UNIVERSIDADE FEDERAL DO CEARÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO DO MESTRADO PROFISSIONAL
EM POLÍTICAS PÚBLICAS E GESTÃO DA EDUCAÇÃO SUPERIOR – POLEDUC

MANUAL

Orientador para implementação do *framework* de adequação à LGPD na UNEMAT

Assunto: Produto técnico oriundo dos resultados da dissertação “Proposta de um *Framework* de Adequação à LGPD na UNEMAT estabelecendo segurança jurídica, técnica e organizacional no tratamento de dados pessoais” pertencente ao Mestrado Profissional em Políticas Públicas e Gestão da Educação Superior.

Claudinei da Silva Lara
ALUNO

Heráclito Lopes Jaguaribe
Sidney Guerra Reginaldo
ORIENTADORES

FORTALEZA, 2026.

RESUMO

O presente manual constitui produto técnico derivado da dissertação Proposta de um *Framework* de Adequação à LGPD na UNEMAT estabelecendo segurança jurídica, técnica e organizacional no tratamento de dados pessoais. A pesquisa identificou a necessidade de organizar, de forma integrada e progressiva, as ações institucionais direcionadas à conformidade com a Lei Geral de Proteção de Dados Pessoais, considerando a complexidade administrativa, acadêmica e tecnológica da universidade pública de multicampus. O produto propõe um *framework* aplicável à Universidade do Estado de Mato Grosso, estruturado em dimensões jurídica, técnica e organizacional, com módulos, fluxos, matriz de responsabilidades, instrumentos de verificação e orientações de implementação. A finalidade é apoiar gestores, setores administrativos, unidades acadêmicas, tecnologia da informação, assessoria jurídica, controle interno, arquivo central, ouvidoria e encarregado pelo tratamento de dados pessoais na padronização de práticas, na prevenção de riscos, no atendimento aos titulares e na produção de evidências de conformidade. Trata-se de um instrumento de gestão pública que adapta conhecimento normativos, técnicos e organizacionais ao contexto institucional da UNEMAT, com potencial de replicação em outras instituições públicas de ensino superior.

Palavras-chave: LGPD; Governança de dados; proteção de dados pessoais; produto técnico.

SUMÁRIO

1 APRESENTAÇÃO

A proteção de dados pessoais tornou-se uma exigência jurídica. Administrativa e tecnológica para as instituições públicas de ensino superior. No ambiente universitário, o tratamento de dados pessoais ocorre de forma cotidiana e transversal, abrangendo processos de ingresso, matrícula, registro acadêmico, assistência estudantil, gestão de pessoas, pesquisa, extensão, comunicação institucional, gestão documental, tecnologia da informação e prestação de serviços à comunidade.

No caso da Universidade do Estado de Mato Grosso, a necessidade de um instrumento orientador é ampliada por sua configuração multicampi, pela diversidade de unidades administrativas e acadêmicas e pela circulação de dados entre setores, sistemas e agentes institucionais. Conforme sistematizado na dissertação que originou este produto técnico, a UNEMAT possui sede administrativa em Cáceres, e atuação distribuída no território do Estado de Mato Grosso, realidade que exige padronização mínima, responsabilidades e instrumentos que possibilitem rastreabilidade, monitoramento e tomada de decisão.

O problema enfrentado pela pesquisa pode ser sintetizado na seguinte questão, “como uma instituição pública de ensino superior pode se adequar à LGPD de forma eficaz, assegurando segurança jurídica, técnica e organizacional no tratamento de dados pessoais?” Em resposta a essa necessidade, este manual apresenta um *framework* de adequação à LGPD aplicável à UNEMAT, organizado como produto técnico de natureza prática, direcionado a orientar a implementação progressiva de medidas de conformidade, governança de dados, segurança da informação e proteção dos direitos dos titulares.

O produto técnico origina da dissertação, pois traduz os requisitos legais, os fundamentos teóricos, o diagnóstico institucional, as lacunas identificadas e a proposta de intervenção em um documento aplicado. A proposta é oferecer uma estrutura orientadora capaz de apoiar a gestão universitária na organização de ações, responsabilidades, fluxos, evidências e indicadores relacionados à proteção de dados pessoais.

2 OBJETIVOS

Estabelecer diretrizes, etapas e instrumentos operacionais para orientar a implementação do *framework* de adequação à Lei Geral de Proteção de Dados Pessoais

na Universidade do Estado de Mato Grosso, fortalecendo da segurança jurídica, técnica e organizacional no tratamento de dados pessoais.

3.2 Objetivos específicos

1. Orientar a organização das ações institucionais de adequação à LGPD em dimensões, módulos e etapas progressivas de implementação;
2. Definir referências para estruturação de papéis, responsabilidades e fluxos relacionados ao tratamento de dados pessoais;
3. Subsidiar a adoção de medidas jurídicas, técnicas e organizacionais de conformidade, segurança da informação e governança de dados;
4. Apoiar a padronização de procedimentos administrativos, registros, evidências e instrumentos de acompanhamento;
5. Promover a consolidação de cultura institucional de proteção de dados pessoais, transparência, prevenção de riscos e responsabilização.

