
MPPI
Ministério Público
do Estado do Piauí

MINISTÉRIO PÚBLICO DO ESTADO DO PIAUÍ

PLANO DIRETOR DO MINISTÉRIO PÚBLICO DO ESTADO DO PIAUÍ – MPPI

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Sumário

APRESENTAÇÃO

Este documento formaliza o Plano Diretor para a execução do Programa de Proteção de Dados do Ministério Público do Estado do Piauí (MPPI), fundamentado no "Manual de Referência de Elaboração dos Planos Diretores do CNMP", disponível no portal do Conselho (link: _Manual_de_referência_de_elaboração_dos_planos__2ª_versão.pdf (cnmp.mp.br)). Observando os dispositivos legais - Lei nº 13.709/18 e Resolução CNMP nº 281/23, o Plano visa direcionar efetivamente a implementação do Programa de Privacidade do MPPI. Sua elaboração está alinhada ao Planejamento Estratégico Institucional (PEI/MPPI-2021/2023) para assegurar a adequada alocação de recursos e atenção às áreas de maior relevância, visando a otimização das despesas públicas e aprimoramento dos serviços oferecidos aos cidadãos.

O presente Plano Diretor, com vigência para o biênio 2024-2025, será submetido à revisão anual, possibilitando a atualização de diretrizes, formulação de planos e contribuição essencial para o planejamento orçamentário subsequente.

O Plano Diretor de Proteção de Dados Pessoais (PDPD) e suas revisões necessitam de aprovação pelo Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), sendo posteriormente ratificados pela alta direção do MPPI, conforme estipula o parágrafo segundo do Artigo 2º da Resolução CD/MPPI nº 3, de 25 de janeiro de 2023.

O CEPDAP reserva-se o direito de promover atualizações conforme as exigências emergentes, garantindo a integração de novas demandas e estratégias. O presente plano inclui um diagnóstico da condição atual do Programa em Privacidade do MPPI e delineia o planejamento estratégico para sanar as necessidades detectadas, propondo planos e intervenções para alcançar os resultados desejados.

1. INTRODUÇÃO

A transformação tecnológica em andamento tem sido fonte tanto de avanços quanto de desafios para a sociedade. O crescente estado de interconexão digital levanta preocupações significativas sobre a preservação da privacidade e segurança da informação pessoal dos indivíduos.

Em resposta a essas questões, surgiram normativas focadas na salvaguarda de dados pessoais. Tais regulamentações são cruciais, pois estabelecem um marco legal que endossa a transparência e protege tanto a privacidade quanto a segurança dos dados, enquanto impõe diretrizes e responsabilidades às entidades que gerenciam informações pessoais.

Em destaque, o Regulamento Geral sobre a Proteção de Dados (GDPR) da EU, aplicado desde 2018, prescreve procedimentos detalhados para assegurar a privacidade e a proteção dos dados de cidadãos europeus. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) regula o processamento de dados pessoais, incluindo em mídias digitais, com a finalidade de proteger as liberdades fundamentais e a privacidade, além de fomentar o desenvolvimento da personalidade do indivíduo. Importante salientar que as prescrições da LGPD possuem relevância nacional e são aplicáveis a todos os níveis administrativos - federal, estadual e municipal.

Visando a implantação de um sistema de proteção de dados coerente em todo o Ministério Público e uma política consistente em âmbito nacional, foi promulgada a Resolução CNMP 281/23.

Tal resolução institui o Sistema Nacional de Proteção de Dados Pessoais (SINPRODAP/MP), cujo objetivo primordial é conceder ao Ministério Público a função de tutelar de forma abrangente os dados pessoais, assegurando o direito à autodeterminação informativa frente a infrações externas, bem como a conformidade dos órgãos internos com as normativas que orientam a Política Nacional de Proteção de Dados Pessoais na instituição.

Os Comitês Estratégicos de Proteção de Dados Pessoais (CEPDAP) integram o SINPRODAP, sendo presididos pelos Encarregados de Proteção de DaDos e tendo como missão coordenar a criação e atualização do Plano Diretor de Proteção de Dados Pessoais. O CEPDAP do MPPI foi estabelecido pela Portaria n ° 1386/2024

No desenvolvimento do Plano Diretor de Proteção de Dados Pessoais do MPPI, serão seguidas as práticas e a governança recomendadas que definem a estrutura organizacional, métodos de operação, processos (inclusive os que envolvem queixas e solicitações de titulares de dados), protocolos de segurança, critérios técnicos, encargos específicos dos participantes no processo de tratamento de dados, atividades educativas, métodos internos de controle e redução de riscos, entre outras questões inerentes ao tratamento de informações pessoais, em consonância com o disposto na Resolução CNMP 281/23.

2. TERMOS E ABREVIATURAS

Quadro 1 - Termos e Descrições

SIGLA	DESCRIÇÃO
APDP/MP	Autoridade de Proteção de Dados Pessoais do Ministério Público.
MPPI	Autoridade Nacional de Proteção de Dados Pessoais.
CEPDAP	Comitê Estratégico de Proteção de Dados Pessoais.
CNMP	Conselho Nacional do Ministério Público.
CONEDAP	Comitê Nacional de Encarregados de Proteção de Dados Pessoais.
LGPD	Lei Geral de Proteção de Dados Pessoais.
RIDP	Relatório de Impacto à Proteção de Dados Pessoais.
SEPRODAP	Secretaria Executiva de Proteção de Dados Pessoais.
SINPRODAP/MP	Sistema Naci'onal de Proteção de Dados Pessoais do Ministério Público.
CEAF	Centro de Estudos e Aperfeiçoamento Funcional.
PROCON	Programa Estadual de Proteção e Defesa do Consumidor.
GSI	Gabinete de Segurança Institucional.
CTI	Coordenadoria de Segurança da Informação.
TCMS	Termo de Compromisso de Manutenção de Sigilo.
LAI	Lei de Acesso à Informação.
PDPD	Plano Diretor de Proteção de Dados.

Elaborado pelos autores.

