FUNDAÇÃO DE MEDICINA TROPICAL DR. HEITOR VIEIRA DOURADO (FMT-HVD)

PLANO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

MANAUS – AM

2025

Versão 1.0 – 05/11/2025

FICHA TÉCNICA

Dr. Marcus Vinítius de Férias Guerra

Diretor Presidente

Flávio Azevedo de Lima

Diretor Administrativo e Financeiro

Dr. Silvio César Pereira Fragoso

Diretor de Assistência Médica

Dra. Gisely Cardoso de Melo

Diretora de Ensino e Pesquisa

EQUIPE TÉCNICA DE ELABORAÇÃO

Clenilton Cruz de Alencar

Karinna Kathleen Nascimento

Eda Cristina da Silva Chagas

Frank Brunner de Souza Marinho

Marly Marques de Melo

Lana Márcia Girão Silva

Taysa Ferreira Pimentel

Sumário

Apresentação

A proteção à privacidade e o cuidado adequado com o tratamento de dados pessoais, em uma sociedade que avança no uso de tecnologias digitais, são desafios comuns a todas as organizações ao redor do mundo. Nesse cenário, a partir do dia 18 de setembro de 2020, passou a vigorar no Brasil a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709/2018, que tem como princípio basilar a proteção dos direitos dos/as titulares dos dados pessoais. Para as instituições públicas, dada a sua especificidade, esse desafio pode ser especialmente complexo ao envolver uma transformação cultural.

A Fundação de Medicina Tropical Dr. Heitor Vieira Dourado (FMT-HVD), na busca da conformidade com a nova legislação, constituiu, por meio da Portaria nº 095/2025-GDP/FMT-HVD, uma comissão de implementação e adequação à Lei Geral de Proteção de Dados com a finalidade de estruturar uma estratégia de adequação à LGPD.

Nesse sentido, apresentamos este documento, o Plano de Adequação à LGPD – 2025-2026, o qual tem como objetivo propor uma metodologia de adequação para assegurar os direitos dos/as titulares, a partir de recomendações de medidas de segurança e controles. Assim, este Plano está pautado em quatro eixos estruturantes: apoio da alta administração; envolvimento das áreas administrativa, assistência e ensino e pesquisa; medidas de segurança e gestão de riscos; e monitoramento e aperfeiçoamento contínuos.

Salienta-se que esse é um projeto inicial de adequação, o qual busca apontar estratégias de aderência à nova legislação, que traz em seu arcabouço mudanças culturais significativas, com referência ao direito à titularidade e aos processos de tratamento de dados pessoais.

Frisamos que, por ser uma proposta inicial, é esperado que, ao longo do caminho percorrido, esta possa e deva ter modificações durante a sua execução, tendo em vista o necessário amadurecimento do processo de adequação e as diretrizes a serem estabelecidas pela Autoridade Nacional de Proteção de Dados - ANPD, recentemente criada.

Ao elaborar este documento, a FMT-HVD demonstra estar em consonância com seus princípios de conformidade legal, de transparência e integridade, no que se refere aos seus processos administrativos, de assistência, de ensino e pesquisa, reafirmando o seu compromisso de diálogo aberto com a sua comunidade científica,

a qual poderá acompanhar e contribuir com a efetivação do projeto de aderência à proteção de dados pessoais.

1. Introdução

Do ponto de vista histórico, a Constituição Federal de 1988 garante direitos individuais ao/à cidadão/ã, cabendo explicitar, no contexto deste Plano de Adequação, o direito fundamental à privacidade, expresso no Art. 5º, inciso X, da CF: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". Ao mesmo tempo o texto constitucional também garante o direito de acesso às informações públicas, conforme Art. 5º, inciso XXXIII: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

Ademais, a Constituição Federal de 1988 consolidou a gestão de documentos no parágrafo 2°, do Art. 216, ao afirmar que "cabem à Administração Pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem". Em 1991, a Lei de Arquivos (Lei n° 8.159/1991) garantia, pela primeira vez no Brasil, a ideia de uma política nacional de arquivos. Sua implementação na esfera federal, estadual e municipal propiciou avanços, principalmente, na gestão de documentos como instrumento de racionalidade e transparência da Administração Pública, dedicando o capítulo V ao "acesso e sigilo de documentos públicos".

Dessa forma, surge a Lei n° 12.527/2011 (Lei de Acesso à Informação - LAI) para promover a transparência da Administração Pública e regulamentar o direito constitucional ao acesso à informação, considerando a publicidade como regra e o sigilo como exceção. Diante disso, o Art. 31 da LAI e o Art. 55 do Decreto n° 7.724/2012, ao regulamentar o acesso às informações pessoais, impuseram deveres de salvaguarda à Administração Pública, quando estas digam respeito à intimidade, vida privada, honra e imagem, tratando-se de direitos fundamentais de personalidade, conforme expresso no Art. 5º, inciso X, da Constituição Federal. As informações pessoais a que se referem esses artigos terão seu acesso restrito pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção, podendo ser acessadas pelos próprios indivíduos, pelos agentes públicos legalmente autorizados ou por terceiros, diante de previsão legal ou consentimento expresso da pessoa a qual elas se referirem.

