Programa de Governança em Privacidade

Ministério da Gestão e da Inovação em Serviços Públicos

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Ministra da Gestão e da Inovação em Serviços Públicos

Esther Dweck

Secretaria Executiva

Cristina Kiomi Mori

Secretaria de Serviços Compartilhados

Cilair Rodrigues de Abreu

Diretoria de Gestão Estratégica

Wanessa Queiroz de Souza Oliveira

Coordenação-Geral de Proteção de Dados Pessoais

Luiz Fernando Bastos Coura
Maria Clara Souza Caribé Frutuoso
Andreia Queiroz Correia Dummar
Lucilene Ferreira da Silva Lopes

Comitê de Proteção de Dados Pessoais:

Autoridade titular da Secretaria-Executiva do MGI
Cristina Kiomi Mori (titular) e Adauto Modesto Júnior (suplente)
Autoridade titular encarregada pela Proteção de Dados Pessoais
Luiz Fernando Bastos Coura (titular) e Maria Clara Souza Frutuoso (suplente)
Gabinete da Ministra – GM
Fernanda Tsunematsu (titular) e Miriam Barbuda Fernandes Chaves (suplente)
Secretaria-Extraordinária para a Transformação do Estado – SETE
Guilherme Alberto Almeida de Almeida (titular) e Renata Bernardo (suplente)
Secretaria de Gestão e Inovação – SEGES
Leandro Bahia (titular) e Rodrigo Morais Lima Delgado (suplente)

Secretaria de Governo Digital – SGD

Leonardo Rodrigo Ferreira (titular) e Loriza Andrade Vaz de Melo (suplente)

Secretaria de Gestão de Pessoas – SGP

Antonio Fiuza de Sousa Landim (titular) e Rogério Mendes Meneguim (suplente)

Secretaria de Relações de Trabalho – SRT

Lair Maria de Oliveira (titular) e Edi Damasceno Maciel (suplente)

Secretaria de Coordenação e Governança das Empresas Estatais – SEST

João Paulo Garrido de Andrade (titular) e Maria Abadia da Silva Alves (suplente)

Secretaria do Patrimônio da União – SPU

Clauber Teixeira Rodrigues (titular) e Ronny Peterson Guimarães (suplente)

Secretaria de Serviços Compartilhados – SSC

Fabio Valotto (titular) e Rudson Pereira Costa da Silva (suplente)

Arquivo Nacional – AN

Alex Pereira de Holanda (titular) e Bruno de Freitas Tavares da Silva (suplente)

Assessoria Especial de Controle Interno – AECI

Francisco Eduardo de Holanda Bessa (titular) e Dilson Gonzaga Pereira Neto (suplente)

Ouvidoria

Ana Carolina Quintanilha dos Santos Loriato (titular) e Rildo Pereira Peixoto (suplente)

Corregedoria

Fernanda Álvares da Rocha (titular) e Anderson Moreno Luz (suplente)

Colaboradores:

Julierme Rodrigues da Silva (SGD)

Marco Antônio Fragoso de Souza (SEST)

Abril de 2024

Sumário

1 PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

1.1 Definição

O Programa de Governança em Privacidade (PGP) está previsto na Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Embora não seja obrigatório, a implementação de um Programa de Governança em Privacidade demonstra interesse do agente de tratamento no estabelecimento de diretrizes que influenciarão a forma com que os dados pessoais serão manuseados durante seu ciclo de vida. Sua elaboração inicia pela captura e consolidação dos requisitos de privacidade e segurança que, após serem levantados, passam por uma análise de maturidade nessa área (*gap analysis*), seguida por uma proposta de plano de ação com expectativas alinhadas com a alta administração.

Abaixo, segue a transcrição de trecho da LGPD relacionado ao conteúdo mínimo de um Programa de Governança em Privacidade (LGPD, Art. 50, § 2º):

> CAPÍTULO VII – DA SEGURANÇA E DAS BOAS PRÁTICAS [...]
> Seção II - Das Boas Práticas e da Governança
> Art. 50 [...]
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I - implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja **aplicável a todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> (BRASIL, 2018, grifos nossos)

Inicialmente, importa destacar, que a natureza de um programa implica em um instrumento perene de articulação de um conjunto de ações passíveis de aferição por indicadores coerentes com o objetivo estabelecido. Nesse sentido, a construção de um PGP representa uma ação institucional de natureza contínua, que traduz uma política de atuação em busca de melhorias no tratamento de dados pessoais do titular.

Embora tenha a natureza de programa, o presente PGP prevê a elaboração de um plano de ações de periodicidade bianual com avaliação e revisão semestrais, conforme detalhado na seção 2.3. Ademais, as ações podem ser desdobradas em projetos direcionados ao alcance dos objetivos do programa.