3. METODOLOGIA APLICADA

O processo de formulação do Plano teve início com a exposição, por parte da Encarregada de Dados, das metas centrais que o Comitê Estratégico de Proteção de Dados (CEPDAP) almejava alcançar no biênio 2024-2025. Após a assimilação das diretrizes básicas do CEPDAP, procedeu-se com uma análise de cenário adotando-se a ferramenta SWOT. Seguiu-se então à deliberação dos objetivos de contribuição, à composição do portfólio de ações e à seleção das iniciativas/projetos, tudo isso levando em conta os desfechos da SWOT e as orientações contidas na Resolução CNMP 281/23.

Figura 1 - Produtos do Plano Diretor do Comitê Estratégico de Proteção de Dados

Elaborada pelos autores.

É imprescindível sublinhar que, conforme característica de qualquer planejamento, o Plano Diretor do Comitê Estratégico de Proteção de Dados 2024-2025 é um esquema adaptável, passível de modificação, seja em relação ao escopo ou ao cronograma de execução das ações e dos projetos iniciados. Por essa razão, foi planejada uma revisão no término do último trimestre do ano inicial de implementação, momento oportuno para avaliar o progresso obtido e ajustar o portfólio de ações para acompanhar a conjuntura do ano seguinte. Revisões excepcionais também estão previstas, caso novas circunstâncias surjam e impactem significativamente o desenvolvimento do Plano.

4. DOCUMENTOS DE REFERÊNCIA

Os documentos utilizados para subsidiar a elaboração deste PDPDP estão expostos na tabela a seguir.

Quadro 2 - Documentos de referência para a elaboração do PDPDP.

ID	LEI/DECRETO	DESCRIÇÃO
DR01	Lei n° 12.527/2011 (Lei de Acesso à Informação).	Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
DR02	Decreto n° 7.724/2012	regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
DR03	Lei n° 12.965/2014 (Marco Civil da Internet)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
DR04	Decreto n° 8.771/2016	Regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações;
DR05	Lei n° 13.709/2018, Lei Geral de Proteção dos Dados – LGPD	Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;
DR06	Lei n° 13.853/2019	Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados;
DR07	Resolução n. 64/10 - CNMP	Determina a implantação das Ouvidorias no Ministério Público dos Estados, da União e no âmbito do Conselho Nacional do Ministério Público;

ID	LEI/DECRETO	DESCRIÇÃO
DR08	ATO/PGJ/PI 1282/23	Institui a Política de Privacidade de Dados do MPPI;
DR09	Resolução 281/23 - CNMP	Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público;
DR10	Guias, manuais, processos e metodologias.	Guia de elaboração de Programa de Governança em Privacidade; Guia de Elaboração de Inventário de Dados Pessoais; Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos; Guia de Elaboração de Avaliação de Riscos; Guia de elaboração de Requisitos e Obrigações quanto a Segurança da Informação e Privacidade; Guia de Elaboração de Impacto de Proteção de Dados – RIPD; Guia do Framework de Segurança; Manual de Referência de Planos Diretores do CNMP;
DR11	Melhores práticas de gestão e governança de Dados e TI.	ISO/IEC 27001. ISO/IEC 272002.
DR12	Decreto n. 9.637/18	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
DR13	DECRETO Nº 11.856, DE 26 DE DEZEMBRO DE 2023	Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança;
DR14	Lei n° 9.507/1997	Regula o direito de acesso a informações e disciplina o rito processual do habeas data;
DR15	Lei n° 9.784/1999	Regula o processo administrativo no âmbito da Administração Pública Federal;
DR16	Lei n° 14.534/23	Determina o CPF como número único e suficiente para identificação do cidadão nos bancos de dados de serviços públicos;

Elaborado pelos autores.

5. PRINCÍPIOS E DIRETRIZES

Os princípios representam os valores e preceitos do PDPDP, determinando o ponto de partida para o planejamento. Por sua vez, as diretrizes definem os caminhos e estabelecem as estratégias que devem ser dotados para alcançar os objetivos do PDPDP. Os princípios e as diretrizes norteadores para a elaboração deste PDPGPDP estão expostos, respectivamente, nos Quadros 3 e 4.

Quadro 3 - Princípios do PDPDP

ID	PRINCÍPIO	ORIGEM
PR01	Legalidade	Constituição da República Federativa do Brasil.
PR02	Impessoalidade	Constituição da República Federativa do Brasil.
PR03	Moralidade	Constituição da República Federativa do Brasil.
PR04	Publicidade.	Constituição da República Federativa do Brasil.
PR05	Eficiência.	Constituição da República Federativa do Brasil.
PR06	Finalidade.	Lei 13709/18 –LGPD.
PR07	Adequação.	Lei 13709/18 –LGPD.
PR08	Necessidade.	Lei 13709/18 –LGPD.
PR09	Livre acesso.	Lei 13709/18 –LGPD.
PR10	Qualidade dos dados.	Lei 13709/18 –LGPD.
PR11	Transparência.	Lei 13709/18 –LGPD.
PR12	Segurança.	Lei 13709/18 –LGPD.
PR13	Prevenção.	Lei 13709/18 –LGPD.
PR14	Não discriminação.	Lei 13709/18 –LGPD.
PR15	Responsabilização e prestação de contas.	Lei 13709/18 –LGPD.
PR16	Proporcionalidade e razoabilidade.	Resolução CNMP n. 281/23.
PR17	Vedação da proteção insuficiente na tutela dos direitos fundamentais.	Resolução CNMP n. 281/23.

Elaborado pelos autores.