Acrescenta-se a esse contexto o Marco Civil da Internet (Lei n° 12.965/2014), que regulamenta o uso da Internet no país, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. Tem como princípios essenciais, de acordo com o seu artigo 3°: i) a garantia da liberdade de expressão, comunicação e manifestação do pensamento; ii) a proteção da privacidade dos/as usuários/as e de seus dados pessoais; e iii) a garantia da neutralidade da rede.

Além desses dispositivos legais apresentados, o tratamento de dados pessoais, no contexto de transformação digital, deve vir acompanhado de medidas de segurança capazes de assegurar a adequada proteção desses dados, garantindo assim direitos constitucionais, como a privacidade, a intimidade e a inviolabilidade da honra e da imagem das pessoas. Nesse viés, o arcabouço legal brasileiro é alterado pela promulgação da Lei Geral de Proteção de Dados Pessoais – LGPD, com o intuito de enfrentar desafios da era digital e assegurar direitos constitucionais.

Inspirada na GDPR (*General Data Protection Regulation*), legislação que regulamenta a privacidade de dados nos países europeus, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), no Brasil, altera o Marco Civil da Internet (Lei nº 12.965/2012) e encontra-se em vigência desde 18 de setembro de 2020. Com a nova legislação, são apresentados novos conceitos, trazendo obrigações para a Administração Pública e fortalecendo os direitos dos/das titulares de dados. Nesse viés, empresas e órgãos públicos precisam promover mudanças e estabelecer regras de coleta, armazenamento, tratamento e compartilhamento de dados pessoais, restando às instituições públicas e privadas a sua adequação no menor prazo possível.

Os especialistas em proteção de dados apontam que será um processo longo e complexo e que, portanto, nenhuma instituição, provavelmente, conseguirá se adequar em curto ou médio prazos.

É importante ressaltar que o objetivo da Lei nº 13.709/2018 é proteger os direitos fundamentais de liberdade e de privacidade do titular dos dados e que existem penalidades para a não adequação.

Diante disso, a Administração Pública, no papel de custodiante dos dados dos/das cidadãos/ãs, deve fornecer a segurança necessária para proteger adequadamente os dados que custodia e/ou trata. Nesse cenário, a FURG designou uma comissão, por meio da Portaria nº 095/2025-GDP/FMT-HVD, para elaborar uma estratégia de adequação à nova legislação e preencher o questionário de diagnóstico institucional, com perguntas que abordam aspectos de adequação à LGPD. Assim,

este documento, o "Plano de Adequação à Lei Geral de Proteção de Dados Pessoais – LGPD (2025-2026) ", é resultado do trabalho dessa comissão, buscando propor uma metodologia para a implementação da Lei Geral de Proteção de Dados Pessoais no âmbito da FMT-HVD.

Mas de que dados exatamente estamos falando e o que são dados pessoais?

A LGPD trata da proteção dos dados pessoais. Ressalta-se que se uma informação identifica ou permite a identificação de uma pessoa natural, ela é considerada um dado pessoal.

Nesse sentido, exemplificamos dados pessoais:

✓ nome e sobrenome; gênero; data de nascimento; documentos pessoais (CPF, RG, CNH, Carteira de Trabalho, Passaporte e Título de Eleitor); matrícula dos(as) servidores(as) e dos(as) discentes; unidade em que trabalha; endereço residencial; localização via GPS; número de telefone; endereço de e-mail.

Entre os dados pessoais, temos os que se constituem como sensíveis, por serem passíveis de gerar discriminações ou preconceitos, como:

✓ origem racial ou étnica; convicção religiosa ou filosófica; opinião política; filiação à sindicato ou organização de caráter religioso, filosófico ou político; informações genéticas, biométricas ou sobre a saúde ou a vida sexual.

É importante mencionar que a operação dos dados pessoais não é absoluta, pois existem princípios que devem ser observados, conforme a LGDP, Art. 6º, além do princípio da boa-fé. A Lei prevê que para o tratamento de dados devem ser seguidos os seguintes princípios essenciais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e prestação de contas. Abaixo, detalhamos cada um dos princípios:

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao/à titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Adequação: compatibilidade do tratamento com as finalidades informadas ao/à titular, de acordo com o contexto do tratamento;

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;

Livre acesso: garantia, aos/às titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

Qualidade dos dados: garantia, aos/às titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: garantia, aos/às titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os/as respectivos/as agentes de tratamento, observados os segredos comercial e industrial;

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;

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Responsabilização e prestação de contas: demonstração, pelo/a 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.

Nesse sentido, dos princípios essenciais da Lei de Proteção de Dados Pessoais, ressaltamos que na FMT-HVD tratamos os dados pessoais de pacientes, servidores/as, colaboradores/as, pesquisadores e fornecedores/as com a finalidade, essencialmente, de executar políticas públicas. Esses dados são coletados, armazenados, podendo ser compartilhados para outros órgãos governamentais ou não. Nesse viés, destaca-se a importância de mapear o fluxo do tratamento de dados pessoais, identificando a rastreabilidade desses dados, além de promover a revisão das cláusulas contratuais entre a FMT-HVD e as pessoas físicas e/ou jurídicas, especialmente, quando há compartilhamento de dados pessoais, para fins de adequação da Instituição à LGPD.

