Delson Ferreira Bonfim

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

Lei nº 13.709/2018 e suas aplicabilidades

EDUFPI

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Lei nº 13.709/2018 e suas aplicabilidades

Delson Ferreira Bonfim

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Lei nº 13.709/2018 e suas aplicabilidades

edufpi

FICHA CATALOGRÁFICA

Universidade Federal do Piauí

Biblioteca Comunitária Jornalista Carlos Castello Branco

Divisão de Representação da Informação

B7131 Bonfim, Delson Ferreira.
Lei geral de proteção de dados pessoais - LGPD : lei nº 13.709/2018 e suas aplicabilidades / Delson Ferreira Bonfim. – [Teresina] : EDUFPI, [2026].
245 p.

ISBN **978-65-5904-509-9**

1. Proteção de dados - Legislação - Brasil. 2. Lei geral de proteção de dados pessoais (LGPD). 3. Política de privacidade de dados. I. Título.

CDD 341.2

Elaborada por Fabíola Nunes Brasilino CRB 3/ 1014

SUMÁRIO

APRESENTAÇÃO

Prezado(a) Servidor(a) da UFPI,

É com grande satisfação que apresentamos esta apostila sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei nº 13.709/2018. Este material foi desenvolvido especialmente para você, servidor(a) da Universidade Federal do Piauí, como parte do curso de capacitação sobre a LGPD.

Em um mundo cada vez mais digital, a proteção de dados pessoais tornou-se um direito fundamental dos cidadãos e uma obrigação legal para instituições públicas e privadas. A LGPD regula como os dados pessoais devem ser coletados, processados, armazenados e compartilhados, estabelecendo princípios, direitos e responsabilidades para garantir a privacidade e a segurança dessas informações.

Para as instituições públicas, incluindo as universidades federais, a adequação à LGPD é um desafio e uma oportunidade para aprimorar a governança de dados, garantir a transparência e fortalecer a confiança da comunidade acadêmica e do público em geral.

Esta apostila está estruturada em quatro módulos, abordando desde os fundamentos e princípios da LGPD até as responsabilidades e boas práticas no tratamento de dados pessoais, com foco especial na aplicação no contexto da administração pública e das instituições de ensino.

Esperamos que este material contribua para sua formação e para a implementação efetiva da LGPD em nossa instituição.

Boa leitura e bom curso!

Delson Ferreira Bonfim
Instrutor Institucional UFPI/SGP/CDP

MÓDULO 1 — FUNDAMENTOS DA LGPD

1.1. Contexto histórico e objetivos da lei

Contexto histórico

A preocupação com a proteção de dados pessoais não é recente no cenário mundial. Com o avanço tecnológico e a intensificação do uso da internet, a coleta e o processamento de dados pessoais tornaram-se práticas comuns e essenciais para o funcionamento de diversos serviços e negócios.

A primeira legislação específica sobre proteção de dados surgiu na Alemanha, em 1970, com a Lei de Proteção de Dados do estado de Hesse. Em 1981, a Convenção 108 do Conselho da Europa estabeleceu princípios para a proteção de dados pessoais. Mas foi com a Diretiva 95/46/CE da União Europeia que se estabeleceu um marco regulatório mais abrangente.

Em 2016, a União Europeia aprovou o Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor em 2018, tornando-se referência mundial para legislações de proteção de dados. O GDPR influenciou diretamente a elaboração da LGPD brasileira.

No Brasil, a proteção de dados era tratada de forma fragmentada em diferentes legislações, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei do Cadastro Positivo. Foi somente com a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que o país passou a contar com um marco legal abrangente e específico sobre o tema.

A LGPD foi inspirada no GDPR europeu, mas adaptada à realidade brasileira. Inicialmente, estava prevista para entrar em vigor em fevereiro de 2020, mas teve sua vigência adiada para agosto de 2020 e, posteriormente, para setembro de 2020, com as sanções administrativas aplicáveis a partir de agosto de 2021.

Objetivos da LGPD

Conforme estabelecido em seu art. 1º, a LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Para isso, a lei estabelece regras sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Os principais objetivos da LGPD podem ser resumidos em:

- Proteger os direitos fundamentais de privacidade e liberdade: Garantir que as pessoas tenham controle sobre seus dados pessoais e como eles são utilizados.
- Estabelecer regras claras sobre o tratamento de dados: Definir quando e como os dados pessoais podem ser coletados, processados, armazenados e compartilhados.
- Promover o desenvolvimento econômico e tecnológico: Criar um ambiente de segurança jurídica que favoreça a inovação e o desenvolvimento de novos produtos e serviços.
- Prevenir danos aos titulares: Evitar que o uso indevido de dados pessoais cause prejuízos materiais ou morais aos indivíduos.
- Fortalecer a confiança nas relações digitais: Aumentar a transparência e a responsabilidade no tratamento de dados, fortalecendo a confiança dos cidadãos.
- Padronizar normas e práticas: Unificar a regulamentação sobre proteção de dados no país, facilitando o cumprimento por parte das organizações.

- Adequar o Brasil a padrões internacionais: Alinhar a legislação brasileira a normas internacionais, facilitando o fluxo de dados entre países e a inserção do Brasil na economia global.

A LGPD representa um importante avanço na proteção dos direitos dos cidadãos e na regulação do uso de dados pessoais no Brasil, afetando diretamente a forma como instituições públicas e privadas coletam, armazenam e utilizam informações pessoais.

1.2. Conceitos fundamentais

A LGPD introduz diversos conceitos fundamentais para a compreensão e aplicação adequada da lei. Conhecer esses conceitos é essencial para identificar situações em que a lei se aplica e como proceder corretamente no tratamento de dados pessoais. Vejamos os principais:

Dado pessoal (Art. 5º, I)

Informação relacionada a pessoa natural identificada ou identificável. Ou seja, é qualquer informação que, isoladamente ou combinada com outras, permita identificar uma pessoa. Exemplos: nome, CPF, endereço, telefone, e-mail, data de nascimento, etc.

No contexto universitário, são dados pessoais: matrícula do aluno, notas, frequência, endereço, dados bancários de servidores, etc.

Dado pessoal sensível (Art. 5º, II)

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.

Esses dados recebem proteção especial por poderem ser utilizados para discriminação. Na UFPI, exemplos incluem: atestados médicos, registros de necessidades especiais, dados biométricos para controle de acesso, etc.

Dado anonimizado (Art. 5º, III)

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dados anonimizados não são considerados dados pessoais para os fins da LGPD, exceto quando o processo de anonimização for revertido.

Banco de dados (Art. 5º, IV)

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Inclui sistemas acadêmicos, cadastros de servidores, bibliotecas digitais, etc.

Titular (Art. 5º, V)

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Na universidade, são titulares: alunos, professores, servidores técnico-administrativos, terceirizados, visitantes, etc.

Controlador (Art. 5º, VI)

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso da UFPI, a própria instituição é a controladora dos dados que coleta e trata.

Operador (Art. 5º, VII)

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Podem ser empresas contratadas que processam dados em nome da universidade.

Encarregado ou DPO (Art. 5º, VIII)

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). É responsável por orientar funcionários sobre práticas de proteção de dados e receber reclamações e comunicações dos titulares.

Tratamento (Art. 5º, X)

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

Praticamente qualquer ação envolvendo dados pessoais é considerada tratamento, desde o momento da coleta até seu descarte.

Consentimento (Art. 5º, XII)

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. É uma das bases legais para o tratamento de dados, mas não a única, especialmente para órgãos públicos.

Relatório de impacto à proteção de dados pessoais (Art. 5º, XVII)

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.

Autoridade Nacional de Proteção de Dados — ANPD (Art. 5º, XIX)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. A ANPD foi criada pela Lei nº 13.853/2019 e tem competência para regular, fiscalizar e aplicar sanções em caso de descumprimento da LGPD.

A compreensão desses conceitos é fundamental para a aplicação correta da LGPD no contexto da administração pública e, especificamente, nas instituições de ensino superior como a UFPI.

1.3. Princípios da proteção de dados

A LGPD estabelece em seu artigo 6º dez princípios fundamentais que devem nortear todo e qualquer tratamento de dados pessoais. Esses princípios são a base para a interpretação e aplicação da lei, oferecendo diretrizes para situações não explicitamente previstas. Vejamos cada um deles:

1. Princípio da Finalidade

O tratamento de dados deve ter propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Aplicação prática: A universidade deve especificar claramente por que está coletando determinados dados dos alunos, professores ou funcionários. Por exemplo, ao coletar endereços residenciais, deve informar que isso serve para envio de correspondências oficiais ou para registro acadêmico.

2. Princípio da Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Aplicação prática: Se a UFPI coleta o número de telefone de um aluno para contato em casos de emergência, não deve utilizar esse dado para enviar propagandas ou para outras finalidades não relacionadas.

3. Princípio da Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Aplicação prática: Em um formulário de matrícula, a universidade não deve solicitar informações que não sejam necessárias para o processo educacional, como preferências de consumo ou hobbies não relacionados ao curso.

4. Princípio do Livre Acesso

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Aplicação prática: A UFPI deve disponibilizar mecanismos para que alunos, professores e servidores possam acessar facilmente todos os dados pessoais que a instituição mantém sobre eles.

5. Princípio da Qualidade dos Dados

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Aplicação prática: A universidade deve implementar processos para manter os dados de sua comunidade acadêmica atualizados e precisos, como solicitações periódicas de atualização cadastral.

6. Princípio da Transparência

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Aplicação prática: A UFPI deve ter políticas de privacidade claras e acessíveis, explicando como coleta, utiliza, armazena e compartilha dados pessoais.

7. Princípio da Segurança

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Aplicação prática: Implementação de controles de acesso a sistemas, criptografia de dados sensíveis, backups regulares, e treinamento de pessoal sobre segurança da informação.

8. Princípio da Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Aplicação prática: Realização de avaliações de impacto à proteção de dados antes de implementar novos processos ou sistemas que envolvam o tratamento de dados pessoais significativos.

9. Princípio da Não Discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Aplicação prática: A universidade não deve utilizar dados sobre origem racial, orientação sexual ou opiniões políticas para discriminar estudantes ou funcionários em processos de seleção, avaliação ou promoção.

10. Princípio da Responsabilização e Prestação de Contas

Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Aplicação prática: A UFPI deve documentar todas as medidas adotadas para cumprir a LGPD, como políticas internas, treinamentos, contratos com fornecedores, e estar preparada para demonstrar esse cumprimento quando solicitado pela ANPD ou pelos titulares.

Estes princípios não são meras recomendações, mas requisitos legais que devem ser observados em todas as operações de tratamento de dados pessoais. Eles fornecem um quadro ético e legal para orientar decisões sobre como lidar com dados pessoais na instituição.

1.4. Direitos dos titulares

A LGPD fortalece significativamente os direitos dos titulares em relação aos seus dados pessoais. O artigo 18 da lei estabelece um catálogo de direitos que devem ser respeitados por todos os agentes de tratamento, incluindo as instituições públicas. Conhecer e garantir esses direitos é essencial para o cumprimento da lei.

Direito à confirmação de existência de tratamento

O titular tem o direito de saber se a instituição realiza tratamento de seus dados pessoais.

Exemplo: Um ex-aluno pode solicitar à UFPI confirmação sobre se seus dados ainda estão armazenados nos sistemas da universidade.

Direito de acesso aos dados

O titular tem direito a acessar todos os seus dados pessoais que estão sendo tratados pela instituição.

Exemplo: Um servidor pode solicitar acesso a todos os seus dados funcionais, incluindo avaliações de desempenho e registros de ponto.

Direito à correção de dados incompletos, inexatos ou desatualizados

O titular pode solicitar a correção de dados que estejam incorretos ou desatualizados.

Exemplo: Um professor pode solicitar a correção de seu endereço ou telefone no cadastro da universidade.

Direito à anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos

O titular pode solicitar que seus dados sejam anonimizados, bloqueados ou eliminados quando forem desnecessários ou excessivos para a finalidade do tratamento.

Exemplo: Um aluno pode solicitar que informações sobre sua religião, coletadas em um formulário antigo, sejam removidas por não serem necessárias para fins acadêmicos.

Direito à portabilidade dos dados

O titular pode solicitar que seus dados sejam transferidos para outro fornecedor de serviço ou produto, respeitados os segredos comercial e industrial.

Exemplo: Um aluno que está se transferindo para outra instituição pode solicitar que seus dados acadêmicos sejam fornecidos em formato que permita a transferência.

Direito à eliminação dos dados tratados com consentimento

O titular pode solicitar a eliminação de dados tratados com base no seu consentimento.

Exemplo: Um participante de pesquisa acadêmica que consentiu com o uso de seus dados pode revogar esse consentimento e solicitar a eliminação dos dados.

Direito à informação sobre compartilhamento de dados

O titular tem direito a informações sobre as entidades públicas e privadas com as quais seus dados foram compartilhados.

Exemplo: Um servidor pode solicitar informações sobre quais órgãos externos receberam seus dados funcionais.

Direito à informação sobre a possibilidade de não fornecer consentimento

O titular deve ser informado sobre as consequências de não fornecer consentimento para o tratamento de seus dados.

Exemplo: Um aluno deve ser informado que, ao não consentir com o uso de sua imagem, não poderá participar de determinadas atividades que envolvam registros fotográficos ou audiovisuais.

Direito à revogação do consentimento

O titular pode revogar o consentimento a qualquer momento, mediante manifestação expressa.

Exemplo: Um servidor que consentiu com o uso de sua imagem em materiais promocionais da universidade pode revogar esse consentimento para usos futuros.

Direito de petição à ANPD

O titular tem direito de peticionar contra o controlador perante a Autoridade Nacional de Proteção de Dados (ANPD).

Exemplo: Um aluno que teve seu pedido de acesso aos dados negado pela universidade pode apresentar uma reclamação à ANPD.

Direito de oposição

O titular pode se opor ao tratamento realizado com base em outras hipóteses de dispensa de consentimento, em caso de descumprimento da lei.

Exemplo: Um servidor pode se opor ao uso de seus dados para finalidades que considere incompatíveis com o propósito original da coleta.

Como garantir os direitos dos titulares na UFPI

Para garantir o efetivo exercício desses direitos, a UFPI deve:

- Estabelecer canais de comunicação claros: Definir e divulgar os meios pelos quais os titulares podem exercer seus direitos, como e-mail específico, formulário online ou atendimento presencial.
- Definir procedimentos internos: Estabelecer fluxos de trabalho para recebimento, análise e resposta às solicitações dos titulares, com prazos definidos.
- Treinar equipes: Capacitar os servidores responsáveis pelo atendimento às solicitações, garantindo conhecimento sobre a lei e os procedimentos internos.
- Manter registro das solicitações: Documentar todas as solicitações recebidas e as providências tomadas, para fins de prestação de contas.
- Responder em tempo adequado: A LGPD estabelece que as solicitações dos titulares devem ser atendidas sem custos e em formato simplificado imediatamente, ou por meio de declaração clara e completa em até 15 dias.
- Justificar negativas: Quando não for possível atender a uma solicitação, a instituição deve informar as razões de fato ou de direito que impedem a adoção imediata da providência.

O respeito aos direitos dos titulares é um dos pilares da LGPD e demonstra o compromisso da instituição com a transparência e a ética no tratamento de dados pessoais. Além disso, reduz riscos de sanções e

fortalece a confiança da comunidade acadêmica na gestão de dados pela universidade.

1.5. Aplicabilidade na administração pública

A LGPD aplica-se a toda pessoa natural ou jurídica, de direito público ou privado, que realize tratamento de dados pessoais. As instituições públicas, incluindo as universidades federais como a UFPI, estão, portanto, sujeitas às disposições da lei, com algumas particularidades importantes.

Especificidades da LGPD para o setor público

A LGPD contém disposições específicas para o tratamento de dados pela administração pública, reconhecendo sua natureza e finalidades particulares. Vamos explorar os principais aspectos relevantes para a UFPI:

1. Bases legais específicas (Art. 7º e 11)

A administração pública pode realizar tratamento de dados pessoais, incluindo dados sensíveis, para atender sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais ou cumprir suas atribuições legais.

Exemplo na UFPI: A universidade pode tratar dados de alunos sem necessidade de consentimento quando esse tratamento for necessário para a execução de políticas públicas educacionais previstas em leis ou regulamentos.

2. Compartilhamento de dados entre órgãos públicos (Art. 26)

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal, respeitados os princípios de proteção de dados.

Exemplo na UFPI: A universidade pode compartilhar dados de alunos com o Ministério da Educação para fins de censo educacional, desde que respeitados os princípios da LGPD.

3. Dispensa de consentimento para políticas públicas (Art. 7º, III)

O consentimento não é necessário quando o tratamento de dados for necessário para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Exemplo na UFPI: A coleta de dados socioeconômicos para programas de assistência estudantil pode ser realizada com base no interesse público, sem necessidade de consentimento específico.

4. Transparência ativa (Art. 23, I)

Os órgãos públicos devem informar as hipóteses em que realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas.

Exemplo na UFPI: A universidade deve publicar em seu site uma política de privacidade detalhando como trata os dados pessoais de alunos, servidores e terceiros.

5. Indicação de encarregado (Art. 23, III)

Os órgãos públicos devem indicar um encarregado pelo tratamento de dados pessoais (DPO — Data Protection Officer).

Exemplo na UFPI: A universidade deve designar formalmente um servidor ou equipe responsável por atuar como canal de comunicação entre a instituição, os titulares dos dados e a ANPD.

6. Sanções específicas (Art. 52, §3º)

As sanções aplicáveis aos órgãos públicos são diferentes das aplicáveis às entidades privadas, não incluindo multas pecuniárias, mas podendo incluir publicização da infração, bloqueio dos dados e eliminação dos dados pessoais.

Exemplo na UFPI: Em caso de vazamento de dados por falha de segurança, a universidade pode ser obrigada a divulgar publicamente a ocorrência e implementar medidas corretivas.

Desafios da implementação da LGPD em instituições federais de ensino

1. Volume e diversidade de dados

Universidades lidam com um grande volume de dados pessoais, de diversos tipos e para múltiplas finalidades: dados acadêmicos, funcionais, de pesquisa, de extensão, etc.

2. Múltiplos setores e sistemas

A descentralização administrativa e a existência de diversos sistemas de informação, muitas vezes não integrados, dificultam a gestão unificada dos dados.

3. Cultura organizacional

Mudar práticas estabelecidas e criar uma cultura de proteção de dados exige esforço contínuo de conscientização e capacitação.

4. Restrições orçamentárias

A implementação de medidas técnicas e administrativas para adequação à LGPD pode exigir investimentos em tecnologia, consultoria e capacitação.

Boas práticas para implementação da LGPD na UFPI

1. Criar uma Política de Privacidade e Proteção de Dados

Desenvolver e publicar um documento que estabeleça diretrizes claras sobre como a universidade trata dados pessoais.

2. Estabelecer Governança de Dados

Criar estruturas de governança, como comitês ou grupos de trabalho, para coordenar as ações de adequação à LGPD.

3. Mapear o ciclo de vida dos dados

Identificar todos os processos que envolvem dados pessoais, desde a coleta até o descarte, documentando finalidades, bases legais e medidas de segurança.

4. Revisar contratos e convênios

Adequar instrumentos jurídicos que envolvam compartilhamento de dados com terceiros, incluindo cláusulas específicas sobre proteção de dados.

5. Implementar medidas de segurança

Adotar controles técnicos e administrativos para proteger os dados contra acessos não autorizados, vazamentos e outros incidentes.

6. Desenvolver procedimentos para atender direitos dos titulares

Estabelecer fluxos claros para recebimento e resposta a solicitações de acesso, correção, eliminação e outros direitos garantidos pela LGPD.

7. Promover capacitação contínua

Realizar treinamentos e campanhas de conscientização para servidores, professores e colaboradores sobre a importância da proteção de dados.

A implementação da LGPD na administração pública, e especificamente em instituições federais de ensino como a UFPI, representa um desafio significativo, mas também uma oportunidade para aprimorar a gestão de dados, aumentar a transparência e fortalecer a confiança da comunidade acadêmica. Ao seguir as boas práticas e compreender as especificidades da lei para o setor público, a universidade pode não apenas cumprir suas obrigações legais, mas também se tornar referência em governança e proteção de dados.

MÓDULO 2 — DADOS PESSOAIS: IDENTIFICAÇÃO E CLASSIFICAÇÃO

2.1. Definição e tipos de dados pessoais

Definição de dados pessoais na LGPD

De acordo com o art. 5º, inciso I da LGPD, dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". Esta definição é intencionalmente ampla para abranger diversos tipos de informações que, direta ou indiretamente, possam levar à identificação de uma pessoa.

A definição contempla dois cenários:

- Pessoa identificada: quando a informação já revela diretamente quem é a pessoa.
- Pessoa identificável: quando a informação, combinada com outras, permite identificar a pessoa, mesmo que não o faça imediatamente.

Tipos de dados pessoais

Os dados pessoais podem ser classificados de diferentes formas, dependendo de sua natureza e do risco associado ao seu tratamento. Vamos analisar os principais tipos:

1. Dados de identificação direta

São aqueles que identificam a pessoa imediatamente, sem necessidade de combinação com outras informações:

- Nome completo

- CPF, RG, passaporte
- Carteira de trabalho, título de eleitor
- Número de matrícula institucional
- Foto
- Endereço residencial completo
- Endereço de e-mail pessoal/institucional
- Número de telefone

2. Dados de identificação indireta

São aqueles que, isoladamente, podem não identificar uma pessoa, mas quando combinados com outros dados, permitem sua identificação:

- Data de nascimento
- Profissão
- Cargo
- Formação acadêmica
- Dados de localização (GPS)
- Endereço IP
- Cookies de navegação
- Matrícula funcional genérica

3. Dados pessoais sensíveis

Conforme o art. 5º, inciso II da LGPD, dados pessoais sensíveis são aqueles sobre:

- Origem racial ou étnica
- Convicção religiosa
- Opinião política

- Filiação a sindicato ou organização de caráter religioso, filosófico ou político
- Dados referentes à saúde ou à vida sexual
- Dados genéticos ou biométricos

Estes dados recebem proteção especial da lei por seu potencial discriminatório ou por revelarem aspectos íntimos da personalidade, dignidade ou privacidade do titular.

4. Dados anonimizados

São dados que, após passarem por técnicas de anonimização, não podem mais ser associados a um indivíduo específico, considerando meios técnicos razoáveis e disponíveis. Conforme o art. 12 da LGPD, dados anonimizados não são considerados dados pessoais, exceto quando o processo de anonimização for revertido.

5. Dados pseudonimizados

São dados que passaram por processo no qual um elemento identificador (como nome ou CPF) é substituído por um pseudônimo (código ou identificador artificial). A pseudonimização não é anonimização completa, pois permite a reidentificação mediante uso de informações adicionais mantidas separadamente. Dados pseudonimizados continuam sendo considerados dados pessoais.

Dados pessoais no contexto universitário

No ambiente de uma universidade federal como a UFPI, diversos tipos de dados pessoais são tratados rotineiramente:

Dados de estudantes:

- Informações cadastrais (nome, RG, CPF, endereço)
- Histórico acadêmico e notas
- Frequência às aulas
- Dados socioeconômicos (para programas de assistência)

- Informações sobre deficiências e necessidades especiais
- Registros de atendimento psicológico ou médico
- Dados de contato de familiares ou responsáveis
- Biometria (para acesso a laboratórios ou restaurantes)
- Registros de acesso ao campus e uso de sistemas

Dados de servidores (docentes e técnicos):

- Informações cadastrais e funcionais
- Dados bancários
- Histórico profissional e acadêmico
- Avaliações de desempenho
- Registros de ponto e licenças
- Prontuários médicos ocupacionais
- Filiação sindical
- Dados de dependentes

Dados de terceiros:

- Informações de fornecedores e prestadores de serviço
- Dados de visitantes
- Participantes de eventos e projetos de extensão
- Voluntários de pesquisas acadêmicas

Identificação de dados pessoais: perguntas-chave

Para ajudar a identificar se uma informação constitui dado pessoal, considere as seguintes perguntas:

- A informação está relacionada a uma pessoa natural?
- Se estiver relacionada a pessoa jurídica, não é dado pessoal
- Se for dado anonimizado de forma irreversível, não é dado pessoal

- A informação permite identificar a pessoa diretamente?
- Nome, documento, foto, etc.
- A informação, combinada com outras, permite identificar a pessoa?
- Cargo + departamento
- Data de nascimento + cidade natal + profissão
- A informação revela aspectos sensíveis sobre a pessoa?
- Saúde, religião, opinião política, etc.
- A informação está relacionada à vida privada da pessoa?
- Hábitos, preferências, relacionamentos, etc.

Compreender o conceito e os diferentes tipos de dados pessoais é o primeiro passo para implementar adequadamente a LGPD, pois permite identificar corretamente quais informações estão sujeitas à proteção da lei e quais exigem cuidados específicos no tratamento.

2.2. Dados pessoais sensíveis

Os dados pessoais sensíveis merecem atenção especial na LGPD devido ao seu potencial de causar discriminação ou danos significativos aos titulares se utilizados indevidamente. A lei estabelece proteções mais rigorosas e bases legais específicas para o tratamento dessas informações.

Definição legal de dados sensíveis

Conforme o art. 5º, inciso II da LGPD, dado pessoal sensível é:

"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."

Categorias de dados sensíveis

Vamos analisar cada categoria de dados sensíveis prevista na LGPD:

1. Origem racial ou étnica

Informações sobre raça, cor, etnia, nacionalidade ou origem geográfica que possam identificar determinado grupo étnico-racial.

Exemplos na UFPI:

- Autodeclarações para políticas de ações afirmativas
- Registros de nacionalidade de estudantes estrangeiros
- Dados coletados em censos institucionais sobre composição étnico-racial

2. Convicção religiosa

Informações sobre crenças, filiação religiosa, participação em cerimônias religiosas ou solicitações de acomodações por motivos religiosos.

Exemplos na UFPI:

- Registros de necessidades especiais por motivos religiosos (como alimentação ou data de exames)
- Informações sobre filiação religiosa em pesquisas acadêmicas

3. Opinião política

Informações sobre posições políticas, participação em manifestações, filiação partidária ou apoio a causas políticas.

Exemplos na UFPI:

- Registros de filiação a grupos estudantis de natureza política
- Dados sobre posicionamentos políticos em pesquisas acadêmicas

4. Filiação a sindicato ou organização de caráter religioso, filosófico ou político

Informações sobre associação a entidades que revelem perspectivas ideológicas, filosóficas ou políticas.

Exemplos na UFPI:

- Registros de descontos de contribuição sindical em folha de pagamento
- Dados sobre participação em greves ou movimentos sindicais
- Afiliações a organizações estudantis

5. Dados referentes à saúde

Informações sobre estado de saúde física ou mental, histórico médico, tratamentos, doenças, deficiências ou qualquer dado relacionado à saúde de um indivíduo.

Exemplos na UFPI:

- Atestados médicos
- Laudos de condições especiais para acessibilidade
- Registros de saúde ocupacional de servidores
- Dados de prontuários dos serviços de assistência estudantil
- Informações sobre deficiências para adaptações pedagógicas
- Resultados de exames médicos admissionais

6. Dados referentes à vida sexual

Informações sobre orientação sexual, identidade de gênero, comportamento sexual ou questões relacionadas à intimidade sexual.

Exemplos na UFPI:

- Registros para uso de nome social
- Dados de estudos e pesquisas sobre sexualidade
- Informações para políticas específicas para população LGBTQIA+

7. Dados genéticos

Informações sobre características hereditárias ou adquiridas de uma pessoa natural, obtidas pela análise de amostra biológica.

Exemplos na UFPI:

- Dados de pesquisas científicas envolvendo material genético
- Registros de laboratórios de genética
- Resultados de testes genéticos realizados em pesquisas ou serviços de saúde

8. Dados biométricos

Características físicas, fisiológicas ou comportamentais que podem identificar univocamente uma pessoa.

Exemplos na UFPI:

- Registros de impressões digitais para controle de acesso
- Reconhecimento facial em sistemas de segurança
- Padrões de voz para autenticação em sistemas
- Assinaturas manuscritas digitalizadas

Bases legais para tratamento de dados sensíveis

O art. 11 da LGPD estabelece as hipóteses em que o tratamento de dados sensíveis é permitido. As principais são:

- Consentimento específico e destacado: O titular consente de forma específica e destacada para finalidades específicas.
- Cumprimento de obrigação legal: Quando necessário para cumprimento de obrigação legal ou regulatória pelo controlador.
- Políticas públicas: Pela administração pública, para execução de políticas públicas previstas em leis ou regulamentos.
- Estudos por órgão de pesquisa: Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados.
- Exercício regular de direitos: Em processos judiciais, administrativos ou arbitrais.
- Proteção da vida ou incolumidade física: Do titular ou terceiro, quando necessário.

- Tutela da saúde: Exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- Garantia de prevenção à fraude e segurança: Em processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Cuidados específicos no tratamento de dados sensíveis

Ao tratar dados sensíveis, a UFPI deve adotar cuidados específicos:

1. Medidas de segurança reforçadas

- Criptografia de dados sensíveis
- Controles de acesso mais rigorosos
- Registro detalhado (logs) de acesso a dados sensíveis
- Avaliação periódica de vulnerabilidades

2. Minimização da coleta

- Coletar apenas dados sensíveis estritamente necessários
- Verificar se alternativas menos invasivas estão disponíveis
- Descartar dados sensíveis quando não forem mais necessários

3. Anonimização quando possível

- Utilizar técnicas de anonimização para pesquisas acadêmicas
- Considerar o uso de dados agregados em vez de individualizados
- Implementar técnicas de pseudonimização como medida de segurança

4. Transparência reforçada

- Informar claramente o titular sobre a coleta de dados sensíveis
- Destacar as finalidades específicas do tratamento
- Explicar por que o tratamento é necessário e as consequências

5. Relatório de impacto

- Realizar Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para tratamentos envolvendo grande volume de dados sensíveis
- Documentar medidas mitigadoras de riscos implementadas

6. Consentimento específico

- Quando o consentimento for a base legal, garantir que seja:
- Específico para cada finalidade
- Destacado das demais autorizações
- Informado sobre consequências do fornecimento
- Passível de revogação facilitada

Dados sensíveis em instituições de ensino: desafios específicos

Instituições como a UFPI enfrentam desafios particulares no tratamento de dados sensíveis:

1. Pesquisas acadêmicas

Muitas pesquisas envolvem coleta de dados sensíveis, exigindo protocolos éticos rigorosos e aprovação de comitês de ética.

2. Assistência estudantil

Programas de assistência frequentemente necessitam de dados socioeconômicos, de saúde ou outros dados sensíveis para determinar elegibilidade e oferecer suporte adequado.

3. Acessibilidade e inclusão

Para garantir acessibilidade, a instituição precisa coletar dados sobre deficiências e necessidades especiais.

4. Saúde ocupacional

A gestão de recursos humanos envolve o tratamento de dados de saúde de servidores para licenças, abonos e programas de saúde ocupacional.

5. Ações afirmativas

Políticas de cotas e ações afirmativas exigem tratamento de dados sobre origem racial, deficiências e outros dados sensíveis.

O tratamento adequado dos dados sensíveis é crucial não apenas para o cumprimento da LGPD, mas também para a proteção da dignidade e dos direitos fundamentais dos titulares. Ao implementar medidas técnicas e organizacionais específicas para esses dados, a UFPI demonstra seu compromisso com a privacidade e a não discriminação da sua comunidade acadêmica.

2.3. Dados de crianças e adolescentes

A LGPD dedica uma seção específica (Seção III do Capítulo II) ao tratamento de dados de crianças e adolescentes, reconhecendo a vulnerabilidade desse grupo e estabelecendo proteções especiais. Para instituições de ensino como a UFPI, que podem ter alunos menores de idade em seus cursos de graduação ou em programas de extensão, esse tema merece atenção especial.