3 PÚBLICO-ALVO

O manual destina-se às instâncias responsáveis pela formulação, coordenação, execução e monitoramento de atividades que envolvam tratamento de dados pessoais na UNEMAT. O público-alvo compreende a administração superior, pró-reitorias, diretorias, assessorias, coordenações, unidades acadêmicas e administrativas, tecnologia da informação, setor jurídico, controle interno, arquivo central, ouvidoria, encarregado pelo tratamento de dados pessoais, comissões ou grupos de trabalho vinculados à proteção de dados e demais servidores que atuem em processos de coleta, registro, acesso, uso, compartilhamento, armazenamento, arquivamento, eliminação ou outra forma de tratamento de dados pessoais.

Pode ser utilizado por gestores de campi, núcleos pedagógicos, polos de educação a distância e unidades setoriais que necessitem compreender suas responsabilidades no ciclo de vida dos dados pessoais. Embora tenha sido elaborado com base no contexto da sede administrativa da UNEMAT, o produto apresenta potencial de utilização por outras instituições públicas de ensino superior, desde que observadas suas particularidades normativas, administrativas e tecnológicas.

4 FUNDAMENTAÇÃO

A fundamentação deste produto técnico parte da compreensão de que a proteção de dados pessoais integra o campo dos direitos fundamentais e deve orientar a atuação do Poder Público. A Constituição Federal, especialmente após a Emenda Constitucional nº 115/2022, reconhece a proteção de dados pessoais como direito fundamental, reforçando a necessidade de que órgãos e entidades públicas adotem medidas compatíveis com a dignidade da pessoa humana, a privacidade, a transparência e a segurança jurídica (Brasil, 1988, Brasil, 2022).

A Lei nº 13.709/2018 estabelece princípios, bases legais, direitos dos titulares, deveres dos agentes de tratamento e medidas de segurança aplicáveis ao tratamento de dados pessoais. No âmbito público, sua aplicação exige conciliar finalidade pública, interesse público, transparência, necessidade, adequação, segurança, prevenção e responsabilização, de modo que a conformidade não se limite à indicação formal de base legal, mas envolva organização institucional, documentação e controle das operações de tratamento (Brasil, 2018; ANPD, 2024).

A literatura especializada evidencia que a proteção de dados deve ser compreendida como processo de governança, e não apenas como cumprimento pontual de obrigações legais. Bioni (2019) destaca a centralidade da proteção de dados pessoais para a autonomia informacional dos titulares, enquanto Donda (2020) enfatiza a necessidade de transformar a LGPD em práticas institucionais, com processos, responsabilidades, controles e evidencias. Nessa direção, *frameworks*, politicas, matrizes e protocolos são instrumentos úteis para reduzir assimetrias, organizar responsabilidades e padronizar procedimentos.

Sob a perspectiva técnica, normas e modelos de referência em segurança da informação e privacidade, como a ABNT NBR ISO/IEC 29100, a ABNT NBR ISO/IEC 27701 e o NIST *Cybersecurity Framework*, contribuem para estruturar princípios, controles e processos de gestão de riscos. Esses referenciais auxiliam a instituição a organizar medidas de identificação, proteção, detecção, resposta, recuperação e governança, alinhando requisitos de segurança da informação às exigências de privacidade e proteção de dados pessoais (ABNT, 2022; ABNT, 2019; NIST, 2024).

No campo da gestão pública, a governança envolve mecanismos de liderança, estratégia e controle destinados a avaliar, direcionar e monitorar a atuação institucional. Aplicada à proteção de dados, essa lógica exige que a universidade estabeleça papéis, fluxos, normas, indicadores, mecanismos de prestação de contas e processos de melhoria

contínua. Assim, o *framework* proposto articula fundamentos jurídicos, técnicos e organizacionais para transformar obrigações legais em práticas administrativas verificáveis e sustentáveis.

5 **METODOLOGIA DE CONSTRUÇÃO**

Este produto técnico foi construído a partir da dissertação desenvolvida no Mestrado Profissional em Políticas Públicas e Gestão da Educação Superior, com o propósito de desenvolver um *framework* de adequação à LGPD para a UNEMAT.

A construção do produto decorreu da articulação entre revisão bibliográfica, análise documental, levantamento de requisitos normativos, análise de práticas institucionais e sistematização de informações obtidas junto a servidores públicos da instituição que participaram da pesquisa, conforme descrito na dissertação. O diagnóstico resultante indicou a necessidade de organizar a adequação à LGPD em dimensões integradas, com instrumentos capazes de apoiar a gestão, registrar evidências e orientar a implementação de medidas de conformidade.