Salienta-se que outro aspecto importante da Lei é que a segurança e a privacidade no tratamento dos dados não se restringem apenas àqueles dados que são tratados eletronicamente, mas também aos que são coletados por meio de papel e que, por vezes, ficam em nossas mesas. Nesse sentido, a comissão sublinha que são necessárias capacitações, com o objetivo de mudança na cultura organizacional, com o estabelecimento de boas práticas em relação à proteção de documentos físicos/digitais, quando envolvem dados pessoais, tais como: a política da "mesa limpa/tela limpa" (princípio estabelecido na Norma ABNT NBR/ISSO/IEC 27:001), a limitação de acessos, a utilização de senhas e a correta retenção e armazenamento dos dados pessoais.

Nesse cenário, apresentamos os atores envolvidos no fluxo de tratamento de dados para que se possibilite a adequação à LGPD.

2. Atores Envolvidos

Para uma efetiva aderência à Lei Geral de Proteção de Dados Pessoais, serão necessários o envolvimento e o comprometimento de todas as áreas de atuação da FMT-HVD. Nesse sentido, é importante detalhar alguns atores e suas respectivas responsabilidades, previstas na referida Lei.

Primeiramente, salientamos que a LGPD tem como princípio basilar a proteção dos direitos dos/as titulares dos dados pessoais, sendo, portanto, **titular**, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

No contexto da FMT-HVD, temos como **titulares dos dados pessoais** os/as discentes, servidores/as públicos/as, assim como, todos/as os/as colaboradores/as, terceirizados/as, estagiários/as, bolsistas e, também, a comunidade externa que venha a utilizar os serviços prestados pela Instituição.

Além disso, **o/a controlador/a** é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Dessa forma, temos a FMT-HVD como **controladora** dos dados pessoais coletados no âmbito da execução das suas políticas públicas. A LGPD traz, ainda, a figura do/a **operador/a**, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do/a controlador/a. Portanto, o/a **controlador/a** e o/a **operador/a** são chamados/as de **agentes de tratamentos** pela LGPD.

Destaca-se, ainda, a figura do/a **encarregado/a** pelo tratamento de dados pessoais, que atuará como canal de comunicação entre o controlador/a, os/as titulares dos dados e a **Autoridade Nacional de Proteção de Dados - ANPD.** Dessa forma, o/a controlador/a deverá indicar o/a encarregado/a, sendo a identidade e as informações de contato publicadas de forma clara e objetiva, pois as atividades do/a encarregado/a consistem, principalmente, em:

I - aceitar reclamações e comunicações dos/as titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os/as funcionários/as e os/as contratados/as da entidade, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador/a ou estabelecidas em normas complementares.

Por fim, a LGPD, traz a figura da Autoridade Nacional de Proteção de Dados - ANPD, órgão do Poder Executivo Federal, que poderá estabelecer normas complementares para a definição e as atribuições do encarregado e diretrizes para a efetiva aderência à LGPD.

Além dos atores previstos na Lei nº 13.709/2018, como estratégia para a adequação à LGPD, considerando o contexto institucional, este Plano sugere: (i) a designação de pontos focais nas áreas administrativa, assistência, ensino e pesquisa, para que possam atuar como multiplicadores da LGPD, em suas respectivas unidades, contribuindo para a conformidade com a legislação; e (ii) a criação do Comitê Gestor de Proteção de Dados Pessoais - CGPD para atuar como o encarregado pelo tratamento de dados pessoais no âmbito da FMT-HVD, haja vista os diferentes conhecimentos e competências necessárias para exercer as atribuições de implementação, recomendação e monitoramento para adequação à LGPD.

3. Bases legais para tratamento de Dados Pessoais

A LGPD estabeleceu as hipóteses que autorizam o tratamento de dados pessoais, assim como os requisitos para execução do tratamento. Portanto, conforme o Art. 7º da LGPD, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo/a titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador/a;

III - pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário, para a execução de contrato ou de procedimentos preliminares relacionados a contrato, do qual seja parte o/a titular, a pedido do/a titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do/a titular ou de terceiros;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário, para atender aos interesses legítimos do/a controlador/a ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do/a titular, que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Ao referenciar os itens acima, ressalta-se que a LGPD, em seus artigos 6º, 7º, 9º, 11 e 26, prevê que a Administração Pública tem a prerrogativa de tratar dados sem o consentimento do/a titular, desde que seja para a execução de políticas públicas, devidamente estabelecida por lei. No entanto, salienta-se que todas as obrigações e direitos decorrentes da própria LGPD deverão ser devidamente observados. Nesse viés, mencionamos abaixo os direitos dos/as titulares.

4. Direitos dos Titulares

O/A titular do dado tem direito às informações sobre: quais dados seus são coletados; para quais necessidades; se aquelas informações são compartilhadas com outras instituições e/ou empresas e se estão protegidas. O/A titular também poderá fazer questionamentos, pedir alterações ou solicitar a revogação do consentimento de seus dados a qualquer momento. Abaixo, detalhamos alguns artigos da LGPD sobre os direitos dos/as titulares:

- Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao/à titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades: Art. 6º, I ;
- Direito ao tratamento adequado, compatível com as finalidades informadas ao/à titular, de acordo com o contexto do tratamento: Art. 6º, II
- Direito à 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: Art. 6º, III
- Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais: Art. 6º, IV
- Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento: Art. 6º, V
- Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os/as respectivos/as agentes de tratamento, observados os segredos comercial e industrial: Art. 6º, VI
- Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos/as agentes de tratamento, de 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: Art. 6º, VII
- Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais: Art. 6º, VIII
- Direito de não ser discriminado/a de forma ilícita ou abusiva: Art. 6º, IX
- Direito de exigir a adequada responsabilização e a prestação de contas por parte dos/as agentes de tratamento, ao qual se contrapõe o dever, por parte destes/as, de adoção de medidas eficazes e capazes de comprovar a

observância e o cumprimento das normas de proteção de dados pessoais: Art. 6º, X

- Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do/a titular, salvo as exceções legais: Arts. 7º, I, e 8º
- Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento: Art. 7º, § 6º
- Direito à inversão do ônus da prova quanto ao consentimento: Art. 8º, § 2º
- Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais: Art. 8º, § 4º
- Direito de requerer a nulidade do consentimento, caso as informações fornecidas ao/à titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca: Art. 9º, § 1º
- Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do/a titular, por procedimento gratuito e facilitado: Art. 8º, § 5º

É importante salientar que para a adequação da LGPD faz-se necessário um processo de transformação cultural nas instituições, tendo em vista o novo paradigma estabelecido pela Lei, no sentido do reconhecimento de que o dado pertence ao/a titular. Assim, entende-se que todo o processo de aderência à LGPD precisa estar fundamentado no comprometimento da administração superior e na sensibilização da comunidade da Instituição.

5. Diagnóstico Institucional

A partir da designação da comissão de implementação e adequação à Lei Geral de Proteção de Dados, feita pela Portaria nº 095/2025-GDP/FMT-HVD, foram realizadas reuniões, sendo a primeira no dia 20 de agosto de 2020. A pauta inicial tratada pela comissão foi o preenchimento do questionário de diagnóstico institucional da Lei Geral de Proteção de Dados Pessoais – LGPD. Com base no resultado do diagnóstico, foi possível perceber aspectos que configuram como vulnerabilidades da Instituição para adequação à LGPD.

Dessa forma, a comissão buscou definir as estratégias e a metodologia a serem adotadas para adequação à Lei, tendo como base o diagnóstico institucional e o Guia de Boas Práticas da Lei Geral de Proteção de Dados - LGPD, além de outros normativos que pudessem ser relevantes para o trabalho a ser realizado, referenciados ao final deste documento.

Nesse viés, a comissão entendeu que o processo para a adequação deve ser implementado com ações de curto, médio e longo prazos, com a definição de alguns marcos de adequação, considerando o período de 2025-2026, além de outros que poderão ser agregados posteriormente, em decorrência das atividades realizadas durante a execução deste plano e/ou de diretrizes definidas pela Autoridade Nacional de Proteção de Dados - ANPD.

6. Adequação à LGPD

Considerando as atribuições da Portaria nº 0229/2025-GDP/FMT-HVD e os princípios da Lei Geral de Proteção de Dados Pessoais, foram estabelecidos os seguintes objetivos para este Plano, no âmbito do tratamento de dados pessoais da FMT-HVD:

- Propor uma metodologia de adequação à LGPD;
- Recomendar medidas de segurança e controles;
- Assegurar os direitos dos/as titulares.

Buscando alcançar os objetivos estabelecidos, estruturou-se este Plano de Adequação, com a definição de quatro eixos para a efetiva implementação e aderência à LGPD, detalhados a seguir.

6.1. Eixos Estruturantes de adequação

Os eixos estruturantes são: apoio da alta administração; envolvimento da comunidade acadêmica, assistencial e de ensino e pesquisa; medidas de segurança e gestão de riscos; monitoramento e aperfeiçoamento contínuos.

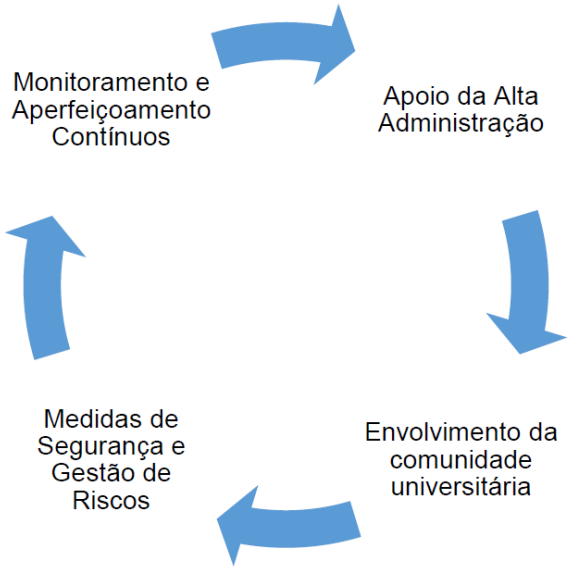

Figura 1 – Eixos estruturantes de adequação à LGPD

6.1.1 Apoio da Alta Administração

A LGPD traz em seu escopo novos conceitos, no que se refere aos direitos dos/as titulares de dados, atribuindo para a Administração Pública novas obrigações, com o intuito de garantir e assegurar proteção adequada para os dados pessoais custodiados

e/ou tratados. Nesse sentido, medidas de segurança e controles precisam ser implementados pela Instituição, garantindo, assim, essa proteção em todo ciclo de tratamento do dado. Portanto, são de extrema relevância, para a adequação da Instituição à LGPD, o comprometimento e o apoio da alta administração, visto que é um processo que demanda o envolvimento de todas as áreas e inclui todos os processos organizacionais da FMT-HVD.