Definições importantes

- Criança: Pessoa até 12 anos de idade incompletos (conforme Estatuto da Criança e do Adolescente — ECA)
- Adolescente: Pessoa entre 12 e 18 anos de idade (conforme ECA)
- Responsável legal: Pais ou tutores legalmente designados

Regras específicas para tratamento de dados de crianças e adolescentes

1. Consentimento específico por pelo menos um dos pais ou responsável legal (Art. 14, §1º)

O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Esta é uma regra fundamental que diferencia o tratamento de dados de crianças dos demais.

Aplicação na UFPI:

- Formulários de matrícula em cursos de extensão para menores
- Autorizações para participação em atividades acadêmicas
- Consentimento para uso de imagem em eventos institucionais

2. Exceção ao consentimento (Art. 14, §3º)

O consentimento não é exigido quando a coleta for necessária para contatar os pais ou o responsável legal, utilizada uma única vez e sem armazenamento, ou para proteção da criança, e em nenhum caso poderá ser repassada a terceiro sem consentimento.

Aplicação na UFPI:

- Coleta de contato dos pais durante uma visita escolar ao campus
- Registro temporário para emissão de crachá de acesso

3. Melhor interesse da criança e do adolescente (Art. 14, caput)

O tratamento de dados deve ser realizado no melhor interesse da criança e do adolescente, ou seja, priorizando seu desenvolvimento saudável e proteção integral.

Aplicação na UFPI:

- Uso de dados para garantir acessibilidade e inclusão
- Coleta de informações para adequar métodos pedagógicos

4. Informações simples, claras e acessíveis (Art. 14, §6º)

Os controladores devem manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos, em formato acessível e adequado ao entendimento de crianças e adolescentes.

Aplicação na UFPI:

- Políticas de privacidade em linguagem simplificada
- Materiais informativos adaptados para diferentes faixas etárias

5. Vedação de condicionamento (Art. 14, §4º)

É vedado condicionar a participação em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Aplicação na UFPI:

- Plataformas educacionais não podem exigir dados excessivos
- Atividades extracurriculares não podem depender de dados desnecessários

Cuidados especiais no ambiente universitário

1. Identificação de menores de idade

A universidade deve ter mecanismos para identificar alunos menores de idade e aplicar as proteções especiais previstas na LGPD.

Boas práticas:

- Marcação especial em sistemas acadêmicos para estudantes menores de 18 anos
- Fluxos diferenciados para coleta e tratamento de dados desses estudantes

2. Programas de extensão com participação de menores

Atividades de extensão que envolvam crianças e adolescentes devem contar com processos específicos para obtenção de consentimento dos responsáveis.

Boas práticas:

- Termos de consentimento específicos com linguagem clara
- Procedimentos de verificação da autorização do responsável

3. Pesquisas acadêmicas envolvendo menores

Pesquisas que coletam dados de crianças e adolescentes devem seguir protocolos éticos rigorosos e específicos, além das exigências da LGPD.

Boas práticas:

- Aprovação pelo Comitê de Ética em Pesquisa
- Consentimento dos responsáveis e assentimento dos menores, quando possível
- Anonimização prioritária dos dados

4. Eventos e registros audiovisuais

Eventos universitários que possam contar com a participação de menores devem ter cuidados específicos quanto ao registro e uso de imagens.

Boas práticas:

- Autorizações específicas para uso de imagem assinadas pelos responsáveis
- Sinalização clara em áreas onde estão sendo realizadas gravações
- Opção de não identificação em publicações de fotos e vídeos

5. Proteção contra acesso indevido

Dados de menores devem contar com proteções de segurança reforçadas para evitar acessos não autorizados.

Boas práticas:

- Controles de acesso mais rigorosos para bases de dados com informações de menores
- Criptografia de dados sensíveis de crianças e adolescentes
- Restrição de compartilhamento com terceiros

Desafios específicos para instituições de ensino superior

1. Alunos de graduação menores de idade

Muitos estudantes ingressam na universidade antes de completar 18 anos, criando situações em que a instituição deve equilibrar a autonomia do estudante universitário com as proteções legais aos menores de idade.

Abordagem recomendada:

- Identificar claramente os alunos menores de idade nos sistemas

- Criar procedimentos específicos para situações que exijam consentimento dos responsáveis
- Desenvolver políticas que respeitem a crescente autonomia do adolescente enquanto cumprem as exigências legais

2. Projetos com escolas

Universidades frequentemente desenvolvem projetos em parceria com escolas de educação básica, envolvendo interação com crianças e adolescentes.

Abordagem recomendada:

- Estabelecer protocolos claros para obtenção de consentimento através das escolas parceiras
- Definir responsabilidades de cada instituição quanto à proteção de dados
- Limitar a coleta de dados ao mínimo necessário para a finalidade educacional

3. Estágios em licenciaturas

Estudantes de licenciatura realizam estágios em escolas, podendo ter acesso a dados de alunos menores de idade.

Abordagem recomendada:

- Incluir orientações sobre proteção de dados na preparação para estágios
- Estabelecer termos de confidencialidade específicos
- Orientar sobre as responsabilidades legais ao lidar com dados de menores

A proteção especial aos dados de crianças e adolescentes é um dos pontos mais sensíveis da LGPD e requer atenção particular das instituições de ensino. Ao implementar controles específicos para esse grupo, a UFPI não apenas cumpre a legislação, mas também reforça seu compromisso com a proteção integral das crianças e adolescentes que participam de suas atividades acadêmicas, de pesquisa e extensão.

2.4. Ciclo de vida dos dados

O ciclo de vida dos dados pessoais compreende todas as fases desde sua coleta inicial até sua eliminação definitiva. Compreender esse ciclo é fundamental para uma gestão adequada de dados conforme a LGPD, pois cada fase requer procedimentos e cuidados específicos para garantir a conformidade legal e a proteção dos direitos dos titulares.

Fases do ciclo de vida dos dados

1. Coleta

A fase inicial em que os dados são obtidos do titular ou de outras fontes.

Requisitos LGPD:

- Identificar a base legal aplicável
- Obter consentimento quando necessário
- Informar a finalidade da coleta
- Coletar apenas dados necessários (minimização)

Exemplos na UFPI:

- Formulários de matrícula
- Cadastro de servidores
- Inscrições em processos seletivos
- Registros de atendimentos
- Questionários de pesquisa

Boas práticas:

- Revisar formulários para eliminar campos desnecessários
- Criar avisos de privacidade claros
- Separar dados obrigatórios de opcionais
- Documentar a base legal para cada categoria de dado coletado

2. Processamento

Fase em que os dados são utilizados, manipulados, organizados ou alterados para cumprir a finalidade para a qual foram coletados.

Requisitos LGPD:

- Respeitar a finalidade informada
- Garantir a qualidade dos dados
- Limitar o processamento ao necessário
- Registrar as operações de tratamento

Exemplos na UFPI:

- Cálculo de notas e frequências
- Processamento de folha de pagamento
- Análise de dados para relatórios institucionais
- Verificação de elegibilidade para programas de assistência

Boas práticas:

- Documentar procedimentos de processamento
- Implementar controles de acesso baseados em perfis
- Validar periodicamente a qualidade e precisão dos dados
- Realizar auditorias de tratamento

3. Armazenamento

Fase em que os dados são guardados em sistemas, bancos de dados, arquivos físicos ou outros meios.

Requisitos LGPD:

- Implementar medidas de segurança técnicas e administrativas
- Definir prazos de retenção
- Proteger contra acessos não autorizados

- Garantir a integridade dos dados

Exemplos na UFPI:

- Sistemas acadêmicos
- Sistemas de recursos humanos
- Arquivos físicos de documentos
- Backups e cópias de segurança
- Bancos de dados de pesquisa

Boas práticas:

- Definir políticas de retenção por categoria de dados
- Implementar criptografia para dados sensíveis
- Realizar testes periódicos de restauração de backups
- Documentar os locais físicos e digitais onde os dados são armazenados

4. Compartilhamento

Fase em que os dados são transferidos para terceiros ou compartilhados entre diferentes setores da instituição.

Requisitos LGPD:

- Verificar a base legal para compartilhamento
- Informar os titulares sobre compartilhamentos
- Estabelecer contratos com operadores
- Registrar todas as transferências

Exemplos na UFPI:

- Envio de dados para o MEC (Censo da Educação Superior)
- Compartilhamento entre departamentos da universidade
- Transferências para instituições parceiras
- Compartilhamento com órgãos de fomento à pesquisa

Boas práticas:

- Mapear todos os compartilhamentos de dados
- Estabelecer acordos de compartilhamento formais
- Utilizar meios seguros para transferência de dados
- Avaliar a necessidade e proporcionalidade de cada compartilhamento

5. Arquivamento

Fase em que os dados não são mais utilizados regularmente, mas são mantidos para fins históricos, estatísticos, de auditoria ou obrigações legais.

Requisitos LGPD:

- Manter apenas pelo tempo necessário
- Implementar controles de acesso mais restritos
- Garantir a integridade dos dados arquivados
- Documentar a justificativa para retenção prolongada

Exemplos na UFPI:

- Históricos acadêmicos de ex-alunos
- Registros funcionais de servidores aposentados
- Dados de pesquisas concluídas
- Documentos institucionais históricos

Boas práticas:

- Definir política específica para arquivamento
- Revisar periodicamente a necessidade de manutenção
- Considerar técnicas de pseudonimização
- Estabelecer níveis de acesso diferentes para dados arquivados

6. Eliminação

Fase final em que os dados são removidos permanentemente dos sistemas e arquivos.

Requisitos LGPD:

- Eliminar dados quando a finalidade foi alcançada
- Atender solicitações de eliminação dos titulares
- Documentar o processo de eliminação
- Garantir que a eliminação seja completa e segura

Exemplos na UFPI:

- Exclusão de dados de candidatos não aprovados após prazo legal
- Descarte seguro de documentos físicos
- Eliminação de dados de pesquisas após período de guarda
- Limpeza de bancos de dados temporários

Boas práticas:

- Implementar rotinas automatizadas de eliminação baseadas em prazos
- Utilizar técnicas seguras de eliminação digital (wipe)
- Criar registros de eliminação para fins de auditoria
- Estabelecer procedimentos específicos para descarte de mídias físicas

Gestão do ciclo de vida dos dados

Para gerenciar adequadamente o ciclo de vida dos dados segundo a LGPD, a UFPI deve implementar:

1. Inventário de dados pessoais

Documento que identifica quais dados são coletados, para quais finalidades, com quais bases legais, onde são armazenados, e assim por diante. O inventário é a base para qualquer programa de governança de dados.

Elementos essenciais:

- Categorias de dados pessoais

- Finalidades do tratamento
- Bases legais utilizadas
- Locais de armazenamento
- Período de retenção
- Medidas de segurança adotadas
- Compartilhamentos realizados

2. Política de retenção de dados

Documento que estabelece por quanto tempo cada categoria de dados deve ser mantida, com base em requisitos legais, necessidades operacionais e direitos dos titulares.

Aspectos a considerar:

- Requisitos legais (ex: legislação trabalhista, normas do MEC)
- Período necessário para cumprir a finalidade
- Riscos de manutenção prolongada
- Processos de revisão periódica

3. Procedimentos para exercício de direitos dos titulares

Processos definidos para atender solicitações dos titulares em cada fase do ciclo de vida, como acesso, correção, anonimização, exclusão, etc.

Requisitos básicos:

- Canal de atendimento dedicado
- Prazos de resposta definidos
- Fluxos de aprovação internos
- Documentação das solicitações e respostas

4. Classificação de dados

Sistema para categorizar os dados de acordo com sua sensibilidade e requisitos de proteção.

Exemplo de classificação:

- Públicos: dados que podem ser amplamente divulgados
- Internos: dados com acesso restrito à comunidade universitária
- Confidenciais: dados com acesso limitado a pessoas específicas
- Restritos: dados sensíveis com controles de acesso rigorosos

Desafios do ciclo de vida em instituições de ensino

Instituições como a UFPI enfrentam desafios específicos na gestão do ciclo de vida dos dados:

1. Longo período de retenção acadêmica

Registros acadêmicos muitas vezes precisam ser mantidos por décadas ou permanentemente, criando desafios para atualização, segurança e gestão.

Abordagem recomendada:

- Definir diferentes níveis de acesso conforme a antiguidade dos dados
- Implementar revisões periódicas para dados mantidos por longos períodos
- Considerar a pseudonimização ou anonimização de dados históricos quando possível

2. Múltiplos sistemas e repositórios

Universidades tipicamente utilizam diversos sistemas que coletam e armazenam dados, muitas vezes sem integração.

Abordagem recomendada:

- Mapear todos os sistemas que processam dados pessoais
- Implementar governança centralizada de dados
- Desenvolver políticas unificadas de ciclo de vida
- Trabalhar para integrar ou harmonizar sistemas dispersos

3. Pesquisas acadêmicas

Dados coletados para pesquisas têm requisitos específicos de armazenamento, compartilhamento e publicação.

Abordagem recomendada:

- Estabelecer diretrizes específicas para dados de pesquisa
- Promover a anonimização sempre que possível
- Definir políticas para compartilhamento internacional de dados
- Criar repositórios seguros para dados de pesquisa

4. Transferência de conhecimento institucional

A rotatividade de pessoal e mudanças administrativas podem levar à perda de conhecimento sobre dados históricos.

Abordagem recomendada:

- Documentar metadados e contexto dos dados
- Criar manuais de procedimentos para gestão de dados
- Implementar treinamento contínuo sobre gestão do ciclo de vida
- Estabelecer responsabilidades claras para custódia de dados

A gestão adequada do ciclo de vida dos dados é essencial para o cumprimento da LGPD e para a proteção efetiva dos direitos dos titulares. Ao implementar controles em cada fase, a UFPI não apenas reduz riscos legais, mas também melhora a qualidade e a confiabilidade de seus dados, resultando em processos mais eficientes e transparentes.

2.5. Mapeamento de dados na instituição

O mapeamento de dados é um processo fundamental para a adequação à LGPD, pois permite identificar onde, como e por que os dados pessoais são tratados na instituição. Este processo serve como base para outras ações de conformidade e ajuda a instituição a compreender seus fluxos de dados de forma abrangente.

Objetivos do mapeamento de dados

- Identificar todos os dados pessoais tratados pela instituição em seus diversos departamentos e sistemas
- Documentar os fluxos de dados desde a coleta até a eliminação
- Identificar riscos e vulnerabilidades no tratamento de dados
- Avaliar a conformidade com os princípios e requisitos da LGPD
- Fornecer base para decisões sobre medidas de adequação necessárias
- Permitir a transparência com os titulares sobre o tratamento de seus dados

Etapas do mapeamento de dados

1. Planejamento

Nesta fase inicial, definem-se o escopo, os recursos necessários e a metodologia a ser utilizada no mapeamento.

Atividades principais:

- Formar equipe multidisciplinar (TI, jurídico, áreas finalísticas)
- Definir cronograma e metodologia
- Identificar stakeholders em cada área
- Elaborar questionários e templates
- Definir ferramentas de documentação

2. Identificação de processos de tratamento

Levantamento de todos os processos institucionais que envolvem dados pessoais.

Atividades principais:

- Entrevistar gestores e equipes
- Analisar documentação existente
- Revisar procedimentos operacionais

- Identificar sistemas e aplicações
- Listar bancos de dados e repositórios

Exemplos na UFPI:

- Processo seletivo e matrícula
- Gestão acadêmica (notas, frequência, histórico)
- Gestão de recursos humanos
- Assistência estudantil
- Biblioteca
- Pesquisa e extensão
- Comunicação institucional

3. Catalogação dos dados pessoais

Documentação detalhada de cada categoria de dado pessoal tratado, incluindo suas características e contexto.

Informações a registrar:

- Tipos e categorias de dados pessoais
- Classificação (comum ou sensível)
- Volume aproximado
- Formato de armazenamento (físico/digital)
- Finalidades do tratamento
- Base legal aplicável
- Responsáveis pelo tratamento
- Período de retenção

Exemplo de categorização para um departamento acadêmico:

- Dados cadastrais: matrícula, nome, CPF, data de nascimento
- Dados de contato: endereço, telefone, e-mail

- Dados acadêmicos: notas, frequência, histórico, trabalhos
- Dados sensíveis: informações de saúde para abono de faltas, dados biométricos para acesso a laboratórios

4. Mapeamento de fluxos de dados

Análise e documentação do caminho que os dados percorrem dentro e fora da instituição.

Aspectos a mapear:

- Origem dos dados (de onde vêm)
- Sistemas e locais de armazenamento
- Transferências internas entre departamentos
- Compartilhamentos externos
- Perfis de acesso e níveis de permissão
- Processos de backup e recuperação
- Procedimentos de eliminação

Técnicas de documentação:

- Diagramas de fluxo de dados
- Mapas de calor de dados
- Matrizes de relacionamento
- Inventários de sistemas

5. Avaliação de riscos

Identificação e análise dos riscos associados ao tratamento de dados em cada processo.

Riscos a considerar:

- Acesso não autorizado
- Vazamento de dados

- Uso para finalidades não informadas
- Retenção excessiva
- Dados excessivos ou desnecessários
- Falta de base legal adequada
- Vulnerabilidades técnicas ou organizacionais

Metodologia de avaliação:

- Determinar probabilidade e impacto de cada risco
- Priorizar riscos com base na severidade
- Identificar controles existentes e lacunas
- Recomendar medidas mitigadoras

6. Documentação e relatórios

Consolidação das informações levantadas em documentos estruturados para consulta e uso em ações de adequação.

Documentos a produzir:

- Inventário de dados pessoais
- Registro das atividades de tratamento
- Matriz de riscos
- Relatório de gaps de conformidade
- Recomendações de adequação

Setores críticos para mapeamento na UFPI

1. Secretaria Acadêmica

Dados tratados: informações cadastrais, registros acadêmicos, históricos, certificados Sistemas típicos: sistema de gestão acadêmica, arquivo físico de documentos Pontos críticos: volume de dados históricos, múltiplas finalidades de uso, longo período de retenção

2. Recursos Humanos

Dados tratados: dados funcionais, bancários, de saúde, dependentes Sistemas típicos: SIGRH, pastas funcionais, prontuários médicos Pontos críticos: dados sensíveis, múltiplos departamentos com acesso, obrigações legais específicas

3. Assistência Estudantil

Dados tratados: dados socioeconômicos, saúde, situação familiar Sistemas típicos: sistemas próprios, processos físicos, prontuários Pontos críticos: alta concentração de dados sensíveis, necessidade de compartilhamento interno

4. Departamentos de Pesquisa

Dados tratados: dados de participantes de pesquisas, resultados, publicações Sistemas típicos: bancos de dados de pesquisa, repositórios, questionários Pontos críticos: consentimento específico, compartilhamento externo, publicação de resultados

5. Tecnologia da Informação

Dados tratados: credenciais de acesso, logs, backups Sistemas típicos: servidores, sistemas de autenticação, ferramentas de monitoramento Pontos críticos: acesso privilegiado a todos os dados, controles de segurança, políticas de backup e recuperação

Ferramentas e métodos para mapeamento

1. Questionários e entrevistas

Aplicados aos responsáveis pelos setores para coleta inicial de informações sobre tratamento de dados.

2. Workshops de processo

Sessões colaborativas para mapear fluxos de dados em processos específicos com participação dos envolvidos.

3. Análise de documentação

Revisão de políticas, procedimentos, termos de uso e contratos para identificar tratamentos de dados documentados.

4. Inspeção de sistemas

Análise técnica dos sistemas para identificar quais dados são coletados, armazenados e processados.

5. Ferramentas de descoberta de dados

Soluções tecnológicas que ajudam a identificar automaticamente onde os dados pessoais estão armazenados na rede.

Desafios comuns no mapeamento

1. Dados dispersos

Informações pessoais frequentemente estão espalhadas em múltiplos sistemas, departamentos e até dispositivos pessoais.

Solução: abordagem metodológica que inclua todos os possíveis repositórios, incluindo sistemas-sombra.

2. Falta de documentação

Processos históricos ou desenvolvidos organicamente podem não ter documentação adequada sobre dados.

Solução: combinar entrevistas, análise de sistemas e verificação prática para reconstruir o conhecimento.

3. Complexidade organizacional

Universidades têm estruturas complexas com relativa autonomia entre departamentos e faculdades.

Solução: estabelecer pontos focais em cada unidade e padronizar a metodologia de coleta.

4. Volume de dados

O grande volume de dados acumulados ao longo do tempo torna o mapeamento completo desafiador.

Solução: abordagem por fases, priorizando áreas de maior risco ou volume de dados sensíveis.

O mapeamento de dados não é um evento único, mas um processo contínuo que deve ser atualizado sempre que novos processos são implementados ou mudanças significativas ocorrem. A UFPI deve estabelecer procedimentos para manter seu inventário de dados atualizado, garantindo que continue funcionando como uma base confiável para a gestão da privacidade na instituição.

MÓDULO 3 — TRATAMENTO DE DADOS

3.1. Bases legais para tratamento

A LGPD determina que todo tratamento de dados pessoais deve estar fundamentado em pelo menos uma das bases legais previstas na lei. Estas bases legais representam as hipóteses em que o tratamento de dados é permitido e são essenciais para garantir a licitude das operações realizadas pela UFPI.

Bases legais para dados pessoais comuns (Art. 7º)

1. Consentimento

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

Características:

- Deve ser específico para finalidades determinadas
- Precisa ser livre (sem coerção ou condicionamentos)
- Deve ser informado (com informações claras sobre o tratamento)
- Pode ser revogado a qualquer momento

Exemplos na UFPI:

- Autorização para uso de imagem em materiais institucionais
- Consentimento para receber informações sobre eventos
- Autorização para participação em pesquisas não obrigatórias

Limitações:

- Não é a base legal mais adequada para tratamentos necessários à prestação de serviços educacionais principais
- Não deve ser utilizada quando outra base legal for mais apropriada
- Pode ser fragilizada por desequilíbrios de poder entre controlador e titular

2. Cumprimento de obrigação legal ou regulatória

Definição: Tratamento necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador.

Características:

- Deve haver previsão legal ou regulatória específica
- A obrigação deve recair sobre o controlador
- O tratamento deve ser necessário para cumprir a obrigação

Exemplos na UFPI:

- Coleta de dados para o Censo da Educação Superior (obrigação junto ao MEC)
- Tratamento de dados para emissão de diplomas (conforme regulamentação)
- Registros de ponto de servidores (legislação trabalhista)
- Dados necessários para prestação de contas a órgãos de controle

3. Execução de políticas públicas

Definição: Tratamento necessário para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Características:

- Aplicável à administração pública, como a UFPI
- Deve haver vinculação clara com política pública estabelecida

- Necessita transparência sobre a finalidade e forma de tratamento

Exemplos na UFPI:

- Dados para programas de assistência estudantil
- Informações para implementação de políticas de ações afirmativas
- Registros para programas de integração com o mercado de trabalho
- Dados para avaliação e monitoramento de políticas educacionais

4. Realização de estudos por órgão de pesquisa

Definição: Tratamento para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Características:

- Aplicável a órgãos de pesquisa (a universidade se qualifica como tal)
- Deve priorizar a anonimização quando possível
- Finalidade estritamente acadêmica ou estatística

Exemplos na UFPI:

- Pesquisas acadêmicas desenvolvidas por docentes e discentes
- Estudos estatísticos sobre evasão, permanência e desempenho
- Avaliações institucionais e levantamentos
- Análises de perfil socioeconômico dos estudantes

5. Execução de contrato

Definição: Tratamento necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular.

Características:

- Deve existir uma relação contratual ou pré-contratual
- O tratamento deve ser necessário (e não apenas conveniente)

- Limitado aos dados essenciais para a finalidade contratual

Exemplos na UFPI:

- Dados para matrícula (contrato educacional)
- Informações para contratos de estágio
- Registros para convênios de intercâmbio
- Dados necessários para contratos de prestação de serviços

6. Exercício regular de direitos

Definição: Tratamento necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Características:

- Vinculado a processos formais (judiciais ou administrativos)
- Incluí tanto a defesa quanto a proposição de direitos
- Limitado aos dados necessários ao processo específico

Exemplos na UFPI:

- Dados utilizados em processos administrativos disciplinares
- Informações para defesa da instituição em ações judiciais
- Registros para processos de sindicância
- Documentação para processos de reconhecimento de direitos

7. Proteção da vida ou incolumidade física

Definição: Tratamento necessário para a proteção da vida ou da incolumidade física do titular ou de terceiro.

Características:

- Aplicável em situações de emergência ou risco à vida/saúde
- Não requer consentimento devido à urgência ou impossibilidade
- Limitado ao necessário para a proteção pretendida

Exemplos na UFPI:

- Dados de saúde para atendimento emergencial
- Informações de contato para situações de emergência
- Registros de condições médicas relevantes para atividades de risco
- Dados para protocolos de segurança em laboratórios

8. Tutela da saúde

Definição: Tratamento necessário para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Características:

- Exclusivo para procedimentos de saúde
- Realizado por profissionais capacitados
- Sujeito ao sigilo profissional

Exemplos na UFPI:

- Atendimentos no serviço de saúde da universidade
- Prontuários médicos de servidores e alunos
- Dados para acompanhamento psicológico estudantil
- Informações para perícias médicas

9. Legítimo interesse

Definição: Tratamento necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular.

Características:

- Exige teste de balanceamento (interesse x direitos do titular)
- Deve atender expectativas razoáveis do titular
- Requer medidas de transparência reforçadas

- Não é aplicável à administração pública para dados tratados no exercício de suas competências legais

Exemplos na UFPI (casos potenciais, com ressalvas sobre aplicabilidade):

- Medidas de segurança do campus
- Análise de uso de recursos institucionais
- Comunicações institucionais relacionadas a serviços prestados
- Desenvolvimento e melhoria de serviços educacionais

10. Proteção ao crédito

Definição: Tratamento de dados para proteção do crédito.

Características:

- Específica para análise de risco de crédito
- Aplicação limitada no contexto universitário público

Exemplos na UFPI (aplicação restrita):

- Verificação de histórico para concessão de bolsas reembolsáveis
- Análise para parcelamento de taxas quando aplicáveis

Bases legais para dados pessoais sensíveis (Art. 11)

Para dados sensíveis, as bases legais são mais restritas:

1. Consentimento específico e destacado

Definição: Consentimento específico e em destaque para finalidades específicas.

Exemplo na UFPI:

- Autorização para coleta de dados de saúde em programas voluntários
- Consentimento para tratamento de dados biométricos para acesso

2. Cumprimento de obrigação legal ou regulatória

Exemplo na UFPI:

- Dados de saúde para afastamentos legais
- Informações sobre deficiência para cumprimento de cotas em concursos

3. Execução de políticas públicas

Exemplo na UFPI:

- Dados para políticas de inclusão e acessibilidade
- Informações sobre raça/etnia para políticas de ações afirmativas

4. Realização de estudos por órgão de pesquisa

Exemplo na UFPI:

- Pesquisas na área de saúde com dados anonimizados
- Estudos sobre perfil étnico-racial da comunidade acadêmica

5. Exercício regular de direitos

Exemplo na UFPI:

- Dados sensíveis necessários para defesa em processo administrativo
- Informações de saúde para comprovação de direitos

6. Proteção da vida ou incolumidade física

Exemplo na UFPI:

- Informações sobre alergias ou condições médicas em situações de emergência
- Dados de saúde para protocolos de segurança em laboratórios

7. Tutela da saúde

Exemplo na UFPI:

- Atendimento médico e psicológico no serviço de saúde universitário
- Registros de condições de saúde para adaptações pedagógicas

8. Garantia de prevenção à fraude e segurança

Exemplo na UFPI:

- Dados biométricos para acesso a áreas restritas
- Sistemas de segurança para proteção patrimonial e pessoal

Escolhendo a base legal adequada

A escolha da base legal deve considerar:

- Finalidade do tratamento: Para que os dados serão utilizados?
- Contexto da relação: Qual a natureza da relação com o titular?
- Tipo de dado: Dados sensíveis têm bases legais mais restritas
- Expectativa do titular: O que seria razoável esperar nessa situação?
- Necessidade: É possível atingir a finalidade por outros meios?
- Riscos: Quais os potenciais impactos para os direitos do titular?

Considerações específicas para a UFPI

Como instituição pública de ensino superior, a UFPI deve priorizar as seguintes bases legais:

- Execução de políticas públicas: Para atividades finalísticas da universidade
- Cumprimento de obrigação legal: Para requisitos legais do setor educacional
- Realização de estudos: Para atividades de pesquisa acadêmica
- Execução de contrato: Para relações específicas e formalizadas

O consentimento, embora importante, deve ser utilizado com cautela, principalmente quando há desequilíbrio na relação entre a universidade e o titular (estudante ou servidor), privilegiando-se outras bases legais quando aplicáveis.

Documentação das bases legais

É fundamental documentar a base legal utilizada para cada operação de tratamento, mantendo registros que demonstrem:

- Qual base legal foi aplicada
- Por que ela foi considerada a mais adequada
- Como os requisitos específicos dessa base foram cumpridos
- Quais medidas foram adotadas para proteger os direitos dos titulares

A escolha e documentação adequada das bases legais é um pilar fundamental da conformidade com a LGPD, garantindo que todo tratamento de dados realizado pela UFPI tenha uma justificativa legal consistente e apropriada.

3.2. Tratamento de dados no setor público

O tratamento de dados pessoais pelo setor público, incluindo instituições federais de ensino superior como a UFPI, possui características e requisitos específicos na LGPD. A lei reconhece as particularidades da administração pública e estabelece disposições próprias para o tratamento de dados no contexto da execução de políticas públicas e prestação de serviços públicos.

Particularidades do tratamento de dados pelo poder público

1. Finalidade pública (Art. 23, caput)

O tratamento de dados pessoais pela administração pública deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Implicações para a UFPI:

- Os dados devem ser tratados dentro do escopo da missão institucional (ensino, pesquisa, extensão e gestão)
- A finalidade do tratamento deve estar alinhada com os objetivos educacionais e administrativos definidos em lei
- Deve haver conexão clara entre o tratamento e o interesse público

2. Requisitos específicos de transparência (Art. 23, I)

O poder público deve informar as hipóteses em que realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas.

Implicações para a UFPI:

- Necessidade de política de privacidade específica e detalhada
- Divulgação ativa das bases legais e finalidades de tratamento
- Transparência sobre procedimentos adotados para proteção de dados

3. Indicação de encarregado (Art. 23, III)

Órgãos públicos devem indicar um encarregado pelo tratamento de dados pessoais.

Implicações para a UFPI:

- Designação formal de um encarregado ou criação de um escritório de proteção de dados
- Divulgação da identidade e informações de contato do encarregado
- Estrutura de governança para suportar as atividades do encarregado

4. Compartilhamento entre órgãos públicos (Art. 26)

O uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas.

Implicações para a UFPI:

- Necessidade de instrumentos formais para compartilhamento (convênios, acordos, termos)
- Verificação da compatibilidade das finalidades entre os órgãos
- Observância dos princípios de proteção de dados no compartilhamento

5. Interoperabilidade (Art. 25)

Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Implicações para a UFPI:

- Adoção de padrões técnicos que facilitem interoperabilidade
- Estruturação adequada de bancos de dados
- Documentação de metadados e formatos

6. Restrições ao uso do legítimo interesse (Art. 7º, §7º)

A base legal do legítimo interesse não se aplica ao tratamento de dados pessoais pela administração pública quando realizado no exercício de suas competências legais.

Implicações para a UFPI:

- Necessidade de basear o tratamento em outras hipóteses legais
- Uso predominante das bases de execução de políticas públicas e cumprimento de obrigação legal

7. Sanções diferenciadas (Art. 52, §3º)

As sanções aplicáveis aos órgãos públicos são diferentes das aplicáveis ao setor privado, não incluindo multas pecuniárias diretas.

