trabalhista |
| Proteção da vida ou da incolumidade física | Art. 11, II, “e” | Compartilhamento de alergias graves de aluno em situação de emergência |
| Tutela da saúde | Art. 11, II, “f” | Atendimento por médico, psicólogo ou enfermeiro da instituição |
| Prevenção à fraude e à segurança do titular | Art. 11, II, “g” | Utilização de biometria para controle de acesso a sistemas institucionais |

**3. Bases legais para o tratamento de dados pessoais de crianças e adolescentes**

O tratamento de dados pessoais de crianças e adolescentes deve observar, em qualquer situação, o princípio do melhor interesse da criança e do adolescente, conforme previsto na LGPD.

**Obs.1:** Como regra geral, o tratamento deve ser realizado com o consentimento específico e em destaque de pelo menos um dos pais ou do responsável legal.

**Obs. 2:** De acordo com o Enunciado CD/ANPD nº 1, de 22 de maio de 2023, "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Consentimento de pelo menos um dos pais ou responsável legal | Art. 14, § 1º | Uso da foto de estudante em campanha institucional |

| Hipótese Legal | Base Legal | Exemplo Prático |
|---|---|---|
| Melhor interesse | Art. 14, *caput* | Tratamento dos dados acadêmicos para acompanhamento pedagógico |
| Contato com os pais ou responsável | Art. 14, § 3º | Coleta de telefone do responsável para confirmar matrícula de criança |
| Proteção | Art. 14, § 3º | Compartilhamento de informações para atendimento emergencial de saúde |

# 16 Fluxo para Tratamento de Dados Pessoais

Fluxo para tratamento de Dados Pessoais