6.1.2. Envolvimento de todas as áreas

O novo arcabouço da LGPD muda a forma de funcionamento das instituições, no que diz respeito ao tratamento de dados pessoais, sendo necessário o estabelecimento de regras muito bem definidas, com o intuito de garantir os direitos dos/as titulares. Assim, para promover a devida adequação à LGPD, faz-se necessário que todos os membros de todas as áreas (administrativa, assistência, ensino e pesquisa) sejam sensibilizados e capacitados para essas mudanças, visando uma efetiva garantia dos direitos dos/as titulares de dados pessoais, desde a coleta até a eliminação (descarte) do dado, e que todo o ciclo de tratamento esteja em consonância com os princípios estabelecidos na Lei.

6.1.3. Medidas de Segurança e Gestão de Riscos

Os/As agentes de tratamento, controlador/a e operador/a, ou qualquer pessoa que participe do tratamento de dados pessoais, desempenham um papel imprescindível para assegurar a sua proteção, por meio de medidas de segurança, técnicas e administrativas, conforme estabelecido no caput do Art. 46 da LGPD. Ressalta-se que essas medidas devem ser observadas desde a fase de concepção do serviço até a sua execução, também, chamada de *privacy by design*.

Nesse sentido, a identificação dos riscos à privacidade no fluxo de tratamento dos dados é fundamental para adequação à LGPD.

A partir da gestão de riscos, a FURG poderá mitigar aqueles que comprometam a segurança dos dados pessoais, conforme a probabilidade e a gravidade dos danos para os/as titulares dos dados, de forma a garantir os princípios estabelecidos na LGPD. A contenção desses riscos tem como objetivo a proteção dos dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, conforme art. 6º da referida Lei. Assim, é fundamental que

este plano esteja em consonância com as Políticas de Segurança da Informação e de Gestão de Riscos da FMT-HVD.

6.1.4. Monitoramento e aperfeiçoamento contínuos

A complexidade trazida pela LGPD, no que se refere ao tratamento de dados pessoais, exige alterações de rotinas diárias; gestão de riscos para implementação de medidas de segurança e controles durante o ciclo da vida do dado; e transformação cultural, no que tange aos direitos dos/as titulares. Nesse sentido, para que a FMT-HVD promova a devida proteção dos dados custodiados e/ou tratados, é necessário que se faça um monitoramento e aperfeiçoamento contínuos, buscando pautá-los sempre nos princípios estabelecidos na LGPD.

Para além do monitoramento pela própria Instituição, será disponibilizado um canal de comunicação com os/as titulares dos dados para questionamentos, reclamações e denúncias, relativos a proteção de dados pessoais, além de um e-mail para contato com o/a encarregado/a.

7. Marcos de adequação à LGPD

A partir do resultado do diagnóstico institucional e dos eixos estruturantes deste Plano, apresentamos os seguintes marcos de adequação como estratégia inicial para a aderência da FMT-HVD à LGPD:

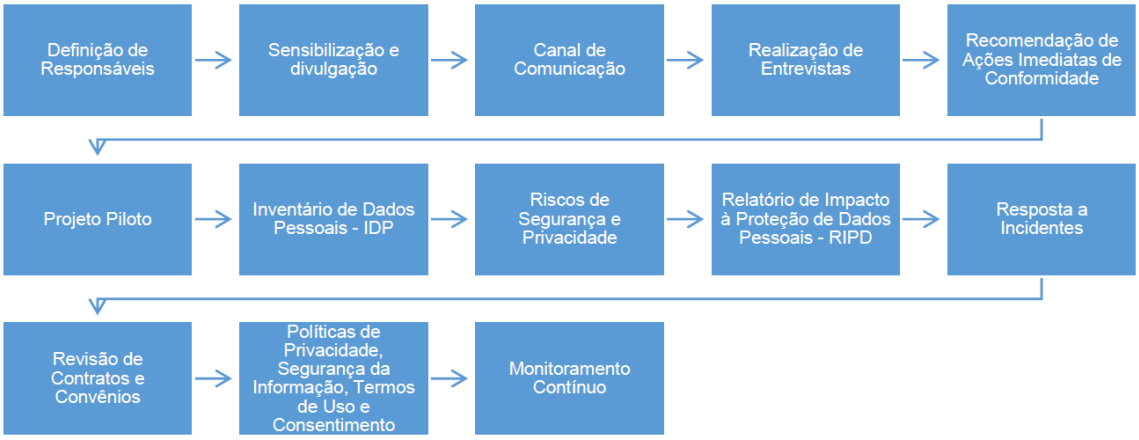

Figura 2 – Marcos de adequação à LGPD

Com referência aos marcos de adequação à LGPD, detalharemos abaixo as ações necessárias para a aderência à Lei.

7.1. Definição de responsáveis

Inicialmente, é necessário salientar que a responsabilidade pelo cumprimento da Lei é de toda a FMT-HVD, desde a autoridade máxima, passando pelas áreas meio e fim, pois sua efetivação se dá na execução dos serviços e processos de trabalho diários da Instituição. Dessa forma, a metodologia aqui proposta tem caráter multidisciplinar, multissetorial e de impacto no órgão como um todo. Consequentemente, essa responsabilidade não pode ser delegada a uma só pessoa ou a um grupo fechado de pessoas, porém é necessário definir alguns responsáveis que irão auxiliar no processo de adequação à LGPD, tais como:

- Comitê de Privacidade e Proteção de Dados - CPPD;
- Pontos focais responsáveis pelas frentes de atuação no tratamento de dados pessoais em cada Unidade Administrativa e Acadêmica;
- Encarregado/a pelo tratamento de dados pessoais na FMT-HVD.