A metodologia de construção do manual seguiu cinco estratégias, identificação do problema institucional; extração dos requisitos em módulos funcionais; definição de etapas de implementação; e elaboração de instrumentos de apoio, como checklists, formulários e matrizes. Esse percurso permitiu transformar achados da pesquisa em um produto técnico aplicável, verificável e replicável.

6 DESCRIÇÃO DO PRODUTO

6.1 Enquadramento e finalidade

O produto técnico é enquadrado como Manual, por reunir diretrizes, orientações, fluxos, instrumentos de verificação e procedimentos direcionados à implementação do *framework* de adequação à LGPD na UNEMAT. O conteúdo possui natureza de instrumento de gestão, pois sistematiza práticas institucionais e traduz conhecimentos jurídicos, técnicos e organizacionais em ações aplicáveis ao cotidiano universitário.

A finalidade do manual é orientar a universidade na organização de um processo contínuo de adequação à LGPD, com foco na identificação das operações de

tratamento, definição de responsabilidades, gestão de riscos, segurança da informação, atendimento aos titulares, resposta a incidentes, capacitação institucional e monitoramento da maturidade.

6.2 Arquitetura do *framework*

O *framework* está estruturado em três dimensões, jurídica, técnica e organizacional que se desdobram em módulos. As dimensões dependem de articulação permanente entre gestão, tecnologia da informação, assessoria jurídica, arquivo central, controle interno, ouvidoria, encarregado, setores administrativos e unidades acadêmicas.

6.3 Módulos do *framework*

Os módulos organizam o *framework,* cada módulo possui objetivo próprio, mas todos se conectam ao ciclo de vida dos dados e à necessidade de produzir evidências de conformidade. Os módulos vêm detalhado no Quadro 1.

Quadro 1 – Módulos do *framework*

Módulo	Objetivo operacional	Instrumentos de apoio
Governança de dados	Definir instâncias, papéis, responsabilidades, fluxos decisórios e mecanismos de acompanhamento.	Matriz de responsabilidades, atas, plano de ação e *checklist* de governança.
Inventário e mapeamento	Identificar operações de tratamento, bases legais, finalidades, dados tratados, sistemas, compartilhamentos e retenção.	Formulário de registro das operações de tratamento e mapa de fluxo de dados.
Gestão de riscos e AIPD	Avaliar riscos aos titulares, vulnerabilidades institucionais e necessidade de medidas mitigadoras.	*Checklist* de riscos e modelo de Avaliação de Impacto à Proteção de Dados.
Controles técnicos e segurança	Orientar medidas de proteção, acesso, rastreabilidade, confidencialidade, integridade e disponibilidade.	Inventário de ativos, controle de acesso, plano de resposta a incidentes e registros técnicos.
Direitos dos titulares	Padronizar o recebimento, análise, encaminhamento e resposta às solicitações dos titulares.	Formulário de atendimento aos titulares e fluxo de resposta.
Incidentes de segurança	Registrar, classificar, tratar e comunicar incidentes envolvendo dados pessoais, quando cabível.	Formulário de registro de incidentes e fluxo de acionamento institucional.
Capacitação e cultura	Promover sensibilização e formação continuada sobre privacidade, segurança e proteção de dados.	Plano de capacitação, materiais orientativos e registros de participação.
Monitoramento e melhoria contínua	Acompanhar a execução das ações, indicadores, maturidade e revisão periódica do *framework*.	Painel de indicadores, relatórios de acompanhamento e ciclos de revisão.

Fonte: elaborado pelo autor (2026).

6.4 Fluxo de *framework*

A implementação do *framework* deve ocorrer de forma progressiva, respeitando a capacidade institucional e a necessidade de envolver diferentes setores. O fluxo lógico recomendado é apresentado no Quadro 2.