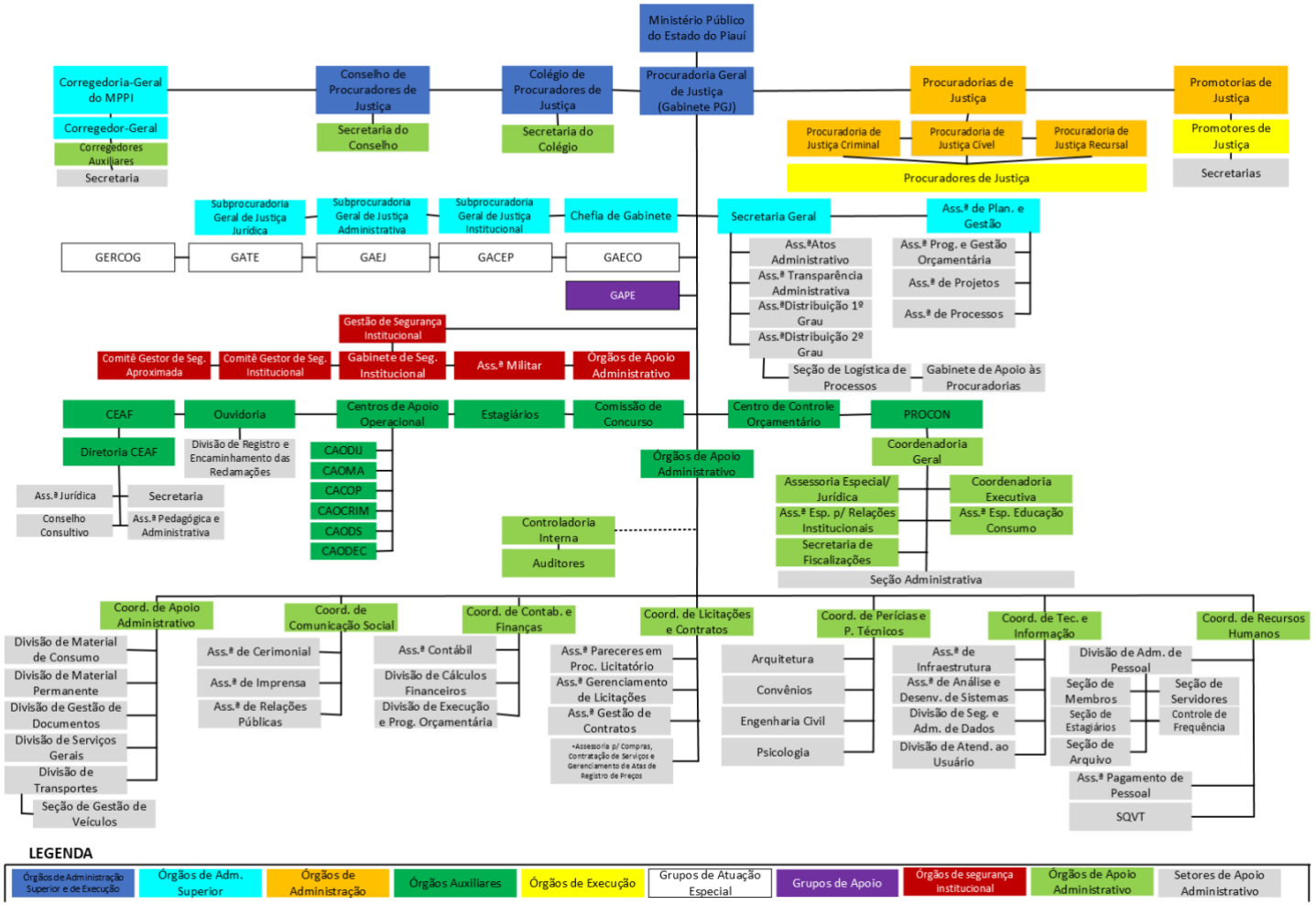
Quatro 4 - Diretrizes do PDPDP

ID	DIRETRIZ	ORIGEM
DI01	Assegurar que o MPPI, no pleno exercício de suas atividades e na defesa do regime democrático e da ordem jurídica, em especial quanto à tutela dos direitos fundamentais, realize o tratamento de dados pessoais de forma a conciliar o dever de transparência e o interesse público com a proteção da intimidade e da vida privada.	Resolução 281/23 do CNMP
DI02	Instituir, no âmbito do MPPI, estruturas especializadas, procedimentos e medidas necessárias para a conciliação da imprescindibilidade de tratamento de dados pessoais, a autodeterminação informativa e a proteção à privacidade e à intimidade a eles inerentes.	Resolução 281/23 do CNMP

ID	DIRETRIZ	ORIGEM
DI03	Disseminar a cultura de proteção de dados pessoais, com o objetivo de promover a conscientização sobre os riscos derivados do tratamento e formas de minimizá-lo em diferentes ambientes, especialmente tecnológicos.	Resolução 281/23 do CNMP
DI04	Fomentar a capacitação contínua de membros e servidores quanto à proteção de dados pessoais em diferentes relações sociais e garantir acesso ao conhecimento necessário ao manejo de medidas administrativas e judiciais adequadas para a tutela integral de direitos violados ou ameaçados.	Resolução 281/23 do CNMP
DI05	Promover o aprimoramento contínuo de mecanismos de proteção de dados pessoais, inclusive nos campos do planejamento, governança, administração de processos e procedimentos, elaboração de normas, rotinas operacionais, práticas organizacionais, desenvolvimento e gestão de sistemas de informação e relação com a imprensa.	Resolução 281/23 do CNMP
DI06	Aprimorar a Governança de dados, para que o Ministério Público concretize a tutela do direito fundamental à proteção de dados pessoais por meio de seus órgãos de execução, nas hipóteses de lesão ou ameaça de lesão ocasionadas por pessoa natural ou pessoa jurídica de direito público ou privado, independentemente do meio, de sua sede ou do país onde estejam localizados os dados pessoais, consoante a legislação vigente.	Resolução 281/23 do CNMP

Elaborado pelos autores.