Implicações para a UFPI:

- Possibilidade de sanções como advertência, publicização da infração, bloqueio ou eliminação dos dados
- Responsabilização funcional dos agentes públicos envolvidos

Bases legais mais relevantes para o setor público

1. Execução de políticas públicas (Art. 7º, III e Art. 11, II, "b")

Esta é a principal base legal para o tratamento de dados (inclusive sensíveis) pela administração pública, permitindo o tratamento necessário

para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Exemplos práticos de políticas públicas executadas pela UFPI:

- Programas de acesso e permanência (cotas, bolsas)
- Assistência estudantil (auxílios, moradia, alimentação)
- Programas de pesquisa e extensão
- Desenvolvimento de atividades de ensino
- Políticas de inclusão e acessibilidade

2. Cumprimento de obrigação legal ou regulatória (Art. 7º, II e Art. 11, II, "a")

Permite o tratamento necessário para cumprir uma determinação legal ou regulatória específica imposta ao controlador.

Exemplos na UFPI:

- Manutenção de registros acadêmicos conforme legislação educacional
- Transmissão de dados ao MEC para o Censo da Educação Superior
- Cumprimento de obrigações trabalhistas e previdenciárias
- Atendimento a requisições de órgãos de controle (TCU, CGU)
- Implementação de políticas de transparência pública

3. Realização de estudos por órgão de pesquisa (Art. 7º, IV e Art. 11, II, "c")

Permite o tratamento para estudos e pesquisas realizados por órgãos de pesquisa, como a própria universidade.

Exemplos na UFPI:

- Pesquisas acadêmicas realizadas por docentes e discentes
- Estudos institucionais sobre evasão, retenção e desempenho
- Avaliações de programas e políticas institucionais

- Pesquisas colaborativas com outras instituições

Equilibrando interesse público e direitos dos titulares

Embora o tratamento de dados no setor público tenha particularidades, a UFPI deve equilibrar a execução de suas finalidades públicas com o respeito aos direitos dos titulares:

1. Princípio da minimização

- Coletar apenas dados estritamente necessários
- Evitar redundâncias e duplicações desnecessárias
- Desidentificar dados quando possível para análises e estudos

2. Transparência ativa

- Informar claramente sobre o tratamento realizado
- Disponibilizar políticas de privacidade acessíveis
- Explicar as finalidades e bases legais utilizadas

3. Medidas de segurança adequadas

- Implementar controles técnicos e administrativos
- Adotar medidas proporcionais à sensibilidade dos dados
- Estabelecer níveis de acesso baseados em necessidade

4. Respeito aos direitos dos titulares

- Estabelecer canais para exercício de direitos
- Responder às solicitações no prazo legal
- Justificar adequadamente eventuais limitações de direitos

Desafios específicos para universidades públicas

1. Múltiplas finalidades de tratamento

Universidades realizam atividades diversas (ensino, pesquisa, extensão, gestão), cada uma com necessidades específicas de tratamento de dados.

Abordagem recomendada:

- Mapear finalidades por área/departamento
- Documentar bases legais específicas para cada finalidade
- Implementar governança que considere essas particularidades

2. Autonomia universitária e proteção de dados

A autonomia universitária precisa ser exercida em harmonia com as regras de proteção de dados.

Abordagem recomendada:

- Estabelecer diretrizes institucionais claras
- Promover cultura de proteção de dados que respeite a autonomia acadêmica
- Criar mecanismos de suporte para pesquisadores e departamentos

3. Parcerias público-privadas

Universidades frequentemente estabelecem parcerias com entidades privadas para pesquisa, estágio e projetos.

Abordagem recomendada:

- Incluir cláusulas de proteção de dados em convênios e parcerias
- Estabelecer responsabilidades claras quanto ao tratamento
- Definir limites para uso e compartilhamento de dados

4. Internacionalização

Cooperação internacional e mobilidade acadêmica envolvem transferência internacional de dados.

Abordagem recomendada:

- Verificar os requisitos legais para transferência internacional
- Estabelecer salvaguardas contratuais quando necessário
- Informar claramente os titulares sobre transferências

O tratamento de dados no setor público, especialmente em uma instituição educacional como a UFPI, requer um equilíbrio cuidadoso entre o cumprimento da missão institucional e o respeito aos direitos dos titulares. Ao compreender as particularidades legais e implementar práticas adequadas, a universidade pode realizar suas atividades com segurança jurídica e transparência.

3.3. Medidas de segurança e boas práticas

A LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. A implementação dessas medidas é fundamental para prevenir incidentes e garantir a confidencialidade, integridade e disponibilidade dos dados tratados pela UFPI.

Requisitos legais de segurança

1. Adoção de medidas de segurança (Art. 46)

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2. Padrão técnico adequado (Art. 46, §1º)

As medidas de segurança devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (privacy by design e privacy by default).

3. Governança em privacidade (Art. 50)

Os controladores podem formular regras de boas práticas e de governança que estabeleçam condições de organização, regime de funcionamento, procedimentos e normas de segurança.

Medidas técnicas de segurança

1. Controles de acesso

Mecanismos que restringem e monitoram o acesso aos dados pessoais.

Implementações recomendadas:

- Autenticação multifator para sistemas críticos
- Política de senhas robustas e atualizações periódicas
- Gestão de privilégios baseada no princípio do menor privilégio
- Revogação imediata de acessos após desligamento
- Revisão periódica de direitos de acesso

2. Criptografia e pseudonimização

Técnicas para proteger a confidencialidade e reduzir riscos no tratamento.

Implementações recomendadas:

- Criptografia de dados sensíveis em repouso
- Comunicações seguras (HTTPS, VPN) para transferências
- Pseudonimização para análises e pesquisas
- Chaves de criptografia gerenciadas adequadamente
- Hashing para senhas e dados críticos

3. Segurança da infraestrutura

Proteção dos sistemas, redes e ambientes físicos onde os dados são armazenados.

Implementações recomendadas:

- Firewalls e sistemas de detecção de intrusão
- Atualização regular de sistemas e aplicações (patches)
- Segmentação de redes e isolamento de dados sensíveis
- Proteção contra malware e vírus
- Hardening de servidores e estações de trabalho

4. Backup e recuperação

Proteção contra perda acidental de dados e garantia de continuidade operacional.

Implementações recomendadas:

- Política de backup regular (3-2-1: três cópias, dois tipos de mídia, uma off-site)
- Testes periódicos de restauração
- Armazenamento seguro das mídias de backup
- Processo documentado de recuperação de desastres
- Retenção de backups alinhada com políticas de dados

5. Monitoramento e registros (logs)

Acompanhamento das atividades relacionadas aos dados para detecção e investigação de incidentes.

Implementações recomendadas:

- Registro de todas as operações críticas de tratamento
- Logs de acesso a dados sensíveis
- Monitoramento de atividades suspeitas
- Proteção dos registros contra alteração
- Retenção adequada dos logs para fins de auditoria

Medidas administrativas de segurança

1. Políticas e procedimentos

Documentos que estabelecem diretrizes, responsabilidades e processos relacionados à segurança da informação.

Implementações recomendadas:

- Política de Segurança da Informação
- Procedimentos de gestão de incidentes
- Normas de uso aceitável de recursos de TI

- Política de classificação da informação
- Procedimentos para descarte seguro de dados

2. Conscientização e treinamento

Ações para desenvolver a cultura de segurança e capacitar as pessoas.

Implementações recomendadas:

- Treinamentos periódicos sobre segurança e privacidade
- Campanhas de conscientização sobre riscos comuns
- Orientações sobre engenharia social e phishing
- Comunicação clara sobre responsabilidades individuais
- Integração da proteção de dados no onboarding de novos servidores

3. Gestão de riscos

Processo contínuo de identificação, avaliação e mitigação de riscos de segurança.

Implementações recomendadas:

- Análise de riscos periódica para ativos de informação
- Planos de tratamento para riscos identificados
- Avaliação de impacto para novos sistemas ou mudanças
- Monitoramento contínuo de ameaças emergentes
- Revisão após incidentes para aprimoramento

4. Gestão de terceiros

Controles para garantir que fornecedores e parceiros mantenham níveis adequados de segurança.

Implementações recomendadas:

- Cláusulas contratuais específicas sobre proteção de dados
- Due diligence de segurança antes da contratação

- Acordos de nível de serviço (SLAs) para segurança
- Auditorias periódicas de fornecedores críticos
- Planos de contingência para falhas de terceiros

5. Resposta a incidentes

Preparação para detectar, responder e recuperar-se de incidentes de segurança.

Implementações recomendadas:

- Equipe de resposta a incidentes designada e treinada
- Procedimentos documentados para diferentes tipos de incidentes
- Canais de comunicação definidos para reportar incidentes
- Processo de notificação à ANPD e aos titulares quando necessário
- Lições aprendidas e melhorias após cada incidente

Boas práticas específicas para o ambiente universitário

1. Proteção de dados acadêmicos

- Controles de acesso granulares para sistemas acadêmicos
- Criptografia de históricos e avaliações
- Políticas de retenção específicas para registros educacionais
- Auditoria regular de acessos a dados acadêmicos sensíveis
- Procedimentos seguros para emissão de documentos oficiais

2. Segurança em ambientes de pesquisa

- Ambientes isolados para pesquisas com dados sensíveis
- Ferramentas de anonimização para conjuntos de dados de pesquisa
- Repositórios seguros para armazenamento de dados de pesquisa
- Orientações específicas para pesquisadores sobre proteção de dados
- Revisão ética e de privacidade para projetos de pesquisa

3. Gestão de acesso em ambiente compartilhado

- Segregação de acesso em laboratórios compartilhados
- Autenticação individual em equipamentos comuns
- Limpeza automática de dados em computadores de uso público
- Controles físicos para áreas com dados sensíveis
- Políticas de mesa e tela limpa

4. Proteção em mobilidade acadêmica

- Criptografia de dispositivos móveis institucionais
- VPN para acesso remoto a sistemas da universidade
- Diretrizes para uso seguro de dispositivos pessoais (BYOD)
- Protocolos seguros para transferência internacional de dados
- Controles específicos para acessos fora do país

Implementação de um programa de segurança na UFPI

Para implementar efetivamente as medidas de segurança, a UFPI deve adotar uma abordagem programática:

1. Estabelecer governança

- Definir papéis e responsabilidades (comitê de segurança, gestor de segurança)
- Integrar segurança da informação e proteção de dados
- Alocar recursos adequados (pessoas, tecnologia, orçamento)
- Estabelecer métricas e indicadores de desempenho
- Obter apoio da alta administração

2. Avaliar o ambiente atual

- Realizar inventário de ativos de informação
- Identificar dados pessoais e sensíveis em cada sistema

- Mapear controles existentes e lacunas
- Avaliar conformidade com regulamentações
- Documentar arquitetura de segurança atual

3. Priorizar ações

- Focar primeiramente em dados sensíveis e sistemas críticos
- Implementar quick wins para demonstrar progresso
- Equilibrar medidas técnicas e administrativas
- Considerar restrições orçamentárias e de recursos
- Alinhar com outros projetos institucionais

4. Implementar controles

- Desenvolver cronograma realista de implementação
- Treinar equipes responsáveis
- Testar controles antes da implantação completa
- Documentar configurações e procedimentos
- Comunicar mudanças aos usuários afetados

5. Monitorar e melhorar continuamente

- Realizar auditorias periódicas
- Testar controles regularmente (testes de penetração, simulações)
- Atualizar medidas conforme novas ameaças e tecnologias
- Coletar feedback dos usuários
- Revisar e aprimorar o programa regularmente

A implementação de medidas de segurança não é apenas uma exigência legal, mas também uma demonstração do compromisso da UFPI com a proteção dos dados de sua comunidade acadêmica. Um programa robusto de segurança protege não apenas os dados, mas também a reputação da instituição e a confiança de alunos, servidores e parceiros.

3.4. Registro das operações

O registro das operações de tratamento de dados, também conhecido como "Record of Processing Activities" (ROPA), é um documento fundamental para a conformidade com a LGPD. Este registro documenta de forma sistemática todas as atividades de tratamento realizadas pela instituição, servindo como base para a transparência, prestação de contas e demonstração de conformidade.

Fundamentos legais do registro de operações

Embora a LGPD não mencione explicitamente a obrigatoriedade de um registro formal das operações, esta prática é derivada de vários requisitos da lei:

- Princípio da responsabilização e prestação de contas (Art. 6º, X): Exige demonstração da adoção de medidas eficazes de cumprimento da lei
- Direito de acesso pelos titulares (Art. 18, II): Requer que a instituição conheça quais dados mantém sobre cada titular
- Relatório de impacto (Art. 5º, XVII): Pressupõe conhecimento detalhado das operações de tratamento
- Boas práticas e governança (Art. 50): Sugere a documentação e registro como parte da governança em privacidade

Objetivos do registro de operações

- Documentar compliance: Demonstrar conformidade com os princípios e requisitos da LGPD
- Facilitar transparência: Fornecer informações claras sobre o tratamento para titulares e autoridades
- Apoiar a gestão de riscos: Identificar e avaliar riscos associados às operações de tratamento
- Embasar decisões: Fundamentar decisões sobre proteção de dados
- Permitir auditorias: Disponibilizar informações estruturadas para auditorias internas e externas

Elementos essenciais do registro de operações

Um registro de operações completo deve documentar, para cada atividade de tratamento:

1. Identificação da atividade

- Nome ou descrição da atividade de tratamento
- Departamento/setor responsável
- Sistemas ou aplicações utilizados
- Finalidade(s) específica(s) do tratamento

Exemplo na UFPI:

- Atividade: Gestão de matrículas
- Responsável: Secretaria Acadêmica
- Sistema: Sistema Integrado de Gestão Acadêmica
- Finalidade: Administração da vida acadêmica dos estudantes

2. Dados pessoais tratados

- Categorias de dados pessoais
- Categorias especiais (dados sensíveis)
- Volume aproximado de dados/titulares
- Origem dos dados (como foram obtidos)

Exemplo na UFPI:

- Categorias: Dados de identificação, contato, acadêmicos
- Dados sensíveis: Informações sobre deficiência (para adaptações)
- Volume: Aproximadamente 25.000 alunos ativos
- Origem: Diretamente dos titulares no processo de matrícula

3. Base legal e consentimento

- Base legal utilizada para o tratamento

- Como e quando o consentimento é obtido (se aplicável)
- Processo para revogação do consentimento (se aplicável)
- Verificação da aplicabilidade contínua da base legal

Exemplo na UFPI:

- Base legal primária: Execução de políticas públicas educacionais
- Base legal secundária: Cumprimento de obrigação legal (LDB, regulamentações do MEC)
- Consentimento: Obtido para usos específicos não cobertos pelas bases primárias (ex: uso de imagem)

4. Ciclo de vida dos dados

- Período de retenção
- Critérios para determinação do período
- Processo de eliminação
- Armazenamento de arquivos históricos

Exemplo na UFPI:

- Retenção: Dados acadêmicos mantidos permanentemente; dados de contato atualizados enquanto o aluno estiver ativo
- Critério: Obrigações regulatórias educacionais e necessidade histórica
- Eliminação: Dados complementares não essenciais eliminados após 5 anos da conclusão do curso

5. Compartilhamento e transferências

- Categorias de destinatários internos
- Categorias de destinatários externos
- Transferências internacionais (se aplicável)
- Salvaguardas utilizadas nas transferências

Exemplo na UFPI:

- Internos: Departamentos acadêmicos, setor de assistência estudantil
- Externos: MEC (Censo), instituições parceiras em programas de intercâmbio
- Transferências internacionais: Para universidades conveniadas em caso de mobilidade acadêmica
- Salvaguardas: Convênios com cláusulas específicas de proteção de dados

6. Medidas de segurança

- Controles técnicos implementados
- Medidas administrativas adotadas
- Controles de acesso
- Procedimentos de backup e recuperação

Exemplo na UFPI:

- Técnicas: Criptografia, autenticação multifator para acesso ao sistema
- Administrativas: Política de acesso baseada em função, treinamento de pessoal
- Acesso: Restrito por perfil, com logs de auditoria
- Backup: Diário com retenção de 30 dias, armazenamento off-site

7. Avaliação de riscos

- Riscos identificados para os direitos dos titulares
- Probabilidade e gravidade dos riscos
- Medidas mitigadoras implementadas
- Avaliações de impacto realizadas (se aplicável)

Exemplo na UFPI:

- Riscos: Acesso não autorizado, uso indevido para avaliação discriminatória

- Impacto: Alto (pode afetar vida acadêmica e profissional do estudante)
- Mitigação: Controles de acesso granulares, auditoria de consultas, pseudonimização para relatórios estatísticos

Formatos e ferramentas para registro

O registro de operações pode ser mantido em diferentes formatos, dependendo do tamanho e complexidade da instituição:

1. Planilhas estruturadas

Adequadas para instituições de menor porte ou como solução inicial:

- Planilha principal com visão geral das atividades
- Abas específicas para detalhamento de cada atividade
- Campos padronizados para facilitar análises
- Controle de versões e atualizações

2. Sistemas de gestão de privacidade

Soluções mais robustas para instituições complexas:

- Software dedicado para gestão de privacidade
- Integração com inventário de ativos de informação
- Workflows automatizados para atualizações
- Relatórios personalizados e dashboards

3. Wikis ou bases de conhecimento

Abordagem colaborativa para documentação:

- Páginas estruturadas por atividade ou departamento
- Facilidade de atualização por múltiplos responsáveis
- Recursos de busca e categorização
- Histórico de alterações incorporado

Implementação do registro de operações na UFPI

Para implementar efetivamente o registro de operações, a UFPI deve:

1. Designar responsabilidades

- Responsável central pela gestão do registro (tipicamente o encarregado/DPO)
- Pontos focais em cada departamento para fornecer informações
- Aprovadores para validação das informações
- Equipe para manutenção e atualização periódica

2. Definir processo de coleta de informações

- Questionários padronizados para levantamento inicial
- Entrevistas com gestores de processos-chave
- Workshops departamentais para identificação de atividades
- Revisão de documentação existente (políticas, contratos, etc.)

3. Estabelecer ciclo de atualização

- Revisão periódica (pelo menos anual) do registro completo
- Processo para atualização em caso de novos tratamentos
- Mecanismo para registrar alterações significativas em tratamentos existentes
- Integração com processo de gestão de mudanças

4. Utilizar o registro para conformidade

- Base para responder a solicitações de titulares
- Referência para elaboração de avisos de privacidade
- Fonte para relatórios à ANPD, se necessário
- Insumo para avaliações de impacto à proteção de dados

5. Integrar com outros processos de governança

- Alinhamento com inventário de ativos de informação
- Conexão com processo de avaliação de riscos
- Integração com sistema de gestão de incidentes
- Vinculação com programa de conscientização

Desafios específicos em universidades

1. Descentralização administrativa

Universidades frequentemente têm estruturas descentralizadas, com diferentes unidades (faculdades, institutos) operando com relativa autonomia.

Abordagem recomendada:

- Modelo federado de governança com diretrizes centrais
- Templates padronizados com flexibilidade para especificidades
- Rede de pontos focais em cada unidade acadêmica
- Validação central para garantir consistência

2. Diversidade de atividades

A multiplicidade de atividades (ensino, pesquisa, extensão, gestão) cria cenários complexos de tratamento de dados.

Abordagem recomendada:

- Categorização de atividades por domínio
- Priorização baseada em volume e sensibilidade dos dados
- Abordagem por fases, começando por processos críticos
- Modelos de registro adaptados para cada categoria

3. Sistemas legados e processos em papel

Muitas universidades ainda mantêm sistemas antigos e processos baseados em papel, dificultando o mapeamento completo.

Abordagem recomendada:

- Incluir repositórios físicos no mapeamento
- Documentar limitações de sistemas legados
- Planejar modernização gradual
- Estabelecer controles compensatórios onde necessário

O registro das operações de tratamento não é apenas uma exigência de compliance, mas uma ferramenta estratégica que proporciona visibilidade sobre o fluxo de dados pessoais na instituição. Quando bem implementado, permite à UFPI conhecer profundamente suas práticas de tratamento de dados, identificar riscos e oportunidades de melhoria, além de demonstrar transparência e responsabilidade perante a comunidade acadêmica e as autoridades.

3.5. Relatório de impacto

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um documento que descreve os processos de tratamento de dados que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação de risco adotados. Este instrumento é fundamental para a avaliação e gestão dos riscos associados ao tratamento de dados pessoais na UFPI.

Definição e base legal

De acordo com o art. 5º, XVII da LGPD, o relatório de impacto à proteção de dados pessoais é a "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".

A ANPD pode determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, conforme o art. 38 da lei.

Quando realizar um RIPD

Embora a LGPD não especifique explicitamente quando um RIPD é obrigatório, boas práticas indicam que deve ser realizado nas seguintes situações:

1. Tratamento em larga escala

- Processamento de dados de um número significativo de titulares
- Tratamento de grandes volumes de dados pessoais
- Abrangência geográfica significativa do tratamento

Exemplos na UFPI:

- Sistemas acadêmicos com dados de todos os estudantes
- Plataformas de ensino à distância usadas por milhares de alunos
- Banco de dados unificado de toda a comunidade acadêmica

2. Uso de novas tecnologias

- Implementação de tecnologias emergentes ou inovadoras
- Aplicação de métodos não convencionais de processamento
- Uso de inteligência artificial ou algoritmos de decisão automatizada

Exemplos na UFPI:

- Sistemas de reconhecimento facial para controle de acesso
- Algoritmos para previsão de evasão ou desempenho estudantil
- Uso de big data para análise de comportamento acadêmico

3. Tratamento de dados sensíveis

- Processamento sistemático de dados sensíveis
- Criação de perfis baseados em dados sensíveis
- Combinação de dados sensíveis com outros conjuntos de dados

Exemplos na UFPI:

- Dados de saúde em programas de assistência estudantil

- Informações biométricas para controle de acesso
- Dados étnico-raciais para políticas de ação afirmativa

4. Monitoramento sistemático

- Observação regular e sistemática dos titulares
- Coleta contínua de dados de comportamento ou localização
- Sistemas de vigilância em espaços públicos

Exemplos na UFPI:

- Monitoramento de acessos à rede institucional
- Sistemas de CCTV no campus
- Rastreamento de uso de recursos digitais educacionais

5. Avaliação sistemática de aspectos pessoais

- Análise ou pontuação de indivíduos
- Criação de perfis para previsão de comportamento
- Tomada de decisões automatizadas com efeitos significativos

Exemplos na UFPI:

- Sistemas de avaliação automatizada
- Processos seletivos baseados em algoritmos
- Análise de perfil para concessão de bolsas ou benefícios

Estrutura e conteúdo do RIPD

Um RIPD bem elaborado deve conter, no mínimo, os seguintes elementos:

1. Descrição sistemática das operações de tratamento

- Natureza, escopo, contexto e finalidades do tratamento
- Categorias de dados pessoais coletados e utilizados
- Categorias de titulares afetados

- Meios utilizados para coleta e processamento
- Fluxo dos dados dentro e fora da organização

2. Necessidade e proporcionalidade do tratamento

- Análise da necessidade do tratamento em relação às finalidades
- Avaliação da proporcionalidade dos dados coletados
- Exame das bases legais utilizadas
- Verificação do período de retenção previsto
- Justificativa para cada categoria de dado coletado

3. Avaliação dos riscos aos direitos e liberdades

- Identificação de riscos específicos para os titulares
- Análise da probabilidade de ocorrência
- Avaliação da gravidade do impacto potencial
- Consideração de danos materiais e imateriais possíveis
- Riscos para grupos vulneráveis específicos (ex: estudantes menores de idade)

4. Medidas para tratamento dos riscos

- Controles técnicos implementados ou planejados
- Medidas organizacionais e administrativas
- Salvaguardas específicas para dados sensíveis
- Mecanismos de exercício de direitos pelos titulares
- Planos de contingência em caso de incidentes

5. Consulta às partes interessadas

- Envolvimento do encarregado (DPO) na avaliação
- Consultas a representantes dos titulares, quando aplicável
- Contribuições de especialistas em privacidade e segurança

- Feedback de gestores das áreas envolvidas
- Documentação das opiniões coletadas

6. Conclusão e recomendações

- Avaliação geral dos riscos residuais
- Justificativa para prosseguir com o tratamento
- Recomendações de melhorias e controles adicionais
- Prazo para implementação das medidas propostas
- Cronograma para revisão do relatório

Processo de elaboração do RIPD

A elaboração de um RIPD envolve geralmente as seguintes etapas:

1. Planejamento

- Definição do escopo e objetivos da avaliação
- Identificação dos envolvidos e responsabilidades
- Estabelecimento de cronograma e recursos
- Definição da metodologia a ser utilizada
- Alinhamento com outras iniciativas de privacidade

2. Coleta de informações

- Entrevistas com responsáveis pelo tratamento
- Revisão de documentação existente
- Análise de sistemas e processos envolvidos
- Consulta a especialistas técnicos
- Levantamento de requisitos legais aplicáveis

3. Identificação e avaliação de riscos

- Workshops de identificação de riscos

- Análise de cenários de ameaças
- Avaliação da probabilidade e impacto
- Priorização dos riscos identificados
- Documentação detalhada dos riscos significativos

4. Definição de medidas mitigadoras

- Identificação de controles existentes
- Análise de lacunas (gap analysis)
- Desenvolvimento de medidas adicionais
- Avaliação de custo-benefício das medidas
- Estabelecimento de responsabilidades e prazos

5. Documentação e aprovação

- Compilação do relatório completo
- Revisão por stakeholders relevantes
- Aprovação pela alta administração
- Registro formal das decisões tomadas
- Comunicação aos envolvidos na implementação

6. Implementação e monitoramento

- Execução das medidas recomendadas
- Acompanhamento da implementação
- Avaliação da eficácia dos controles
- Atualização do RIPD quando necessário
- Integração com a gestão contínua de riscos

Exemplos de RIPD em contexto universitário

Exemplo 1: Sistema biométrico para controle de frequência

Descrição: Implementação de sistema de reconhecimento facial para registro de frequência de estudantes em aulas presenciais.

Riscos potenciais:

- Coleta excessiva de dados biométricos
- Potencial uso para monitoramento não autorizado
- Discriminação de pessoas com certas características faciais
- Vazamento de dados biométricos sensíveis

Medidas mitigadoras:

- Armazenamento de templates biométricos em vez de imagens completas
- Criptografia forte para dados biométricos
- Alternativa não-biométrica para casos especiais
- Rigoroso controle de acesso ao sistema
- Exclusão dos dados após conclusão do curso

Exemplo 2: Programa de suporte à saúde mental

Descrição: Sistema para identificação precoce e acompanhamento de estudantes com potenciais problemas de saúde mental.

Riscos potenciais:

- Estigmatização de estudantes identificados pelo sistema
- Possível discriminação em processos acadêmicos
- Diagnósticos incorretos baseados em dados limitados
- Compartilhamento inadequado de informações sensíveis de saúde

Medidas mitigadoras:

- Pseudonimização de dados para análises gerais
- Acesso estritamente limitado a profissionais de saúde

- Consentimento explícito para participação no programa
- Treinamento específico para todos os envolvidos
- Governança rigorosa com supervisão de comitê de ética

RIPD e governança de dados na UFPI

O RIPD não deve ser visto como um documento isolado, mas como parte integrante do programa de governança de dados da instituição:

1. Integração com o processo de desenvolvimento

- Incorporação da avaliação de impacto no ciclo de desenvolvimento de sistemas
- Aplicação de conceitos de privacy by design e by default
- Realização de avaliações preliminares em fases iniciais de projetos
- Revisões periódicas durante a implementação

2. Alinhamento com gestão de riscos corporativos

- Utilização de metodologias compatíveis com a gestão de riscos institucional
- Inclusão de riscos de privacidade no registro de riscos corporativos
- Consideração de impactos reputacionais, financeiros e operacionais
- Abordagem integrada para tratamento de riscos

3. Conexão com resposta a incidentes

- Uso das avaliações de risco para aprimorar planos de resposta
- Atualização do RIPD após incidentes relevantes
- Teste de controles mitigadores em simulações de incidentes
- Documentação de lições aprendidas

4. Suporte à tomada de decisões

- Utilização do RIPD como ferramenta para decisões informadas

- Documentação da análise risco-benefício para tratamentos complexos
- Embasamento para alocação de recursos em controles de privacidade
- Justificativa para continuidade ou descontinuidade de tratamentos

O Relatório de Impacto à Proteção de Dados Pessoais é uma ferramenta fundamental para a gestão responsável de riscos na UFPI. Mais do que um requisito de conformidade, representa um processo de reflexão crítica sobre as práticas de tratamento de dados, permitindo identificar proativamente riscos e implementar medidas adequadas antes que problemas ocorram. Sua adoção sistemática demonstra o compromisso da instituição com a proteção dos direitos e liberdades fundamentais dos titulares de dados.

MÓDULO 4 — RESPONSABILIDADES E COMPLIANCE

4.1. Agentes de tratamento

A LGPD define claramente os papéis e responsabilidades dos diferentes agentes envolvidos no tratamento de dados pessoais. Compreender essas definições é essencial para determinar as obrigações aplicáveis a cada agente e estabelecer governança adequada no contexto da UFPI.

Definição dos agentes de tratamento

A LGPD define dois principais agentes de tratamento, com funções e responsabilidades distintas:

1. Controlador (Art. 5º, VI)

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

Características:

- Determina as finalidades do tratamento
- Define os meios essenciais do tratamento
- Estabelece como os dados serão utilizados
- Decide quais dados serão coletados
- Determina por quanto tempo os dados serão armazenados

A UFPI como controladora:

A universidade atua como controladora em relação aos dados pessoais de:

- Alunos (graduação, pós-graduação, extensão)
- Servidores (docentes e técnico-administrativos)
- Terceirizados e prestadores de serviço
- Candidatos em processos seletivos
- Participantes de eventos e projetos
- Visitantes e comunidade externa

Exemplos de decisões de controlador na UFPI:

- Determinar quais dados são necessários no processo de matrícula
- Definir o período de retenção de registros acadêmicos
- Estabelecer políticas de compartilhamento de dados com o MEC
- Decidir sobre implementação de sistemas que processam dados pessoais
- Determinar finalidades para uso de dados em pesquisas institucionais

2. Operador (Art. 5º, VII)

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

Características:

- Age sob instruções do controlador
- Não tem poder decisório sobre o tratamento
- Realiza operações técnicas de processamento
- Deve seguir as orientações do controlador
- Não define finalidades próprias para os dados

Exemplos de operadores na relação com a UFPI:

- Empresas de desenvolvimento e manutenção de sistemas
- Fornecedores de serviços de nuvem e hospedagem
- Prestadores de serviços de processamento de folha de pagamento
- Agências de comunicação que gerenciam listas de e-mails
- Empresas de digitalização e gestão documental

UFPI como operadora: Em algumas situações, a universidade pode atuar como operadora:

- Quando processa dados para programas governamentais específicos
- Ao realizar pesquisas em nome de agências de fomento
- Em projetos colaborativos onde outra instituição é a controladora
- Ao executar atividades de processamento sob orientação específica de órgãos reguladores

Outros agentes relevantes

1. Encarregado (DPO — Data Protection Officer) (Art. 5º, VIII)

Definição: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

O papel do encarregado será tratado em detalhe no tópico 4.2.

2. Titular (Art. 5º, V)

Definição: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Embora não seja tecnicamente um "agente de tratamento", o titular é parte fundamental do processo e possui direitos específicos, conforme abordado no módulo 1.

3. ANPD — Autoridade Nacional de Proteção de Dados (Art. 5º, XIX)

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

Papel: Embora não participe diretamente do tratamento, a ANPD tem funções regulatórias, fiscalizadoras e sancionatórias essenciais para a aplicação da lei.