A partir da sugestão constante no Plano, de que as atribuições do/a encarregado/a sejam exercidas pelo CPPD, sugerimos, também, a composição mínima do referido Comitê, pelas seguintes áreas:

- Tecnologia da Informação;
- Faturamento;
- Ouvidoria;
- Controle Interno;
- Assessoria Jurídica;
- Gerência de Compras;
- Gerência de Pessoal;
- Gerências de Ambulatório (infectologia, dermatologia e IST/Aids);
- Gerência de Enfermagem;
- Gerências de diagnósticos (análises clínicas, bacteriologia, micologia, micobacteriologia, parasitologia e leishmaniose)
- Farmácia ambulatorial e hospitalar;
- Gerências de Orçamento e finanças;
- Gerência de Convênios;
- Diretoria de Ensino e Pesquisa.

7.2. Sensibilização e divulgação

Conforme mencionado anteriormente, o processo de adequação à Lei está na execução dos serviços e processos de trabalho diários da Instituição, envolvendo todos os setores.

Portanto, é necessária uma transformação cultural para a efetiva implementação da LGPD.

Dessa forma, este Plano propõe etapas iniciais de apresentação da LGPD à comunidade em geral, assim como, a divulgação do canal de comunicação e o contato do/a encarregado/a pelo tratamento dos dados pessoais, no âmbito da FMT-HVD.

Além disso, será imprescindível a elaboração, junto à Assessoria de Comunicação, de um plano de comunicação para divulgação e sensibilização, tanto da LGPD, quanto do seu impacto na FMT-HVD, por meio dos trabalhos desenvolvidos no âmbito deste Plano de Adequação.

7.3 Realização de Entrevistas

Partindo da necessidade de sensibilização e de divulgação dos impactos da LGPD, a proposta inicial é a realização de entrevistas com a área meio e área fim,

conforme o cronograma estabelecido neste Plano, sensibilizando os/as gestores/as e servidores/as, com intuito de orientar as Unidades a se adequarem aos princípios estabelecidos na LGPD. Dessa forma, será elaborado um roteiro semiestruturado como instrumento para realização das entrevistas, com o objetivo de perceber as vulnerabilidades que possam ser mitigadas de forma imediata, em consonância aos princípios e diretrizes estabelecidos na Lei.

7.4 Definição de Ações Imediatas de Conformidade

A partir do diagnóstico institucional e da análise das entrevistas, serão recomendadas ações imediatas de conformidade à LGPD às Unidades Administrativas e Acadêmicas, de acordo com a sua competência. Diante disso, essas ações já poderão impactar de forma positiva na efetiva implementação da LGPD.

7.5 Projeto Piloto

Para a execução deste Plano, será implementado um Projeto Piloto com o objetivo de mensurar os fluxos das etapas e procedimentos, prazos necessários e atores envolvidos no processo. Essa etapa será importante para delinear e aperfeiçoar os marcos de adequação à LGPD, propondo melhorias no formulário de inventário de dados pessoais, no mapeamento das medidas de segurança e, consequentemente, na identificação e mitigação dos riscos.

7.6 Inventário de Dados Pessoais – IDP

O Inventário de Dados Pessoais – IDP consiste no registro das operações de tratamento dos dados pessoais realizados pela Instituição, conforme Art. 37 da LGPD. Nesse sentido, esse inventário envolve descrever informações relativas ao tratamento de dados pessoais realizado pela Instituição, tais como: finalidade específica; hipótese de tratamento; previsão legal; dados pessoais tratados; categoria dos/as titulares; tempo de retenção; instituições com as quais esses dados são compartilhados; transferência internacional de dados; e medidas de segurança atualmente adotadas.

Diante disso, o mapeamento do tratamento dos dados pessoais se dará a partir da aplicação de um formulário específico. Esse questionário será aplicado, primeiramente, no Projeto Piloto e poderá sofrer outros ajustes, conforme necessidade.

Ressaltamos que o IDP representa um significativo instrumento de governança de dados pessoais, o qual permitirá a elaboração do Relatório de Impacto à Proteção de Dados Pessoais - RIPD, verificando a conformidade da Instituição com a LGPD.

7.7. Riscos de Segurança e Privacidade

A partir do trabalho que será realizado pelo Comitê de Privacidade e Proteção de Dados Pessoais – CPPDP, e do preenchimento do formulário para mapeamento do tratamento de dados pessoais, será possível identificar as vulnerabilidades, as medidas e os controles necessários para a mitigação dos riscos encontrados.