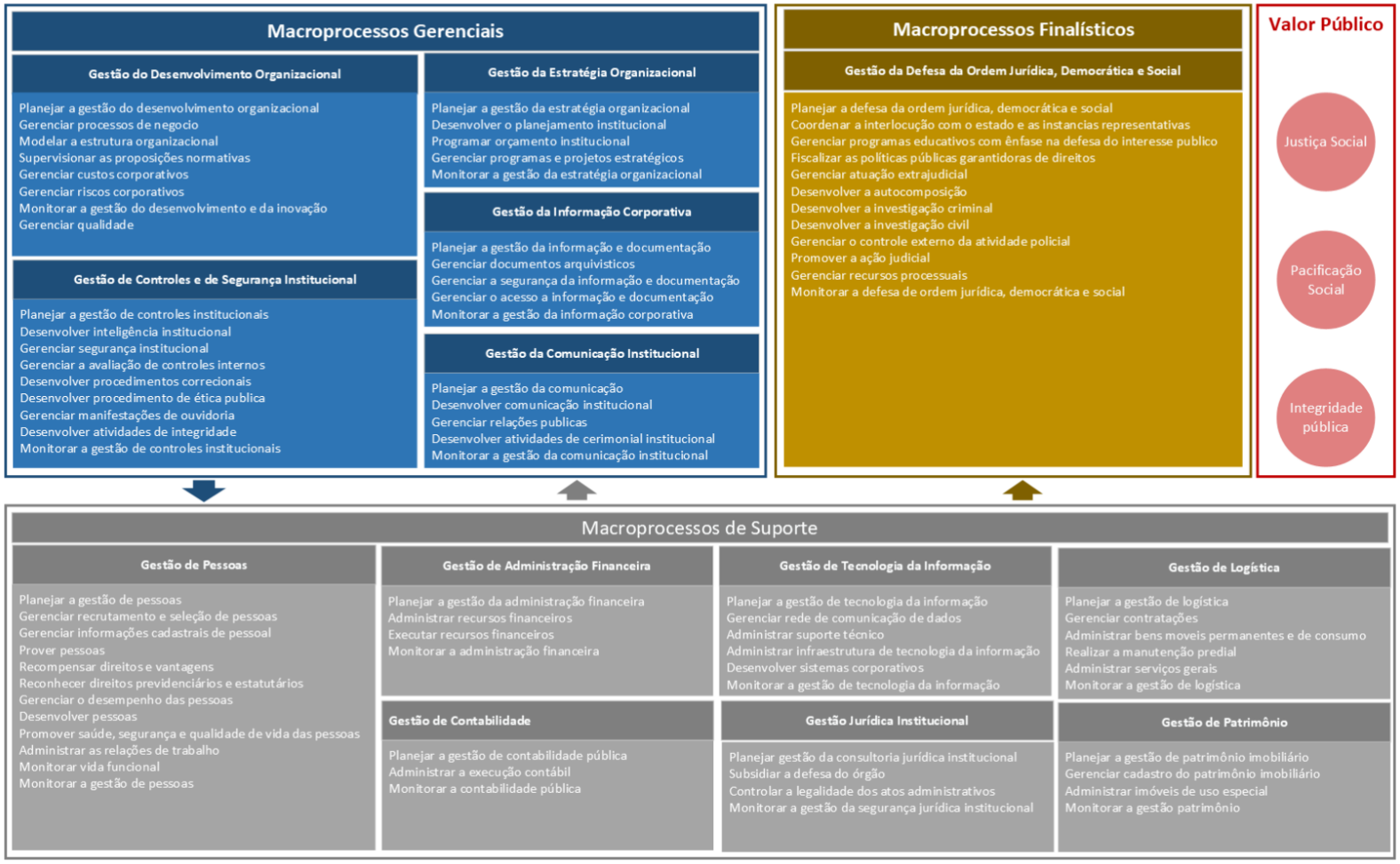
Figura 2 - Organograma da Estrutura Organizacional do MPPI



Fonte: Assessoria de Planejamento e Gestão

Figura 3 – Diagrama de Cadeia de Valor

PROCESSOS DE TRABALHO ESTRUTURADOS EM DIAGRAMA DE CADEIA DE VALOR



Fonte: Assessoria de Planejamento e Gestão

6. DO COMITÊ ESTRATÉGICO DE PROTEÇÃO DE DADOS PESSOAIS

O Comitê Estratégico de Proteção de dados Pessoais-CEPDAP é órgão colegiado de natureza permanente, subordinado à Chefia da Instituição. O CEPDAP compõe a estrutura do Sistema Nacional de Proteção de Dados Pessoais - SINPRODAP, sendo de observância obrigatória pelas Unidades do Ministério Público, de acordo com o artigo 49 da resolução 281/23. Inclui, também, em seu escopo de atuação, monitorar a execução do Plano Diretor de Proteção de Dados Pessoais e adotar as providências necessárias à sua implementação e ao seu cumprimento.

6.1. Atribuições

I - Oferecer diretrizes ao controlador e ao encarregado no que se refere à proteção e governança de dados pessoais;

II - Sugerir as prioridades dos investimentos na área de proteção de dados pessoais para avaliação e decisão pela Chefia da Instituição;

III - Liderar o processo de criação e atualização do Plano Diretor de Proteção de Dados Pessoais;

IV - Supervisionar a implementação do Plano Diretor de Proteção de Dados Pessoais, bem como a execução das medidas necessárias para sua efetivação;

V - Realizar diagnósticos, pesquisas e avaliações contínuas relacionadas ao Plano Diretor de Proteção de Dados Pessoais;

VI - Emitir parecer sobre a criação, revisão, aprovação e divulgação de Relatórios de Impacto à Proteção de Dados Pessoais;

VII - Desenvolver mecanismos e instrumentos para a investigação e prevenção de incidentes de segurança que envolvam dados pessoais, além do manejo de informação confidencial comprometida que diz respeito a dados pessoais;

VIII - Propor critérios relacionados à divulgação dos atos que abarquem a exibição de dados pessoais sob a guarda do Ministério Público;

IX - Assessorar sobre outras matérias que concernem à proteção de dados pessoais.

6.2. Recursos Humanos

Conforme previsto no artigo 49 da Resolução CNMP 281/23, o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) terá a seguinte composição:

I - O encarregado da proteção de dados pessoais que atuará como presidente do Comitê;

II - Um membro indicado pela Corregedoria-Geral;

III - Um membro ou servidor indicado pela Ouvidoria;

IV - O Secretário-Geral ou uma posição equivalente dentro da estrutura organizacional;

V - O Coordenador de Segurança Institucional ou um cargo equivalente;

VI - O Chefe da Secretaria de Tecnologia da Informação ou posição equivalente.

7. RESULTADOS DO PLANO DIRETOR

Este Plano Diretor é inédito no âmbito do MPPI e seu processo de elaboração envolveu a atuação de uma equipe multidisciplinar, sendo o apoio da equipe da Assessoria de Planejamento e gestão, em diferentes momentos, fundamental para que os resultados fossem obtidos.

Em termos de planejamento, o PDPDP, por meio de etapas lógicas e sucessivas, busca subsidiar o programa em privacidade do MPPI e nortear o desenvolvimento de suas atividades de forma eficiente e alinhada aos objetivos da Instituição. Por fim, com o PDPDP busca-se aprimorar os processos internos da unidade ao longo dos anos de 2024 e 2025, sem perder de vista o planejamento institucional do MPPI.