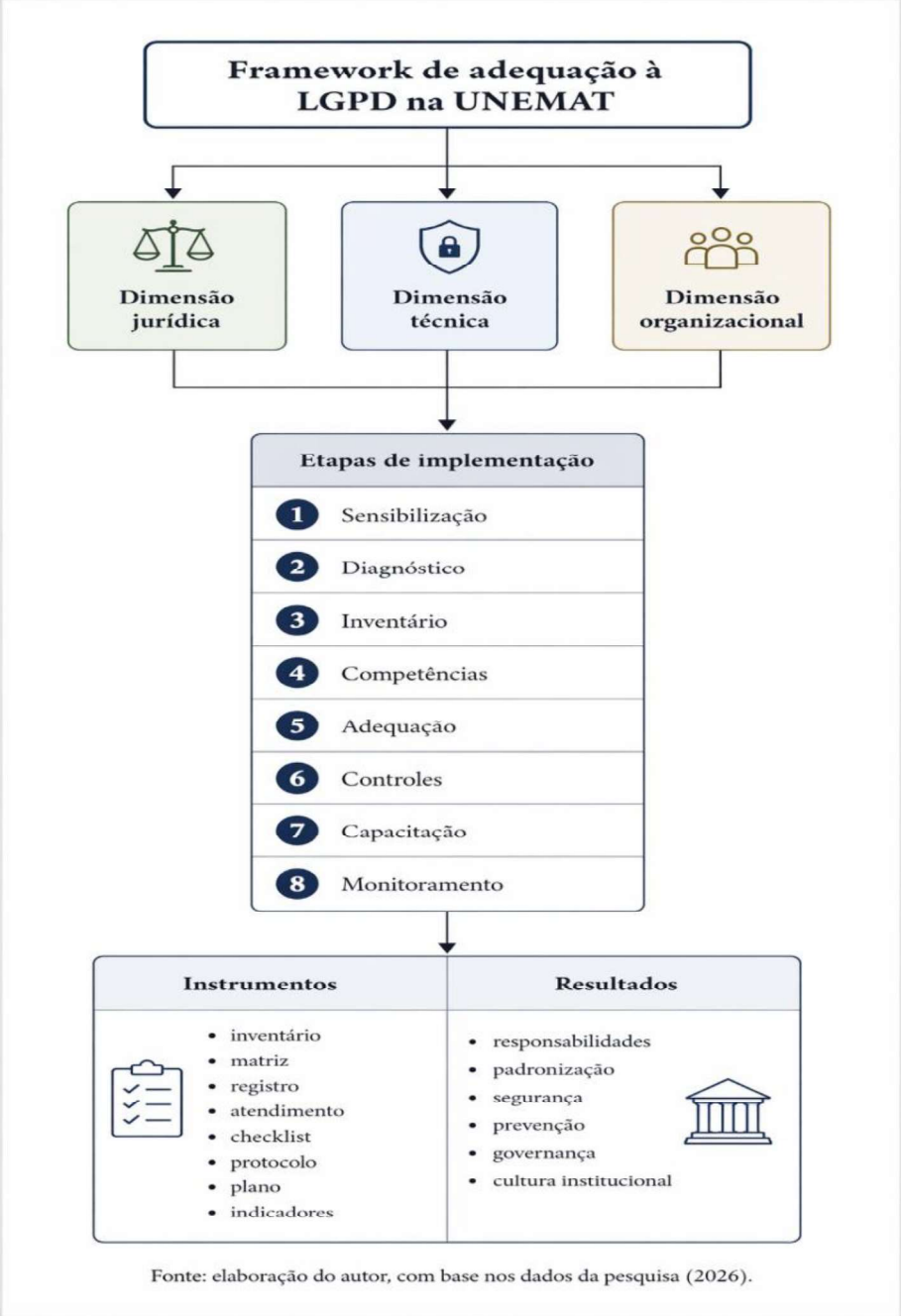
Quadro 2 – Fluxo do *framework*

Etapa	Descrição	Produto ou evidência
1. Sensibilização institucional	Alinhamento da alta gestão e comunicação inicial sobre a importância da proteção de dados.	Registro de reunião, plano inicial e definição de responsáveis.
2. Diagnóstico preliminar	Levantamento de setores, processos, sistemas, bases de dados, normativos e práticas existentes.	Relatório diagnóstico e lista de processos prioritários.
3. Inventário e mapeamento	Registro das operações de tratamento, fluxos informacionais, bases legais e responsáveis.	Inventário de tratamento e mapa de fluxo de dados.
4. Definição de papéis	Formalização de responsabilidades, pontos focais e instâncias de governança.	Matriz de responsabilidades e ato de designação.
5. Adequação normativa e procedimental	Revisão ou elaboração de políticas, orientações, termos, procedimentos e fluxos.	Normativos, POPs, minutas e documentos aprovados.
6. Controles técnicos e administrativos	Implementação de medidas de segurança, controle de acesso, rastreabilidade e registros.	Relatórios técnicos, registros de controle e evidências de mitigação.
7. Capacitação continuada	Formação dos servidores públicos e setores envolvidos no tratamento de dados pessoais.	Plano de capacitação, lista de presença e materiais de apoio.
8. Monitoramento e melhoria contínua	Acompanhamento de indicadores, revisão periódica e atualização do framework.	Relatórios de monitoramento, indicadores e plano de melhoria.

Fonte: elaborado pelo autor (2026).

A Figura 1 apresenta, a estrutura do *framework* de adequação à LGPD na IES, articulando suas dimensões, as etapas de implementação, os instrumentos operacionais e os resultados institucionais esperados.

Figura 1 - Estrutura do *framework* de adequação à LGPD na UNEMAT



Fonte: elaboração do autor, com base nos dados da pesquisa (2026).

A representação visual na Figura 1 evidencia que a adequação à proteção de dados pessoais, no contexto universitário, requer ação integrada entre conformidade normativa, segurança da informação e organização administrativa, permitindo compreender a proposta como processo contínuo de governança e aprimoramento institucional.

6.5 Matriz de responsabilidade

A efetividade do *framework* depende da distribuição de responsabilidades. A matriz a seguir, no Quadro 3, apresenta uma referência inicial, que poderá ser ajustada por ato institucional específico.