Responsabilidades dos agentes de tratamento

Responsabilidades do Controlador (UFPI)

1. Cumprimento dos princípios (Art. 6º)

- Garantir o respeito aos dez princípios da LGPD
- Implementar medidas para demonstrar conformidade
- Documentar como os princípios são aplicados

2. Garantia dos direitos dos titulares (Art. 18)

- Estabelecer canais para exercício de direitos
- Atender solicitações dentro dos prazos legais
- Implementar processos para cada tipo de solicitação

3. Base legal adequada (Art. 7º e 11)

- Identificar e documentar a base legal para cada tratamento
- Garantir que o tratamento esteja conforme a base escolhida
- Revisar periodicamente a aplicabilidade da base legal

4. Segurança e boas práticas (Art. 46 e 50)

- Implementar medidas técnicas e administrativas de proteção
- Desenvolver programa de governança em privacidade
- Adotar padrões de segurança adequados ao risco

5. Relatório de impacto (Art. 38)

- Elaborar relatórios para tratamentos de maior risco

- Documentar análises de risco e medidas mitigadoras
- Fornecer relatórios à ANPD quando solicitado

6. Indicação de encarregado (Art. 41)

- Designar encarregado pela proteção de dados
- Divulgar a identidade e informações de contato
- Fornecer suporte necessário às atividades do encarregado

7. Registro das operações (Art. 37)

- Manter registro das operações de tratamento
- Documentar detalhes sobre cada processamento
- Disponibilizar informações para a ANPD quando solicitado

Responsabilidades do Operador

1. Seguir instruções do controlador (Art. 39)

- Realizar o tratamento conforme as instruções documentadas
- Informar ao controlador caso as instruções violem a LGPD
- Não utilizar os dados para finalidades próprias

2. Implementar medidas de segurança (Art. 37 e 38)

- Adotar medidas de segurança compatíveis com as do controlador
- Proteger os dados contra acessos não autorizados
- Notificar o controlador em caso de incidentes

3. Cooperar com o controlador

- Auxiliar no atendimento às solicitações dos titulares
- Fornecer informações necessárias para demonstrar conformidade
- Contribuir para auditorias e inspeções

4. Confidencialidade

- Garantir que pessoas autorizadas a tratar os dados mantenham confidencialidade
- Implementar controles de acesso adequados
- Restringir o tratamento às finalidades autorizadas

Responsabilidade compartilhada e solidária

A LGPD estabelece um regime de responsabilidade que pode afetar conjuntamente controladores e operadores:

Responsabilidade solidária (Art. 42, §1º, I e II)

O operador responde solidariamente pelos danos causados quando:

- Descumprir as obrigações da legislação de proteção de dados
- Não seguir as instruções lícitas do controlador
- Agir em desacordo com as obrigações legais

Consequências práticas para a UFPI:

Como controladora:

- Selecionar operadores que ofereçam garantias adequadas
- Estabelecer contratos com cláusulas específicas sobre proteção de dados
- Realizar due diligence antes da contratação
- Monitorar o cumprimento por parte dos operadores
- Documentar as instruções fornecidas aos operadores

Como operadora:

- Documentar formalmente as instruções recebidas
- Questionar instruções potencialmente ilegais
- Manter evidências de compliance com as diretrizes
- Implementar controles de qualidade para o tratamento

- Garantir subcontratações adequadas (quando permitidas)

Ok.Implementação prática na UFPI

Para implementar adequadamente a estrutura de agentes de tratamento, a UFPI deve:

1. Mapeamento de relações

- Identificar onde a universidade atua como controladora
- Identificar situações em que atua como operadora
- Mapear todos os operadores que processam dados para a UFPI
- Documentar as relações de controle e operação

2. Formalização de relações

- Revisar e adequar contratos com operadores
- Estabelecer acordos de tratamento de dados (ATDs)
- Documentar instruções para operadores
- Definir requisitos mínimos para subcontratação

3. Governança interna

- Definir papéis e responsabilidades relacionados à proteção de dados
- Estabelecer fluxos de comunicação entre controlador e operadores
- Implementar mecanismos de supervisão e auditoria
- Treinar as equipes sobre suas responsabilidades específicas

4. Gestão de terceiros

- Estabelecer processo de due diligence para novos operadores
- Definir cláusulas contratuais padrão para proteção de dados
- Implementar avaliação periódica de operadores
- Desenvolver plano de resposta para falhas de operadores

A clara definição dos papéis e responsabilidades dos agentes de tratamento é fundamental para a adequada implementação da LGPD na UFPI. Compreender onde a universidade atua como controladora ou operadora permite estabelecer processos adequados de governança, mitigar riscos de responsabilidade e garantir a proteção efetiva dos dados pessoais tratados no ambiente universitário.

4.2. Encarregado (DPO)

O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é uma figura central no sistema de proteção de dados estabelecido pela LGPD. Sua designação é obrigatória para controladores, incluindo órgãos públicos como a UFPI, e representa um pilar importante da governança de privacidade e da demonstração de accountability.

Definição e base legal

De acordo com o art. 5º, VIII da LGPD, o encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

O art. 41 estabelece a obrigatoriedade de sua indicação e define responsabilidades básicas, enquanto a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, fornece detalhamentos adicionais sobre o papel.

Funções e responsabilidades do encarregado

1. Canal de comunicação (Art. 41, §1º)

O encarregado é o ponto focal para comunicações relacionadas à proteção de dados:

- Receber comunicações e reclamações dos titulares
- Prestar esclarecimentos e adotar providências
- Receber comunicações da ANPD

- Orientar funcionários e contratados sobre práticas de proteção

2. Orientação interna (Art. 41, §2º, I)

O encarregado deve:

- Conscientizar as equipes sobre proteção de dados
- Oferecer treinamentos e capacitações
- Estabelecer diretrizes e procedimentos internos
- Esclarecer dúvidas sobre a aplicação da lei

3. Atendimento aos titulares (Art. 41, §2º, I)

O encarregado deve:

- Receber solicitações de titulares
- Encaminhar demandas às áreas responsáveis
- Garantir respostas dentro dos prazos legais
- Documentar todas as interações

4. Interação com a ANPD (Art. 41, §2º, III)

O encarregado deve:

- Responder a solicitações e orientações da ANPD
- Submeter relatórios quando requeridos
- Notificar incidentes de segurança
- Representar a instituição em questões de proteção de dados

5. Aconselhamento sobre RIPD (recomendado)

O encarregado deve:

- Orientar sobre necessidade de realização de RIPDs
- Revisar e validar os relatórios produzidos
- Acompanhar a implementação das medidas recomendadas

- Manter registro de avaliações realizadas

6. Supervisão da conformidade (recomendado)

O encarregado deve:

- Monitorar a conformidade com a LGPD
- Recomendar medidas corretivas quando necessário
- Participar de projetos que envolvam dados pessoais
- Promover a cultura de privacy by design

Qualificações necessárias

A LGPD não estabelece requisitos específicos de qualificação para o encarregado, mas boas práticas indicam:

1. Conhecimentos técnicos e jurídicos

- Compreensão da legislação de proteção de dados
- Familiaridade com normas complementares e regulações setoriais
- Conhecimento sobre segurança da informação
- Entendimento de processos e sistemas da instituição

2. Habilidades pessoais e profissionais

- Capacidade de comunicação com diferentes públicos
- Habilidade para interpretar requisitos legais
- Competência para gerenciar projetos
- Capacidade de trabalhar com múltiplas áreas

3. Experiência e formação

- Experiência em governança de dados ou privacidade
- Formação compatível com as responsabilidades
- Certificações em proteção de dados (desejável)
- Conhecimento do setor educacional (no caso da UFPI)

4. Características específicas para instituições públicas

- Conhecimento sobre normas e procedimentos do setor público
- Compreensão das particularidades da administração pública
- Familiaridade com processos de transparência e acesso à informação
- Entendimento da estrutura e governança de universidades federais

Modelos de implementação do encarregado

A UFPI pode adotar diferentes modelos para a função de encarregado, cada um com vantagens e desafios específicos:

1. Encarregado individual

Descrição: Designação de um servidor específico para exercer exclusivamente a função.

Vantagens:

- Dedicação exclusiva ao tema
- Maior independência
- Foco concentrado nas questões de proteção de dados
- Clara identificação do responsável

Desafios:

- Limitação de recursos humanos
- Possível isolamento em relação a outras áreas
- Sobrecarga de trabalho em instituições grandes
- Dependência de uma única pessoa

2. Encarregado com funções acumuladas

Descrição: Designação de um servidor que acumula outras funções além de encarregado.

Vantagens:

- Otimização de recursos humanos
- Possível sinergia com outras funções relacionadas
- Aproveitamento de conhecimento institucional existente
- Facilidade de implementação inicial

Desafios:

- Conflitos de prioridade
- Limitação de tempo disponível
- Possíveis conflitos de interesse
- Menor especialização

3. Escritório ou comitê de proteção de dados

Descrição: Criação de uma estrutura colegiada, com representantes de diferentes áreas, sendo um deles designado formalmente como encarregado.

Vantagens:

- Representatividade de diferentes perspectivas
- Distribuição de carga de trabalho
- Maior alcance institucional
- Continuidade em caso de transições

Desafios:

- Complexidade de coordenação
- Possível difusão de responsabilidades
- Processos decisórios mais lentos
- Necessidade de governança clara

4. Terceirização parcial ou total

Descrição: Contratação de pessoa física ou jurídica externa para exercer a função.

Vantagens:

- Acesso a expertise especializada
- Independência em relação à estrutura interna
- Transferência de know-how
- Flexibilidade de recursos

Desafios:

- Custos associados
- Menor conhecimento da cultura institucional
- Questões de contratação pública
- Acesso limitado a informações e processos internos

Posicionamento e independência

Independentemente do modelo escolhido, é essencial que o encarregado tenha:

1. Posicionamento adequado na estrutura organizacional

- Acesso direto à alta administração
- Posição que permita visão transversal da instituição
- Independência das áreas operacionais de tratamento
- Autoridade reconhecida na organização

2. Recursos adequados

- Tempo suficiente para as atividades (se acumular funções)
- Equipe de apoio proporcional ao porte da instituição
- Orçamento para atividades e capacitação
- Ferramentas e sistemas necessários

3. Autonomia funcional

- Liberdade para reportar problemas e violações
- Não receber instruções sobre como desempenhar suas funções
- Proteção contra penalizações pelo exercício de suas funções
- Mandato definido (recomendado)

Implementação do encarregado na UFPI

Para implementar efetivamente a função de encarregado, a UFPI deve:

1. Formalização da designação

- Publicação de ato formal de designação
- Definição clara de atribuições e responsabilidades
- Estabelecimento de posição na estrutura organizacional
- Comunicação ampla à comunidade universitária

2. Divulgação da identidade e contato

- Publicação da identidade e informações de contato no site
- Criação de canais dedicados (e-mail, formulário)
- Divulgação em políticas de privacidade e avisos
- Informação à ANPD

3. Estruturação de processos

- Definição de fluxos para atendimento de titulares
- Estabelecimento de procedimentos para notificação de incidentes
- Criação de rotinas de relacionamento com a ANPD
- Integração com processos existentes (ouvidoria, SIC, etc.)

4. Capacitação contínua

- Treinamento inicial específico

- Atualização constante sobre normas e boas práticas
- Participação em eventos e fóruns da área
- Interlocução com encarregados de outras instituições

5. Governança e integração

- Participação em comitês estratégicos
- Integração com áreas relacionadas (segurança da informação, compliance)
- Mecanismos de reporte à alta administração
- Avaliação periódica de desempenho

O encarregado é muito mais que uma exigência legal — é um elemento central da governança de privacidade, que contribui para a cultura de proteção de dados e para a demonstração de accountability. Para a UFPI, um encarregado efetivo representa não apenas conformidade legal, mas também um compromisso institucional com a proteção dos direitos dos titulares e com o uso ético e responsável dos dados pessoais.

4.3. Responsabilidades administrativas

Como controladora de dados pessoais, a UFPI possui diversas responsabilidades administrativas relacionadas à conformidade com a LGPD. Estas responsabilidades vão além do cumprimento direto da lei e incluem a criação de estruturas de governança, procedimentos internos e mecanismos que garantam e demonstrem a adequação às exigências legais.

Governança de privacidade

1. Programa de governança em privacidade (Art. 50)

A LGPD incentiva a adoção de programas de governança que estabeleçam políticas e salvaguardas adequadas com base em processos e estruturas internas que assegurem o cumprimento de normas e boas práticas.

Elementos fundamentais:

- Comprometimento da alta administração: Apoio da Reitoria e dos órgãos colegiados superiores
- Políticas e normas internas: Conjunto coerente de diretrizes formalizadas
- Estrutura organizacional: Definição clara de papéis e responsabilidades
- Processos e procedimentos: Fluxos de trabalho documentados para atividades-chave
- Recursos adequados: Alocação de pessoal, tecnologia e orçamento
- Mecanismos de supervisão: Controles para monitorar a conformidade

2. Políticas e normativos internos

A instituição deve desenvolver e implementar um conjunto de documentos que orientem o tratamento de dados:

- Política de Privacidade e Proteção de Dados: Documento principal que estabelece princípios e diretrizes gerais
- Política de Segurança da Informação: Controles técnicos e administrativos para proteger dados
- Política de Classificação da Informação: Critérios para categorizar dados por sensibilidade
- Normas setoriais: Diretrizes específicas para áreas com tratamentos particulares (ex: pesquisa, assistência estudantil)
- Procedimentos operacionais: Detalhamento de atividades específicas relacionadas a dados pessoais

3. Estruturas organizacionais

Além do encarregado, a UFPI deve considerar a implementação de estruturas adicionais:

- Comitê de Privacidade e Proteção de Dados: Grupo multidisciplinar para decisões estratégicas e coordenação

- Grupo de Trabalho de Implementação: Equipe focada na adequação inicial à LGPD
- Rede de agentes de privacidade: Representantes em cada unidade/departamento
- Integração com estruturas existentes: Comitê de Segurança da Informação, Comitê de Governança Digital, etc.

Processos administrativos essenciais

1. Gestão de solicitações dos titulares

Implementação de processos para atender aos direitos dos titulares:

- Canal centralizado: Ponto único de entrada para solicitações
- Verificação de identidade: Processo para confirmar a identidade do solicitante
- Fluxos de encaminhamento: Direcionamento para áreas responsáveis
- Prazos e respostas padronizadas: Templates e cronogramas definidos
- Documentação e métricas: Registro de todas as solicitações e tempos de resposta
- Revisão periódica: Análise da eficiência e qualidade do atendimento
- Procedimentos recursais: Fluxos para casos de contestação ou insatisfação
- Integração com outros canais: Ouvidoria, e-SIC, atendimento ao aluno

2. Gestão de contratos e fornecedores

Processos para garantir que terceiros que processam dados em nome da UFPI estejam em conformidade:

- Cláusulas contratuais: Inclusão de requisitos específicos de proteção de dados
- Due diligence: Avaliação prévia de fornecedores quanto à conformidade com a LGPD

- Acordos de tratamento de dados: Documentos específicos sobre responsabilidades
- Auditorias e monitoramento: Verificação periódica do cumprimento
- Gestão de incidentes envolvendo terceiros: Procedimentos de notificação e resposta
- Processo de saída: Protocolos para encerramento de contratos com garantia de devolução ou eliminação de dados

3. Gestão de incidentes de segurança

Processos para lidar com violações de segurança que afetem dados pessoais:

- Detecção e classificação: Mecanismos para identificar e categorizar incidentes
- Contenção e mitigação: Procedimentos para limitar danos
- Investigação e análise de causa-raiz: Identificação de fatores contribuintes
- Notificação à ANPD e aos titulares: Protocolos para comunicação conforme art. 48
- Correção e prevenção: Implementação de medidas para evitar recorrência
- Documentação completa: Registro detalhado de todo o processo

4. Gestão de riscos de privacidade

Processos contínuos para identificar, avaliar e tratar riscos:

- Identificação de riscos: Mapeamento de ameaças e vulnerabilidades
- Análise e avaliação: Determinação de probabilidade e impacto
- Priorização: Foco em riscos mais significativos
- Tratamento: Implementação de controles mitigadores
- Monitoramento: Acompanhamento da eficácia dos controles

- Reavaliação periódica: Atualização diante de mudanças no ambiente

5. Gestão de mudanças

Procedimentos para avaliar o impacto de mudanças na privacidade:

- Avaliação prévia: Análise de impacto para novos projetos ou alterações
- Privacy by design: Incorporação de proteção de dados desde a concepção
- Processo de aprovação: Verificação de conformidade antes da implementação
- Atualização de documentação: Revisão de registros de tratamento e políticas
- Comunicação aos titulares: Quando necessário, informar sobre mudanças relevantes
- Gestão de transição: Implementação controlada de alterações significativas

Mecanismos de accountability

A LGPD baseia-se no princípio da responsabilização e prestação de contas, exigindo que a instituição não apenas cumpra a lei, mas também demonstre esse cumprimento:

1. Documentação e registros

Manutenção de evidências que demonstrem conformidade:

- Registro das operações de tratamento: Inventário detalhado e atualizado
- Relatórios de impacto: Documentação de análises para tratamentos de maior risco
- Base legal documentada: Registros da base legal utilizada para cada tratamento
- Evidências de consentimento: Quando esta for a base legal utilizada

- Logs e trilhas de auditoria: Registros de acesso e operações em sistemas
- Registro de incidentes: Documentação completa de violações e resposta

2. Auditorias e avaliações

Verificações periódicas da conformidade:

- Auditorias internas: Avaliações sistemáticas por equipe própria
- Revisões por pares: Análises cruzadas entre departamentos
- Auditorias externas: Avaliações por especialistas independentes
- Testes de controles: Verificação prática da eficácia das medidas
- Avaliações de maturidade: Mensuração do nível de desenvolvimento do programa
- Benchmarking: Comparação com outras instituições públicas similares

3. Relatórios e métricas

Monitoramento contínuo e transparência interna:

- Indicadores-chave de desempenho (KPIs): Métricas sobre aspectos relevantes
- Relatórios periódicos: Documentos regulares para alta administração
- Dashboards de conformidade: Visão consolidada e atualizada da situação
- Análise de tendências: Acompanhamento da evolução ao longo do tempo
- Relatórios de progresso: Status da implementação de controles planejados
- Métricas de incidentes: Quantificação e análise de eventos de segurança

Desafios específicos para instituições públicas

A UFPI, como instituição pública federal, enfrenta desafios particulares:

1. Limitações orçamentárias e de recursos

- Priorização estratégica: Focar recursos em áreas de maior risco
- Soluções incrementais: Implementação gradual do programa
- Reutilização de estruturas: Aproveitamento de comitês e recursos existentes
- Capacitação interna: Desenvolvimento de expertise na própria equipe
- Parcerias: Colaboração com outras instituições para compartilhar recursos

2. Complexidade organizacional

- Abordagem federada: Modelo que respeite a autonomia de unidades
- Clareza na governança: Definição precisa de responsabilidades
- Comunicação eficiente: Estratégias para alcançar toda a instituição
- Engajamento de lideranças intermediárias: Apoio de diretores e coordenadores
- Processo decisório documentado: Fluxos claros para decisões sobre dados

3. Integração com outros requisitos legais

- Harmonização normativa: Alinhamento com LAI, decretos e portarias
- Processos unificados: Integração com práticas de transparência
- Políticas coerentes: Documentos que considerem o conjunto regulatório
- Interpretação consistente: Clareza sobre como aplicar normas sobrepostas
- Mapeamento de requisitos: Identificação de todas as obrigações legais

Boas práticas para a implementação na UFPI

1. Abordagem baseada em riscos

- Priorizar áreas que tratam dados sensíveis ou em grande volume
- Focar inicialmente em processos com alto impacto para titulares
- Implementar controles proporcionais aos riscos identificados
- Revisar periodicamente a análise de riscos

2. Implementação gradual

- Estabelecer roadmap realista com marcos bem definidos
- Dividir o projeto em fases gerenciáveis
- Demonstrar resultados rápidos em áreas críticas
- Comunicar avanços para manter o engajamento

3. Capacitação contínua

- Desenvolver programas de treinamento adaptados a diferentes públicos
- Realizar campanhas de conscientização para toda a comunidade
- Formar multiplicadores nas diversas unidades
- Estabelecer canais para esclarecimento de dúvidas

4. Cultura de privacidade

- Promover a proteção de dados como valor institucional
- Integrar considerações de privacidade em processos decisórios
- Reconhecer e incentivar boas práticas
- Incorporar a privacidade na ética institucional

A implementação de responsabilidades administrativas robustas não apenas garante conformidade legal, mas também fortalece a confiança da comunidade acadêmica na instituição. Ao adotar uma abordagem estruturada e sistemática, a UFPI pode transformar a adequação à LGPD

em uma oportunidade para aprimorar sua governança institucional e demonstrar seu compromisso com os direitos fundamentais dos titulares de dados.

4.4. Sanções e penalidades

A LGPD estabelece um regime sancionatório para o descumprimento das obrigações previstas na lei. Conhecer as possíveis sanções e seus mecanismos de aplicação é fundamental para que a UFPI compreenda os riscos associados à não conformidade e implemente medidas preventivas adequadas.

Sanções administrativas previstas na LGPD

O artigo 52 da LGPD prevê as seguintes sanções, que podem ser aplicadas pela ANPD:

1. Advertência

- Indicação de prazo para adoção de medidas corretivas
- Geralmente aplicada em casos de infrações menos graves
- Serve como alerta formal antes de penalidades mais severas
- Não dispensa a correção das irregularidades identificadas

2. Multa simples

- Até 2% do faturamento da pessoa jurídica de direito privado, limitada a R$ 50 milhões por infração
- Observação: Para entidades públicas como a UFPI, aplica-se regime diferenciado (ver adiante)

3. Multa diária

- Observados os mesmos limites da multa simples
- Aplicável até a cessação da infração
- Pode ser cumulativa com outras sanções

- Observação: Para entidades públicas como a UFPI, aplica-se regime diferenciado (ver adiante)

4. Publicização da infração

- Divulgação pública da ocorrência da infração
- Pode causar danos significativos à reputação
- Aplicável após procedimento administrativo
- Particularmente relevante para instituições públicas

5. Bloqueio dos dados pessoais

- Suspensão temporária do tratamento dos dados relacionados à infração
- Pode afetar significativamente operações da instituição
- Permanece até regularização da situação
- Exige cuidados para não prejudicar titulares

6. Eliminação dos dados pessoais

- Exclusão definitiva dos dados relacionados à infração
- Sanção mais severa, aplicada em casos graves
- Impacto potencialmente irreversível para operações
- Aplicada após análise criteriosa pela ANPD

Regime diferenciado para órgãos públicos

O §3º do art. 52 estabelece que o disposto nos incisos I, IV, V e VI (advertência, publicização, bloqueio e eliminação) é aplicável a entidades e órgãos públicos, sem prejuízo do disposto na Lei nº 8.112/1990 e na Lei nº 8.429/1992.

Na prática, isso significa que:

- Instituições públicas como a UFPI não estão sujeitas a multas pecuniárias diretas

- Aplicam-se as demais sanções (advertência, publicização, bloqueio e eliminação)
- Os servidores envolvidos podem responder pessoalmente em âmbito disciplinar
- Pode haver responsabilização por improbidade administrativa

Critérios para aplicação das sanções

Conforme o art. 52, §1º, a ANPD considerará os seguintes parâmetros e critérios:

1. Gravidade e natureza das infrações
- Tipo de violação (princípios, direitos, bases legais)
- Duração da infração
- Recorrência ou continuidade
- Sistematicidade da prática

2. Boa-fé do infrator
- Comportamento anterior e durante a investigação
- Medidas corretivas adotadas voluntariamente
- Cooperação com a autoridade
- Transparência nas informações prestadas

3. Vantagem auferida ou pretendida
- Benefícios obtidos com a infração
- Motivação para o descumprimento
- Vantagens competitivas ou econômicas
- No caso de instituições públicas, vantagens operacionais ou administrativas

4. Condição econômica do infrator
- Para entidades públicas, considera-se o orçamento disponível

- Porte da instituição
- Impacto da sanção no funcionamento da entidade
- Capacidade de implementação de medidas corretivas

5. Reincidência

- Ocorrência de infrações anteriores
- Tempo decorrido entre as infrações
- Similaridade entre as violações
- Eficácia das medidas corretivas anteriores

6. Grau do dano causado

- Número de titulares afetados
- Tipo de dados comprometidos (sensíveis ou não)
- Consequências concretas para os titulares
- Impacto em direitos fundamentais

7. Cooperação do infrator

- Colaboração durante as investigações
- Fornecimento voluntário de informações
- Adoção proativa de medidas mitigadoras
- Transparência na comunicação com autoridades e titulares

8. Adoção de mecanismos internos

- Existência de políticas e procedimentos de proteção de dados
- Implementação de programa de governança em privacidade
- Medidas técnicas e administrativas preventivas
- Cultura organizacional de conformidade

9. Procedimentos para reverter ou mitigar efeitos

- Resposta a incidentes estruturada
- Ações tomadas para limitar danos
- Comunicação adequada aos titulares
- Medidas compensatórias implementadas

10. Proporcionalidade entre a gravidade da falta e a intensidade da sanção

- Equilíbrio entre violação e penalidade
- Consideração do contexto e circunstâncias
- Avaliação do efeito dissuasório
- Progressividade das sanções

Responsabilidades específicas no contexto universitário

A UFPI deve considerar cenários específicos de responsabilização:

1. Responsabilidade institucional

- A universidade como entidade controladora responde pelas infrações
- As sanções aplicáveis afetam a instituição como um todo
- Necessidade de governança centralizada para mitigar riscos
- Importância de políticas institucionais claras

2. Responsabilidade funcional de servidores

- Servidores podem responder administrativamente (Lei 8.112/90)
- Possibilidade de processo administrativo disciplinar
- Sanções que vão de advertência até demissão
- Nexo causal entre conduta do servidor e a infração

3. Responsabilidade de gestores

- Dirigentes podem responder por omissão na implementação de controles
- Risco de caracterização de improbidade administrativa

- Dever de garantir recursos para adequação à LGPD
- Necessidade de demonstrar diligência na supervisão

4. Cenários acadêmicos específicos

- Tratamento inadequado de dados em pesquisas acadêmicas
- Uso não autorizado de dados de alunos em publicações
- Compartilhamento indevido de informações sensíveis
- Falhas de segurança em sistemas acadêmicos

Medidas preventivas e mitigadoras

Para minimizar o risco de sanções, a UFPI deve adotar medidas preventivas:

1. Programa de conformidade robusto

- Implementação de programa de governança em privacidade
- Adoção de políticas e procedimentos formais
- Treinamento e conscientização de servidores
- Monitoramento contínuo da conformidade

2. Due diligence e documentação

- Mapeamento e registro detalhado de operações de tratamento
- Documentação de decisões e justificativas sobre tratamento
- Registro da base legal utilizada para cada operação
- Evidências de implementação de medidas de segurança

3. Resposta a incidentes estruturada

- Plano de resposta a incidentes formalizado
- Procedimentos claros para notificação à ANPD
- Canais de comunicação estabelecidos com titulares
- Equipe treinada para atuar em caso de violações

4. Auditoria e verificação periódica

- Avaliações regulares de conformidade
- Testes de vulnerabilidade em sistemas
- Revisão de políticas e práticas
- Atualização contínua frente a novas orientações da ANPD

5. Cultura de privacidade e ética

- Promoção da proteção de dados como valor institucional
- Incentivo à comunicação de riscos e vulnerabilidades
- Reconhecimento de boas práticas
- Tolerância zero para uso indevido intencional de dados

Resposta a processos administrativos

Caso a UFPI seja alvo de processos administrativos pela ANPD:

1. Recebimento de notificação

- Encaminhamento imediato ao encarregado e área jurídica
- Análise detalhada das alegações
- Levantamento preliminar de fatos e evidências
- Definição de estratégia de resposta

2. Preparação da defesa

- Coleta de documentação comprobatória
- Entrevistas com pessoas envolvidas
- Análise técnica das circunstâncias
- Elaboração de defesa completa e fundamentada

3. Cooperação com a autoridade

- Fornecimento de informações solicitadas

- Transparência sobre os fatos
- Demonstração de boa-fé
- Disponibilidade para esclarecimentos adicionais

4. Implementação de medidas corretivas

- Correção imediata das irregularidades identificadas
- Desenvolvimento de plano de ação abrangente
- Implementação de medidas para evitar recorrência
- Documentação das ações tomadas

5. Aprendizado organizacional

- Análise de causa-raiz do problema
- Revisão de processos relacionados
- Reforço de treinamentos em áreas críticas
- Atualização de políticas e procedimentos

Embora o regime sancionatório para instituições públicas tenha particularidades, as consequências de não conformidade para a UFPI podem ser significativas, afetando desde a continuidade de serviços até a reputação institucional. A implementação de um programa efetivo de conformidade com a LGPD não apenas mitiga esses riscos, mas também fortalece a confiança da comunidade acadêmica e demonstra o compromisso da universidade com a proteção dos direitos fundamentais dos titulares.

4.5. Boas práticas de governança

A implementação de boas práticas de governança em proteção de dados vai além da simples conformidade legal, representando uma abordagem proativa que integra a privacidade na cultura e nos processos organizacionais da UFPI. O art. 50 da LGPD incentiva explicitamente a adoção de tais práticas, reconhecendo seu papel na mitigação de riscos e na demonstração de accountability.