As ações deste PGP serão conduzidas de forma a possibilitar a gradual harmonização de processos de trabalho e de procedimentos que facilitem e tornem mais eficientes as ações de transparência ativa e passiva do MGI. Assim, não há oposição, mas complementaridade e mútuo fortalecimento dos compromissos institucionais do MGI com a transparência e o atendimento aos pedidos de informação dos cidadãos e o zelo e a proteção dos dados pessoais custodiados pelo Ministério.

1.2 Objetivo

Dessa forma, o presente PGP tem o objetivo de estabelecer metodologia relacionada à área de privacidade e proteção de dados pessoais para influenciar de

forma permanente os processos de tomada de decisão com a finalidade de dar mais transparência, segurança e garantia de direitos aos titulares de dados pessoais tratados pelo MGI.

2 ETAPAS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Figura 1. Etapas do Programa de Governança em Privacidade.

2.1 Iniciação e Planejamento

Como disposto no Guia de Elaboração de Programa de Governança em Privacidade da SGD/MGI (BRASIL. MGI, 2024), a etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que

devem ser conhecidos para início das atividades relacionadas à instituição do Programa de Governança em Privacidade. Assim, o Guia apresenta, conforme figura 2, os sete marcos que constituem essa etapa, que serão detalhados a seguir.

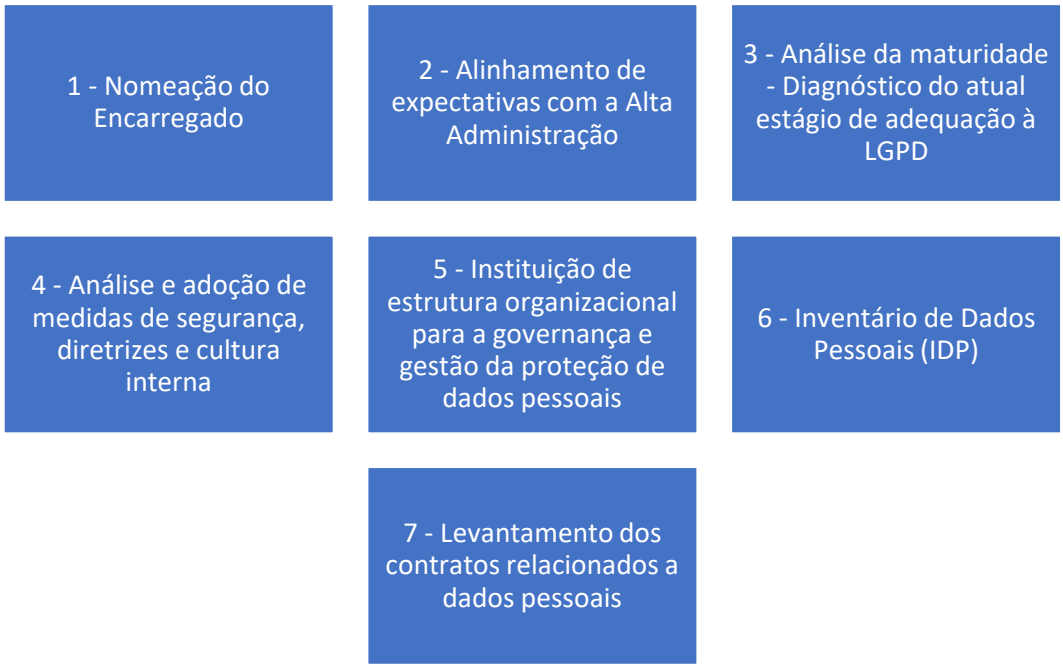

Figura 2. Marcos Etapa Iniciação e Planejamento

2.1.1 O Encarregado

De acordo com o artigo 5°, inciso VIII, da LGPD, o Encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) e, consoante o disposto no artigo 41, parágrafo 2º, da LGPD, as atividades do encarregado consistem em:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados 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 ou estabelecidas em normas complementares.
> (BRASIL, 2018)

Através da Portaria de Pessoal N° 10.906, de 29 de setembro de 2023, houve a designação do Encarregado pelo Tratamento de Dados Pessoais no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos, nos termos do artigo 41 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD).

A indicação do encarregado pelo tratamento de dados pessoais é normatizada pela Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020.

Os dados do encarregado são públicos e estão acessíveis no sítio eletrônico pelo link: https://www.gov.br/gestao/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/privacidade-e-protecao-de-dados-1/privacidade-e-protecao-de-dados.

2.1.2 Alinhamento de expectativas com a Alta Administração

O presente programa foi apresentado ao Comitê de Proteção de Dados Pessoais (CPDP) do MGI – instituído, conforme detalhado na seção 2.1.5, pela Portaria MGI nº 7.601, de 24 de novembro de 2023, (BRASIL. MGI, 2023) – e aprovado por seus membros.