Quadro 3 – Matriz de responsabilidades institucionais

Ator institucional	**Responsabilidades no *framework***
Alta gestão	Aprovar diretrizes, assegurar apoio institucional, priorizar recursos e acompanhar resultados estratégicos.
Encarregado pelo tratamento de dados pessoais	Orientar setores, receber comunicações dos titulares e da ANPD, articular respostas institucionais e apoiar a governança de privacidade.
Comitê ou grupo de governança de dados/LGPD	Coordenar o plano de adequação, acompanhar indicadores, propor normativos e integrar setores envolvidos.
Tecnologia da informação	Apoiar inventário de sistemas, segurança da informação, controles de acesso, resposta a incidentes, *backups* e rastreabilidade.
Assessoria jurídica	Analisar bases legais, contratos, termos, compartilhamentos, riscos jurídicos e minutas normativas.
Arquivo e gestão documental	Orientar prazos de guarda, descarte, classificação documental, preservação e eliminação segura.
Ouvidoria/protocolo/canais institucionais	Receber, registrar e encaminhar solicitações de titulares e manifestações relacionadas à proteção de dados.
Controle interno	Acompanhar conformidade, avaliar evidências, recomendar melhorias e apoiar mecanismos de prestação de contas.
Pró-reitorias, diretorias e setores administrativos	Mapear processos, preencher instrumentos, implementar controles e manter registros atualizados.
Campi, núcleos e unidades	Adequar rotinas locais, indicar pontos focais, participar de capacitações e registrar evidências de conformidade.

Fonte: elaborado pelo autor (2026).

6.6 Instrumentos operacionais

O produto técnico inclui instrumentos de apoio destinados a tornar o *framework* executável e verificável. Esses instrumentos permitem registrar operações, identificar riscos, documentar decisões e produzir evidências institucionais de conformidade. Os modelos constam no **Apêndice A** e podem ser adaptados conforme o setor, o tipo de processo e a maturidade institucional.

- *Checklist* de conformidade do módulo de governança;
- *Checklist* de conformidade do módulo de gestão de riscos;
- *Checklist* de conformidade do módulo de direitos dos titulares;
- Formulário para registro das operações de tratamento de dados pessoais;
- Modelo de Avaliação de Impacto à Proteção de Dados (AIPD);
- Formulário para registro de incidentes de segurança envolvendo dados pessoais;
- Formulário de atendimento aos titulares de dados pessoais.

6.7 Indicadores de acompanhamento

Para assegurar o monitoramento e a melhoria contínua, recomenda-se que a instituição acompanhe os indicadores mínimos de implementação sugeridos no Quadro 4. Os indicadores não devem ser utilizados apenas para controle quantitativo, mas como apoio à tomada de decisão, priorização de riscos e prestação de contas.

Quadro 4 – Indicadores sugeridos para acompanhamento

Indicador	Forma de mensuração	Periodicidade sugerida
Processos mapeados	Percentual de processos prioritários com registro de operação de tratamento preenchido.	Trimestral
Sistemas inventariados	Percentual de sistemas que tratam dados pessoais incluídos no inventário institucional.	Semestral
Setores com ponto focal	Percentual de setores/unidades com responsável indicado para apoio à proteção de dados.	Semestral
Solicitações de titulares respondidas	Quantidade e percentual de demandas respondidas dentro do prazo institucional.	Mensal
Incidentes registrados e tratados	Número de incidentes registrados, classificados, tratados e encerrados.	Mensal
Capacitação institucional	Percentual de servidores de áreas críticas capacitados em LGPD, privacidade e segurança.	Semestral
AIPDs realizadas	Quantidade de avaliações de impacto realizadas em processos de maior risco.	Semestral
Revisões do *framework*	Número de revisões ou atualizações de instrumentos, fluxos e normativos.	Anual

Fonte: elaborado pelo autor (2026).

7 ORIENTAÇÕES DE IMPLEMENTAÇÃO

A implementação de ser conduzida como processo institucional progressivo, com priorização dos processos de maior risco e maior impacto para os titulares. Recomenda-se iniciar pela alta gestão, formalizar responsabilidades, mapear processos críticos e adotar ciclos de melhoria contínua. A proposta no Quadro 5 pode ser ajustada conforme o interesse institucional, a disponibilidade de equipe e a deliberação dos órgãos competentes.