Programa de governança em privacidade

Um programa estruturado de governança em privacidade deve contemplar os seguintes elementos:

1. Compromisso organizacional

- Apoio da alta administração: Envolvimento formal da Reitoria e Conselhos Superiores
- Política institucional de privacidade: Documento aprovado pelas instâncias máximas
- Recursos adequados: Alocação de pessoal, orçamento e infraestrutura
- Monitoramento de nível estratégico: Inclusão da proteção de dados na governança institucional
- Integração com planejamento estratégico: Alinhamento com missão e objetivos da universidade

2. Estrutura de governança

- Definição clara de papéis e responsabilidades: Matriz RACI para atividades relacionadas
- Encarregado (DPO) com posicionamento adequado: Acesso direto à alta administração
- Comitê de Privacidade multidisciplinar: Representação de áreas-chave
- Rede de agentes de privacidade: Pontos focais nas diversas unidades
- Integração com estruturas existentes: Comitês de Segurança, Ética, Governança Digital

3. Framework normativo interno

- Política de Privacidade institucional: Diretrizes gerais e princípios
- Normas complementares: Detalhamento para temas específicos
- Procedimentos operacionais: Instruções detalhadas para processos críticos

- Termos de uso e avisos de privacidade: Documentos de transparência para titulares
- Acordos de confidencialidade: Compromissos formais de servidores e terceiros

4. Processos e controles

- Inventory de dados pessoais: Mapeamento atualizado de todos os tratamentos
- Privacy by Design e by Default: Incorporação da privacidade desde a concepção
- Avaliação de impacto (RIPD): Processo formalizado para novos tratamentos
- Gestão de consentimento: Mecanismos para obtenção e gerenciamento
- Atendimento a direitos dos titulares: Fluxos eficientes para solicitações
- Gestão de incidentes: Processos para detecção, resposta e notificação
- Due diligence de terceiros: Avaliação de fornecedores e parceiros

5. Conscientização e treinamento

- Programa de capacitação contínua: Treinamentos regulares e específicos
- Campanhas de conscientização: Comunicação sistemática sobre o tema
- Materiais educativos: Recursos adaptados a diferentes públicos
- Canais de dúvidas e orientação: Suporte contínuo para servidores
- Integração de novos servidores: Privacidade como parte do onboarding

6. Monitoramento e melhoria contínua

- Auditorias e avaliações periódicas: Verificação sistemática da conformidade
- Indicadores-chave de desempenho (KPIs): Métricas para acompanhamento

- Análise de incidentes e quase-incidentes: Aprendizado a partir de eventos
- Acompanhamento de mudanças regulatórias: Atualização frente a novas normas
- Benchmarking com instituições similares: Comparação e aprendizado

Governança específica para o ambiente universitário

A natureza da universidade, com sua diversidade de atividades e relativa autonomia entre unidades, exige adaptações na governança de privacidade:

1. Governança federada

- Diretrizes centrais com autonomia local: Equilíbrio entre padronização e flexibilidade
- Responsabilidades descentralizadas: Atribuições claras para unidades acadêmicas
- Mecanismos de coordenação: Fóruns e comitês representativos
- Compartilhamento de práticas: Disseminação de casos de sucesso entre unidades
- Monitoramento centralizado: Supervisão institucional com respeito à autonomia

2. Contextos específicos de tratamento

- Ensino: Diretrizes para dados acadêmicos, avaliações e registros
- Pesquisa: Protocolos para dados em projetos científicos, considerando ética em pesquisa
- Extensão: Orientações para programas comunitários e relação com público externo
- Gestão administrativa: Práticas para dados funcionais e institucionais
- Assistência estudantil: Procedimentos para tratamento de dados sensíveis de alunos

3. Interação com instâncias de governança acadêmica

- Conselhos Superiores: Aprovação de políticas institucionais
- Comitês de Ética: Integração com avaliação de projetos de pesquisa
- Colegiados de curso: Implementação de diretrizes em nível operacional
- Comissões permanentes: Incorporação da privacidade em processos avaliativos
- Representações estudantis: Participação de titulares na governança

Privacy by Design e by Default

A adoção desses conceitos fundamentais representa uma abordagem proativa à proteção de dados:

1. Privacy by Design (Privacidade desde a concepção)

Princípios aplicáveis a projetos e sistemas:

- Proatividade, não reatividade: Antecipar e prevenir problemas
- Privacidade como configuração padrão: Proteção automática
- Privacidade incorporada ao design: Integrada, não adicionada posteriormente
- Funcionalidade total: Soma positiva, não jogo de soma zero
- Segurança de ponta a ponta: Proteção durante todo o ciclo de vida
- Visibilidade e transparência: Processos abertos e verificáveis
- Respeito pela privacidade do usuário: Foco no titular dos dados

Implementação na UFPI:

- Checklist de privacidade para novos projetos
- Revisão de privacidade em desenvolvimento de sistemas
- Análise de impacto antes da implementação
- Documentação de decisões relacionadas à privacidade

- Envolvimento do encarregado em fases iniciais de projetos

2. Privacy by Default (Privacidade como padrão)

Configurações que favorecem a proteção de dados:

- Minimização por padrão: Coleta apenas de dados necessários
- Limitação de uso: Utilização restrita às finalidades informadas
- Configurações restritivas: Opções padrão que limitam o compartilhamento
- Retenção limitada: Períodos de armazenamento definidos e justificados
- Acesso controlado: Permissões baseadas na necessidade de conhecer

Implementação na UFPI:

- Revisão de formulários para eliminar campos desnecessários
- Configurações padrão de privacidade em sistemas
- Descarte automático de dados após períodos definidos
- Perfis de acesso baseados em funções
- Limitação técnica de uso para finalidades definidas

Boas práticas para tratamentos específicos

1. Dados acadêmicos

- Acesso granular: Permissões específicas para diferentes tipos de dados
- Transparência sobre uso: Informação clara sobre tratamentos
- Prazos de retenção definidos: Políticas específicas por tipo de registro
- Anonimização para estatísticas: Uso de dados agregados sempre que possível
- Proteção de avaliações: Controles especiais para notas e pareceres

2. Dados de pesquisa

- Protocolos éticos robustos: Integração com Comitês de Ética em Pesquisa
- Consentimento informado: Processos claros para participantes
- Anonimização prioritária: Remoção de identificadores quando viável
- Compartilhamento seguro: Protocolos para colaboração entre pesquisadores
- Preservação controlada: Armazenamento seguro de dados brutos

3. Dados sensíveis

- Inventário específico: Mapeamento detalhado de todos os dados sensíveis
- Controles reforçados: Medidas adicionais de segurança
- Justificativa documentada: Registro da necessidade de cada tratamento
- Acesso extremamente limitado: Permissões apenas para funções essenciais
- Auditorias frequentes: Verificação regular de conformidade

4. Uso de tecnologias emergentes

- Avaliação prévia: Análise de riscos antes da adoção
- Testes controlados: Implementação gradual com monitoramento
- Transparência sobre algoritmos: Explicabilidade de decisões automatizadas
- Salvaguardas técnicas: Controles específicos para novas tecnologias
- Revisão periódica: Reavaliação contínua de impactos

Cultura organizacional de privacidade

Além de estruturas e processos formais, o desenvolvimento de uma cultura de privacidade é essencial:

1. Liderança pelo exemplo

- Comportamento da alta administração: Demonstração de compromisso
- Responsabilidade visível: Gestores como promotores da proteção de dados
- Reconhecimento de boas práticas: Valorização de comportamentos adequados
- Abordagem não punitiva: Incentivo ao relato de problemas
- Comunicação consistente: Mensagens claras sobre a importância do tema

2. Incorporação no cotidiano institucional

- Privacidade como parte da rotina: Não como atividade adicional
- Linguagem acessível: Comunicação clara e não técnica
- Ferramentas práticas: Recursos que facilitem a conformidade
- Acessibilidade da informação: Fácil acesso a orientações
- Canais de suporte: Disponibilidade para esclarecimento de dúvidas

3. Aprendizado contínuo

- Compartilhamento de experiências: Disseminação de lições aprendidas
- Comunidades de prática: Grupos de discussão e troca
- Estudos de caso: Análise de situações reais ou hipotéticas
- Atualização constante: Acompanhamento de evoluções normativas
- Feedback dos titulares: Incorporação de percepções externas

Benefícios da governança robusta

A implementação de boas práticas de governança traz diversos benefícios para a UFPI:

1. Benefícios operacionais

- Maior eficiência: Processos bem definidos reduzem retrabalho

- Qualidade de dados: Melhor gestão do ciclo de vida das informações
- Redução de incidentes: Menos violações e problemas relacionados a dados
- Tomada de decisão fundamentada: Maior clareza sobre tratamentos permitidos
- Interoperabilidade facilitada: Compartilhamento seguro entre sistemas

2. Benefícios reputacionais

- Confiança da comunidade acadêmica: Alunos, servidores e parceiros mais seguros
- Imagem institucional fortalecida: Reconhecimento como referência em boas práticas
- Transparência demonstrada: Evidências concretas de compromisso com direitos
- Relacionamento positivo com a ANPD: Postura proativa valorizada
- Diferenciação entre instituições: Destaque em práticas de governança

3. Benefícios estratégicos

- Segurança jurídica: Redução de riscos legais e regulatórios
- Possibilidade de inovação responsável: Base sólida para novos projetos
- Prevenção de custos: Evita despesas com incidentes e remediação
- Sustentabilidade das operações: Continuidade de serviços sem interrupções
- Melhoria contínua institucional: Aprimoramento de processos em geral

4. Benefícios para os titulares

- Direitos efetivamente garantidos: Exercício facilitado de prerrogativas legais
- Transparência real: Compreensão clara sobre tratamentos realizados

- Minimização de riscos: Menor probabilidade de uso indevido de dados
- Segurança reforçada: Proteção contra acessos não autorizados
- Controle sobre informações pessoais: Maior autonomia do titular

Avaliação de maturidade em governança de privacidade

Para avaliar o nível de implementação das boas práticas, a UFPI pode adotar um modelo de maturidade, com estágios progressivos:

Nível 1: Inicial / Ad hoc

- Práticas de proteção de dados informais e reativas
- Ausência de políticas formalizadas
- Tratamento caso a caso de questões de privacidade
- Baixa conscientização organizacional
- Conformidade mínima ou parcial com requisitos básicos

Nível 2: Repetível / Gerenciado

- Processos básicos estabelecidos para áreas críticas
- Políticas iniciais documentadas
- Responsabilidades primárias definidas
- Conscientização crescente, mas limitada
- Conformidade parcial com a LGPD

Nível 3: Definido

- Processos padronizados em toda a instituição
- Framework completo de políticas e normas
- Estrutura de governança estabelecida
- Programa de conscientização ativo
- Conformidade substancial com a LGPD

Nível 4: Gerenciado quantitativamente

- Processos mensurados com métricas estabelecidas
- Políticas regularmente revisadas e atualizadas
- Governança ativa com supervisão contínua
- Cultura de privacidade em desenvolvimento
- Conformidade completa e monitorada

Nível 5: Otimizado

- Melhoria contínua baseada em métricas e feedback
- Políticas maduras integradas à estratégia institucional
- Governança proativa e adaptativa
- Cultura de privacidade consolidada
- Referência de excelência em proteção de dados

Uma autoavaliação periódica permite identificar pontos fortes e oportunidades de melhoria, orientando o desenvolvimento contínuo do programa de governança.

Tendências e desafios futuros

A governança de privacidade é um campo dinâmico, em constante evolução. Alguns desafios e tendências que a UFPI deve acompanhar incluem:

1. Evolução regulatória

- Regulamentações específicas da ANPD
- Normas setoriais para educação
- Jurisprudência administrativa e judicial
- Harmonização com outras legislações (LAI, Marco Civil, etc.)
- Regulamentos internacionais com impacto em colaborações

2. Avanços tecnológicos

- Inteligência artificial e aprendizado de máquina

- Internet das Coisas (IoT) no campus
- Computação em nuvem e serviços distribuídos
- Biometria e tecnologias de reconhecimento
- Análise de big data em contexto acadêmico

3. Novas demandas dos titulares

- Expectativas crescentes de transparência
- Maior conscientização sobre direitos
- Preocupações com uso ético de dados
- Demanda por controle granular sobre informações
- Atenção à equidade e não discriminação algorítmica

A implementação de boas práticas de governança não é um destino final, mas uma jornada contínua de aprimoramento. Ao adotar uma abordagem estruturada, baseada em princípios sólidos e adaptada ao contexto universitário, a UFPI não apenas garantirá a conformidade com a LGPD, mas também se posicionará como uma instituição comprometida com o tratamento ético e responsável de dados pessoais, fortalecendo a confiança da comunidade acadêmica e da sociedade.

CONCLUSÃO

Ao longo desta apostila, exploramos os fundamentos, conceitos e aplicações práticas da Lei Geral de Proteção de Dados Pessoais (LGPD) no contexto das instituições federais de ensino superior, com foco específico na realidade da Universidade Federal do Piauí.

A LGPD representa muito mais que um conjunto de obrigações legais — é um marco na valorização da privacidade e da autodeterminação informativa como direitos fundamentais no Brasil. Para a UFPI, a adequação à lei constitui tanto um desafio quanto uma oportunidade de aprimorar sua governança institucional e fortalecer a confiança da comunidade acadêmica.

Principais aprendizados

Ao longo dos quatro módulos, pudemos compreender:

- Os fundamentos e princípios da LGPD, que estabelecem as bases conceituais e éticas para todo tratamento de dados pessoais, reconhecendo a importância da finalidade, adequação, necessidade, transparência e outros valores essenciais.
- A identificação e classificação de dados pessoais, permitindo distinguir diferentes categorias de informações e compreender suas implicações específicas, com destaque para os cuidados adicionais necessários para dados sensíveis.
- As práticas adequadas de tratamento de dados, incluindo a identificação das bases legais aplicáveis, a implementação de medidas de segurança, o registro das operações e a avaliação de impactos potenciais.
- As responsabilidades e mecanismos de compliance, abrangendo os papéis dos agentes de tratamento, as funções do encarregado, as possí-

veis sanções e, fundamentalmente, as boas práticas de governança que permitem uma abordagem proativa e sustentável.

Próximos passos para a UFPI

A jornada de adequação à LGPD é contínua e exige comprometimento institucional em todos os níveis. Alguns passos fundamentais para avançar nesse processo incluem:

- Estabelecer uma estrutura formal de governança de privacidade, com políticas institucionais, responsabilidades definidas e mecanismos de supervisão.
- Completar e manter atualizado o mapeamento de dados pessoais tratados em todos os setores e atividades da universidade.
- Implementar medidas técnicas e administrativas adequadas para proteger os dados e garantir os direitos dos titulares.
- Desenvolver e executar um programa contínuo de conscientização e capacitação, alcançando servidores, professores, alunos e colaboradores.
- Integrar a proteção de dados ao DNA institucional, incorporando-a nos processos decisórios, no planejamento estratégico e na cultura organizacional.

Uma visão de futuro

Olhando além da conformidade legal, a UFPI tem a oportunidade de se posicionar como referência no tratamento ético e responsável de dados pessoais no âmbito da educação superior. Isso significa não apenas cumprir as exigências da LGPD, mas adotar uma postura de liderança, inovação e excelência em práticas de proteção de dados.

Uma universidade que respeita e protege adequadamente os dados pessoais constrói um ambiente de confiança que favorece o desenvolvimento acadêmico, a pesquisa responsável e o relacionamento transparente com a sociedade. Em última análise, a proteção de dados alinha-se perfeitamente à missão fundamental da UFPI de produzir e difundir conhecimentos com ética e responsabilidade social.

Este material representa um ponto de partida para essa jornada, fornecendo bases conceituais e orientações práticas. O verdadeiro sucesso, contudo, dependerá do engajamento coletivo e do compromisso contínuo com a privacidade e proteção de dados como valores institucionais fundamentais.

REFERÊNCIAS BIBLIOGRÁFICAS

Legislação

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

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Regulamenta a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Disponível em: https://www.gov.br/anpd/pt-br/ assuntos/noticias/inclusao-de-link-para-a-resolucao/resolucao-cd-anpd--no-2-de-27-de-janeiro-de-2022.pdf

Livros e artigos

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2022.
DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2023.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2023.
TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2022.

Guias e materiais técnicos

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal. Disponível em: https://www.gov.br/anpd/pt-br

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. LGPD Acadêmico: Proteção de Dados Pessoais em Instituições de Ensino. Disponível em: https://www.gov.br/anpd/pt-br/documentos--e-publicacoes/guia-lgpd-cademico_versao-1-0.pdf

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. Guia de Elaboração de Inventário de Dados Pessoais. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e--protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf

SERPRO. Cartilha LGPD: Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/apresentacao-lgpd

Sites e recursos online

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Portal oficial. Disponível em: https://www.gov.br/anpd/pt-br

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. Cursos sobre LGPD. Disponível em: https://www.gov.br/enap/pt-br

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). Observatório da Privacidade e Proteção de Dados. Disponível em: https://www.observatorioprivacidade.com.br/SERPRO. Portal LGPD. Disponível em: https://www.serpro.gov.br/lgpd/

GLOSSÁRIO

ANPD: Autoridade Nacional de Proteção de Dados. Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

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.

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

Base legal: Fundamento jurídico que legitima uma operação de tratamento de dados pessoais, conforme hipóteses previstas nos artigos 7º e 11 da LGPD.

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

Ciclo de vida dos dados: Todas as fases pelas quais os dados pessoais passam, desde sua coleta até sua eliminação.

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

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável.

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.

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

Encarregado (Data Protection Officer — DPO): Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

GDPR: General Data Protection Regulation (Regulamento Geral de Proteção de Dados). Regulamento da União Europeia que inspirou a LGPD brasileira.

Incidente de segurança: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos dados pessoais, como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito.

LGPD: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Privacy by Design: Abordagem que integra a proteção de dados desde a fase de concepção de produtos, serviços e sistemas, garantindo que a privacidade seja considerada durante todo o ciclo de desenvolvimento. os razoáveis e disponíveis na ocasião de seu tratamento.

Privacy by Default: Princípio segundo o qual as configurações padrão de produtos e serviços devem ser as mais protetivas possível em termos de privacidade.

Pseudonimização: 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.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): 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.

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

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

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.

ANEXOS

DOCUMENTOS PRÁTICOS PARA IMPLEMENTAÇÃO DA LGPD NA UFPI

Anexo I - Modelo de Política de Privacidade para a UFPI

Este modelo de Política de Privacidade foi desenvolvido especificamente para a Universidade Federal do Piauí, considerando suas atividades de ensino, pesquisa, extensão e gestão. O documento estabelece diretrizes institucionais sobre o tratamento de dados pessoais, servindo como base para a comunicação transparente com a comunidade acadêmica e o público externo. Esta política deve ser aprovada pelos órgãos colegiados superiores da universidade e amplamente divulgada em todos os canais institucionais.

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DA UNIVERSIDADE FEDERAL DO PIAUÍ

1. INTRODUÇÃO

A Universidade Federal do Piauí (UFPI), instituição federal de ensino superior, pesquisa e extensão, com sede na cidade de Teresina-PI, reconhece a importância da privacidade e da proteção dos dados pessoais de toda a sua comunidade acadêmica e do público externo com o qual se relaciona.

Esta Política de Privacidade e Proteção de Dados Pessoais estabelece as diretrizes e princípios que orientam o tratamento de dados pessoais realizado pela UFPI, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018, bem como com outras normas aplicáveis.

2. ABRANGÊNCIA

Esta política aplica-se a todas as unidades acadêmicas e administrativas da UFPI, incluindo seus campi (Teresina, Parnaíba, Picos, Bom Jesus e Floriano), unidades descentralizadas, hospitais universitários e demais órgãos vinculados à instituição.

Abrange o tratamento de dados pessoais de:

- Estudantes (graduação, pós-graduação, extensão)
- Servidores (docentes e técnico-administrativos)
- Trabalhadores terceirizados
- Fornecedores e prestadores de serviço
- Participantes de pesquisas
- Egressos
- Visitantes e público em geral

3. DEFINIÇÕES

Para os fins desta política, consideram-se:

- **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, saúde, vida sexual, dado genético ou biométrico vinculado a uma pessoa natural.
- **Titular**: pessoa natural a quem se referem os dados pessoais.
- **Tratamento**: toda operação realizada com dados pessoais.
- **Controlador**: a UFPI, responsável pelas decisões referentes ao tratamento.
- **Operador**: pessoa natural ou jurídica que realiza o tratamento de dados em nome da UFPI.
- **Encarregado**: pessoa indicada pela UFPI para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

4. PRINCÍPIOS

A UFPI realiza o tratamento de dados pessoais orientada pelos seguintes princípios:

- **Finalidade**: realização do tratamento para propósitos legítimos, específicos e informados ao titular.
- **Adequação**: compatibilidade do tratamento com as finalidades informadas.
- **Necessidade**: limitação do tratamento ao mínimo necessário para suas finalidades.
- **Livre acesso**: garantia de consulta facilitada aos titulares sobre seus dados.
- **Qualidade dos dados**: garantia de exatidão, clareza e atualização dos dados.
- **Transparência**: informações claras e acessíveis sobre o tratamento.
- **Segurança**: medidas técnicas e administrativas para proteger os dados.
- **Prevenção**: adoção de medidas para prevenir danos.
- **Não discriminação**: impossibilidade de tratamento para fins discriminatórios.
- **Responsabilização e prestação de contas**: demonstração da adoção de medidas eficazes.

5. FINALIDADES DO TRATAMENTO

A UFPI realiza o tratamento de dados pessoais para as seguintes finalidades principais:

5.1. Atividades de Ensino

- Gestão acadêmica (matrícula, registro acadêmico, avaliação)
- Emissão de documentos (diplomas, certificados, históricos)
- Acompanhamento pedagógico
- Acesso a recursos educacionais (biblioteca, laboratórios)
- Mobilidade acadêmica
- Comunicação institucional

5.2. Atividades de Pesquisa

- Condução de projetos de pesquisa
- Análise de dados para fins científicos
- Publicação de resultados de pesquisa
- Formação de pesquisadores
- Registro de propriedade intelectual

5.3. Atividades de Extensão

- Oferta de cursos e atividades de extensão
- Desenvolvimento de projetos comunitários
- Parcerias para projetos sociais
- Eventos culturais e científicos

5.4. Atividades Administrativas

- Gestão de recursos humanos
- Processos seletivos
- Contratações e aquisições
- Gestão patrimonial e financeira
- Segurança das pessoas e do patrimônio
- Comunicação institucional
- Atendimento a requisitos legais e regulatórios

6. BASES LEGAIS

A UFPI realiza o tratamento de dados pessoais com base nas seguintes hipóteses legais:

- **Execução de políticas públicas**: tratamento necessário à execução de políticas públicas educacionais previstas em leis e regulamentos.
- **Cumprimento de obrigação legal**: tratamento necessário para atender obrigações legais específicas da instituição.
- **Execução de contratos**: tratamento necessário para a execução de contratos dos quais o titular seja parte.
- **Consentimento**: quando o tratamento não se enquadra nas hipóteses acima e o titular consente de forma livre, informada e inequívoca.
- **Exercício regular de direitos**: em processos administrativos, judiciais ou arbitrais.
- **Proteção da vida**: quando necessário para a proteção da vida do titular ou de terceiros.
- **Tutela da saúde**: exclusivamente em procedimento realizado por profissional de saúde ou por serviços de saúde.
- **Pesquisa**: estudos por órgão de pesquisa, garantida a anonimização sempre que possível.

7. DIREITOS DOS TITULARES

A UFPI assegura aos titulares de dados os seguintes direitos:

- **Confirmação e acesso**: saber se a UFPI possui seus dados e acessá-los.
- **Correção**: solicitar a correção de dados incompletos, inexatos ou desatualizados.
- **Anonimização, bloqueio ou eliminação**: de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- **Portabilidade**: solicitar a transferência dos dados para outro fornecedor de serviço ou produto.
- **Informação**: ser informado sobre compartilhamento e sobre a possibilidade de não fornecer consentimento.
- **Revogação do consentimento**: quando o tratamento se basear nesta hipótese.
- **Revisão**: solicitar revisão de decisões automatizadas que afetem seus interesses.

Para exercer esses direitos, o titular pode entrar em contato com o Encarregado pelo Tratamento de Dados Pessoais através dos canais indicados no item 14 desta Política.

8. COMPARTILHAMENTO DE DADOS

A UFPI pode compartilhar dados pessoais nas seguintes situações:

8.1. Compartilhamento Interno

- Entre departamentos, coordenações e unidades acadêmicas, conforme necessário para a finalidade específica e com base no princípio da necessidade.

8.2. Compartilhamento Externo

- **Órgãos governamentais**: MEC, CAPES, CNPq, INEP, outros órgãos para cumprimento de obrigações legais.
- **Instituições parceiras**: universidades e organizações parceiras para programas de intercâmbio, pesquisa e extensão, mediante instrumentos jurídicos adequados.
- **Operadores contratados**: empresas contratadas para prestação de serviços específicos, com garantias contratuais adequadas.
- **Empresas de serviços tecnológicos**: provedores de serviços de TI, mediante salvaguardas contratuais.

9. SEGURANÇA DOS DADOS

A UFPI adota medidas de segurança técnicas e administrativas para proteger os dados pessoais, incluindo:

- Controles de acesso físico e lógico
- Política de classificação da informação
- Criptografia para dados sensíveis
- Registro e monitoramento de acessos (logs)
- Cópias de segurança (backups)
- Plano de resposta a incidentes
- Capacitação e conscientização de usuários
- Revisões periódicas de segurança

10. PERÍODO DE RETENÇÃO

A UFPI mantém os dados pessoais pelo tempo necessário para cumprir as finalidades para as quais foram coletados, observando:

- Prazos estabelecidos em legislação específica
- Tabelas de temporalidade da administração pública federal
- Período necessário para a execução de políticas públicas
- Períodos necessários para legitimar decisões tomadas
- Prazo de guarda determinado para dados acadêmicos permanentes

11. COOKIES E TECNOLOGIAS SIMILARES

Os sites e sistemas da UFPI podem utilizar cookies e tecnologias similares para melhorar a experiência do usuário e coletar informações sobre a navegação. Os tipos de cookies utilizados incluem:

- **Cookies essenciais**: necessários para o funcionamento básico das páginas

- **Cookies funcionais**: permitem lembrar escolhas feitas pelo usuário
- **Cookies analíticos**: permitem analisar como os usuários utilizam o site
- **Cookies de terceiros**: inseridos por serviços externos integrados ao site

O usuário pode gerenciar as preferências de cookies através das configurações do seu navegador.

12. TRANSFERÊNCIA INTERNACIONAL

A UFPI pode realizar transferência internacional de dados nas seguintes situações:

- Cooperação internacional para fins acadêmicos e de pesquisa
- Programas de mobilidade e intercâmbio estudantil
- Utilização de serviços de tecnologia hospedados no exterior

Em todos os casos, são adotadas salvaguardas adequadas para garantir a proteção dos dados, como cláusulas contratuais específicas, verificação do nível de proteção do país destinatário ou consentimento específico do titular.

13. GOVERNANÇA E CONFORMIDADE

A UFPI se compromete a manter um programa de governança em privacidade, que inclui:

- Política institucional de proteção de dados
- Encarregado pelo tratamento de dados pessoais
- Comitê de Proteção de Dados Pessoais
- Processos documentados para tratamento de dados
- Avaliações periódicas de conformidade
- Registros das operações de tratamento
- Relatórios de impacto quando necessário
- Programa de conscientização e treinamento
- Procedimentos para resposta a incidentes

14. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

A UFPI designou um Encarregado pelo Tratamento de Dados Pessoais, que atua como canal de comunicação entre a instituição, os titulares e a Autoridade Nacional de Proteção de Dados.

Contato: [e-mail do encarregado]@ufpi.edu.br **Telefone**: (86) XXXX-XXXX **Endereço**: [endereço físico para correspondência] **Formulário online**: [link para formulário de contato]

15. MUDANÇAS NA POLÍTICA DE PRIVACIDADE

Esta Política pode ser atualizada periodicamente para refletir alterações nas práticas de tratamento de dados ou na legislação aplicável. A versão mais recente estará sempre disponível no site da UFPI, com indicação da data da última atualização.

Alterações significativas serão comunicadas pelos canais institucionais antes de sua implementação.

16. DISPOSIÇÕES FINAIS

Esta Política foi aprovada pelo Conselho Universitário da UFPI em [data], através da Resolução nº [número], e entra em vigor na data de sua publicação.

Casos omissos serão resolvidos pelo Comitê de Proteção de Dados Pessoais da UFPI, ouvido o Encarregado.

Data da última atualização: [data]

Anexo II - Formulário de Registro de Tratamento de Dados Pessoais

Este formulário foi elaborado para implementar o registro das operações de tratamento de dados, conforme exigido pela LGPD. Ele serve como ferramenta para documentar de forma estruturada todas as atividades de tratamento realizadas pelos diversos setores da UFPI. O preenchimento deste documento contribui para o inventário de dados da instituição, proporcionando transparência e permitindo a demonstração de conformidade com a lei. Cada setor deve manter seus formulários atualizados e submetê-los periodicamente ao Encarregado de Dados.

FORMULÁRIO DE REGISTRO DE TRATAMENTO DE DADOS PESSOAIS

1. IDENTIFICAÇÃO DA ATIVIDADE

Nome da atividade de tratamento:

Departamento/Setor responsável:

Responsável pelo preenchimento:

Nome: _____
Cargo: _____
E-mail: _____
Telefone: _____

Data do preenchimento: //_____ **Última atualização**: //_____

2. DESCRIÇÃO DA ATIVIDADE

Finalidade(s) específica(s) do tratamento:

Descrição resumida do processo:

Sistemas/aplicações utilizados:

3. DADOS PESSOAIS TRATADOS

3.1. Categorias de dados pessoais comuns

Categoria	Dados específicos	Obrigatório?	Origem dos dados
Identificação	□ Nome completo □ Data de nascimento □ Nacionalidade □ Naturalidade □ RG □ CPF □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Contato	□ Endereço residencial □ E-mail □ Telefone/celular □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Acadêmicos	□ Matrícula □ Histórico escolar □ Notas/conceitos □ Frequência □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Profissionais	□ Cargo/função □ SIAPE □ Histórico funcional □ Avaliações □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Financeiros	□ Dados bancários □ Informações de pagamento □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Outros	□ Especificar: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____

3.2. Dados pessoais sensíveis

Categoria	Dados específicos	Obrigatório?	Origem dos dados
Saúde	□ Atestados médicos □ Condições de saúde □ Exames □ Outros:	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra:
Biométricos	□ Impressão digital □ Reconhecimento facial □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública

			□ Outra: _____
Origem racial/étnica	□ Autodeclaração □ Outros: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Convicção religiosa	□ Especificar: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Opinião política	□ Especificar: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Filiação sindical	□ Especificar: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____
Outros	□ Especificar: _____	□ Sim □ Não	□ Titular □ Terceiro □ Pública □ Outra: _____

3.3. Dados de crianças e adolescentes

Esta atividade trata dados de crianças ou adolescentes (menores de 18 anos)? □ Não □ Sim. Especificar:

3.4. Volume de dados

Estimativa de titulares afetados:

□ Até 100 □ 101-1.000 □ 1.001-10.000 □ 10.001-100.000 □ Mais de 100.000

4. BASE LEGAL E CONSENTIMENTO

4.1. Base legal utilizada

□ Cumprimento de obrigação legal ou regulatória (Art. 7º, II)

Especificar a lei/regulamento:

_____

□ Execução de políticas públicas (Art. 7º, III)

Especificar a política:

_____

□ Execução de contrato (Art. 7º, V)

Especificar o contrato:

_____

□ Exercício regular de direitos (Art. 7º, VI)

Especificar:

_____

□ Proteção da vida ou incolumidade física (Art. 7º, VII)

Especificar:

_____

□ Tutela da saúde (Art. 7º, VIII)

Especificar:

_____

□ Interesses legítimos (Art. 7º, IX)

Especificar:

_____

□ Proteção ao crédito (Art. 7º, X)

Especificar:

_____

□ Consentimento (Art. 7º, I)

Forma de obtenção: _____

Mecanismo para revogação: _____

4.2. Base legal para dados sensíveis (se aplicável)

□ Cumprimento de obrigação legal ou regulatória (Art. 11, II, a)

Especificar a lei/regulamento: _____

□ Execução de políticas públicas (Art. 11, II, b)

Especificar a política: _____

□ Estudos por órgão de pesquisa (Art. 11, II, c)

Especificar: _____

□ Exercício regular de direitos (Art. 11, II, d)

Especificar: _____

□ Proteção da vida ou incolumidade física (Art. 11, II, e)

Especificar: _____

□ Tutela da saúde (Art. 11, II, f)

Especificar: _____

□ Garantia de prevenção à fraude (Art. 11, II, g)

Especificar: _____

□ Consentimento específico (Art. 11, I)

Forma de obtenção: _____

Mecanismo para revogação: _____

5. CICLO DE VIDA DOS DADOS

5.1. Coleta

Método de coleta:

□ Formulário em papel □ Formulário eletrônico □ Sistema informatizado □ E-mail □ Telefone □ Importação de outro sistema/base □ Outro: _____

Informações fornecidas aos titulares no momento da coleta:

□ Finalidade específica □ Base legal □ Compartilhamentos previstos □ Período de retenção □ Direitos dos titulares □ Contato do encarregado □ Outras: _____

5.2. Armazenamento

Formato de armazenamento:

□ Físico (papel) □ Banco de dados □ Arquivos digitais □ Nuvem □ E-mail □ Outro: _____

Local de armazenamento:

Controles de acesso implementados:

5.3. Período de retenção

Prazo de retenção dos dados:

□ Até 1 ano □ 1-5 anos □ 5-10 anos □ 10-30 anos □ permanente

Justificativa para o prazo definido:

□ Requisito legal. Especificar: _____

□ Finalidade do tratamento. Especificar: _____

□ Tabela de temporalidade documental. Especificar: _____

□ Outro. Especificar: _____

5.4. Eliminação

Método de eliminação:

□ Trituração (papel) □ Exclusão lógica □ Exclusão física/sobrescrita

□ Anonimização □ Outro: _____

Processo documentado de eliminação:

□ Sim □ Não □ em desenvolvimento

6. COMPARTILHAMENTO

6.1. Compartilhamento interno

Os dados são compartilhados com outros departamentos/setores da UFPI? □ Não □ Sim. Especificar:

Departamento/Setor	Finalidade	Dados compartilhados

6.2. Compartilhamento externo

Os dados são compartilhados com organizações externas?