Em relação às medidas de segurança, mencionadas no Art. 46 da LGPD, sua aplicação representa o que se espera alcançar, sendo que para isso, os controles configuram ações específicas de segurança que podem ser aplicadas sobre os ativos organizacionais para se atingir a medida. Assim, descrevemos algumas medidas de segurança:

Medida de Segurança	Objetivos dos Controles
Classificação da informação	Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a instituição
Compartilhamento, uso e proteção da informação	Assegurar a privacidade e proteção das informações de identificação pessoal, conforme requerido por legislação e regulamentação pertinente
Continuidade de negócio	A proteção de dados deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização
Controle de Acesso Lógico	Limitar o acesso à informação e aos recursos de processamento da informação
Controles Criptográficos	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação
Controles de Coleta e Preservação de Evidências	A instituição deve definir e aplicar procedimentos para a identificação,

	coleta, aquisição e preservação das informações, as quais podem servir como evidências
Cópia de Segurança	Cópias de segurança das informações, de softwares e das imagens do sistema devem ser efetuadas e testadas regularmetne, conforme a política de geração de cópias de segurança da instituição
Desenvolvimento Seguro	Garantir que a proteção de dados esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação
Gestão de Mudanças	Mudanças na organização, nos processos de negócio, nos recursos de processamento da informação e nos sistemas que afetam a proteção de dados devem ser controladas
Gestão de Riscos	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a instituição. Destinado a fornecer segurança razoável, quanto à proteção dos dados pessoais e à realização de seus objetivos
Organização da Segurança	Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança dos dados dentro da organização.
Política de Segurança	Prover orientação da direção e apoio para a segurança dos dados pessoais

Proteção física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento e informações institucionais
Registro de eventos e rastreabilidade	Registrar eventos e gerar evidências, a fim de proporcionar rastreabilidade
Segurança em Redes	Assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam
Segurança nas Operações	Garantir a operação segura e correta dos recursos de processamento da informação
Tratamento e Resposta a Incidentes	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança que possam acarretar risco ou dano relevante aos/as titulares de dados pessoais, incluindo a comunicação sobre fragilidades e eventos de segurança.

A partir da metodologia a ser adotada pelo CPPDP para a identificação dos riscos à privacidade dos dados pessoais, a FMT-HVD deverá elaborar o Relatório de Impacto à Proteção de Dados Pessoais – RIPD para a mitigação dos riscos, conforme o seu nível de impacto e probabilidade.

7.8 Relatório de Impacto à Proteção de Dados Pessoais – RIPD

Conforme a LGPD, o Relatório de Impacto à Proteção de Dados Pessoais – RIPD é o documento elaborado pelo/a controlador/a, que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos. De acordo com a Lei, o RIPD deverá ser elaborado, observadas as seguintes situações:

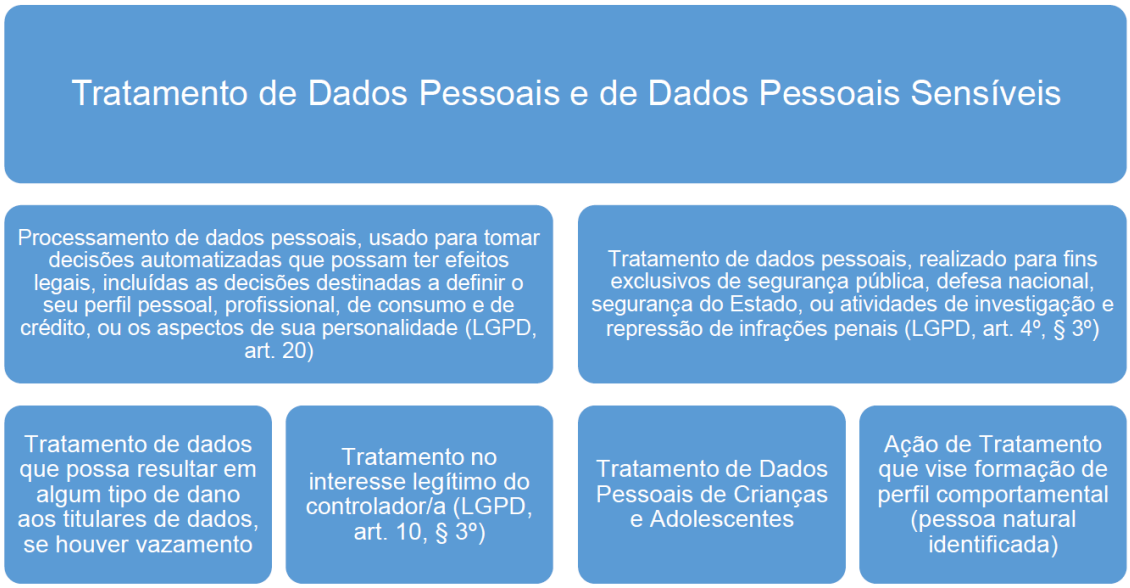

Figura 3 – Hipóteses de elaboração do RIPD

7.9. Respostas a Incidentes

Conforme o Art. 48 da Lei Geral de Proteção de Dados Pessoais, o/a controlador/a deverá comunicar à ANPD e ao/à titular dos dados pessoais a ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos/às titulares. Ainda, a ANPD definirá o prazo para a comunicação e verificará a gravidade, podendo determinar adoção de providências para ampla divulgação e medidas para reverter ou abrandar os efeitos do incidente.

Ressalta-se a importância de estabelecer procedimentos específicos para a detecção, o tratamento, a coleta de evidências e a resposta a incidentes de segurança da informação e privacidade, no intuito de mitigar o nível de risco, ao qual os sistemas de tecnologia da informação estarão expostos, considerando a Política de Gestão de Riscos da FMT-HVD. Nesse viés, a Gestão de Incidentes deverá possuir um plano de comunicação, orientando a forma que os incidentes de segurança, que acarretem riscos ou dano, sejam comunicados aos/as titulares dos dados e à ANPD.