Quadro 5 – Roteiro de implementação

Fase	Prazo sugerido	Ações principais	Responsáveis	Evidências esperadas
Fase 1 – Mobilização e governança	0 a 60 dias	Sensibilizar alta gestão; designar responsáveis; instituir grupo de trabalho; aprovar plano inicial.	Alta gestão; encarregado; setores estratégicos.	Ato de designação, ata de reunião, plano de ação inicial.
Fase 2 – Diagnóstico e priorização	60 a 120 dias	Levantar setores, sistemas, processos críticos, dados tratados e lacunas existentes.	Grupo de trabalho; TI; jurídico; Arquivo central; setores.	Relatório, diagnóstico e lista de processos prioritários.
Fase 3 – Inventário e mapeamento	120 a 240 dias	Preencher registros de tratamento, identificar bases legais, fluxos, compartilhamentos e retenção.	Setores responsáveis; pontos focais; encarregado.	Inventário de operações e matriz de processos.
Fase 4 – Adequação normativa e controles	240 a 360 dias	Revisar normativos; formalizar procedimentos; implantar controles técnicos e administrativos.	Jurídico; TI; gestão documental; controle interno.	Minutas, políticas, POPs, controles e registros.
Fase 5 – Capacitação e disseminação	Contínua	Realizar oficinas, guias rápidos, comunicações internas e capacitações setoriais.	Encarregado; gestão de pessoas; comunicação; TI.	Materiais, listas de presença e certificados.
Fase 6 – Monitoramento e melhoria	Contínua	Acompanhar indicadores, revisar riscos, atualizar instrumentos e produzir relatórios periódicos.	Grupo de governança; controle interno; encarregado.	Relatórios, indicadores e plano de melhoria.

Fonte: elaborado pelo autor (2026).

Recomenda-se, como estratégia de viabilidade, que a implementação comece pelos processos mais sensíveis, como gestão acadêmica, assistência estudantil, recursos humanos, saúde ocupacional, processos seletivos, pesquisa com dados pessoais, sistemas institucionais e compartilhamento com órgãos externos. Essa priorização permite reduzir os riscos mais relevantes e produzir aprendizados institucionais antes da expansão para todos os setores, unidades e campus.

8 MECANISMOS DE DISSEMINAÇÃO

A disseminação do produto técnico deve ocorrer por meio de ações institucionais que tornem o *framework* conhecido, compreensível e utilizável pelos setores. Recomenda-se combinar estratégias formais e pedagógicas, de modo que o produto não fique restrito a um documento, mas seja incorporado às práticas administrativas da instituição, tais como:

- Apresentação do manual à administração superior e às instâncias de governo institucional;
- Realização de oficinais práticas com as pró-reitorias, setores administrativos e campi;
- Disponibilização do manual e dos instrumentos em repositório institucional ou ambiente digital;

- Elaboração de guia rápido para servidores públicos, com linguagem simplificada e orientações de uso dos formulários;
- Integração do tema às capacitações institucionais sobre governança, gestão documental, segurança da informação e atendimento ao público.
- Realização de ciclos anuais de revisão, com coleta de sugestões dos setores.

9 **RESULTADOS ESPERADOS E IMPACTO**

Espera-se que a adoção do *framework* contribua para a organização progressiva da conformidade com a LGPD na UNEMAT. Isso fortalecerá a capacidade institucional de mapear operações de tratamento, atribuir responsabilidades, gerenciar riscos, responder aos titulares e produzir evidências verificáveis de governança de dados pessoais, conforme o Quadro 6.

Quadro 6 – Resultados esperados e impactos

Tipo de impacto	Contribuição esperada
Institucional	Padronização de práticas, fortalecimento da governança, maior integração entre setores e melhoria da rastreabilidade administrativa.
Legal	Redução de riscos, apoio à aplicação dos princípios da LGPD e maior segurança jurídica nas operações de tratamento.
Tecnológico	Aprimoramento dos controles de segurança da informação, inventário de sistemas, resposta a incidentes e gestão de riscos técnicos.
Educacional	Formação continuada de servidores públicos e consolidação de cultura institucional de proteção de dados pessoais.
Econômico/administrativo	Maior eficiência no uso de recursos, prevenção de retrabalho, redução de riscos operacionais e melhoria da gestão documental.
Social	Fortalecimento da confiança dos titulares, transparência institucional e respeito aos direitos fundamentais no serviço público universitário.
Replicabilidade	Possibilidade de adaptação do modelo para outras instituições públicas de ensino superior com estrutura semelhante.

Fonte: elaborado pelo autor (2026).

10 CONSIDERAÇÕES FINAIS

O presente manual apresenta um produto técnico aplicado, o qual foi elaborado com a finalidade de orientar a implementação de um *framework* de adequação à Lei Geral de Proteção de Dados Pessoais na Universidade do Estado de Mato Grosso. A estrutura reúne diretrizes, objetivos, diagnóstico, proposta de intervenção, etapas de implementação e instrumentos operacionais destinados a subsidiar a organização das ações institucionais relacionadas à proteção de dados pessoais.

A adoção do produto técnico tem potencial para contribuir com a segurança jurídica, técnica e organizacional da universidade, promovendo a padronização de procedimentos, a definição de responsabilidades, a melhoria da governança e a consolidação de práticas institucionais compatíveis com as exigências normativas aplicáveis. Contudo, essa adoção depende de adesão institucional, apoio da alta gestão, atualização permanente e integração entre áreas jurídicas, técnicas, administrativas e acadêmicas.