□ Não □ Sim. Especificar: _____

Organização	Tipo de relação	Finalidade	Dados compartilhados	Salvaguardas
	□ Controlador conjunto □ Operador □ Terceiro			□ Contrato □ Convênio □ Termo de uso □ Outros
	□ Controlador conjunto □ Operador			□ Contrato □ Convênio

	□ Terceiro			□ Termo de uso □ Outros
	□ Controlador conjunto □ Operador □ Terceiro			□ Contrato □ Convênio □ Termo de uso □ Outros

6.3. Transferência internacional

Os dados são transferidos para outros países?

□ Não

□ Sim. Especificar: _____

País	Organização	Finalidade	Dados transferidos	Base legal para transferência
				□ Nível adequado de proteção □ Garantias contratuais □ Consentimento □ Outras
				□ Nível adequado de proteção □ Garantias contratuais □ Consentimento □ Outras

7. MEDIDAS DE SEGURANÇA

7.1. Medidas técnicas implementadas

□ Controles de acesso lógico □ Criptografia □ Backup □ Logs de auditoria

□ Firewall/IDS □ Antivírus/antimalware □ Anonimização/pseudonimização

□ Outros: _____

7.2. Medidas administrativas implementadas

□ Política de segurança da informação □ Termo de confidencialidade

□ Treinamento de pessoal □ Controle de acesso físico

□ Classificação da informação □ Gestão de incidentes

□ Outros: _____

8. AVALIAÇÃO DE RISCOS

8.1. Riscos identificados

Risco	Probabilidade	Impacto	Nível de risco	Medidas mitigadoras
	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	

8.2. Relatório de Impacto à Proteção de Dados (RIPD)

Foi realizado um RIPD para esta atividade de tratamento?

□ Não □ Sim, em ___/___/____ □ em elaboração

9. CONFORMIDADE E CONTROLES

9.1. Direitos dos titulares

Mecanismos implementados para atender direitos dos titulares:

□ Confirmação de existência □ Acesso aos dados □ Correção

□ Anonimização/bloqueio/eliminação □ Portabilidade □ Revogação de consentimento

□ Outros: _____

Canal para exercício de direitos:

9.2. Verificações de conformidade

Data da última revisão deste registro: ___/___/_____

Responsável pela revisão: _____

Próxima revisão programada: ___/___/_____

10. APROVAÇÕES

Responsável pelo tratamento:

Nome: _____ Cargo: _____

Assinatura: _____ Data: ___/___/_____

Encarregado de Proteção de Dados:

Nome: _____

Assinatura: _____ Data: ___/___/_____

Anexo III - Modelo de Termo de Consentimento

Este modelo de Termo de Consentimento foi desenvolvido para situações em que a UFPI necessita obter consentimento específico do titular para o tratamento de seus dados pessoais. O documento é estruturado de forma clara e transparente, seguindo as exigências da LGPD para que o consentimento seja livre, informado e inequívoco. Este modelo deve ser adaptado conforme a finalidade específica do tratamento e pode ser utilizado tanto em formato impresso quanto eletrônico, garantindo sempre a documentação adequada do consentimento obtido.

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

IDENTIFICAÇÃO

Controlador: Universidade Federal do Piauí (UFPI), CNPJ 06.517.387/0001-34, com sede no Campus Ministro Petrônio Portella, Bairro Ininga, Teresina-PI, CEP 64049-550.

Setor responsável: [Nome do departamento/setor específico]

Encarregado pelo Tratamento de Dados Pessoais: [Nome do Encarregado]

E-mail: [e-mail do encarregado]@ufpi.edu.br

Telefone: (86) XXXX-XXXX

TITULAR DOS DADOS

Nome completo: _____

CPF: _____ RG: _____

Matrícula/SIAPE (se aplicável): _____

E-mail: _____

Telefone: (____) _____

FINALIDADE DO TRATAMENTO

Este Termo de Consentimento tem como objetivo obter sua autorização para que a Universidade Federal do Piauí (UFPI) realize o tratamento dos seus dados pessoais para a(s) seguinte(s) finalidade(s) específica(s):

- [Descrever detalhadamente cada finalidade específica para a qual o consentimento está sendo solicitado]
- [Exemplo: "Utilização de sua imagem e voz em fotografias e vídeos para divulgação institucional em materiais impressos e digitais da UFPI"]
- [Exemplo: "Coleta e tratamento de dados socioeconômicos para análise estatística sobre o perfil dos estudantes"]
- [Exemplo: "Participação em pesquisa acadêmica sobre _____"]

DADOS PESSOAIS QUE SERÃO TRATADOS

Para atender à(s) finalidade(s) descrita(s) acima, precisaremos tratar os seguintes dados pessoais:

Dados pessoais comuns:

- [Listar todos os dados comuns que serão coletados]
- [Exemplo: nome completo, endereço, telefone, e-mail, data de nascimento]

Dados pessoais sensíveis (se aplicável):

- [Listar todos os dados sensíveis que serão coletados]
- [Exemplo: informações sobre saúde, origem racial ou étnica, dados biométricos]
- [Exemplo: nenhum dado sensível será coletado]

FORMA DE TRATAMENTO

Os dados serão tratados e armazenados em ambiente seguro, mediante a adoção de medidas técnicas e administrativas adequadas para proteger sua privacidade. O tratamento incluirá as seguintes operações:

- [Coleta]
- [Armazenamento]
- [Utilização]
- [Compartilhamento (se aplicável)]
- [Outras operações relevantes]

COMPARTILHAMENTO DE DADOS

Os seus dados pessoais poderão ser compartilhados com:

- [Listar todas as categorias de destinatários com quem os dados serão compartilhados]
- [Exemplo: "Outros departamentos da UFPI envolvidos no processo"]
- [Exemplo: "Ministério da Educação para fins estatísticos"]
- [Exemplo: "Empresas contratadas para processamento específico, como _____"]
- [Exemplo: "Seus dados não serão compartilhados com terceiros"]

PERÍODO DE TRATAMENTO

Os seus dados pessoais serão tratados pelo período de [informar o tempo exato ou critério que determinará o fim do tratamento], após o qual serão [eliminados/anonimizados/armazenados para fins de arquivo], exceto quando houver obrigação legal para sua manutenção.

DIREITOS DO TITULAR

Você, como titular dos dados, possui os seguintes direitos garantidos pela LGPD:

- **Confirmação e acesso**: saber se a UFPI possui seus dados e acessá-los.
- **Correção**: solicitar a correção de dados incompletos, inexatos ou desatualizados.
- **Anonimização, bloqueio ou eliminação**: de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- **Portabilidade**: solicitar a transferência dos dados para outro fornecedor de serviço ou produto.
- **Informação**: ser informado sobre compartilhamento e sobre a possibilidade de não fornecer consentimento.
- **Revogação do consentimento**: a qualquer momento, mediante manifestação expressa.

Para exercer esses direitos, você pode entrar em contato com o Encarregado pelo Tratamento de Dados Pessoais da UFPI, através dos canais informados no início deste documento.

CONSEQUÊNCIAS DA NÃO AUTORIZAÇÃO

O fornecimento do consentimento é voluntário. Caso não deseje autorizar o tratamento dos seus dados para as finalidades especificadas, você [descrever as consequências da não autorização, sem caráter coercitivo].

[Exemplo: "não poderá participar da pesquisa mencionada"]

[Exemplo: "não terá sua imagem utilizada nos materiais de divulgação, mas isso não afetará em nada seu vínculo com a instituição"]

DECLARAÇÃO DE CONSENTIMENTO

Declaro que li e entendi todas as informações contidas neste Termo de Consentimento e, de forma livre e esclarecida:

□ AUTORIZO o tratamento dos meus dados pessoais para todas as finalidades descritas acima.

□ AUTORIZO PARCIALMENTE o tratamento dos meus dados pessoais apenas para as finalidades assinaladas abaixo:

□ [Finalidade 1]

□ [Finalidade 2]

□ [Finalidade 3]

□ NÃO AUTORIZO o tratamento dos meus dados pessoais para as finalidades descritas.

_____, _____ de _____ de _____ (Cidade) (Data)

(Assinatura do Titular)

(Assinatura do Responsável pela Coleta)

Anexo IV - Formulário para Exercício de Direitos do Titular

Este formulário foi desenvolvido para facilitar o exercício dos direitos dos titulares de dados, conforme previsto na LGPD. Ele proporciona um canal estruturado para que estudantes, servidores e demais titulares possam solicitar acesso, correção, eliminação ou outras ações relacionadas aos seus dados pessoais tratados pela UFPI. O documento deve ser disponibilizado tanto em formato físico quanto digital, e o processo de atendimento às solicitações deve ser documentado e gerenciado pelo Encarregado de Proteção de Dados, garantindo resposta dentro dos prazos legais.

FORMULÁRIO PARA EXERCÍCIO DE DIREITOS DO TITULAR

IDENTIFICAÇÃO DO TITULAR

Nome completo: _____

CPF: _____ RG: _____

Vínculo com a UFPI: □ Estudante □ Servidor □ Ex-aluno □ Ex-servidor □ Visitante

□ Outro: _____

Matrícula/SIAPE (se aplicável): _____

Endereço: _____

Cidade: _____ Estado: _____ CEP: _____

E-mail: _____

Telefone: (____) _____

REPRESENTANTE LEGAL (preencher apenas se a solicitação for feita por representante)

Nome completo: _____

CPF: _____ RG: _____

E-mail: _____

Telefone: (____) _____

Obs.: É necessário anexar documentação que comprove a representação legal (procuração, termo de tutela/curatela, etc.).

DIREITO A SER EXERCIDO

Solicito o exercício do seguinte direito em relação aos meus dados pessoais:

□ **Confirmação de existência de tratamento** (Art. 18, I)

Desejo saber se a UFPI realiza o tratamento dos meus dados pessoais.

□ **Acesso aos dados** (Art. 18, II)

Desejo receber uma cópia dos meus dados pessoais que estão sendo tratados pela UFPI.

□ **Correção de dados** (Art. 18, III)

Desejo corrigir dados incompletos, inexatos ou desatualizados.

□ **Anonimização, bloqueio ou eliminação** (Art. 18, IV)

Desejo que meus dados sejam anonimizados, bloqueados ou eliminados quando desnecessários, excessivos ou tratados em desconformidade com a LGPD.

□ **Portabilidade dos dados** (Art. 18, V)

Desejo que meus dados sejam transferidos para outro fornecedor de serviço ou produto.

□ **Eliminação dos dados tratados com consentimento** (Art. 18, VI)

Desejo que sejam eliminados os dados tratados com base no meu consentimento.

□ **Informação sobre compartilhamento** (Art. 18, VII)

Desejo saber com quais entidades públicas e privadas a UFPI compartilha meus dados.

□ **Informação sobre a possibilidade de não consentir** (Art. 18, VIII)

Desejo informações sobre a opção de não fornecer consentimento e as consequências da negativa.

□ **Revogação do consentimento** (Art. 18, IX)

Desejo revogar o consentimento anteriormente fornecido para determinado tratamento de dados.

□ **Revisão de decisões automatizadas** (Art. 20)

Desejo solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

□ **Outro**: Especificar: _____

DESCRIÇÃO DA SOLICITAÇÃO

Descreva detalhadamente sua solicitação, incluindo quais dados pessoais estão envolvidos, em quais circunstâncias foram coletados, qual tratamento está sendo questionado, etc.

ESPECIFICAÇÃO DOS DADOS (para correção)

Preencha caso esteja solicitando a correção de dados:

Dado incorreto/desatualizado	Dado correto

JUSTIFICATIVA (se aplicável)

Se necessário, forneça uma justificativa para sua solicitação:

CANAIS DE RESPOSTA

De que forma prefere receber a resposta a esta solicitação?

□ E-mail □ Correspondência física □ Presencialmente

DECLARAÇÃO

Declaro que as informações fornecidas neste formulário são verdadeiras e que sou o titular dos dados pessoais objeto desta solicitação ou seu representante legal devidamente autorizado.

Estou ciente de que:

- Poderei ser contatado para fornecer informações adicionais necessárias para confirmar minha identidade e garantir que os direitos estão sendo exercidos legitimamente.
- A UFPI tem o prazo de 15 dias, contados a partir do recebimento desta solicitação, para responder, conforme previsto na LGPD.

- Informações falsas ou solicitações fraudulentas podem resultar na recusa da solicitação, além de possíveis consequências administrativas e legais.

_____, _____ de _____ de _____ (Cidade) (Data)

(Assinatura)

PARA USO EXCLUSIVO DA UFPI

Nº do protocolo: _____

Data de recebimento: ___/___/_____

Recebido por: _____

Prazo para resposta: ___/___/_____

Encaminhado para: _____

Observações: _____

Anexo V - Checklist de Adequação à LGPD

Este checklist foi elaborado como ferramenta de autoavaliação para que os diversos setores e departamentos da UFPI possam verificar seu nível de conformidade com a LGPD. O documento permite identificar áreas que necessitam de atenção prioritária e acompanhar o progresso das ações de adequação. Recomenda-se que este checklist seja aplicado periodicamente, com o envolvimento das equipes responsáveis pelo tratamento de dados, e que os resultados sejam reportados ao Encarregado de Proteção de Dados para análise e encaminhamentos necessários.

CHECKLIST DE ADEQUAÇÃO À LGPD

INSTRUÇÕES

Este checklist é uma ferramenta para auxiliar na autoavaliação do nível de adequação à LGPD. Para cada item, marque uma das opções:

- **Implementado**: requisito totalmente atendido, com evidências documentadas
- **Parcial**: implementação em andamento ou incompleta
- **Não implementado**: requisito ainda não atendido
- **Não aplicável**: requisito não se aplica ao contexto específico

Ao final de cada seção, calcule a porcentagem de adequação considerando apenas os itens aplicáveis.

IDENTIFICAÇÃO

Unidade/Departamento: _____

Responsável pelo preenchimento: _____

Data da avaliação: ___/___/_____

1. GOVERNANÇA E CONFORMIDADE

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
1.1	A unidade conhece a Política de Privacidade e Proteção de Dados da UFPI	□	□	□	□	
1.2	Os servidores e colaboradores da unidade foram treinados sobre a LGPD	□	□	□	□	
1.3	Existe uma pessoa designada como ponto focal de proteção de dados na unidade	□	□	□	□	

1.4	A unidade mantém comunicação regular com o Encarregado de Proteção de Dados da UFPI	□	□	□	□	
1.5	Existe um processo documentado para identificar e avaliar novos tratamentos de dados	□	□	□	□	
1.6	A unidade realiza auditorias periódicas de conformidade com a LGPD	□	□	□	□	
1.7	Os riscos relacionados à proteção de dados são formalmente identificados e gerenciados	□	□	□	□	
1.8	A unidade possui plano de ação para adequação contínua à LGPD	□	□	□	□	

Pontuação da Seção 1: _____ de um total de _____ itens aplicáveis (_____%)

2. MAPEAMENTO E REGISTRO DE TRATAMENTO

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
2.1	Todos os tratamentos de dados pessoais realizados pela unidade foram identificados e documentados	□	□	□	□	
2.2	Para cada tratamento, foram identificados os tipos de dados processados	□	□	□	□	
2.3	Para cada tratamento, foi identificada e documentada a base legal aplicável	□	□	□	□	
2.4	Os dados pessoais sensíveis foram devidamente identificados e recebem proteção especial	□	□	□	□	
2.5	O tratamento de dados de crianças e adolescentes foi identificado e possui controles específicos	□	□	□	□	
2.6	O ciclo de vida completo dos dados (coleta, uso, armazenamento, compartilhamento e	□	□	□	□	

	eliminação) está documentado					
2.7	Os formulários de coleta foram revisados para eliminar dados desnecessários	□	□	□	□	
2.8	Existe inventário atualizado de todos os sistemas e bancos de dados que processam dados pessoais	□	□	□	□	

Pontuação da Seção 2: _____ de um total de _____ itens aplicáveis (_____%)

3. BASES LEGAIS E CONSENTIMENTO

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
3.1	As bases legais utilizadas para cada tratamento estão claramente documentadas	□	□	□	□	
3.2	Quando o consentimento é utilizado, ele é obtido de forma livre, informada e inequívoca	□	□	□	□	
3.3	Existe processo para comprovar a obtenção do consentimento	□	□	□	□	
3.4	Existe mecanismo para revogação do consentimento	□	□	□	□	
3.5	Os termos de consentimento são claros, em linguagem simples e específicos quanto às finalidades	□	□	□	□	
3.6	A obtenção específica de consentimento para dados sensíveis está implementada	□	□	□	□	
3.7	O consentimento específico dos pais/responsáveis é obtido para tratamento de dados de crianças	□	□	□	□	
3.8	Foram identificados tratamentos baseados no legítimo interesse e realizado o teste de balanceamento	□	□	□	□	

Pontuação da Seção 3: _____ de um total de _____ itens aplicáveis (_____%)

4. DIREITOS DOS TITULARES

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
4.1	Existe processo para atender solicitações de confirmação de existência de tratamento	□	□	□	□	
4.2	Existe processo para atender solicitações de acesso aos dados	□	□	□	□	
4.3	Existe processo para atender solicitações de correção de dados	□	□	□	□	
4.4	Existe processo para atender solicitações de anonimização, bloqueio ou eliminação	□	□	□	□	
4.5	Existe processo para atender solicitações de portabilidade	□	□	□	□	
4.6	Existe processo para atender solicitações de revogação de consentimento	□	□	□	□	
4.7	Existe processo para informar os titulares sobre compartilhamentos	□	□	□	□	
4.8	As solicitações dos titulares são documentadas e respondidas dentro do prazo legal	□	□	□	□	

Pontuação da Seção 4: _____ de um total de _____ itens aplicáveis (_____%)

5. SEGURANÇA E CONTROLES TÉCNICOS

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
5.1	Controles de acesso adequados estão implementados (físicos e lógicos)	□	□	□	□	
5.2	A criptografia é utilizada para proteção de dados sensíveis	□	□	□	□	
5.3	Existem procedimentos de backup e recuperação	□	□	□	□	

5.4	Logs e trilhas de auditoria são mantidos e monitorados	□	□	□	□	
5.5	Existe processo de resposta a incidentes de segurança	□	□	□	□	
5.6	Os sistemas possuem proteções adequadas contra ameaças (firewall, antivírus, etc.)	□	□	□	□	
5.7	Existem controles para proteção de dados em dispositivos móveis	□	□	□	□	
5.8	Sistemas e aplicações recebem atualizações de segurança regularmente	□	□	□	□	

Pontuação da Seção 5: _____ de um total de _____ itens aplicáveis (_____%)

6. CONTROLES ORGANIZACIONAIS

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
6.1	Existem políticas e procedimentos documentados sobre proteção de dados	□	□	□	□	
6.2	Servidores e colaboradores assinam termos de confidencialidade	□	□	□	□	
6.3	Existe programa de conscientização contínua sobre proteção de dados	□	□	□	□	
6.4	Os acessos aos dados são concedidos com base no princípio do privilégio mínimo	□	□	□	□	
6.5	Existem procedimentos formais para admissão e desligamento que consideram proteção de dados	□	□	□	□	
6.6	A política de mesa e tela limpa é implementada	□	□	□	□	
6.7	Existe processo seguro para descarte de documentos físicos e mídias digitais	□	□	□	□	
6.8	Os contratos de trabalho incluem cláusulas específicas sobre proteção de dados	□	□	□	□	

Pontuação da Seção 6: _____ de um total de _____ itens aplicáveis (_____%)

7. COMPARTILHAMENTO E TRANSFERÊNCIA DE DADOS

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
7.1	Todos os destinatários de dados compartilhados foram identificados e documentados	□	□	□	□	
7.2	Os contratos com operadores incluem cláusulas específicas sobre proteção de dados	□	□	□	□	
7.3	Existe avaliação prévia dos operadores quanto à capacidade de proteger dados	□	□	□	□	
7.4	Existem mecanismos para garantir que os operadores sigam as instruções da UFPI	□	□	□	□	
7.5	Transferências internacionais de dados são realizadas com salvaguardas adequadas	□	□	□	□	
7.6	Existe processo documentado para compartilhamento seguro de dados	□	□	□	□	
7.7	São utilizados canais seguros para transferência de dados	□	□	□	□	
7.8	Os compartilhamentos são revisados periodicamente quanto à necessidade e conformidade	□	□	□	□	

Pontuação da Seção 7: _____ de um total de _____ itens aplicáveis (_____%)

8. AVALIAÇÃO DE RISCOS E RELATÓRIO DE IMPACTO

Nº	Requisito	Implementado	Parcial	Não implementado	Não aplicável	Observações
8.1	Os riscos relacionados ao tratamento de dados são formalmente avaliados	□	□	□	□	
8.2	Relatórios de Impacto à Proteção de Dados são realizados para tratamentos de maior risco	□	□	□	□	

8.3	Existe metodologia definida para condução de Relatórios de Impacto	□	□	□	□	
8.4	Novos projetos e sistemas são avaliados quanto aos riscos à privacidade antes da implementação	□	□	□	□	
8.5	Medidas mitigadoras são implementadas e monitoradas	□	□	□	□	
8.6	O Encarregado participa das avaliações de impacto	□	□	□	□	
8.7	RIPDs são revisados periodicamente	□	□	□	□	
8.8	Os titulares são consultados quando apropriado	□	□	□	□	

Pontuação da Seção 8: _____ de um total de _____ itens aplicáveis (_____%)

RESULTADOS CONSOLIDADOS

Seção	Pontuação	Itens aplicáveis	Percentual
1. Governança e conformidade			%
2. Mapeamento e registro de tratamento			%
3. Bases legais e consentimento			%
4. Direitos dos titulares			%
5. Segurança e controles técnicos			%
6. Controles organizacionais			%
7. Compartilhamento e transferência de dados			%
8. Avaliação de riscos e relatório de impacto			%
TOTAL			**%**

AÇÕES NECESSÁRIAS

Listar os principais itens identificados como "Não implementado" ou "Parcial" que necessitam de atenção prioritária:

1. _____
2. _____
3. _____
4. _____
5. _____

PLANO DE AÇÃO

Item	Ação necessária	Responsável	Prazo	Recursos necessários

ASSINATURAS

Responsável pelo preenchimento:

_____ Data: ___/___/_____

Gestor da unidade:

_____ Data: ___/___/_____

Encarregado de Proteção de Dados:

_____ Data: ___/___/_____

Anexo VI - Modelo de Relatório de Impacto à Proteção de Dados

Este modelo de Relatório de Impacto à Proteção de Dados (RIPD) foi desenvolvido para documentar e avaliar os riscos associados ao tratamento de dados pessoais na UFPI, especialmente em situações que possam gerar riscos significativos aos direitos e liberdades dos titulares. O RIPD é uma ferramenta essencial para implementar o princípio da responsabilização e deve ser realizado antes da implementação de novos projetos, sistemas ou processos que envolvam dados pessoais sensíveis, monitoramento sistemático ou tratamento em larga escala. Este documento deve ser revisado pelo Encarregado de Proteção de Dados e atualizado sempre que houver mudanças significativas no tratamento.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

INFORMAÇÕES GERAIS

Título do tratamento: _____

Unidade responsável: _____

Responsável pelo RIPD: _____

Cargo/função: _____

E-mail: _____ **Telefone**: _____

Data de elaboração: ___/___/_____ **Versão do documento**: _____

Aprovação do Encarregado: □ Sim □ Não □ Pendente

1. DESCRIÇÃO SISTEMÁTICA DO TRATAMENTO

1.1. Descrição geral

Descreva de forma abrangente o projeto, sistema, processo ou atividade que envolve o tratamento de dados pessoais.

_____

_____

_____

1.2. Finalidade(s) específica(s)

Descreva de forma clara e objetiva a(s) finalidade(s) para a(s) qual(is) os dados serão tratados.

1.3. Natureza do tratamento

Descreva as operações que serão realizadas com os dados (coleta, armazenamento, uso, compartilhamento, etc.).

1.4. Escopo do tratamento

Volume aproximado de titulares: _____

Período do tratamento: □ Temporário (___/___/_____ a ___/___/_____) □ Permanente

Abrangência geográfica: _____

1.5. Categorias de dados pessoais

Categoria	Dados específicos	Necessidade	Origem
Dados de identificação			
Dados de contato			
Dados acadêmicos			
Dados profissionais			
Dados financeiros			
Dados de saúde			
Dados biométricos			
Outros dados sensíveis			
Outros			

1.6. Categorias de titulares

□ Estudantes □ Servidores docentes □ Servidores técnico-administrativos
□ Terceirizados □ Participantes de pesquisa □ Visitantes □ Outros: _____

1.7. Fluxo dos dados

Descreva o caminho que os dados percorrem, desde a coleta até o término do tratamento, incluindo transferências e compartilhamentos.

Diagrama de fluxo de dados (anexar ou inserir)

1.8. Compartilhamento de dados

Destinatário	Categoria	Finalidade	Dados compartilhados	Salvaguardas
	□ Interno □ Operador □ Controlador conjunto □ Terceiro			
	□ Interno □ Operador □ Controlador conjunto □ Terceiro			
	□ Interno □ Operador □ Controlador conjunto □ Terceiro			
	□ Interno □ Operador □ Controlador conjunto □ Terceiro			

1.9. Transferência internacional

Existe transferência internacional de dados?

□ Não □ Sim. Complete as informações abaixo:

País	Organização	Finalidade	Dados transferidos	Base legal para transferência
				□ Nível adequado de proteção □ Cláusulas contratuais □ Consentimento específico □ Outra:
				□ Nível adequado de proteção □ Cláusulas contratuais □ Consentimento específico □ Outra: _____

1.10. Sistemas e tecnologias envolvidos

Liste os sistemas, aplicativos, bancos de dados e outras tecnologias utilizados no tratamento.

2. NECESSIDADE E PROPORCIONALIDADE DO TRATAMENTO

2.1. Base legal para o tratamento

Indique qual(is) base(s) legal(is) fundamenta(m) o tratamento e justifique sua aplicação.

□ Cumprimento de obrigação legal ou regulatória (Art. 7º, II)

Justificativa: _____

□ Execução de políticas públicas (Art. 7º, III)

Justificativa: _____

□ Estudos por órgão de pesquisa (Art. 7º, IV)

Justificativa: _____

□ Execução de contrato (Art. 7º, V)

Justificativa: _____

□ Exercício regular de direitos (Art. 7º, VI)

Justificativa: _____

□ Proteção da vida (Art. 7º, VII)

Justificativa: _____

□ Tutela da saúde (Art. 7º, VIII)

Justificativa: _____

□ Legítimo interesse (Art. 7º, IX)

Justificativa: _____

□ Proteção ao crédito (Art. 7º, X)

Justificativa: _____

□ Consentimento (Art. 7º, I)

Justificativa: _____

2.2. Base legal para dados sensíveis (se aplicável)

_____

_____

_____

2.3. Princípios aplicáveis

Explique como cada princípio da LGPD é observado no tratamento:

Finalidade: _____

Adequação: _____

Necessidade: _____

Livre acesso: _____

Qualidade dos dados: _____

Transparência: _____

Segurança: _____

Prevenção: _____

Não discriminação: _____

Responsabilização e prestação de contas: _____

2.4. Minimização dos dados

Explique como foi assegurado que apenas os dados necessários para a finalidade serão coletados e processados.

_____

_____

_____

2.5. Avaliação de alternativas

Foram consideradas alternativas para o tratamento que reduziriam os riscos aos titulares? □ Não □ Sim. Descreva as alternativas consideradas e por que foram adotadas ou rejeitadas:

_____

_____

_____

2.6. Período de retenção

Qual o período de retenção dos dados e qual a justificativa para este prazo?

2.7. Informações aos titulares

Como os titulares são informados sobre o tratamento de seus dados?

3. AVALIAÇÃO DOS RISCOS AOS DIREITOS E LIBERDADES

3.1. Identificação de riscos

ID	Descrição do risco	Possíveis causas	Possíveis consequências para os titulares
R1			
R2			
R3			
R4			
R5			

3.2. Análise e avaliação de riscos

ID	Probabilidade	Impacto	Nível de risco	Justificativa/Critérios
R1	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
R2	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
R3	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
R4	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto □ Crítico	
R5	□ Baixa □ Média □ Alta	□ Baixo □ Médio □ Alto	□ Baixo □ Médio □ Alto	

			□ Crítico	

3.3. Análise de vulnerabilidades existentes

_____

_____

_____

3.4. Avaliação de impacto para grupos vulneráveis

O tratamento afeta particularmente grupos vulneráveis (crianças, idosos, pessoas com deficiência, etc.)?

□ Não □ Sim. Descreva os impactos específicos:

_____

_____

_____

4. MEDIDAS PARA TRATAMENTO DOS RISCOS

4.1. Medidas técnicas e administrativas

ID do Risco	Medida	Descrição	Status	Responsável	Prazo
			□ Implementada □ Em implementação □ Planejada		
			□ Implementada □ Em implementação □ Planejada		
			□ Implementada □ Em implementação □ Planejada		
			□ Implementada □ Em implementação □ Planejada		
			□ Implementada □ Em implementação □ Planejada		

4.2. Controles de segurança implementados

□ Controle de acesso lógico □ Criptografia □ Anonimização/pseudonimização

□ Backup □ Trilhas de auditoria □ Gerenciamento de vulnerabilidades

□ Outros: _____

4.3. Controles organizacionais implementados

□ Política de proteção de dados □ Treinamento □ Termos de confidencialidade

□ Procedimentos documentados □ Gestão de incidentes
□ Outros: _____

4.4. Salvaguardas para direitos dos titulares

□ Canal específico para exercício de direitos □ Procedimentos documentados

□ Informações claras aos titulares □ Verificação de identidade

□ Outros: _____

4.5. Avaliação de risco residual

ID	Risco residual (após medidas)	Aceitável?	Justificativa
R1	□ Baixo □ Médio □ Alto □ Crítico	□ Sim □ Não	
R2	□ Baixo □ Médio □ Alto □ Crítico	□ Sim □ Não	
R3	□ Baixo □ Médio □ Alto □ Crítico	□ Sim □ Não	
R4	□ Baixo □ Médio □ Alto □ Crítico	□ Sim □ Não	
R5	□ Baixo □ Médio □ Alto □ Crítico	□ Sim □ Não	

5. CONSULTA ÀS PARTES INTERESSADAS

5.1. Consulta interna

Foram realizadas consultas a outras áreas da UFPI?

□ Não □ Sim. Indique quais áreas foram consultadas e qual foi a contribuição:

_____

_____

_____

5.2. Consulta ao Encarregado

O Encarregado pelo Tratamento de Dados Pessoais foi consultado? □ Não □ Sim. Indique as recomendações do Encarregado:

_____

_____

_____

5.3. Consulta aos titulares

Houve consulta aos titulares dos dados ou seus representantes? □ Não □ Sim. Descreva como foi realizada e os resultados:

_____

_____

_____

5.4. Consulta a especialistas

Houve consulta a especialistas (internos ou externos) em segurança, privacidade ou áreas técnicas relacionadas?

□ Não □ Sim. Indique quais especialistas foram consultados e suas contribuições:

_____

_____

_____

6. CONCLUSÃO E RECOMENDAÇÕES

6.1. Conclusão da avaliação de impacto

Com base na avaliação realizada, conclui-se que:

□ O tratamento não apresenta riscos significativos aos direitos e liberdades dos titulares.