Dessa forma, entende-se que as diretrizes e metodologias aqui apresentadas compreendem direcionamentos da alta administração do MGI em busca de um adequado grau de implementação da LGPD no âmbito do ministério.

Para manutenção desse alinhamento, a criação e revisão dos planos de ação bianuais também passará pelo crivo do CPDP, bem como seu monitoramento semestral.

2.1.3 **Análise da maturidade**

Em outubro de 2023, através de formulário disponibilizado pela SGD/MGI, foi realizado o primeiro passo para o diagnóstico de maturidade do Ministério.

Como ferramenta para análise da maturidade, o questionário apresentou elementos para a formalização e cálculo de um índice de maturidade e as respostas serviram como subsídio para direcionar os esforços e a priorização das ações necessárias para conformidade à Lei Geral de Proteção de Dados Pessoais.

Além disso, a equipe de proteção de dados pessoais também realizou uma nova avaliação de maturidade com base no autodiagnóstico elaborado pelo Tribunal de Contas da União (TCU) resultante do Acórdão nº 1.384/2022 TCU-Plenário (BRASIL. TCU, 2022).

A ideia é que as duas avaliações realizadas sirvam para estabelecer uma linha histórica de comparação com os indicadores de conformidade detalhados na seção 2.3. Ademais, grande parte das ações previstas para o primeiro plano foram previstas como forma de prover a conformidade estrutural ao MGI.

2.1.4 **Análise e adoção de medidas de segurança**

Conforme o caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> (BRASIL, 2018)

Em seu parágrafo 2º, o mencionado artigo salienta que as medidas de segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

> Art. 46 [...]
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
> (BRASIL, 2018)

Privacidade desde a Concepção (do inglês *Privacy by Design*) representa um conceito fundamental para a proteção da privacidade dos dados pessoais, que significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Assim, as ações realizadas e os trabalhos desenvolvidos no âmbito deste Ministério para adequação à LGPD serão construídos seguindo os preceitos do conceito de *Privacy by Design*.

Para ajudar as áreas do ministério a tirarem suas dúvidas com relação à Privacidade desde a Concepção, num primeiro momento, está previsto o lançamento de um guia orientativo com ação cadastrada no Plano de Ações PGP-2024-2025 (disponível no portal do CPDP na internet).

2.1.5 **Instituição de estrutura organizacional para a governança e gestão da proteção de dados pessoais**

O Ministério da Gestão e da Inovação em Serviços Públicos - MGI, por meio da Portaria MGI nº 7.601, de 24 de novembro de 2023, (BRASIL. MGI, 2023) institui seu Comitê de Proteção de Dados Pessoais (CPDP). O objetivo é promover a proteção de dados pessoais e a adequação do ministério à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Compete ao Comitê, entre outros, elaborar o Programa de Governança em Privacidade do MGI; avaliar mecanismos de tratamento e proteção de dados existentes, propor e coordenar iniciativas de melhoria, promover a cultura e conhecimento relativos ao tema; além de assessorar o Comitê Ministerial de Governança.

O Comitê de Proteção de Dados Pessoais é composto pelas autoridades titulares da Secretaria-Executiva do MGI e da área responsável pela Proteção de Dados Pessoais; e representantes do Gabinete da Ministra; da Secretaria Extraordinária para a Transformação do Estado; da Secretaria de Gestão e Inovação; da Secretaria de Governo Digital; da Secretaria de Gestão de Pessoas; da Secretaria de Relações de Trabalho; da Secretaria de Coordenação e Governança das Empresas Estatais; da Secretaria do Patrimônio da União; da Secretaria de Serviços Compartilhados; do Arquivo Nacional; da Assessoria Especial de Controle Interno; da Ouvidoria; e da Corregedoria.

Conforme sua portaria de instituição, as reuniões ordinárias devem ocorrer ao menos duas vezes ao ano, com quórum mínimo da maioria absoluta de membras e membros. As deliberações ocorrem por aprovação de maioria simples, cabendo ao seu Presidente, em caso de empate, o voto de qualidade.

Em relação à estrutura de governança, cabe citar que a portaria que institui o CPDP também ratificou a Resolução CEPPDP/ME nº 6, de 22 de fevereiro de 2022, (BRASIL. ME, 2022 b) a qual trata sobre a estrutura de governança de proteção de dados pessoais no âmbito do MGI. Nessa resolução, são estabelecidos como atores: o titular, o controlador, o Comitê de Proteção de Dados Pessoais, o Comitê Ministerial de Governança, o encarregado pelo tratamento de dados pessoais e o operador. Também são estabelecidos: mecanismo para controladoria conjunta de dados pessoais (Art. 3º, § 1º); atividades do encarregado pela proteção de dados pessoais (Art. 5º); responsabilidade do operador (Art. 6º); entre outras disposições.