Como limitação, destaca-se que o manual não substitui a análise jurídica específica de casos concretos, nem dispensa a edição de normativos internos, a realização de avaliações de impacto quando necessárias e o acompanhamento das orientações da Autoridade Nacional de Proteção de Dados. Ainda assim, constituiu uma referência prática para iniciar, organizar e monitorar a adequação à LGPD em ambiente universitário público, podendo ser replicado e adaptado por outras instituições de ensino superior.

Este manual deve ser compreendido como instrumento orientador progressivo, sujeito a atualização e aperfeiçoamento conforme a evolução das necessidades institucionais e das condições organizacionais da universidade.

11 Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR- **ISO/IEC 29100**: Segurança da informação, segurança cibernética e proteção à privacidade – controle de segurança da informação**:** ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR **ISO/IEC 27701**: técnicas de segurança: extensão da ABNT NBR **ISO/IEC 27001** e ABNT NBR **ISO/IEC 27002** para gestão da privacidade da informação: requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo: tratamento de dados pessoais pelo Poder Público**. Brasília, DF: ANPD, 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a **Constituição Federal** para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia do Programa de Governança em Privacidade**. Brasília, DF: Governo Digital, 2024.

BIONI, Bruno Ricardo. **Proteção de dados Pessoais: A Função e os Limites do Consentimento.** Rio de janeiro, Ed. Forense, 1ª Ed, 2019.

DONDA, Daniel. **Guia prático de implementação da LGPD**. 1. ed. São Paulo: Labrador, 2020. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 14 maio 2025.

LARA, Claudinei da Silva. Proposta de um *Framework* de Adequação à LGPD na UNEMAT estabelecendo segurança jurídica, técnica e organizacional no tratamento de dados pessoais. 2026. **Dissertação** (Mestrado em Políticas Públicas e Gestão da Educação
Superior) – Poleduc, Universidade Federal do Ceará, Fortaleza, 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *The NIST Cybersecurity Framework (CSF)*. Gaithersburg: NIST, 2024.
UNEMAT. Universidade do Estado de Mato Grosso. Política de Privacidade e Proteção de Dados Pessoais. Cáceres: UNEMAT, 2026.

UNEMAT. Universidade do Estado de Mato Grosso. **Resolução nº 005/2026 –** Ad Referendum do CONSUNI. Cáceres: UNEMAT, 2026.

APÊNDICE A - Produtos de apoio do *framework* de adequação à LGPD

Os produtos de apoio apresentados a seguir foram estruturados para traduzir o *framework* de adequação à LGPD em instrumentos aplicáveis ao cotidiano institucional da UNEMAT. Em conjunto, esses quadros favorecem a padronização das rotinas, a rastreabilidade dos processos, a geração de evidências de conformidade, o monitoramento institucional e a futura replicação da proposta nos campi.

Quadro 1 – *Checklist* de conformidade do módulo de governança

Item de verificação	Sim	Não	Parcial	Evidência / Observação
Existe política institucional de proteção de dados aprovada e vigente?				
Há designação formal do Encarregado pelo Tratamento de Dados Pessoais?				
O Comitê Setorial de Proteção de Dados está formalmente instituído?				
O Comitê Setorial de Segurança da Informação está formalmente instituído?				
Há definição dos papéis e responsabilidades para proteção de dados?				
Existem normativas internas complementares sobre segurança e privacidade?				
As instâncias de governança realizam reuniões periódicas?				
Existem atas, relatórios ou registros das deliberações realizadas?				
Existe articulação entre TI, jurídico, arquivo, ouvidoria e controle interno?				
Há canal institucional para orientação dos setores sobre LGPD?				
Existe acompanhamento da implementação das ações de adequação?				
Há revisão periódica das políticas e das estruturas de governança?				

Fonte: elaborado pelo autor (2026).

Quadro 2 – *Checklist* de conformidade do módulo de gestão de riscos

Item de verificação	Sim	Não	Parcial	Evidência / Observação
Os processos críticos de tratamento de dados foram identificados?				
Há levantamento dos principais riscos associados ao tratamento?				
Existe classificação dos riscos por criticidade e impacto?				

Item de verificação	Sim	Não	Parcial	Evidência / Observação
Há registro das vulnerabilidades identificadas?				
São adotadas medidas mitigadoras para riscos relevantes?				
Existe procedimento para revisão periódica dos riscos?				
As atividades de alto risco contam com AIPD, quando cabível?				
Há fluxo definido para resposta a incidentes envolvendo dados pessoais?				
Existem responsáveis formalmente definidos para monitorar riscos?				
Os riscos identificados são comunicados às instâncias de governança?				
Há registro das ações corretivas adotadas após incidentes ou não conformidades?				
Existe integração entre avaliação de riscos e revisão dos processos?				

Fonte: elaborado pelo autor (2026).