□ O tratamento apresenta riscos significativos, porém as medidas adotadas/planejadas são adequadas para mitigá-los a níveis aceitáveis.

□ O tratamento apresenta riscos significativos e não totalmente mitigados, porém é necessário para [justificativa], conforme parecer da alta administração anexo.

□ O tratamento apresenta riscos excessivos e deve ser redesenhado antes de sua implementação.

6.2. Principais recomendações

Liste as principais recomendações resultantes deste relatório:

1. _____
2. _____
3. _____
4. _____
5. _____

6.3. Monitoramento e revisão

Este RIPD deverá ser revisado nas seguintes situações:

□ Periodicamente, a cada _____ meses.

□ Quando houver mudanças significativas no tratamento.

□ Quando ocorrerem incidentes relacionados a este tratamento.

□ Quando houver alterações na legislação aplicável.

□ Outras situações: _____

Data da próxima revisão programada: ___/___/_____

7. APROVAÇÕES

7.1. Elaboração e revisão

Elaborado por:

Nome: _____ Cargo: _____

Assinatura: _____ Data: ___/___/_____

Revisado por:

Nome: _____ Cargo: _____

Assinatura: _____ Data: ___/___/_____

7.2. Parecer do Encarregado

□ Favorável

□ Favorável com ressalvas

□ Desfavorável

Observações: _____

_____

_____

Nome: _____ Assinatura: _____
Data: ___/___/_____

7.3. Aprovação da área responsável

Nome: _____ Cargo: _____

Assinatura: _____ Data: ___/___/_____

7.4. Aprovação da alta administração (quando necessário)

Nome: _____ Cargo: _____

Assinatura: _____ Data: //_____

Anexo VII - Procedimento de Resposta a Incidentes de Segurança

Este procedimento foi desenvolvido para orientar a UFPI na resposta a incidentes de segurança envolvendo dados pessoais, conforme exigido pela LGPD. Ele estabelece um processo estruturado para detecção, análise, contenção, erradicação e recuperação após incidentes, além de definir os critérios e fluxos para notificação à ANPD e aos titulares afetados. Este documento deve ser integrado ao processo de gestão de incidentes de segurança da informação da universidade e revisado periodicamente para garantir sua eficácia e atualização conforme novas ameaças e requisitos legais.

PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

1. OBJETIVO

Estabelecer diretrizes, responsabilidades e procedimentos para a gestão de incidentes de segurança que envolvam dados pessoais no âmbito da Universidade Federal do Piauí (UFPI), visando garantir uma resposta rápida, eficaz e em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

2. ABRANGÊNCIA

Este procedimento aplica-se a todos os incidentes de segurança que envolvam dados pessoais sob responsabilidade da UFPI, incluindo todas as suas unidades, departamentos e campi, abrangendo servidores, terceirizados, parceiros e prestadores de serviço que realizem tratamento de dados em nome da instituição.

3. DEFINIÇÕES

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito.

Dados pessoais: informação relacionada a pessoa natural identificada ou identificável.

Dados pessoais sensíveis: dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos.

Encarregado: pessoa indicada pela UFPI para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

ANPD: Autoridade Nacional de Proteção de Dados, órgão responsável por zelar pela proteção dos dados pessoais e fiscalizar o cumprimento da LGPD.

Equipe de Resposta a Incidentes: grupo de profissionais designados para coordenar e executar as ações de resposta a incidentes de segurança.

4. EQUIPE DE RESPOSTA A INCIDENTES

4.1. Composição

A Equipe de Resposta a Incidentes de Segurança envolvendo dados pessoais será composta por:

- Diretor/Coordenador de Tecnologia da Informação (coordenador)
- Encarregado pelo Tratamento de Dados Pessoais
- Representante da Segurança da Informação
- Representante da área Jurídica
- Representante da Comunicação Institucional
- Representante da área afetada (convocado conforme o incidente)
- Especialistas técnicos (convocados conforme necessidade)

4.2. Responsabilidades

Coordenador da Equipe:

- Coordenar todas as atividades de resposta
- Reportar à alta administração
- Aprovar comunicações externas
- Garantir os recursos necessários

Encarregado pelo Tratamento de Dados Pessoais:

- Avaliar o impacto do incidente sobre os titulares
- Determinar a necessidade de notificação à ANPD e aos titulares
- Atuar como ponto de contato com a ANPD
- Assegurar conformidade com a LGPD durante a resposta

Representante de Segurança da Informação:

- Coordenar a investigação técnica
- Determinar a causa raiz do incidente
- Recomendar medidas de contenção e remediação
- Documentar aspectos técnicos do incidente

Representante Jurídico:

- Avaliar implicações legais do incidente
- Revisar comunicações externas
- Orientar sobre obrigações legais
- Assessorar sobre eventual responsabilização

Representante de Comunicação:

- Preparar comunicações internas e externas
- Coordenar a comunicação com os titulares afetados
- Gerenciar comunicação com a imprensa, se necessário
- Garantir transparência adequada

Representante da área afetada:

- Fornecer informações específicas sobre os dados afetados
- Auxiliar na identificação de titulares impactados
- Implementar medidas corretivas específicas da área
- Dar suporte à investigação

Especialistas técnicos:

- Fornecer suporte técnico especializado
- Realizar análise forense, quando necessário
- Implementar soluções técnicas de contenção e remediação
- Recomendar melhorias nos controles

5. FLUXO DE RESPOSTA A INCIDENTES

5.1. Detecção e Comunicação Inicial

Fontes de detecção:

- Ferramentas de monitoramento (IDS, IPS, SIEM)
- Notificações de usuários
- Alertas de antivírus/antimalware
- Análise de logs
- Comunicação de parceiros ou fornecedores
- Denúncias internas ou externas

Processo de comunicação inicial:

1. Qualquer pessoa que identifique ou suspeite de um incidente deve reportá-lo imediatamente ao Canal de Incidentes de Segurança:
    - E-mail: seguranca@ufpi.edu.br
    - Telefone: (86) 3215-5591 (horário comercial)
    - Telefone: (86) 3215-5591 (plantão 24h)
    - Sistema de registro de incidentes: [endereço do sistema]
2. O comunicante deve fornecer as seguintes informações:
    - Descrição do incidente ou da suspeita
    - Data e hora da detecção
    - Sistemas, equipamentos ou dados potencialmente afetados
    - Ações já tomadas, se houver
    - Informações de contato do comunicante
3. A equipe de plantão deve registrar todas as informações no sistema de gestão de incidentes e notificar o Coordenador da Equipe de Resposta e o Encarregado.

5.2. Análise e Classificação

O Coordenador da Equipe, em conjunto com o Encarregado e o representante de Segurança da Informação, deve realizar uma análise preliminar para:

1. Confirmar se o evento constitui um incidente de segurança
2. Verificar se envolve dados pessoais
3. Classificar o incidente quanto à:

Severidade:

- **Crítica**: comprometimento significativo de dados sensíveis, com potencial impacto grave aos titulares (ex: vazamento de prontuários médicos)
- **Alta**: comprometimento de dados pessoais sensíveis ou dados pessoais em grande volume (ex: base de dados de alunos)
- **Média**: comprometimento limitado de dados pessoais (ex: lista de e-mails de um departamento)
- **Baixa**: potencial exposição mínima de dados pessoais, sem impacto significativo aos titulares

Escopo:

- Número estimado de titulares afetados
- Tipos de dados comprometidos
- Sistemas e processos afetados
- Unidades organizacionais impactadas

Ativação da Equipe de Resposta:

- Incidentes de severidade Crítica ou Alta: ativação completa da equipe
- Incidentes de severidade Média: ativação parcial, conforme avaliação do Coordenador
- Incidentes de severidade Baixa: tratamento pela equipe de TI, com reportes ao Encarregado

5.3. Contenção

Medidas para limitar o dano e evitar agravamento do incidente:

Contenção imediata:

- Isolamento de sistemas comprometidos
- Bloqueio de acessos suspeitos
- Desativação de funções ou serviços comprometidos
- Suspensão temporária de contas ou privilégios
- Preservação de evidências (logs, imagens forenses)

Estratégia de contenção:

1. Identificar o vetor de ataque ou causa do incidente
2. Determinar o método de contenção mais apropriado
3. Implementar as medidas de contenção
4. Monitorar a eficácia das medidas
5. Ajustar a estratégia conforme necessário

Documentação:

- Registrar todas as ações de contenção realizadas
- Documentar o momento, responsável e resultado de cada ação
- Preservar o estado dos sistemas antes das intervenções (quando possível)

5.4. Investigação

Processo para compreender a natureza, extensão e impacto do incidente:

Coleta de evidências:

- Cópia forense de sistemas comprometidos (quando aplicável)
- Logs de servidores, aplicações, firewalls e sistemas de segurança
- Registros de acesso físico e lógico
- Comunicações relacionadas ao incidente
- Imagens de câmeras de segurança (se pertinente)

Análise técnica:

- Identificação de indicadores de comprometimento
- Análise de malware (se aplicável)
- Revisão de logs e evidências para determinar:
    - Como ocorreu o incidente
    - Quais dados foram afetados e como
    - Extensão temporal do comprometimento
    - Ações realizadas pelo invasor/sistema comprometido

Determinação de impacto:

- Identificação precisa dos dados pessoais afetados
- Determinação do número de titulares impactados
- Avaliação dos possíveis danos aos titulares
- Análise de possíveis violações legais ou contratuais

5.5. Notificação

O processo de notificação deve seguir as disposições do Art. 48 da LGPD:

Avaliação da necessidade de notificação à ANPD: O Encarregado, com suporte da Equipe de Resposta, deve avaliar:

- Se o incidente pode resultar em risco ou dano relevante aos titulares
- A natureza dos dados afetados
- O nível de exposição (dados visualizados, extraídos, alterados)
- A extensão do incidente (número de titulares)
- As medidas de segurança implementadas (ex: criptografia)

Notificação à ANPD: Se necessária, a notificação deve:

- Ser realizada em prazo razoável, conforme determinado pela ANPD
- Ser enviada pelo Encarregado, após aprovação jurídica
- Conter, no mínimo:
    - Descrição da natureza dos dados afetados
    - Informações sobre os titulares envolvidos
    - Indicação de medidas técnicas e de segurança utilizadas
    - Riscos relacionados ao incidente
    - Medidas adotadas para reverter ou mitigar os efeitos
    - Medidas e protocolos utilizados para garantir a segurança das informações

Notificação aos titulares: A comunicação aos titulares deve ser realizada quando:

- O incidente possa acarretar risco ou dano relevante aos titulares
- Quando determinado pela ANPD

A comunicação deve:

- Utilizar linguagem clara e simples
- Ocorrer em prazo razoável
- Conter, no mínimo:
    - Descrição do incidente
    - Quais dados foram afetados
    - Medidas de proteção tomadas
    - Riscos relacionados
    - Medidas que o titular pode adotar para se proteger
    - Canais de contato para mais informações

Notificação interna:

- Alta administração da UFPI
- Gestores das áreas afetadas
- Comitê de Governança Digital
- Outras partes interessadas internas

Notificação a terceiros:

- Operadores envolvidos
- Instituições parceiras afetadas
- Órgãos reguladores setoriais (quando aplicável)
- Forças policiais (em caso de atividade criminosa)

5.6. Erradicação

Processo para eliminar os elementos do incidente nos sistemas afetados:

Remoção de acesso não autorizado:

- Alteração de credenciais comprometidas
- Revogação de tokens/certificados
- Fechamento de brechas de segurança
- Aplicação de patches e correções

Remoção de código malicioso:

- Identificação completa de malware e suas variantes
- Limpeza de sistemas afetados
- Verificação de persistência do malware
- Varredura completa dos sistemas

Correção de vulnerabilidades:

- Identificação de vulnerabilidades exploradas
- Aplicação de patches de segurança
- Implementação de correções temporárias (workarounds)

- Revisão de configurações

Verificação de eficácia:

- Testes para confirmar a erradicação completa
- Monitoramento intensivo após medidas de erradicação
- Verificação de integridade dos sistemas

5.7. Recuperação

Processo para restaurar sistemas e dados ao estado operacional normal:

Restauração de dados:

- Validação da integridade dos backups
- Restauração a partir de backups não comprometidos
- Verificação de integridade após restauração
- Priorização de serviços críticos

Retorno à operação:

- Implementação de monitoramento adicional
- Retorno gradual de serviços, com testes em cada etapa
- Verificação de funcionalidade antes da liberação para usuários
- Acompanhamento pós-incidente por período determinado

Validação:

- Testes funcionais dos sistemas restaurados
- Verificação de integridade dos dados
- Confirmação de que não há sinais de permanência do incidente
- Certificação de que as medidas de segurança estão adequadas

5.8. Documentação e Lições Aprendidas

Relatório final do incidente:

- Cronologia detalhada do incidente
- Descrição da natureza e impacto
- Ações de resposta realizadas
- Resultado das investigações
- Causas raiz identificadas
- Eficácia das medidas adotadas
- Recomendações para prevenção futura

Revisão pós-incidente:

- Reunião formal de revisão com a Equipe de Resposta
- Avaliação da eficácia do procedimento de resposta
- Identificação de falhas na detecção, resposta ou recuperação
- Análise de oportunidades de melhoria

Plano de melhorias:

- Ações corretivas para as vulnerabilidades identificadas
- Atualizações necessárias em procedimentos e políticas
- Necessidades de treinamento ou conscientização
- Requisitos de investimento em ferramentas ou recursos

Comunicação das lições aprendidas:

- Compartilhamento de aprendizados com áreas relevantes
- Atualização de materiais de treinamento
- Comunicação à alta administração
- Incorporação em programas de conscientização

6. CRITÉRIOS PARA NOTIFICAÇÃO À ANPD

6.1. Avaliação de risco relevante

A avaliação sobre risco ou dano relevante considerará:

Fatores de alto risco:

- Exposição de dados sensíveis
- Exposição de dados que possam facilitar fraudes de identidade (CPF, RG, data de nascimento)
- Exposição de credenciais ou tokens de autenticação
- Volume significativo de titulares afetados
- Potencial para dano à reputação, discriminação ou prejuízo financeiro aos titulares
- Dados de pessoas vulneráveis (crianças, idosos, pessoas com deficiência)
- Incidente resultante de ação maliciosa intencional
- Falha em controles básicos de segurança

Fatores de risco reduzido:

- Dados afetados eram criptografados (com chave não comprometida)
- Dados anonimizados ou pseudonimizados
- Exposição limitada ou acidental, sem evidência de acesso efetivo
- Dados de baixa sensibilidade sem elementos de identificação direta
- Incidente contido rapidamente, com possibilidade remota de uso indevido
- Impacto limitado a pequeno número de titulares

6.2. Procedimento de notificação à ANPD

Preparação da notificação:

1. O Encarregado, com suporte da Equipe de Resposta, prepara a notificação contendo:
    - Descrição da natureza do incidente
    - Natureza, categoria e quantidade de titulares afetados
    - Natureza e quantidade de dados afetados
    - Consequências concretas ou prováveis
    - Medidas técnicas e de segurança preventivas já implementadas
    - Medidas adotadas ou propostas para reverter ou mitigar os efeitos
    - Nome e dados de contato do Encarregado ou outro ponto de contato
2. A minuta da notificação é revisada pela área Jurídica.
3. O Coordenador da Equipe e o Encarregado aprovam a versão final.

Envio da notificação:

1. A notificação é enviada à ANPD pelo canal oficial disponibilizado pela autoridade.
2. É mantido registro documentado do envio, incluindo:
    - Data e hora do envio
    - Método de envio
    - Confirmação de recebimento (quando disponível)
    - Cópia do conteúdo enviado

Acompanhamento:

1. O Encarregado mantém canal aberto com a ANPD para:
    - Responder a solicitações de informações adicionais
    - Informar sobre evolução do caso
    - Relatar medidas adicionais implementadas
    - Documentar todas as interações

7. NOTIFICAÇÃO AOS TITULARES

7.1. Critérios para notificação

A notificação aos titulares será realizada:

- Quando o incidente puder acarretar risco ou dano relevante aos titulares
- Quando determinado pela ANPD
- Quando a notificação puder auxiliar os titulares a adotar medidas de proteção

7.2. Conteúdo da notificação

A comunicação deve incluir, em linguagem clara e acessível:

- Descrição da natureza do incidente
- Quais dados foram afetados
- Informações sobre os riscos relacionados
- Medidas tomadas pela UFPI para proteção dos dados
- Medidas que o titular pode tomar para se proteger
- Canais de atendimento para mais informações
- Recomendações específicas conforme o tipo de dado exposto

7.3. Canais e formato

Canais de comunicação:

- E-mail (quando disponível e não comprometido pelo incidente)
- Correspondência física
- Telefone (para casos urgentes ou titulares sem acesso digital)
- SMS (para notificações breves com direcionamento)
- Site institucional da UFPI (para incidentes de grande escala)
- Sistemas acadêmicos e administrativos da UFPI

Formatos:

- Comunicações individuais (preferencial)

- Comunicações em massa (para incidentes de grande escala)
- Comunicação em camadas (resumo inicial + detalhes em link/anexo)

7.4. Prazos

- A comunicação deve ser realizada em prazo razoável, considerando a urgência de potenciais medidas preventivas que os titulares possam adotar
- Para incidentes críticos: notificação assim que houver confirmação do escopo
- Para outros incidentes: notificação após investigação preliminar

7.5. Documentação

Manter registros de todas as comunicações:

- Cópia das comunicações enviadas
- Data e canal utilizado
- Lista de titulares notificados
- Estatísticas de entrega (quando disponíveis)
- Respostas recebidas dos titulares

8. MÉTRICAS E INDICADORES

8.1. Métricas de desempenho

Para avaliar a eficácia do processo de resposta a incidentes:

- Tempo entre ocorrência e detecção
- Tempo entre detecção e início da contenção
- Tempo para conclusão da investigação
- Tempo para notificação à ANPD (quando aplicável)
- Tempo para notificação aos titulares (quando aplicável)
- Tempo total até a resolução completa

8.2. Indicadores de qualidade

- Precisão na classificação inicial do incidente
- Eficácia das medidas de contenção
- Abrangência da investigação
- Qualidade da documentação
- Eficácia das medidas de erradicação
- Adequação da comunicação com as partes interessadas

8.3. Relatórios periódicos

O Encarregado, em conjunto com a Equipe de Resposta, deve preparar:

- Relatórios trimestrais sobre incidentes (para a alta administração)
- Relatório anual consolidado (para o Comitê de Governança Digital)
- Análises de tendências e estatísticas

9. TREINAMENTO E SIMULAÇÕES

9.1. Treinamento da equipe

- Todos os membros da Equipe de Resposta devem receber treinamento específico sobre:
  - Este procedimento
  - Técnicas de investigação de incidentes
  - Coleta e preservação de evidências
  - Técnicas de contenção
  - Comunicação em situações de crise
  - Requisitos da LGPD relativos a incidentes
- Treinamentos adicionais específicos por função:
  - Análise forense (equipe técnica)
  - Aspectos jurídicos (representante jurídico)
  - Comunicação de crise (comunicação institucional)
  - Notificação às autoridades (Encarregado)

9.2. Conscientização geral

- Programa de conscientização para toda a comunidade acadêmica sobre:
  - Como identificar potenciais incidentes
  - Canais para comunicação de suspeitas
  - Responsabilidades na prevenção de incidentes
  - Resposta a situações suspeitas

9.3. Simulações e testes

- Realização de simulações periódicas (no mínimo anuais) para testar:
  - Fluxo de comunicação
  - Capacidade de resposta da equipe
  - Eficácia dos procedimentos
  - Tempo de resposta
  - Comunicação interna e externa
- Tipos de simulações:
  - Exercícios de mesa (tabletop exercises)
  - Simulações técnicas controladas
  - Testes de comunicação

10. REVISÃO E ATUALIZAÇÃO DO PROCEDIMENTO

10.1. Revisão periódica

Este procedimento deve ser revisado:

- No mínimo anualmente
- Após incidentes significativos
- Quando houver alterações relevantes na legislação
- Quando houver mudanças significativas na infraestrutura ou estrutura organizacional

10.2. Responsabilidade pela revisão

- Encarregado pelo Tratamento de Dados Pessoais (coordenação)
- Coordenador da Equipe de Resposta a Incidentes

- Representante de Segurança da Informação
- Representante Jurídico

10.3. Aprovação de revisões

As revisões deste procedimento devem ser aprovadas por:

- Comitê de Governança Digital
- Pró-Reitoria de Administração (ou equivalente)
- Reitoria (em casos de alterações significativas)

10.4. Controle de versões

Versão atual: 1.0 Data de aprovação: [DD/MM/AAAA] Aprovado por: [Nome e cargo] Próxima revisão programada: [MM/AAAA]

11. ANEXOS

Anexo A - Formulário de Registro Inicial de Incidente

Anexo B - Modelo de Relatório de Incidente

Anexo C - Modelo de Notificação à ANPD

Anexo D - Modelo de Notificação aos Titulares

Anexo E - Lista de Contatos da Equipe de Resposta

Anexo F - Fluxograma de Resposta a Incidentes

Anexo VIII - Modelo de Cláusulas Contratuais para Operadores

Este modelo de cláusulas contratuais foi desenvolvido para inclusão em contratos firmados entre a UFPI e seus operadores de dados (fornecedores, prestadores de serviço e parceiros que realizam tratamento de dados pessoais em nome da universidade). As cláusulas estabelecem obrigações e responsabilidades específicas relacionadas à proteção de dados pessoais, em conformidade com a LGPD, e devem ser adaptadas conforme a natureza do serviço contratado e os tipos de dados envolvidos. É recomendável que a Procuradoria Jurídica da UFPI valide estas cláusulas antes de sua inclusão em contratos.

CLÁUSULAS DE PROTEÇÃO DE DADOS PESSOAIS

DEFINIÇÕES

Para os fins destas cláusulas, os termos a seguir terão os seguintes significados:

LGPD: Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

Dados Pessoais: informação relacionada a pessoa natural identificada ou identificável.

Dados Pessoais Sensíveis: dados pessoais 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.

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.

Controlador: a UNIVERSIDADE FEDERAL DO PIAUÍ (UFPI), a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: a [NOME DA EMPRESA/INSTITUIÇÃO CONTRATADA], que realizará o tratamento de dados pessoais em nome do Controlador.

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

Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ANPD: Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Violação de Dados Pessoais: violação da 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.

CLÁUSULA PRIMEIRA – OBJETO

1.1. As presentes cláusulas têm por objeto estabelecer as condições, obrigações e responsabilidades das Partes quanto ao tratamento de dados pessoais realizado pelo Operador em nome do Controlador, em decorrência do Contrato Principal firmado entre as Partes.

1.2. Estas cláusulas complementam o Contrato Principal e prevalecerão sobre quaisquer disposições contraditórias do Contrato Principal em matéria de proteção de dados pessoais.

1.3. O Operador tratará dados pessoais apenas em nome do Controlador e de acordo com as instruções documentadas do Controlador e com a LGPD.

CLÁUSULA SEGUNDA – TRATAMENTO DE DADOS PESSOAIS

2.1. O Operador tratará os seguintes tipos de dados pessoais em nome do Controlador:

[ESPECIFICAR OS TIPOS DE DADOS PESSOAIS – Exemplos:]

- Dados de identificação (nome, RG, CPF, matrícula)
- Dados de contato (endereço, e-mail, telefone)
- Dados acadêmicos (curso, notas, frequência)
- Dados funcionais (cargo, lotação, histórico funcional)
- Dados financeiros (informações bancárias, pagamentos)
- Dados sensíveis (informações de saúde, biometria) [se aplicável]

2.2. As categorias de titulares cujos dados pessoais serão tratados pelo Operador incluem:

[ESPECIFICAR AS CATEGORIAS DE TITULARES – Exemplos:]

- Estudantes de graduação e pós-graduação
- Servidores docentes e técnico-administrativos
- Terceirizados e colaboradores
- Participantes de eventos e projetos
- Candidatos em processos seletivos

2.3. O Operador realizará as seguintes operações de tratamento:

[ESPECIFICAR AS OPERAÇÕES DE TRATAMENTO – Exemplos:]

- Coleta
- Armazenamento
- Processamento
- Organização
- Classificação
- Transmissão
- Eliminação

2.4. A finalidade do tratamento de dados pelo Operador é exclusivamente:

[ESPECIFICAR A FINALIDADE – Exemplo: "Fornecimento e manutenção do sistema de gestão acadêmica"]

2.5. A duração do tratamento será: [ESPECIFICAR DURAÇÃO – Exemplo: "Durante a vigência do contrato e por mais 30 dias após seu término para fins de transição"]

CLÁUSULA TERCEIRA – OBRIGAÇÕES DO OPERADOR

3.1. O Operador compromete-se a:

a) Tratar os dados pessoais somente de acordo com as instruções documentadas do Controlador, inclusive no que diz respeito à transferência de dados pessoais para país estrangeiro ou organização internacional, a menos que seja obrigado a fazê-lo por lei; nesse caso, o Operador informará o Controlador dessa exigência jurídica antes do tratamento, a menos que a lei proíba tal informação por motivos importantes de interesse público;

b) Garantir que as pessoas autorizadas a tratar dados pessoais tenham se comprometido à confidencialidade ou estejam sujeitas a adequadas obrigações legais de confidencialidade;

c) Adotar todas as medidas técnicas e administrativas de segurança previstas no art. 46 da LGPD, adequadas para garantir a proteção dos dados pessoais;

d) Respeitar as condições para contratar outro operador (suboperador);

e) Auxiliar o Controlador, tendo em conta a natureza do tratamento, através de medidas técnicas e organizacionais adequadas, para permitir que o Controlador cumpra sua obrigação de responder às solicitações dos titulares de dados;

f) Auxiliar o Controlador a garantir o cumprimento das obrigações de segurança, notificação de violações, avaliação de impacto e consulta à ANPD, tendo em conta a natureza do tratamento e as informações ao dispor do Operador;

g) Ao término da prestação de serviços relacionados ao tratamento, apagar ou devolver todos os dados pessoais ao Controlador, conforme opção do Controlador, e apagar as cópias existentes, a menos que a legislação exija a conservação dos dados pessoais;

h) Disponibilizar ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na LGPD e nestas cláusulas, e permitir e contribuir para as auditorias, inclusive inspeções, realizadas pelo Controlador ou por outro auditor por ele autorizado;

i) Informar imediatamente o Controlador se, em sua opinião, uma instrução do Controlador violar a LGPD ou outras disposições legais relativas à proteção de dados.

CLÁUSULA QUARTA – CONTRATAÇÃO DE SUBOPERADOR

4.1. O Operador não contratará outro operador (suboperador) sem autorização prévia, específica ou geral, por escrito, do Controlador.

4.2. No caso de autorização geral por escrito, o Operador informará o Controlador sobre quaisquer alterações pretendidas quanto ao acréscimo ou substituição de suboperadores, dando assim ao Controlador a oportunidade de se opor a tais alterações.

4.3. Quando o Operador contratar outro operador para realizar operações específicas de tratamento em nome do Controlador, serão impostas a esse outro operador, por contrato, as mesmas obrigações de proteção de dados estabelecidas nestas cláusulas.

4.4. O Operador permanecerá plenamente responsável perante o Controlador pelo cumprimento das obrigações de qualquer suboperador contratado.

CLÁUSULA QUINTA – MEDIDAS DE SEGURANÇA

5.1. O Operador implementará e manterá medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado aos riscos apresentados pelo tratamento, em particular contra a destruição, perda, alteração, divulgação ou acesso não autorizados, de forma acidental ou ilícita, aos dados pessoais tratados.

5.2. Tais medidas incluirão, conforme apropriado e sem limitação:

a) Pseudonimização e criptografia de dados pessoais;

b) Capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de tratamento;

c) Capacidade de restaurar a disponibilidade e o acesso a dados pessoais em tempo hábil no caso de um incidente físico ou técnico;

d) Processo para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento.

5.3. O Operador garantirá que qualquer pessoa que atue sob sua autoridade e tenha acesso a dados pessoais não os tratará, exceto mediante instruções do Controlador, a menos que seja obrigada a fazê-lo por lei.

CLÁUSULA SEXTA – VIOLAÇÃO DE DADOS PESSOAIS

6.1. Em caso de violação de dados pessoais, o Operador notificará o Controlador sem demora injustificada e, em qualquer caso, no prazo máximo de 24 (vinte e quatro) horas após tomar conhecimento da violação.

6.2. A notificação incluirá, pelo menos:

a) A natureza da violação de dados pessoais, incluindo, quando possível, as categorias e o número aproximado de titulares afetados, bem como as categorias e o número aproximado de registros de dados pessoais em questão;

b) O nome e os detalhes de contato do encarregado do Operador ou outro ponto de contato onde mais informações podem ser obtidas;

c) As consequências prováveis da violação de dados pessoais;

d) As medidas tomadas ou propostas pelo Operador para resolver a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar possíveis efeitos adversos.

6.3. O Operador documentará todas as violações de dados pessoais, incluindo os fatos relacionados à violação, seus efeitos e as medidas corretivas tomadas.

6.4. O Operador cooperará com o Controlador e tomará as medidas razoáveis conforme instruído pelo Controlador para auxiliar na investigação, mitigação e remediação de cada violação de dados pessoais.

CLÁUSULA SÉTIMA – DIREITOS DOS TITULARES

7.1. O Operador assistirá o Controlador, por meio de medidas técnicas e organizacionais adequadas, no cumprimento da obrigação do Controlador de responder às solicitações dos titulares de dados para exercer seus direitos, conforme previsto na LGPD.

7.2. Se um titular de dados entrar em contato diretamente com o Operador para exercer qualquer um de seus direitos sob a LGPD, o Operador encaminhará a solicitação ao Controlador no prazo máximo de 2 (dois) dias úteis.

7.3. O Operador não responderá diretamente a nenhuma solicitação do titular, a menos que autorizado pelo Controlador.

CLÁUSULA OITAVA – TRANSFERÊNCIA INTERNACIONAL

8.1. O Operador não transferirá dados pessoais para fora do Brasil sem o consentimento prévio por escrito do Controlador.

8.2. Se o Controlador consentir com uma transferência, o Operador garantirá que:

a) O país ou organização internacional de destino proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD; ou

b) O Controlador ou o Operador tenha fornecido garantias adequadas, e sob condição de que os titulares dos dados disponham de direitos oponíveis e medidas jurídicas corretivas eficazes; ou

c) Se aplique uma das hipóteses de exceção previstas na LGPD para transferências internacionais.

CLÁUSULA NONA – AUDITORIAS

9.1. O Operador disponibilizará ao Controlador, mediante solicitação, todas as informações necessárias para demonstrar conformidade com as obrigações estabelecidas nestas cláusulas e permitirá e contribuirá para auditorias, incluindo inspeções, conduzidas pelo Controlador ou por outro auditor autorizado pelo Controlador.

9.2. O Controlador dará aviso razoável de qualquer auditoria ou inspeção a ser conduzida e fará esforços razoáveis para evitar causar danos ou interrupção às instalações, equipamentos, pessoal e negócios do Operador.

9.3. O Operador corrigirá prontamente quaisquer não conformidades identificadas durante tais auditorias.

CLÁUSULA DÉCIMA – RESPONSABILIDADE

10.1. O Operador será responsabilizado perante o Controlador pelos danos causados por violações destas cláusulas ou da LGPD.

10.2. O Operador responderá solidariamente pelos danos causados pelo tratamento quando:

a) Não cumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do Controlador; ou

b) Descumprir as obrigações específicas direcionadas aos operadores previstas na LGPD; ou

c) Tiver agido em desacordo com as disposições destas cláusulas.