Desde sua criação, o MGI vem consolidando sua estrutura de governança, ao instituir o Comitê Ministerial de Governança, o Comitê de Compras e

Contratações Estratégicas, o Comitê de Governança Digital e Segurança da Informação e o Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle e o Subcomitê de Integridade.

Informações sobre o Comitê de Proteção de Dados Pessoais do MGI estão disponíveis no Portal do MGI (gov.br/gestao).

2.1.6 Inventário de Dados Pessoais

O objetivo principal do Inventário de Dados Pessoais (IDP) é documentar o tratamento de dados pessoais realizado pela instituição. De acordo com o art. 37 da LGPD, o "controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem [...]". O inventário de dados pessoais vem atender precisamente essa determinação da LGPD no que se refere à manutenção de registro do levantamento do tratamento de dados pessoais realizados pela instituição.

De forma geral, o registro mantido pelo IDP descreve informações em relação ao tratamento de dados pessoais realizado pelo Ministério, consistindo em fazer um balanço do que é feito com os dados pessoais disponíveis em seus sistemas, identificando os agentes de tratamento, quais dados pessoais são tratados, onde estão armazenados e que operações são realizadas com eles. Atualizado regularmente, o inventário permitirá atender tanto o requisito de manter um registro das operações de tratamento de dados pessoais, quanto o de auxiliar no controle do atendimento aos princípios, ambos estabelecidos pela LGPD.

2.1.7 Levantamento dos contratos relacionados a dados pessoais

A elaboração do Inventário de Dados Pessoais demonstra quais os serviços que tratam dados pessoais e os eventuais operadores desses dados, permitindo relacionar com os contratos que os suportam. Esse mapeamento dos contratos relativos ao tratamento de dados pessoais contribui para possíveis e

necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

Essa ação está prevista no plano de Plano de Ações PGP-2024-2025 (disponível no portal do CPDP na internet) dentro do escopo da ação “atualizar IDP” e precede as ações de adequação contratual que são realizadas na fase de construção e execução explicitada na seção 2.2.5.

2.2 Construção e Execução

Como disposto no Guia de Elaboração de Programa de Governança em Privacidade da SGD/MGI (BRASIL. MGI, 2024), na etapa de Construção e Execução, os marcos a serem alcançados são:

1 - Políticas e práticas para a proteção da privacidade do cidadão
2 - Cultura de segurança e proteção de dados e *Privacy by Design*
3 - Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
4 - Política de Privacidade e Política de Segurança da Informação
5 - Adequação de cláusulas contratuais
6 - Termo de Uso

2.2.1 Políticas e práticas para a proteção da privacidade do cidadão

A Administração Pública deve estabelecer políticas e práticas para proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais sejam conhecidos e adequados às leis, bem como haja proteção contra mau uso ou revelação inadvertida ou deliberada.

O termo política de privacidade pode ser utilizado para se referir às políticas de privacidade interna e externas à organização. No âmbito do MGI, a Portaria MGI nº 7.601/2023, (BRASIL. MGI, 2023) ratificou a Resolução CEPPDP-ME nº 07/2022, (BRASIL. MGI, 2022 c) com alterações trazidas pela Resolução CEPPDP/ME nº 13/2022, (BRASIL. MGI, 2022 d). Essas resoluções tratam da Política de Proteção de Dados Pessoais (PPDP) no ministério. A PPDP define normas **internas** e diretrizes para o tratamento de dados pessoais no MGI e tem o

objetivo de garantir os direitos fundamentais de liberdade, de intimidade e de privacidade dos titulares de dados pessoais.

Entre outras cláusulas, ela detalha os diretos dos titulares nos termos da LGPD, da Lei de Acesso à Informação (LAI) e do Marco Civil da Internet (MCI). Ela também estabelece: (i) deveres do ministério como operador e controlador; (ii) regras e conteúdo mínimo para os Termos de Uso e Avisos de Privacidades desenvolvidos pelo MGI; (iii) dever de comunicação em incidentes com o tratamento de dados pessoais; e (iv) ações de desenvolvimento para a área de proteção de dados pessoais conforme disposto no Plano de Desenvolvimento de Pessoas do MGI.

Já com relação à “política de privacidade externa”, o ministério está utilizando o termo “aviso de privacidade” para se referir a esse tipo de política. Conforme artigo 10 do PPDP, o ministério deverá criar e manter atualizados os avisos de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos.

O Aviso de Privacidade origina-se da responsabilidade de que os agentes de tratamento de dados sejam transparentes com o titular de dados pessoais e informem como as atividades de tratamento de tais dados atendem ao princípio da transparência, disposto no Art. 6º da LGPD. O documento deve informar como os dados pessoais serão tratados, armazenados e transmitidos para atender às necessidades organizacionais e às legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados.