8. DIAGNÓSTICO DA UNIDADE

A concepção de um planejamento estratégico eficaz demanda um entendimento detalhado tanto da organização em análise quanto do ambiente em que ela opera. Nessa perspectiva, o estágio diagnóstico deste Plano Diretor visou discernir a condição vigente da Comissão Estratégica de Proteção de Dados, e, dentro desse contexto, identificar áreas suscetíveis a melhorias e oportunidades que podem ser capitalizadas.

Empregou-se como metodologia a análise SWOT, um acrônimo do inglês para Strengths (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças). Este modelo divide-se em elementos internos - Forças e Fraquezas - e elementos externos - Oportunidades e Ameaças.

Através desta técnica, foi possível realizar a interseção dos fatores internos e externos, oriundos dela emergem quatro estratégias distintas:

- **Expansão** – com o predomínio dos elementos Forças e Oportunidades, a organização deve alavancar suas vantagens intrínsecas para maximizar o aproveitamento das oportunidades detectadas.

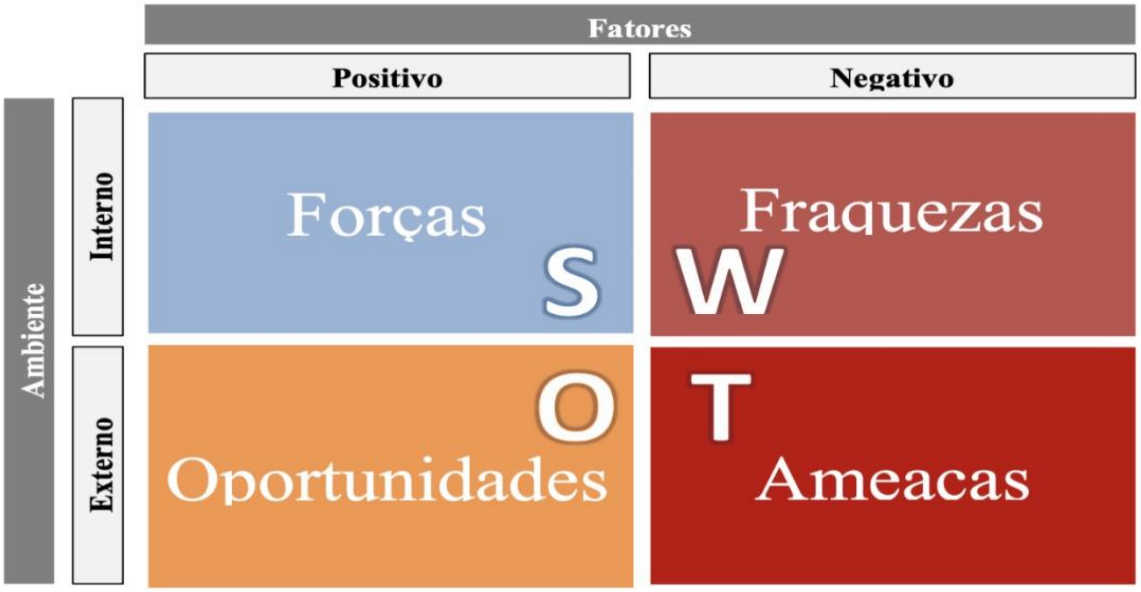
- **Incremento** – quando Fraquezas e Oportunidades são predominantes, a organização necessita atenuar os efeitos prejudiciais de suas deficiências internas enquanto capitaliza as oportunidades disponíveis.

- **Resiliência** – em um contexto em que Forças e Ameaças sobressaem-se, é imperativo que a organização utilize suas vantagens para diminuir o impacto das ameaças identificadas.

- **Contenção** – caracterizado pela preponderância de Fraquezas e Ameaças, este é considerado o cenário mais desafiador. Aqui, o foco da organização deve ser a implementação de medidas mitigadoras que possam reduzir suas vulnerabilidades internas e enfrentar as ameaças externas.

Ao empregar a análise SWOT, a Comissão Estratégica de Proteção de Dados Pessoais está equipada não apenas para compreender melhor sua posição atual, mas também para desenvolver estratégias que reforcem suas competências e garantam uma gestão ambiental eficaz e adaptável aos desafios futuros.

Figura 4 – Modelo da Matriz SWOT



Fonte: Elaborado pelos autores.

8.1. Construção da Matriz SWOT

Conforme estabelecido pela metodologia adotada, realizou-se uma análise detalhada das forças e fraquezas inerentes ao ambiente interno, bem como das oportunidades e ameaças presentes no contexto externo relacionado à Comissão Estratégica de Proteção de Dados Pessoais. No âmbito externo, foram consideradas todas as variáveis que escapam ao seu controle e autoridade direta, tais como outras áreas e órgãos do MPPI.

Para elaboração da matriz, foi conduzida uma oficina com a participação ativa da equipe vinculada à Comissão Estratégica de Proteção de Dados Pessoais, incluindo servidores e

membros. Inicialmente, os participantes, individualmente, registraram os fatores que julgaram relevantes a cada aspecto da matriz SWOT. Posteriormente, os integrantes da Comissão discutiram e sintetizaram os pontos levantados em afirmações concisas.

Após esse processo, os participantes foram solicitados a priorizar cada uma das assertivas elencadas, empregando um questionário no qual se atribuía uma importância a cada item, numa escala de 1 a 5, onde 1 denota "pouco importante" e 5 indica "muito importante".