10.3. O Operador ficará isento de responsabilidade se provar que não deu causa à violação.

CLÁUSULA DÉCIMA PRIMEIRA – INDENIZAÇÃO

11.1. O Operador indenizará o Controlador por quaisquer perdas, danos, custos, despesas, responsabilidades, ações, reclamações ou processos que o Controlador possa sofrer como resultado direto de qualquer violação destas cláusulas pelo Operador.

CLÁUSULA DÉCIMA SEGUNDA – TÉRMINO DO TRATAMENTO

12.1. Após o término da prestação dos serviços de tratamento de dados, o Operador, à escolha do Controlador:

a) Devolverá todos os dados pessoais ao Controlador e apagará as cópias existentes; ou

b) Destruirá todos os dados pessoais e certificará ao Controlador que o fez, a menos que a legislação exija o armazenamento dos dados pessoais.

12.2. Em caso de devolução, os dados serão fornecidos no formato [ESPECIFICAR FORMATO – Exemplo: "CSV ou outro formato aberto e interoperável"].

12.3. O Operador implementará medidas técnicas apropriadas para garantir a exclusão segura ou a anonimização irreversível dos dados pessoais.

12.4. O Operador fornecerá ao Controlador um certificado de exclusão/destruição dos dados pessoais no prazo de 30 (trinta) dias após o término do tratamento.

CLÁUSULA DÉCIMA TERCEIRA – DISPOSIÇÕES GERAIS

13.1. Estas cláusulas constituem parte integrante do Contrato Principal e terão a mesma duração deste.

13.2. Em caso de contradição entre estas cláusulas e disposições de outros acordos entre as Partes, estas cláusulas prevalecerão no que diz respeito à proteção de dados pessoais.

13.3. Estas cláusulas serão regidas e interpretadas de acordo com as leis da República Federativa do Brasil.

13.4. Qualquer alteração a estas cláusulas devem ser feitas por escrito e assinada por ambas as Partes.

13.5. O Controlador pode, mediante notificação por escrito ao Operador, modificar qualquer parte destas cláusulas, conforme necessário para cumprir com as leis e regulamentos aplicáveis, com efeito a partir da data especificada em tal notificação.

E, por estarem assim justas e contratadas, as Partes assinam estas cláusulas em 2 (duas) vias de igual teor e forma, na presença das testemunhas abaixo.

Local: _____ Data: ___/___/_____

UNIVERSIDADE FEDERAL DO PIAUÍ (Controlador) [Nome e cargo do representante legal]

[NOME DA EMPRESA/INSTITUIÇÃO] (Operador) [Nome e cargo do representante legal]

Testemunhas:

1. _____

Nome: CPF:

2. _____

Nome: CPF:

ESTUDOS DE CASO: LGPD NA PRÁTICA UNIVERSITÁRIA

Estes estudos de caso foram desenvolvidos para ilustrar situações reais que podem ocorrer no ambiente universitário e como aplicar os princípios da LGPD de forma prática.

CASO 1: DIVULGAÇÃO DE RESULTADOS DE PROCESSO SELETIVO

Situação: A Coordenação de Pós-Graduação precisa divulgar os resultados de um processo seletivo para mestrado, incluindo notas dos candidatos em cada etapa da seleção.

Problema: Como publicar os resultados sem violar a privacidade dos candidatos, considerando que tradicionalmente eram publicadas listas com nomes completos e notas?

Solução LGPD:

- Utilizar números de inscrição ou CPF parcialmente oculto (ex: XXX.XXX.123-45) em vez do nome completo.
- Criar área restrita no sistema acadêmico onde cada candidato acessa apenas seu próprio resultado.
- Publicar apenas os dados estritamente necessários (princípio da minimização).
- Estabelecer prazo para remoção dos resultados do site após período de recursos.
- Incluir aviso de privacidade explicando a finalidade do tratamento.

Princípios LGPD aplicados: Minimização, Necessidade, Adequação, Segurança, Transparência.

CASO 2: PESQUISA ACADÊMICA COM DADOS SENSÍVEIS

Situação: Professor do departamento de psicologia conduzirá uma pesquisa sobre saúde mental entre estudantes universitários durante a pandemia, coletando dados sobre condições psicológicas, histórico médico e comportamentos de risco.

Problema: Como garantir a conformidade com a LGPD ao coletar, processar e armazenar dados sensíveis para fins de pesquisa acadêmica?

Solução LGPD:

- Submeter o projeto ao Comitê de Ética em Pesquisa antes de iniciar a coleta.
- Elaborar termo de consentimento específico, detalhando todas as finalidades da pesquisa.
- Aplicar técnicas de pseudonimização, separando os identificadores diretos dos dados sensíveis.
- Implementar controles de acesso rigorosos, limitando-o apenas à equipe autorizada.
- Definir prazo para anonimização ou eliminação dos dados após conclusão da pesquisa.
- Realizar Relatório de Impacto à Proteção de Dados Pessoais (RIPD) devido à natureza sensível.
- Garantir que publicações resultantes não permitam a identificação individual dos participantes.

Princípios LGPD aplicados: Finalidade específica, Segurança, Adequação, Livre acesso, Não discriminação.

CASO 3: MONITORAMENTO DE ACESSO AO CAMPUS

Situação: A administração da universidade decidiu implementar sistema de reconhecimento facial para controle de acesso aos prédios do campus, substituindo as catracas com cartão magnético.

Problema: O reconhecimento facial envolve coleta e processamento de dados biométricos, que são considerados sensíveis pela LGPD.

Solução LGPD:

- Realizar Relatório de Impacto à Proteção de Dados antes da implementação.
- Oferecer método alternativo de identificação para quem não consentir com o uso de biometria.
- Obter consentimento específico e destacado para a coleta dos dados biométricos.
- Garantir que os dados biométricos sejam armazenados de forma criptografada.
- Definir política de retenção e eliminação dos registros de acesso.
- Implementar medidas de segurança robustas contra acesso não autorizado.
- Disponibilizar informações claras sobre o tratamento para a comunidade acadêmica.

Princípios LGPD aplicados: Segurança, Necessidade, Transparência, Não discriminação, Responsabilização.

CASO 4: COMPARTILHAMENTO DE DADOS COM EMPRESAS PARCEIRAS DE ESTÁGIO

Situação: O setor de estágios da universidade mantém parceria com diversas empresas e costuma compartilhar listas de alunos elegíveis para programas de estágio específicos.

Problema: Como compartilhar dados dos alunos com as empresas sem violar a LGPD?

Solução LGPD:

- Revisar os tipos de dados compartilhados, limitando ao mínimo necessário (nome, curso, período).
- Obter consentimento específico dos alunos para compartilhamento para fins de oportunidades de estágio.
- Criar portal onde alunos possam gerenciar suas preferências e revogar consentimentos.
- Estabelecer acordos formais com as empresas parceiras, especificando limitações do uso dos dados.
- Documentar cada compartilhamento realizado, mantendo trilha de auditoria.
- Verificar periodicamente se as empresas parceiras mantêm práticas adequadas de proteção de dados.
- Implementar sistema que permita alunos manifestarem interesse específico em vagas, em vez de compartilhamento automático de listas.

Princípios LGPD aplicados: Finalidade, Necessidade, Adequação, Livre acesso, Transparência.

CASO 5: SISTEMA DE ACOMPANHAMENTO DE EGRESSOS

Situação: A universidade deseja implementar um sistema para acompanhamento de egressos, mantendo contato e coletando informações sobre inserção no mercado de trabalho mesmo anos após a formatura.

Problema: Como manter um tratamento lícito dos dados de ex-alunos por período prolongado?

Solução LGPD:

- Basear o tratamento no legítimo interesse da instituição em avaliar a eficácia de seus cursos, documentando a avaliação de legítimo interesse.
- Criar canal simples para opt-out, permitindo que egressos solicitem exclusão de seus dados a qualquer momento.
- Aplicar minimização de dados, coletando apenas informações relevantes para a finalidade.
- Estabelecer ciclo regular de atualização de dados, pedindo confirmação periódica.
- Implementar níveis diferentes de anonimização para estatísticas de longo prazo.
- Ser transparente sobre como os dados serão utilizados para melhorias institucionais.
- Fornecer feedback aos egressos sobre como suas informações contribuem para melhorias nos cursos.

Princípios LGPD aplicados: Finalidade, Transparência, Adequação, Livre acesso, Qualidade dos dados.

CASO 6: ACESSO A HISTÓRICO DE ALUNOS POR COORDENADORES

Situação: Coordenadores de curso necessitam acessar históricos completos dos alunos para orientação acadêmica, análise de desempenho e detecção de situações de risco de evasão.

Problema: Como garantir acesso adequado aos dados acadêmicos pelos coordenadores sem criar exposição desnecessária de informações pessoais?

Solução LGPD:

- Definir níveis de permissão adequados no sistema acadêmico (coordenador acessa apenas alunos do seu curso).
- Implementar logs de auditoria para registrar todos os acessos aos dados.
- Estabelecer termos de responsabilidade específicos para coordenadores.
- Configurar acessos temporários para períodos específicos (matrícula, avaliação de curso).
- Criar dashboards analíticos que apresentem dados agregados sem exposição individual desnecessária.
- Treinar coordenadores sobre suas responsabilidades no tratamento dos dados.
- Avaliar periodicamente a necessidade de cada tipo de dado disponível para os coordenadores.

Princípios LGPD aplicados: Necessidade, Segurança, Prevenção, Responsabilização.

CASO 7: PRONTUÁRIOS DE ATENDIMENTO PSI-COLÓGICO ESTUDANTIL

Situação: O serviço de assistência estudantil mantém prontuários de atendimento psicológico de alunos que buscam apoio emocional durante o período acadêmico.

Problema: Como garantir a conformidade com a LGPD no tratamento desses dados sensíveis de saúde, considerando aspectos como sigilo profissional e período de guarda?

Solução LGPD:

- Basear o tratamento na base legal de tutela da saúde, com profissionais adequados.
- Implementar controles de acesso extremamente restritivos aos prontuários.
- Utilizar criptografia forte para armazenamento digital e armários seguros para registros físicos.
- Estabelecer política de retenção específica, considerando aspectos legais da profissão e direitos dos titulares.
- Criar procedimentos para portabilidade caso o aluno deseje transferir seu histórico para outro profissional.
- Desenvolver protocolo para situações excepcionais onde pode haver quebra do sigilo (risco de vida).
- Documentar detalhadamente cada acesso aos registros.

Princípios LGPD aplicados: Segurança, Adequação, Necessidade, Prevenção, Qualidade dos dados.

CASO 8: PUBLICAÇÃO DE IMAGENS EM REDES SOCIAIS INSTITUCIONAIS

Situação: O setor de comunicação da universidade registra eventos, aulas e atividades de extensão, publicando imagens em redes sociais e materiais promocionais da instituição.

Problema: Como utilizar adequadamente a imagem de estudantes, professores e visitantes em conformidade com a LGPD?

Solução LGPD:

- Implementar termo de consentimento específico para uso de imagem em diferentes contextos.
- Sinalizar claramente eventos que serão fotografados/filmados, com opção de não participação.
- Criar processo simples para solicitação de remoção de imagens das redes institucionais.
- Utilizar legendas genéricas em fotos de grupos, evitando identificação nominal desnecessária.
- Aplicar políticas diferentes para imagens de menores de idade (estudantes de projetos de extensão).
- Avaliar a real necessidade de identificação individual em cada contexto de comunicação.
- Estabelecer período máximo de exposição para cada tipo de conteúdo.

Princípios LGPD aplicados: Finalidade, Adequação, Transparência, Livre acesso.

CASO 9: QUESTIONÁRIO SOCIOECONÔMICO PARA AUXÍLIO ESTUDANTIL

Situação: A Pró-Reitoria de Assuntos Estudantis aplica questionário socioeconômico detalhado para conceder auxílios financeiros a estudantes de baixa renda.

Problema: O questionário coleta dados sensíveis e informações familiares que vão além do próprio aluno, como renda dos pais, condições de moradia e situações de vulnerabilidade.

Solução LGPD:

- Revisar o questionário para solicitar apenas dados estritamente necessários para avaliação.
- Explicar claramente a finalidade da coleta e como os dados influenciam na concessão do auxílio.
- Implementar medidas técnicas para compartimentalização dos dados socioeconômicos dos demais dados acadêmicos.
- Definir política específica de retenção, mantendo os dados apenas pelo período necessário.
- Treinar a equipe de assistência social sobre tratamento adequado de dados sensíveis.
- Estabelecer processo seguro para verificação documental que minimize exposição.
- Desenvolver sistema que permita ao estudante acompanhar quais de seus dados estão sendo considerados e por quê.

Princípios LGPD aplicados: Necessidade, Transparência, Segurança, Não discriminação, Adequação.

CASO 10: DESENVOLVIMENTO DE SISTEMA ACADÊMICO POR EMPRESA TERCEIRIZADA

Situação: A universidade contratou empresa especializada para desenvolver novo sistema de gestão acadêmica, que terá acesso a todo histórico de alunos e dados cadastrais durante a migração e implementação.

Problema: Como garantir que a empresa contratada (operador) trate adequadamente os dados sob responsabilidade da universidade (controladora)?

Solução LGPD:

- Incluir cláusulas contratuais específicas sobre proteção de dados, definindo obrigações do operador.
- Realizar due diligence da empresa quanto às práticas de segurança da informação.
- Exigir assinatura de acordos de confidencialidade por todos os funcionários da contratada que terão acesso aos dados.
- Implementar ambiente de testes com dados fictícios ou anonimizados para desenvolvimento.
- Estabelecer processo de aprovação para acesso a dados reais, apenas quando estritamente necessário.
- Definir procedimentos de notificação imediata em caso de incidentes de segurança.
- Auditar regularmente as atividades da empresa durante o desenvolvimento e implementação.
- Garantir que todo acesso aos dados seja registrado e possa ser auditado.

Princípios LGPD aplicados: Segurança, Prevenção, Responsabilização e prestação de contas.

EXERCÍCIOS PRÁTICOS PARA FIXAÇÃO

Este conjunto de exercícios foi desenvolvido para ajudar na fixação dos conceitos apresentados em cada módulo da apostila. As atividades foram elaboradas para promover reflexão e aplicação prática no contexto universitário.

MÓDULO 1 — FUNDAMENTOS DA LGPD

Exercício 1.1: Identificação de Princípios

Objetivo: Reconhecer os princípios da LGPD em situações práticas.

Atividade: Associe cada situação descrita abaixo ao(s) princípio(s) da LGPD correspondente(s):

- A Secretaria Acadêmica solicita apenas informações essenciais para a matrícula de novos alunos.
- O sistema de biblioteca informa aos usuários que seus históricos de empréstimo são utilizados para melhorar o acervo.
- Um professor armazena os trabalhos dos alunos apenas pelo período necessário para avaliação e revisão.
- O portal do aluno permite que cada estudante acesse e verifique seus próprios dados cadastrais.
- A universidade implementa criptografia para proteger dados sensíveis de saúde coletados pelo serviço médico.

Exercício 1.2: Análise de Casos — Direito dos Titulares

Objetivo: Compreender como aplicar os direitos dos titulares no ambiente universitário.

Atividade: Leia os casos abaixo e responda:

Caso A: Um ex-aluno formado há 10 anos solicita à universidade a exclusão de todos os seus dados pessoais, incluindo seu histórico acadêmico. A UFPI deve atender completamente a essa solicitação? Justifique com base na LGPD.

Caso B: Um servidor técnico-administrativo deseja saber quais órgãos externos tiveram acesso aos seus dados funcionais nos últimos 2 anos. Que informações a universidade deve fornecer e qual o prazo legal para resposta?

Caso C: Uma estudante solicita a correção de seu nome social em todos os sistemas da universidade. Quais providências a UFPI deve tomar para garantir o efetivo exercício desse direito?

Exercício 1.3: Oficina de Política de Privacidade

Objetivo: Aplicar os conceitos fundamentais na elaboração de avisos de privacidade.

Atividade: Trabalhando em grupos de 3-4 pessoas, elabore um aviso de privacidade simplificado (máximo de 1 página) para um dos seguintes contextos:

- Formulário de inscrição para evento acadêmico
- Pesquisa institucional de avaliação de disciplinas
- Cadastro para utilização dos laboratórios de informática
- Formulário para solicitação de auxílio estudantil

O aviso deve conter, no mínimo: finalidade da coleta, dados coletados, base legal, compartilhamentos previstos, período de armazenamento e canal para exercício de direitos.

MÓDULO 2 — DADOS PESSOAIS: IDENTIFICAÇÃO E CLASSIFICAÇÃO

Exercício 2.1: Categorização de Dados

Objetivo: Desenvolver habilidade para classificar diferentes tipos de dados pessoais.

Atividade: Classifique os dados abaixo nas categorias: "Dado pessoal comum", "Dado pessoal sensível", "Dado anonimizado" ou "Não é dado pessoal":

- Nome completo de um professor
- Estatísticas de evasão por curso sem identificação individual
- Registro de acesso biométrico ao restaurante universitário
- CNPJ da empresa fornecedora de material de escritório
- Endereço IP de um computador de laboratório
- Informação sobre filiação sindical de um servidor
- Foto no crachá institucional
- Número do patrimônio de um equipamento
- Atestado médico apresentado para justificativa de falta
- Percentual médio de aprovação em uma disciplina

Exercício 2.2: Identificação de Dados Sensíveis

Objetivo: Reconhecer dados sensíveis em documentos universitários.

Atividade: Analise os documentos/formulários abaixo e identifique quais contêm dados sensíveis, explicando por quê:

- Histórico escolar padrão
- Formulário de matrícula
- Ficha de inscrição em projeto de pesquisa
- Formulário de solicitação de regime especial por motivo de saúde
- Questionário socioeconômico para assistência estudantil
- Lista de presença em aula
- Declaração de participação em evento
- Termo de adesão ao programa de cotas raciais

Exercício 2.3: Mapeamento do Ciclo de Vida dos Dados

Objetivo: Compreender o fluxo de dados em processos universitários.

Atividade: Escolha um dos processos abaixo e elabore um diagrama representando o ciclo de vida dos dados envolvidos, desde a coleta até a eliminação:

- Processo seletivo para bolsas de iniciação científica
- Emissão de diploma de graduação
- Avaliação de desempenho de servidores
- Empréstimo de livros na biblioteca

Para cada fase do ciclo, indique: quais dados são tratados, quem tem acesso, onde são armazenados, por quanto tempo e quais medidas de segurança são aplicáveis.

MÓDULO 3 — TRATAMENTO DE DADOS

Exercício 3.1: Identificação de Bases Legais

Objetivo: Aplicar as bases legais corretas para diferentes operações de tratamento.

Atividade: Indique qual(is) base(s) legal(is) mais adequada(s) para cada situação e justifique:

- Divulgação de fotos institucionais de formatura no site da universidade
- Coleta de dados para emissão de diploma
- Compartilhamento de dados de alunos com o MEC para o Censo da Educação Superior
- Monitoramento por câmeras de segurança nos estacionamentos do campus
- Coleta de informações sobre deficiência para adaptações de acessibilidade
- Envio de boletim informativo sobre eventos acadêmicos para e-mails cadastrados
- Tratamento de dados de saúde pelo serviço médico universitário
- Compartilhamento de dados de alunos com empresas parceiras para oportunidades de estágio

Exercício 3.2: Elaboração de Registro de Tratamento

Objetivo: Desenvolver habilidade para documentar operações de tratamento.

Atividade: Utilizando o modelo de Registro de Tratamento fornecido no Anexo II da apostila, elabore um registro completo para uma das seguintes atividades:

- Gestão de frequência de alunos
- Avaliação de estágio probatório de servidores
- Procedimento de solicitação de bolsa permanência
- Processo de afastamento para qualificação

Exercício 3.3: Análise de Riscos e Medidas de Segurança

Objetivo: Desenvolver capacidade de identificar riscos e propor medidas de proteção.

Atividade: Para o cenário descrito abaixo, identifique pelo menos 3 riscos potenciais e proponha medidas técnicas e administrativas para mitigá-los:

Cenário: A UFPI está desenvolvendo um novo aplicativo móvel que permitirá aos alunos consultar notas, frequência, horários de aula e realizar solicitações acadêmicas. O aplicativo exigirá login com credenciais institucionais e armazenará alguns dados no dispositivo para acesso offline.

Utilize o formato:

- Risco 1: [descrição]
- Probabilidade: Alta/Média/Baixa
- Impacto: Alto/Médio/Baixo
- Medidas técnicas: [listar]
- Medidas administrativas: [listar]

MÓDULO 4 — RESPONSABILIDADES E COMPLIANCE

Exercício 4.1: Definição de Papéis e Responsabilidades

Objetivo: Compreender os diferentes agentes de tratamento e suas atribuições.

Atividade: Analise as situações abaixo e identifique quem atua como controlador, operador ou encarregado:

- Empresa contratada para desenvolvimento e manutenção do sistema acadêmico
- Coordenador de curso que acessa dados dos alunos para orientação acadêmica
- Servidor designado como ponto de contato entre a UFPI, os titulares e a ANPD
- Fundação de apoio que processa pagamentos de bolsas em nome da universidade
- Professor que coleta dados para pesquisa institucional sob orientação da Pró-Reitoria
- UFPI em relação aos dados de seus servidores
- Empresa de digitalização contratada para converter prontuários médicos físicos em digitais

Exercício 4.2: Simulação de Incidente de Segurança

Objetivo: Aplicar o procedimento de resposta a incidentes em uma situ-ação hipotética.

Atividade: Com base no cenário descrito, elabore um plano de resposta seguindo as etapas do Procedimento de Resposta a Incidentes (Anexo VII):

Cenário: Um funcionário do setor de TI identifica um acesso não autorizado ao banco de dados que contém históricos acadêmicos. Há evidências de que dados de aproximadamente 500 alunos podem ter sido acessados por um endereço IP externo à universidade nas últimas 24 horas. Não há confirmação de extração de dados, apenas de acesso.

Seu plano deve incluir:

- Medidas imediatas de contenção
- Processo de investigação
- Análise da necessidade de notificação à ANPD e aos titulares
- Comunicação interna e externa
- Medidas corretivas

Exercício 4.3: Elaboração de Plano de Adequação

Objetivo: Desenvolver visão estratégica para implementação da LGPD.

Atividade: Imagine que você foi designado como membro do comitê de implementação da LGPD na UFPI. Elabore um plano de adequação simplificado para um dos seguintes setores:

- Departamento de Recursos Humanos
- Secretaria Acadêmica
- Serviço de Assistência Estudantil
- Núcleo de Tecnologia da Informação

O plano deve contemplar:

- Principais desafios específicos do setor escolhido
- 5 ações prioritárias com prazo e responsáveis

- Recursos necessários (humanos, tecnológicos, financeiros)
- Indicadores para medir o progresso da implementação
- Estratégia de conscientização para os colaboradores do setor

Exercício 4.4: Estudo Dirigido — Boas Práticas

Objetivo: Pesquisar e analisar boas práticas de outras instituições.

Atividade: Pesquise como outra instituição federal de ensino superior implementou a LGPD e elabore um relatório sintético (máximo 2 páginas) contendo:

- Nome da instituição analisada
- Principais medidas implementadas
- Estrutura de governança adotada
- Documentos e políticas publicados
- Práticas que poderiam ser adaptadas para a UFPI
- Referências consultadas

ESTUDO DE CASO INTEGRADOR

Exercício Final: Análise Completa de Conformidade

Objetivo: Integrar os conhecimentos dos quatro módulos em um caso prático.

Atividade: Analise o seguinte caso e responda às questões, aplicando os conceitos estudados:

Caso: A UFPI está desenvolvendo um projeto de pesquisa institucional para avaliar fatores relacionados à evasão e retenção de alunos. O projeto prevê a coleta de dados de todos os alunos ativos e daqueles que

abandonaram a universidade nos últimos 5 anos, incluindo: dados acadêmicos (notas, frequência, disciplinas cursadas), dados socioeconômicos (renda familiar, escola de origem), dados de saúde mental (resultado de avaliações psicológicas voluntárias) e padrões de uso dos serviços universitários (biblioteca, restaurante, laboratórios). Os resultados serão usados para políticas institucionais e publicados em artigos científicos.

Questões:

- Quais categorias de dados pessoais estão envolvidas? Identifique se há dados sensíveis.
- Quais as bases legais aplicáveis para esse tratamento? Justifique.
- Seria necessário obter consentimento dos alunos? Em quais circunstâncias?
- Que medidas de segurança seriam recomendadas para esse projeto?
- Seria necessário elaborar um Relatório de Impacto (RIPD)? Por quê?
- Como os direitos dos titulares poderiam ser garantidos neste contexto?
- Quais cuidados devem ser tomados para a publicação dos resultados?
- Como deveria ser o ciclo de vida desses dados, da coleta à eliminação?

GLOSSÁRIO VISUAL LGPD: GUIA RÁPIDO DE REFERÊNCIA

Este glossário visual foi desenvolvido como ferramenta de consulta rápida para os principais conceitos da LGPD aplicados ao contexto universitário. Utilize-o como referência durante suas atividades diárias na UFPI.

CONCEITOS FUNDAMENTAIS

DADO PESSOAL

Definição simplificada: Qualquer informação relacionada a uma pessoa identificada ou identificável.

Exemplos na UFPI:

- Nome de aluno ou servidor
- Matrícula/SIAPE
- E-mail institucional ou pessoal
- Endereço residencial
- Número de telefone

Dica prática: Se a informação, sozinha ou combinada com outras, permitir identificar uma pessoa específica, é um dado pessoal.

DADO PESSOAL SENSÍVEL

Definição simplificada: Dado sobre origem racial/étnica, religião, opinião política, saúde, vida sexual, genético ou biométrico.

Exemplos na UFPI:

- Atestados médicos

- Registros de impressão digital
- Autodeclaração étnico-racial
- Prontuários psicológicos
- Filiação sindical de servidores

Dica prática: Requer proteção especial e, geralmente, consentimento específico ou base legal robusta.

TITULAR

Definição simplificada: Pessoa natural a quem se referem os dados pessoais.

Exemplos na UFPI:

- Estudantes
- Professores
- Técnicos administrativos
- Terceirizados
- Participantes de pesquisas

Dica prática: É o "dono" dos dados, com direitos garantidos pela LGPD.

CONTROLADOR

Definição simplificada: Quem toma as decisões sobre o tratamento de dados pessoais.

Exemplo na UFPI: A própria Universidade Federal do Piauí, como instituição.

Dica prática: Responsável por definir "por que" e "como" os dados são tratados.

OPERADOR

Definição simplificada: Quem realiza o tratamento de dados em nome do controlador.

GUIA RÁPIDO DE REFERÊNCIA LGPD

PARA SERVIDORES DA UFPI

Este guia sintetiza os principais pontos da LGPD aplicáveis ao dia a dia da universidade. Mantenha-o à mão para consultas rápidas.

PRINCÍPIOS DA LGPD

Princípio	O que significa na prática
Finalidade	Colete dados apenas para propósitos específicos e informados
Adequação	Use os dados de forma compatível com as finalidades informadas
Necessidade	Colete apenas o mínimo necessário para a finalidade
Livre acesso	Permita que titulares consultem seus dados facilmente
Qualidade	Mantenha dados exatos, claros e atualizados
Transparência	Informe claramente como os dados são tratados
Segurança	Proteja os dados contra acessos não autorizados
Prevenção	Adote medidas para prevenir danos causados pelo tratamento
Não discriminação	Não use dados para fins discriminatórios
Responsabilização	Demonstre o cumprimento das normas de proteção

VERIFICAÇÃO RÁPIDA DE CONFORMIDADE

Antes de coletar, usar ou compartilhar dados pessoais, faça estas perguntas:

- [ ] Necessidade: Estes dados são realmente necessários?
- [ ] Base legal: Tenho base legal válida para este tratamento?
- [ ] Transparência: O titular foi informado sobre este tratamento?
- [ ] Segurança: Estou adotando medidas adequadas de proteção?
- [ ] Retenção: Por quanto tempo manterei estes dados?

- [ ] Compartilhamento: Preciso compartilhar estes dados? Com quem?

DADOS SENSÍVEIS — CUIDADO ESPECIAL

Requerem proteção reforçada e base legal específica:

- Dados de saúde
- Biometria
- Origem racial/étnica
- Convicção religiosa
- Opinião política
- Filiação sindical
- Vida sexual
- Dados genéticos

BASES LEGAIS PARA TRATAMENTO

Base Legal	Exemplos na UFPI
Execução de políticas públicas	Matrícula, registros acadêmicos, assistência estudantil
Obrigação legal	Emissão de diplomas, Censo MEC, obrigações trabalhistas
Consentimento	Uso de imagem, pesquisas não obrigatórias, comunicações opcionais
Execução de contrato	Contratos de estágio, convênios específicos
Estudos por órgão de pesquisa	Pesquisas acadêmicas e institucionais
Tutela da saúde	Atendimentos médicos e psicológicos no campus

INCIDENTES DE SEGURANÇA — AÇÃO IMEDIATA

Se identificar uma violação de dados (vazamento, acesso não autorizado, perda):

- Não ignore ou tente resolver sozinho
- Reporte imediatamente ao setor de TI e ao Encarregado de Dados
- Documente tudo que souber sobre o incidente
- Preserve evidências (não apague logs ou registros)
- Siga as instruções da equipe de resposta a incidentes

PROTEÇÃO DE DADOS NO DIA A DIA

Em documentos físicos:

- Mantenha armários trancados
- Adote política de mesa limpa
- Triture documentos antes do descarte
- Não deixe documentos sensíveis em copiadoras/impressoras
- Transporte documentos em pastas fechadas

Em meios digitais:

- Use senhas fortes e exclusivas
- Bloqueie a tela ao se ausentar
- Não compartilhe credenciais
- Use e-mail institucional para assuntos de trabalho
- Criptografe dados sensíveis
- Faça backups regulares

Em e-mails e comunicações:

- Verifique destinatários antes do envio
- Use cópia oculta (Cco/Bcc) para múltiplos destinatários
- Não encaminhe e-mails sem verificar todo o histórico

- Tenha cuidado com anexos contendo dados pessoais
- Não envie dados sensíveis por mensageiros não oficiais

ATENDIMENTO AOS DIREITOS DOS TITULARES

Se um aluno, servidor ou qualquer titular solicitar:

- Acesso aos seus dados
- Correção de informações
- Eliminação de dados
- Informações sobre uso ou compartilhamento

→ Encaminhe ao Encarregado de Dados (lgpd@ufpi.edu.br) → Prazo legal para resposta: 15 dias

QUANDO CONSULTAR O ENCARREGADO DE DADOS

- Antes de coletar novos tipos de dados pessoais
- Antes de usar dados para finalidade diferente da original
- Antes de compartilhar dados com terceiros
- Ao receber solicitações de titulares
- Ao detectar possíveis incidentes de segurança
- Ao desenvolver novos projetos/sistemas que envolvam dados pessoais
- Quando tiver dúvidas sobre a aplicação da LGPD

CONTATO DO ENCARREGADO DE DADOS DA UFPI

Nome: [Nome do Encarregado] E-mail: lgpd@ufpi.edu.br Telefone: (86) 3215-5591 Site: http://ufpi.br/lgpd/

SOBRE O AUTOR

Delson Ferreira Bonfim é Instrutor Institucional da Universidade Federal do Piauí, vinculado à Superintendência de Gestão de Pessoas e à Coordenação de Desenvolvimento de Pessoas.

Atua na elaboração e condução de ações formativas voltadas ao desenvolvimento de servidores, com ênfase em temas institucionais, administrativos e de conformidade, incluindo a proteção de dados pessoais no contexto da administração pública federal.

Mestre Profissional em Gestão Pública e Doutorando em Educação pela Universidade Federal. Atua como Tutor e Professor Formador EAD pela UFPI em curso de Graduação e Pós-Graduação.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

Lei nº 13.709/2018 e suas aplicabilidades

EDUFPI