Com o intuito de complementar e consolidar as informações pessoais tratadas pelo ministério, o Plano de Ações PGP 2024-2025 previu a publicação de um Aviso de Privacidade Institucional do MGI, o qual conterá a lista das hipóteses legais e finalidades utilizadas para o tratamento de dados pessoais no âmbito do MGI, entre outros pontos. Esse aviso institucional terá característica diversa dos demais Avisos de Privacidade elaborados para cada sistema ou serviço, tendo em

vista ter como objetivo a consolidação e publicação única do aviso, não dispensando a elaboração de Avisos de Privacidade específicos para cada caso.

2.2.2 Cultura de segurança e proteção de dados e *Privacy by Design*

O art. 46 da LGPD apregoa que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Tal proteção dos dados pessoais é alcançada por meio de medidas que deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, que é a instituição da cultura de Privacidade desde a Concepção (*privacy by design*). Assim, capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção seja instituída.

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Conforme o Guia de Boas Práticas da LGPD (BRASIL. CGGD, 2020) elaborado pelo Comitê Central de Governança de Dados, a privacidade desde a concepção pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009), listados a seguir:

- **Proativo, e não reativo; preventivo, e não corretivo**: A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram.
- **Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio:** Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer

ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

- **Privacidade incorporada ao projeto (design):** A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

- **Funcionalidade total**: A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.
- **Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados**: Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.
- **Visibilidade e Transparência:** A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança.
- **Respeito pela privacidade do usuário:** Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os

interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

O Plano de Ações PGP 2024-2025 (disponível no portal do CPDP na internet) prevê a elaboração de Guia Orientativo Privacy by Design.

2.2.3 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Consoante o art. 5º, XVII da LGPD, o relatório de impacto à proteção de dados pessoais é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

O art. 32 da LGPD preconiza que a ANPD poderá solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

O conteúdo mínimo do RIPD é indicado pelo parágrafo único do art. 38, conforme abaixo.

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
> (BRASIL, 2018)

O RIPD deve conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações

e a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados. Também no art. 38 da LGPD, está previsto que a ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

A Secretaria de Governo Digital disponibiliza um modelo para auxiliar a elaboração desse documento, que pode ser acessado através do link https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos.

Em Oficina Dirigida sobre RIPD, realizada em 2020, a SGD apresentou os principais papéis envolvidos na elaboração do documento, assim como as suas etapas:

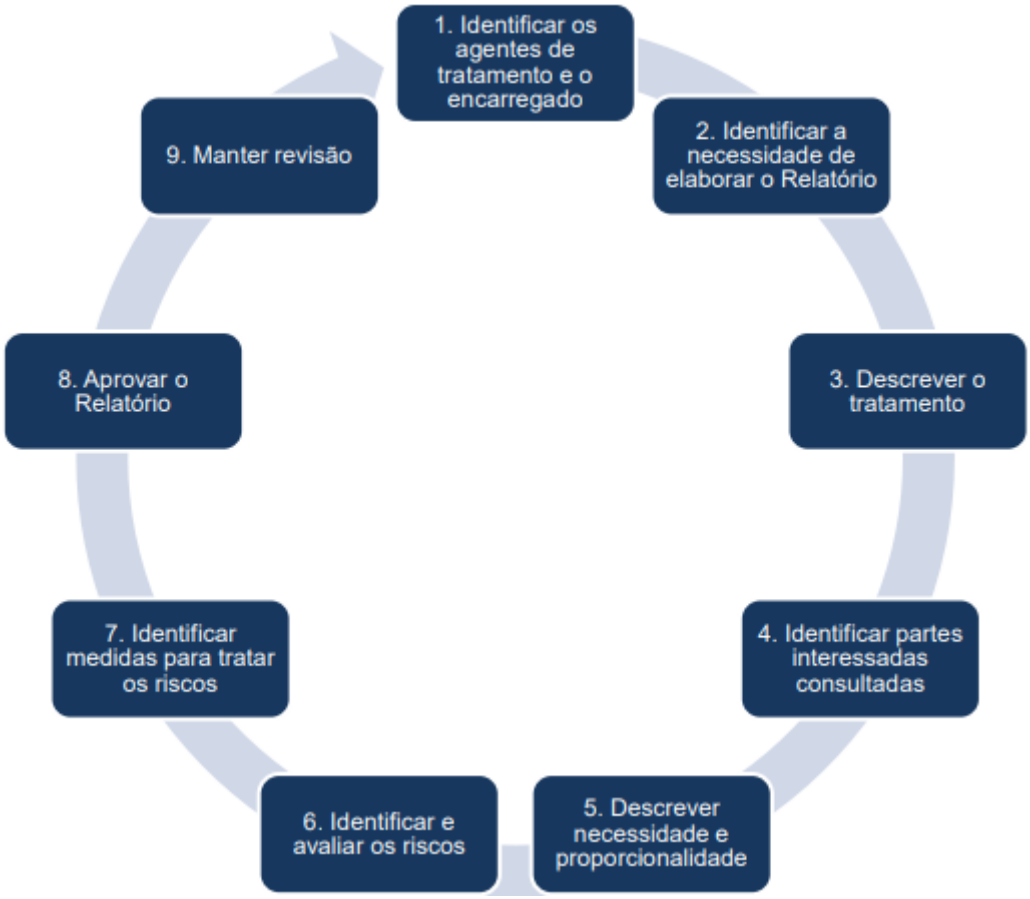

Figura 3. Etapas de elaboração do RIPD.

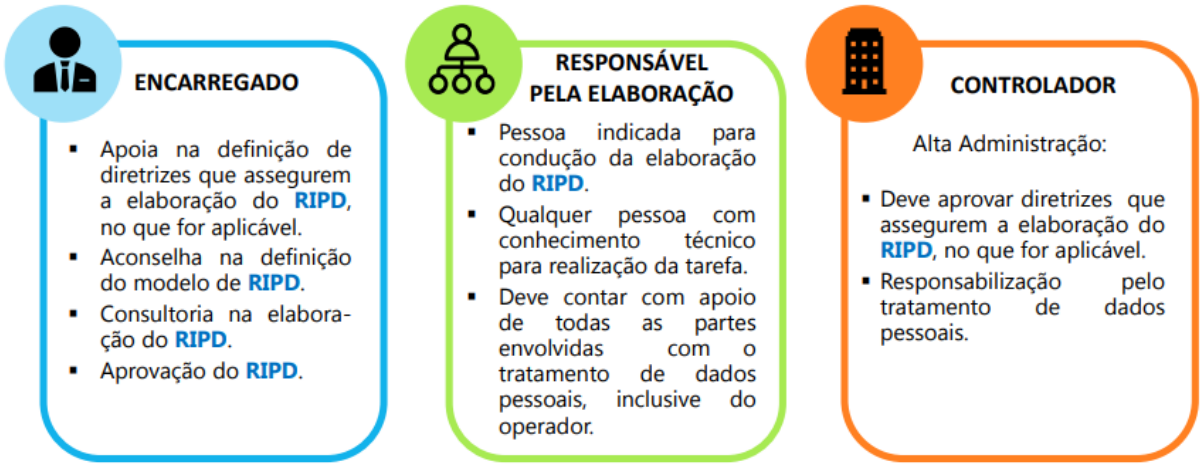

Figura 4. Principais papéis envolvidos na elaboração do RIPD.

Em seu Guia de Boas Práticas LGPD, seção 2.4, a SGD orienta que o RIPD seja publicado em versão resumida, contemplando o fornecimento das informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dos tratamentos de dados pessoais.

É importante que o RIPD seja revisto e atualizado anualmente ou quando houver mudança que atinja o tratamento dos dados pessoais realizados pela instituição.

Como a elaboração do RIPD impõe uma análise mais aprofundada do tratamento dos dados pessoais, é recomendável que as instituições possuam metodologia para verificar a necessidade de sua elaboração. Nesse sentido, o MGI possui dois instrumentos que podem auxiliar a identificação dessa necessidade: a Resolução CEPPDP/ME nº 14/2022 (BRASIL. ME, 2022 e) e a Resolução Conjunta CEPPDP/ME e CRTCI/ME nº 1/2022 (BRASIL. ME, 2022 f). Essas resoluções foram ratificadas pela Portaria MGI nº 7.601/2023, (BRASIL. MGI, 2023) e servem como referencial de auxílio para os gestores em caso de dúvida sobre a necessidade de elaboração de RIPD.

O Plano de Ações PGP 2024-2025 (disponível no portal do CPDP na internet) prevê a elaboração de um modelo padrão de RIPD para o MGI, bem com a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais.

2.2.4 Política de Privacidade e Política de Segurança da Informação

A LGPD, em seu art. 6º, apresenta características da política de privacidade, que deve estabelecer, entre outros:

● Obrigatoriedade de tratamento somente para fins legítimos, específicos, explícitos, sem possibilidade posterior de forma incompatível com essas finalidades (art. 6º, I).

● 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 (art. 6º, III).

● Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV).

● Critérios de qualidade dos dados, para garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V).

● Critérios de transparência, para garantir, aos titulares, o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI).

● Critérios de segurança, para que se utilize 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); e adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII); um conjunto de

procedimentos que devem ser realizados caso haja uma violação na proteção de dados.

● Critérios de não discriminação, para garantir que não se realize o tratamento de dados para fins discriminatórios ilícitos ou abusivos (art. 6º, IX).