Os resultados desse levantamento, que se alinham à análise SWOT realizada pela Comissão Estratégica de Proteção de Dados Pessoais, estão apresentados a seguir, organizados de maneira a refletir a ordem decrescente de prioridade das assertivas:

Quadro 5 – Variáveis identificadas na aplicação da SWOT

AMBIENTE INTERNO	
FORÇAS	**FATOR**
Criação recente: Permite a implementação de um plano estratégico desde o início, sem vícios institucionais.	5,0
Composto por membros experientes: Assegura conhecimento técnico e prático na área de proteção de dados.	4,75
Apoio da alta cúpula do MPPI: Demonstra compromisso com a temática e facilita a obtenção de recursos.	5,0
Existência da Lei Geral de Proteção de Dados (LGPD): Fornece um marco legal robusto para embasar as ações do CEPDAP.	4,5
Resolução CNMP 281/23: Diretrizes específicas para a atuação do MP na proteção de dados.	4,5
FRAQUEZAS	**FATOR**
Falta de histórico de atuação: Dificulta a avaliação da efetividade das ações do CEPDAP.	4,0
Desafios na implementação da LGPD: Complexidade da lei e da sua aplicação prática.	4,0
Baixo nível de conhecimento da LGPD no MP: Exige investimento em treinamento e capacitação.	4,75
Falta de cultura de proteção de dados no MP: Necessidade de mudança de mentalidade e hábitos.	4,75
AMBIENTE EXTERNO	
OPORTUNIDADES	**FATOR**
Fortalecer a imagem do MP como defensor da proteção de dados: Ganhar a confiança da sociedade e dos órgãos de controle.	5,0
Atuar como referência em proteção de dados para outros órgãos públicos: Compartilhar conhecimento e boas práticas.	5,0

Promover a cultura de proteção de dados no MP: Através de campanhas de conscientização e treinamentos.	4,75
Desenvolver parcerias com outras instituições: Ampliar a capacidade de atuação do CEPDAP.	5,0
Captar recursos externos: Financiar projetos e ações estratégicas.	4,75
AMEAÇAS	**FATOR**
Mudanças na legislação de proteção de dados: Alterações legais e regulamentares que podem surgir, tornando o cenário da proteção de dados mais complexo e desafiador.	4,5
. **Resistência à mudança:** Dificulta a implementação da cultura de proteção de dados.	4,75
Novas e cada vez mais sofisticadas técnicas de ataques cibernéticos que ameaçam a segurança da informação.	4,0
Cortes no orçamento do MP: Podem comprometer a viabilidade das ações do CEPDAP..	5,0
Ações judiciais contra o MP: Risco de danos à reputação da instituição.	4,5
Reconhecimento e cooperação dos órgãos externos ao MP	

Após a tabulação das médias das notas atribuidas, estabeleceu-se uma correlação com os elementos da matriz SWOT, com o objetivo de identificar os fatores mais significativos na unidade e, por conseguinte, determinar a estratégia metodologica que melhor se alinha ao cenario vigente.

A partir deta analise, constatou-se que a maior pontuacao corresponde à intersecção das Strengths (forças) com Opportunities (oportunidades), indicando, portanto, que, com base na abordagem SWOT, a estratégia de Desenvolvimento é a mais pertinente. Assim, sugere-se que a unidade se empenhe na aplicação de suas forças como meio de maximizar as oportunidades identificadas.

9. OBJETIVO DE CONTRIBUIÇÃO

Os objetivos de contribuição de qualquer comissão ou departamento dentro de uma organização, como a Comissão Estratégica de Proteção de Dados Pessoais, são fundamentais para assegurar que as ações da comissão estejam alinhadas com as metas e estratégias globais do Ministério Público do Estado do Piauí (MPPI).

A definição desses objetivos geralmente segue um processo estruturado:

1. **Análise da Matriz SWOT**: Inicialmente, a comissão avalia seus pontos fortes, pontos fracos, oportunidades e ameaças para entender melhor em que condição se encontra atualmente e quais são as perspectivas para o futuro. Com base nessa análise, a comissão pode determinar quais áreas necessitam de mais atenção e onde estão as maiores chances de fazer contribuições significativas.

2. **Mapa Estratégico**: Este é um instrumento de gestão que traduz a estratégia da organização em objetivos interconectados, permitindo uma visualização clara das relações de causa e efeito entre eles. A comissão usará o mapa estratégico do MPPI para garantir que suas ações apoiem os objetivos mais amplos da organização de uma maneira coordenada e coesa.

3. **Compatibilização com as Necessidades Internas**: Os objetivos selecionados devem ser não apenas alinhados com a estratégia geral do MPPI, mas também devem levar em consideração as necessidades e capacidades internas da própria comissão. Isto é particularmente importante para maximizar a eficiência e eficácia das ações planejadas.

4. **Conformidade com as Diretrizes Externas**: No caso mencionado, os objetivos escolhidos estão alinhados com a Resolução CNMP 281/2023, que dita diretrizes relevantes para questões de proteção de dados pessoais. Esta conformidade com normativas externas assegura que a atuação da comissão esteja dentro dos parâmetros da regulação e legislação vigentes.

Com todos esses fatores considerados, a Comissão Estratégica de Proteção de Dados Pessoais do MPPI estabeleceu os seguintes objetivos de contribuição:

1. Estabelecer uma Estrutura de Governança de Dados Robusta:

Objetivo: Construir e manter um sistema de governança de dados pessoais capaz de assegurar que todas as atividades de tratamento estejam em conformidade com a LGPD e com a Resolução CNMP nº 281/23, enfatizando a responsabilidade e a transparência institucional.

2. Definir e Implementar Procedimentos Operacionais Claros:

Objetivo: Desenvolver e documentar procedimentos internos padronizados para o tratamento de dados pessoais, incluindo o recebimento e processamento de reclamações e petições dos titulares, garantindo a sua resolução eficaz e eficiente.

3. Assegurar Conformidade com as Normas de Segurança:

Objetivo: Assegurar que as normas técnicas e padrões de segurança estejam plenamente integrados, eficazes e atualizados, protegendo os dados pessoais contra acessos não autorizados, perdas ou divulgações indevidas.

4. Estabelecer Obrigações Específicas para os Agentes de Tratamento:

Objetivo: Definir e comunicar as responsabilidades específicas de cada um dos envolvidos no tratamento de dados, desde seu manuseio até sua eliminação, promovendo uma cultura de privacidade e proteção de dados em todas as esferas da organização.

5. Impulsionar Iniciativas de Educação e Treinamento:

Objetivo: Desenvolver e implementar um programa de treinamento contínuo e educação em proteção de dados para membros e servidores, elevando a consciência sobre a importância da privacidade e fomentando práticas seguras no tratamento de dados.

6. Implantar Mecanismos de Supervisão Interna:

Objetivo: Estabelecer mecanismos internos de supervisão eficientes para monitorar e avaliar continuamente as práticas de tratamento de dados, identificando e endereçando proativamente as vulnerabilidades e possíveis não conformidades.