Quadro 3 – *Checklist* de conformidade do módulo de direitos dos titulares

Item de verificação	Sim	Não	Parcial	Evidência / Observação
Existe canal institucional para recebimento de solicitações dos titulares?				
O procedimento de atendimento aos titulares está formalizado?				
Há mecanismo de validação da identidade do solicitante?				
Existe controle de prazo para resposta às solicitações?				
As demandas são registradas em sistema, protocolo ou formulário próprio?				
Existe definição do setor responsável pela análise de cada tipo de solicitação?				
Existe modelo padronizado de resposta ao titular?				
As respostas são arquivadas como evidência do atendimento?				
Há encaminhamento formal à Encarregada, quando necessário?				
O titular é informado sobre providências adotadas e limitações legais aplicáveis?				
Existe controle de solicitações concluídas, pendentes e indeferidas?				
Há revisão dos procedimentos de atendimento com base nas demandas recebidas?				

Fonte: elaborado pelo autor (2026).

Quadro 4 – Formulário para registro das operações de tratamento de dados pessoais

Campo	Conteúdo a preencher	Observações
Identificação da operação de tratamento		
Setor responsável		
Unidade executora		
Processo vinculado		
Finalidade do tratamento		
Base legal aplicável		
Categoria de dados pessoais tratados		
Categoria de titulares envolvidos		
Tipo de tratamento realizado		Coleta, uso, armazenamento, compartilhamento, eliminação etc.
Origem dos dados		
Sistema, plataforma ou suporte utilizado		
Compartilhamento interno		Informar setores/unidades destinatárias
Compartilhamento externo		Informar órgãos ou instituições destinatárias
Prazo de retenção		
Critério de descarte ou guarda permanente		
Medidas de segurança adotadas		
Riscos identificados		
Responsável pelo preenchimento		
Data do registro		
Observações complementares		

Fonte: elaborado pelo autor (2026).

Quadro 5 – Modelo de Avaliação de Impacto à Proteção de Dados (AIPD)

Campo	Conteúdo a preencher	Observações
Identificação da atividade ou processo		
Setor responsável		
Descrição da operação de tratamento		
Finalidade do tratamento		
Base legal aplicável		
Categoria de dados pessoais envolvidas		
Categoria de titulares afetados		
Volume estimado de dados tratados		
Sistemas ou tecnologias utilizados		
Compartilhamentos previstos		Internos e externos
Riscos identificados aos titulares		

Campo	Conteúdo a preencher	Observações
Probabilidade de ocorrência		Baixa, média ou alta
Impacto potencial		Jurídico, operacional, reputacional e ao titular
Medidas mitigadoras existentes		
Medidas mitigadoras recomendadas		
Necessidade de revisão do processo		
Responsável pela avaliação		
Data da avaliação		
Data prevista para revisão		
Parecer conclusivo		

Fonte: elaborado pelo autor (2026).

Quadro 6 – Formulário de registro de incidentes de segurança envolvendo dados pessoais

Campo	Conteúdo a preencher	Observações
Número do registro		
Data e hora da ocorrência		
Data e hora da identificação		
Setor envolvido		
Responsável pelo registro		
Descrição do incidente		
Categoria de dados afetados		
Quantidade estimada de titulares afetados		
Sistema, ambiente ou suporte envolvido		
Provável causa do incidente		
Impacto preliminar identificado		
Medidas adotadas imediatamente		
Setores acionados		TI, Encarregada, jurídico, gestão etc.
Necessidade de comunicação interna		
Necessidade de comunicação externa		Titulares, ANPD ou outros órgãos, quando cabível
Providências corretivas		
Providências preventivas		
Status do incidente		Aberto, em tratamento, concluído
Data de encerramento		
Observações complementares		

Fonte: elaborado pelo autor (2026).

Quadro 7 – Formulário de atendimento aos titulares de dados pessoais

Campo	Conteúdo a preencher	Observações
Número da solicitação		
Data do recebimento		
Nome do titular		
CPF ou outro identificador		
Meio de recebimento da solicitação		E-mail, protocolo, formulário, ouvidoria etc.
Tipo de direito exercido		Acesso, correção, eliminação, informação, revisão etc.
Validação da identidade realizada		Sim / Não / Parcial
Setor responsável pela análise		
Encarregado acionado		Sim / Não
Descrição da demanda		
Providências adotadas		
Data de encaminhamento interno		
Prazo final para resposta		
Data da resposta ao titular		
Resultado do atendimento		Atendido, parcialmente atendido, indeferido
Fundamentação da resposta		
Responsável pela resposta		
Registro da evidência do atendimento		
Observações complementares		

Fonte: elaborado pelo autor (2026).

Em conjunto, esses produtos de apoio fortalecem o caráter aplicado do *framework* de adequação à LGPD na UNEMAT, pois tornam o modelo executável e verificável no cotidiano institucional. Ao padronizar registros, apoiar a verificação da conformidade e organizar respostas a situações críticas, esses instrumentos contribuem para ampliar a rastreabilidade dos processos, para o monitoramento contínuo e para a sustentabilidade operacional da proposta.