Cabe, ainda, destacar que a ANPD poderá solicitar eventual comprovação de que foram adotadas medidas técnicas adequadas, no sentido de tornarem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

7.10. Revisão de contratos e convênios

Após a construção do inventário de dados pessoais, avaliação de riscos de segurança e privacidade e elaboração de RIPD, é preciso avaliar a necessidade de adequação de novas cláusulas em contratos, convênios e outros instrumentos, novos

ou existentes, que impliquem no tratamento de dados pessoais, conforme os princípios da LGPD, como, por exemplo:

- responsabilidades bem definidas do/a controlador/a e operadores/as;
- transparência no tratamento dos dados pessoais;
- detalhamento de quem tem acesso aos dados;
- responsável pelo seu uso e tratamento;
- forma de armazenamento e medidas de segurança e privacidade dos dados coletados e armazenados pelo/a contratado/a.

7.11. Políticas de Privacidade, Segurança da Informação, Termos de Uso e Consentimento

O Termo de Uso e a Política de Privacidade são documentos que surgem para atender ao princípio da transparência estabelecido na LGPD. Em relação ao Termo de Uso, esse é um documento que estabelece as regras e condições de uso de um serviço, formas de acesso, requisitos, etapas do processo e prazos para a prestação do serviço. Deve ser constantemente atualizado para refletir, de modo claro e preciso, as seguintes finalidades: coleta, uso, armazenamento, tratamento e proteção. Dessa forma, esse documento tem como objetivo a exposição das regras e condições dos serviços a que, a partir do aceite do/a usuário/a, sua utilização estará vinculada.

Com referência à Política de Privacidade, que faz parte dos Termos de Uso, trata-se de um documento que informa ao usuário sobre o tratamento dos dados pessoais e privacidade fornecida, em consonância aos princípios do Art. 6º da LGPD. Diante disso, o objetivo é dar transparência à forma de tratamento de dados pessoais. Ainda, é necessário ter a Política de Segurança da Informação atualizada, conforme Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), e em consonância com a LGPD.

Cabe ressaltar, ainda, que a Administração Pública tem a prerrogativa de tratar dados sem o consentimento do/a titular, desde que seja para a execução de políticas públicas, devidamente estabelecida por lei, observando os princípios da LGPD. No entanto, em casos excetuados à finalidade legalmente estabelecida, um termo de consentimento expresso deverá ser assinado pelo/a usuário/a, podendo ser revogado a qualquer tempo.

7.12. Canal de Comunicação

O/A encarregado/a pelo tratamento dos dados pessoais tem como competências aceitar reclamações e comunicações dos/as titulares, prestar esclarecimentos e adotar providências.

Dessa forma, a identidade e as informações de contato do/a encarregado/a deverão ser divulgadas, de forma clara e objetiva, no sítio institucional da FMT-HVD. Essa comunicação será feita, preferencialmente, pelo e-mail: lgpd@fmt.am.gov.br.

Para a comunicação com o/a titular, também, será disponibilizada a Ouvidoria da FMT-HVD, como um canal oficial de recebimento de manifestações que envolvam os direitos desses/as titulares, por meio da Plataforma Integrada de Ouvidoria e Acesso à Informação (Fala.BR): https://falabr.cgu.gov.br/.

7.13. Monitoramento contínuo

O monitoramento contínuo é importante para a conformidade com a LGPD, a fim de que as ações previstas neste Plano ou no decorrer dos trabalhos realizados pelo CPPD possam ser avaliadas e aperfeiçoadas, durante o processo de adequação, que é uma atividade contínua.

Salienta-se o papel do/a encarregado/a na articulação dessa etapa, compreendendo o gerenciamento a partir do estabelecimento de indicadores para acompanhar as ações do Plano de Adequação e da divulgação dos resultados para a alta administração e comunidade universitária.

8. Cronograma de adequação à LGPD

Como estratégia inicial de adequação, a metodologia apresentada neste Plano estabelece algumas ações de curto, médio e longo prazo, conforme cronograma a seguir, que podem ser atualizadas e aperfeiçoadas periodicamente, em decorrência da maturidade da Instituição, em relação à proteção de dados pessoais.

Ação	Responsável/eis	2025				2026											
		09	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12
Criar e designar o CPPD	Diretoria																
Nomear encarregado	Diretoria																
Indicar os pontos focais	Diretoria																
Divulgar os dados do encarregado e o canal de comunicação	Gerência de Informática e Assessoria de Comunicação																
Elaborar Plano de Comunicação	CPPD e Assessoria de Comunicação																
Sensibilizar servidores e clientes	CPPD e Assessoria de Comunicação																
Promover capacitação	CPPD																
Realizar entrevistas com os setores	CPPD																
Implementar o Projeto Piloto	CPPD																
Elaborar políticas de privacidade, segurança da informação e termos de uso e consentimento	DTO e CPPD																
Mapear o fluxo de tratamento de dados pessoais	Setores e CPPD																
Elaborar RIPD	CPPD																
Revisar cláusulas contratuais e de convênios	Gerência de Convênios e Contratos e CPPD																
Publicar o RIPD no website	Gerência de Informática																

Obs.: Este cronograma pode e deve ser revisado periodicamente de modo a se adequar à realidade diante dos fluxos de trabalhos existentes na FMT-HVD.