7. Desenvolver e Refinar Estratégias de Mitigação de Riscos:

Objetivo: Implementar uma abordagem sistemática de avaliação de riscos e desenvolver estratégias proativas para mitigar potenciais impactos adversos do tratamento de dados pessoais, incluindo a realização de Avaliações de Impacto à Proteção de Dados (AIPD).

8. Promover uma Cultura de Melhoria Contínua:

Objetivo: Encorajar e adotar uma cultura de melhoria contínua através da reavaliação regular das práticas de tratamento de dados, visando a optimização dos processos e elevação dos padrões de privacidade e segurança da informação.

Os objetivos apresentados abarcam uma estratégia integral para fortalecer a proteção de dados dentro da organização, ancorados nas melhores práticas e exigências regulatórias. A postura proativa e de liderança em privacidade não apenas atende à legislação, mas também posiciona a instituição como referência em respeito à privacidade e direitos dos cidadãos.

10. PRIORIZAÇÃO DAS AÇÕES

A conclusão do processo de análise e priorização das ações vai determinar quais iniciativas o Ministério Público do Estado do Piauí (MPPI) precisará implementar com maior rigor para cumprir com as exigências legais relacionadas à proteção de dados pessoais e à privacidade. O uso da matriz GUT é fundamental para organizar e dar sentido de urgência e gravidade às diversas atividades.

O portfólio de ações elaborado pelo MPPI, utilizando a matriz GUT, estabelecerá a ordem de importância dos projetos que deverão ser executados. Embora a descrição do portfólio de ações não esteja completa na sua pergunta, é possível inferir que as ações definidas estarão direcionadas para cumprir os objetivos específicos já mencionados e garantir que o MPPI esteja em conformidade com a legislação aplicável.

Cada ação planejada deve ser acompanhada por iniciativas e/ou projetos detalhados nos planos de gestão anuais. Eles deverão incluir medidas específicas, como a revisão de processos internos, a adoção de novas tecnologias e sistemas de segurança da informação, programas de treinamento e conscientização, revisão de políticas de privacidade, entre outros.

O sucesso das ações selecionadas dependerá fortemente do comprometimento e apoio das lideranças, da suficiência de recursos alocados, e da habilidade da equipe do MPPI em executar as medidas necessárias de forma efetiva.

A priorização considera o impacto de não realizar uma ação (Gravidade), o quão rapidamente essa ação precisa ser feita (Urgência) e o quão pior a situação pode se tornar se a ação for adiada (Tendência). Ações com maior pontuação na matriz GUT indicam tópicos que requerem atenção imediata e, portanto, devem ser encaradas como as mais críticas no planejamento.

Espera-se que, através desse processo, o MPPI possa não apenas atender as regulamentações, mas também estabelecer um sistema robusto de proteção de dados que assegure a privacidade e confiança de todas as partes interessadas, incluindo o público em geral, funcionários e parceiros. A Matriz GUT é uma ferramenta de gestão que auxilia na priorização de problemas ou projetos com base em três critérios:

Gravidade (G), Urgência (U) e Tendência (T). Cada critério é avaliado numa escala de 1 (menos grave, urgente ou tendencioso) a 5 (mais grave, urgente ou tendencioso), e o projeto com a maior pontuação total deve ser tratado primeiro.

Para montar o portfólio de ações utilizando a Matriz GUT com base nos objetivos de contribuição estabelecidos, vamos pontuar cada um dos objetivos segundo os critérios mencionados e depois calcular a pontuação final.

10.1 Do Portfólio de Ações

1. Estabelecer uma Estrutura de Governança de Dados Robusta:

Priorização de Ações:

- Nomear um Encarregado de Dados (Data Protection Officer – DPO) com profundo conhecimento regulatório e técnico.
- Criar um comitê de governança de dados com representantes de todos os departamentos relevantes.
- Mapear os processos de tratamento de dados existentes e identificar os riscos associados a eles.
- Desenvolver políticas e procedimentos abrangentes de proteção de dados e privacidade, incluindo um manual de governança.

2. Definir e Implementar Procedimentos Operacionais Claros:

Priorização de Ações:

- Documentar todos os processos de tratamento de dados de forma clara e acessível.
- Estabelecer um canal transparente e eficiente para a comunicação de reclamações e petições dos titulares.
- Treinar a equipe responsável pelo atendimento aos titulares para garantir a consistência e qualidade das respostas.
- Monitorar continuamente a eficácia dos procedimentos implementados, ajustandoos conforme necessário.

3. Assegurar Conformidade com as Normas de Segurança:

Priorização de Ações:

- Realizar uma auditoria de segurança de dados para identificar vulnerabilidades.
- Implementar medidas de segurança baseadas na Análise de Impacto sobre a Proteção de Dados (AIPD).
- Definir e testar um plano de resposta a incidentes de segurança.
- Realizar atualizações e treinamentos regulares em segurança da informação.

4. Estabelecer Obrigações Específicas para os Agentes de Tratamento:

Priorização de Ações:

- Desenvolver um código de conduta detalhando as obrigações de cada agente de tratamento.

- Firmar acordos de nível de serviço (SLAs) e termos de processamento de dados com terceiros.

- Realizar auditorias regulares de conformidade dos processos de tratamento interno e terceirizado.

- Estabelecer um sistema de responsabilidade e relato com repercussões para casos de não conformidade.

5. Impulsionar Iniciativas de Educação e Treinamento:

Priorização de Ações:

- Definir um currículo abrangente de treinamento em proteção de dados.
- Realizar sessões de treinamento regulares e adaptáveis aos diversos papéis dos colaboradores.
- Desenvolver materiais de conscientização (cartilhas, vídeos, etc.).
- Avaliar periodicamente a eficácia do treinamento e atualizá-lo conforme necessário.

6. Implantar Mecanismos de Supervisão Interna:

Priorização de Ações:

- Definir indicadores-chave de desempenho (KPIs) para monitorar a conformidade de proteção de dados.
- Estabelecer rotinas de revisão e auditoria dos processos de tratamento de dados.
- Utilizar ferramentas de monitoramento em tempo real para detectar quaisquer atividades anômalas.
- Gerar relatórios regulares de supervisão para a alta gestão e partes interessadas.

7. Desenvolver e Refinar Estratégias de Mitigação de Riscos:

Priorização de Ações:

- Implementar uma metodologia padronizada para a realização de Avaliações de Impacto à Proteção de Dados (AIPD).
- Desenvolver estratégias de mitigação personalizadas para cada risco identificado.
- Garantir a integração da gestão de riscos no ciclo de vida de projetos e processos.

- Estabelecer um processo de revisão e atualização contínua das estratégias de mitigação de riscos.

8. Promover uma Cultura de Melhoria Contínua:

Priorização de Ações:

- Criar um ambiente onde o feedback é valorizado e utilizado para a melhoria contínua.
- Incentivar a inovação e a adoção de melhores práticas e tecnologias emergentes em proteção de dados.
- Revisar e atualizar periodicamente as políticas e procedimentos de proteção de dados.
- Reconhecer os esforços bem-sucedidos e as contribuições individuais para fortalecer a cultura da proteção de dados.

A execução coordenada destas ações priorizadas, aliada a um compromisso com a responsabilidade e transparência, garantirá que a organização não apenas atenda às exigências da Resolução CNMP nº 281/23, mas também estabeleça um padrão de excelência em proteção de dados pessoais.

Para facilitar a priorização e execução das ações para cada um dos objetivos mencionados, pode-se utilizar a matriz GUT, que é um método de priorização de problemas ou ações que considera a Gravidade, a Urgência e a Tendência (GUT) de cada situação.

A seguir está uma representação da tabela GUT para a priorização de ações dentro de cada objetivo, levando em conta a Resolução CNMP nº 281/23. Cada ação será avaliada quanto à Gravidade (G), à Urgência (U) e à Tendência (T), em uma escala de 1 (menos crítico) a 5 (mais crítico). O resultado GUT é calculado multiplicando-se estes três valores (G x U x T), e as ações são priorizadas de acordo com os maiores resultados obtidos.

Quadro 6 - Representação da tabela GUT para a priorização de ações dentro de cada objetivo

OBJETIVO DE CONTRIBUIÇÃO	AÇÕES DE PRIORIZAÇÃO	G	U	T	GUT
Estrutura de Governança de Dados Robusta	Mapear riscos	5	4	5	100
	Desenvolver políticas	4	3	4	48
Procedimentos Operacionais Claros	Documentar processos	4	4	3	48
	Canal de comunicação	3	5	3	45
	Treinar equipe	4	4	4	64
	Monitorar procedimentos	3	3	4	38
Conformidade com Segurança	Auditoria de segurança	5	5	5	125
	AIPD e medidas de segurança	5	4	4	80
	Plano de resposta a incidentes	4	5	4	80
	Atualizações e treinamentos	3	4	5	60

OBJETIVO DE CONTRIBUIÇÃO	AÇÕES DE PRIORIZAÇÃO	G	U	T	GUT
Obrigações para Agentes de Tratamento	Código de conduta	4	3	4	48
	SLAs e termos	3	4	3	36
	Auditorias	4	4	4	64
	Sistemas de Responsabilidades	5	4	4	80
Educação e Treinamento	Currículo de treinamento	4	3	4	48
	Sessões de treinamento	3	4	3	36
	Materiais de conscientização	3	3	4	36
	Avaliar eficácia do treinamento	4	4	4	64
Mecanismos de Supervisão Interna	Definir KPIs	4	4	5	80
	Rotinas de revisão	4	3	4	48
	Monitoramento em tempo real	5	5	5	125
	Gerar relatórios	3	3	3	27
Estratégias de Mitigação de Riscos	AIPD padronizada	5	4	5	100
	Estratégias de mitigação	5	4	4	80
	Integração da gestão de riscos	4	3	4	48
	Revisão de estratégias	3	5	4	60
Cultura de Melhoria Contínua	Feedback e melhoria	3	4	3	36
	Incentivar inovação	3	4	3	36
	Revisar políticas	4	2	4	32
	Reconhecer esforços	3	2	3	18

Fonte: Elaborado pelos autores.

A partir dessa tabela, as ações com os maiores resultados GUT devem ser priorizadas. Por exemplo, a nomeação do DPO e o mapeamento de riscos receberam as maiores pontuações e, portanto, deveriam ser tratados como prioridades imediatas. As ações devem ser revistas e a tabela atualizada conforme as circunstâncias mudarem.

11. FATORES CRÍTICOS DE SUCESSO

Os elementos essenciais para assegurar o sucesso na execução do PDPDP são descritos a seguir. Saliente-se que a falta ou presença insuficiente de qualquer um desses itens pode impactar negativamente no desenvolvimento do plano e refletir nas operações do MPPI.

O atendimento integral aos fatores críticos de sucesso listados adiante é considerado crucial para a obtenção dos objetivos do PDPDP:

- ✓ Aprovação do PDPDP;
- ✓ Monitoramento ativo do PDPDP pelo CEPDAP;

- ✓ Revisão sistemática do PDPDP pelo CEPDAP;
- ✓ Divulgação ampla do PDPDP junto ao MPPI e à sociedade;
- ✓ Engajamento da liderança do MPPI;
- ✓ Conscientização das áreas solicitantes sobre a relevância do PDPDP;
- ✓ Disponibilidade de recursos financeiros;
- ✓ Capacitação e dedicação da equipe.

12. CONCLUSÃO

Este documento expressa o planejamento estratégico para as iniciativas de Governança de Dados do MPPI para o biênio 2024-2025, visando atingir as metas institucionais e honrar o compromisso de proteger os dados pessoais geridos pelo MPPI. O PDPDP é, portanto, um documento-chave para a organização e intenta promover o emprego eficiente dos recursos disponíveis em busca de melhores resultados e maior retorno sobre os investimentos em proteção de dados e segurança da informação. Isso, alinhado aos objetivos estratégicos do MPPI, visa também fomentar a transparência em relação às atividades de Governança de Dados. Para tanto, o andamento das ações previstas será continuamente acompanhado ao longo da validade do PDPDP. Ademais, dado o cenário de formação da Comissão Estratégica de Proteção de Dados (CEPDAP), torna-se imprescindível revisar periodicamente este documento durante seu período de aplicação, a fim de ajustar as estratégias às eventuais mudanças de cenário.