● A responsabilização e prestação de contas, para que, para cada tratamento de dados se possa demonstrar a 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 (art. 6º, X).

● Casos em que, preferencialmente, o processo de anonimização deve ser utilizado.

As medidas de segurança para a proteção dos dados pessoais devem considerar práticas preventivas, gestão de risco, segurança desde a Concepção (*security by design*), gestão de incidentes, assim como devem gerenciar os direitos dos titulares.

A Política de Privacidade, emitida no âmbito do MGI com o nome de “Política de Proteção de Dados Pessoais (PPDP)” (vide explicação na seção 2.2.1) origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados pessoais e informarem como as atividades de tratamento desses dados atendem os princípios dispostos no artigo 6º da LGPD. Portanto, este documento constitui, ao mesmo tempo, um dever do controlador e um direito do titular.

Com relação à Política de Segurança da Informação, atualmente, ela encontra-se formalizada na Portaria ME nº 218/2020 (BRASIL. ME, 2020), alterada pela Portaria ME nº 2.800/2022 (BRASIL. ME, 2022 a), e possui a finalidade de estabelecer princípios e diretrizes para a implementação de ações de segurança da informação e, no que couber, para o relacionamento com outros órgãos públicos ou entidades privadas.

O Plano de Ações PGP-MGI 2024-2025 prevê ação para atualização da Política de Proteção de Dados Pessoais do MGI, bem como medidas de segurança de monitoramento, análise de riscos (RIPD), segurança desde a concepção, gestão de incidentes e a proteção dos direitos dos titulares de dados pessoais.

2.2.5 Adequação de cláusulas contratuais

Este marco está diretamente relacionado ao IDP e ao levantamento dos contratos relacionados a dados pessoais, pois possui o escopo de adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados na etapa de Iniciação e Planejamento. Assim, é importante rever os documentos vigentes e os dados já coletados.

Com base no princípio da Transparência, apresentado no art. 6° da LGPD, é importante que os contratos firmados apresentem informações claras e objetivas, abordando, se pertinente:

- Delimitações claras e objetivas das responsabilidades do controlador e operador;
- A forma que é realizada a coleta e o tratamento de dados;
- A existência da possibilidade de o titular acessar os seus dados coletados;
- A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
- A existência da possibilidade de revogação do consentimento dado pelo titular;
- O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
- As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

A priorização inicial de análise das cláusulas contratuais será feita quando da elaboração dos RIPDs para os sistemas entendidos como críticos, conforme seção 2.2.3. Após a análise dos contratos relacionados aos RIPDs, será feita a análise das demais cláusulas de contratos firmados com operadores de dados pessoais no MGI. Essas ações estão previstas no Plano de Ações PGP-MGI 2024-2025.

2.2.6 Termo de Uso

Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade, publicados pela SGD, Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele.

O Termo de Uso ou Contrato de Termo de Uso é uma espécie de contrato de adesão cujas cláusulas são estabelecidas de forma unilateral pelo fornecedor do serviço sem que o usuário possa discutir ou modificar substancialmente seu conteúdo. Esse contrato é celebrado entre o prestador e o usuário do serviço e estabelece os direitos e obrigações de cada uma das partes

O Termo de Uso e a Política de Privacidade, essa última denominada como “Aviso de Privacidade” no âmbito do MGI (ver seção 2.2.1), podem ser consolidados em um documento único ou constar em documentos separados. A depender da conveniência e do contexto do serviço prestado, deve-se avaliar a melhor forma de apresentá-los ao cidadão. Esses documentos devem ser constantemente atualizados a fim de refletir, de modo claro e preciso, as regras aplicáveis ao serviço e as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que geralmente serão utilizados pelo órgão e entidade no exercício de suas competências legais ou execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Conforme artigo 9º da Política de Proteção de Dados Pessoais (PPDP) do MGI (BRASIL. MGI, 2022 c), o ministério, para cada serviço ofertado que trate dados

pessoais, informatizado ou não, deverá requerer do titular a ciência com o termo de uso daquele serviço. Em síntese, esse artigo torna obrigatória a emissão do Termo de Uso para qualquer serviço que trate dados pessoais no MGI. Ademais, a PPDP define os seguintes conteúdos mínimos:

> Art. 9º O Ministério da Economia, para cada serviço ofertado que trate dados pessoais, informatizado ou não, deverá requerer do titular a ciência com o termo de uso daquele serviço.
> Parágrafo único. Os termos de uso deverão ser editados em linguagem acessível, clara e simples, nos quais constarão, no mínimo, as seguintes informações: (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> I - termos e políticas aplicáveis, bem como respectivas ciências ou aceitações, conforme a necessidade;
> II - definições;
> III - descrição do serviço;
> IV - arcabouço legal;
> V - direitos do usuário do serviço;
> VI - responsabilidades do usuário do serviço;
> VII - responsabilidades do Ministério da Economia;
> VIII - no caso dos sítios, portais e aplicativos móveis, quando aplicável, o detalhamento de requisitos técnicos:
> a) tipo de navegador;
> b) sistema operacional;
> c) recursos de memória e processamento; e,
> d) demais requisitos aplicáveis.
> IX - informações sobre os canais nos quais o usuário poderá obter orientações acerca do serviço; (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> X - forma de comunicação das mudanças no termo de uso;
> XI - foro;
> XII - versão e data do documento.
> Art. 10. O Ministério da Economia deverá criar e manter atualizados os avisos de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos.
> Parágrafo único. Os avisos de privacidade deverão: (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> I - ser editados em linguagem acessível, clara e simples;
> II - ser expostos em local de fácil acesso e visualização; e
> III - conter minimamente as seguintes informações:
> a) descrição de cada um dos dados tratados, sua natureza e, principalmente, sua necessidade para o cumprimento da finalidade;
> b) finalidade(s) específica(s) do(s) tratamento(s) realizado(s); (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> c) descrição do(s) tratamento(s) realizado(s);
> d) hipótese(s) legal(is) do(s) tratamento(s) realizado(s); (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> e) duração do(s) tratamento(s) realizado(s);
> f) ocorrência de transferência ou de compartilhamento dos dados coletados, com sua fundamentação legal, inclusive para transferências internacionais;

> g) controles de segurança aplicados ao(s) tratamento(s);
> h) agentes de tratamento (identificação, endereço e informações de contato) e respectivas responsabilidades legais;
> i) identificação e informações de contato do(s) encarregado(s);
> j) informações sobre consentimento do titular dos dados pessoais: quando legalmente requerido, consequências de eventual não fornecimento e como o titular poderá revogá-lo; (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> k) justificativa para a utilização do legítimo interesse, quando for essa a hipótese legal para o(s) tratamento(s) realizado(s); (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> l) informações sobre cada tratamento posterior, se houver, assim como sua fundamentação legal e a finalidade;
> m) cookies utilizados para armazenamento dos dados pessoais, contemplando as informações, quando aplicáveis, contidas nas alíneas “a” a “l” do inciso III do parágrafo único do caput. (Redação dada pela Resolução CEPPDP nº 13, Art. 1º)
> n) direitos do titular dos dados pessoais contidos no art. 18 e no art. 20 da Lei nº 13.709, de 2018;
> o) forma de comunicação das mudanças no aviso de privacidade;
> p) versão e data do documento.
> (BRASIL. MGI, 2022 c; 2022 d)

Vale destacar que a Portaria MGI nº 7.601, de 24 de novembro de 2023, (BRASIL. MGI, 2023) também ratificou o guia de Orientações para Elaboração de Termos de Uso e Avisos de Privacidade (BRASIL. ME, 2022 a) que embora careça de ajustes, tendo em vista ter sido inicialmente elaborado pelo Ministério da Economia (ME), pode ser acessado em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/documentos-do-ceppdp/OrientacoesParaElaboracaoDeTermosDeUsoAvisosDePrivacidadev1.1.pdf.

2.3 Monitoramento

O monitoramento será realizado a cada fechamento de semestre com o objetivo de mensurar o grau de conformidade com a LGPD e garantir o aperfeiçoamento do Programa, com base nas seguintes categorias: (i) Indicadores de Conformidade; (ii) de Normatização; (iii) de Documentação; (iv) de Execução; (v) de Contratação; (vi) de Governança de Dados Pessoais; (vii) de Capacitação; (viii) de Monitoramento; e (ix) de Performance.

2.3.1 Regras de cálculo

Como medida para prover equilíbrio no cálculo do indicador final, as seguintes regras precisam ser observadas:

2.3.1.1. O cálculo dos nove indicadores propostos levará em consideração o peso unitário para cada categoria, portanto, caso seja utilizado mais de um indicador por categoria, o valor desse indicador será somado ao outro de mesma categoria para aferição do indicador final de adequação do MGI (iLGPD-MGI). Cada indicador deve retornar um valor entre 0 e 1 com objetivo de adequação ao valor final do iLGPD-MGI que também será expresso dentro dessa faixa, sendo o menor valor de adequação 0 (zero) e o maior 1 (um).

2.3.1.2. A apuração final do valor será obtida através do cálculo da média dos valores aferidos, sendo desconsiderados da média as categorias que não tiverem ações associadas no período em análise. De acordo com a fórmula abaixo:

$$iLGPD\text{-}MGI = \frac{\sum iCategorias\ Utilizadas}{nº\ Categorias\ Utilizadas}$$

Legenda: *iLGPD-MGI* – indicador de adequação à LGPD do MGI
iCategoriasUtilizadas – representa todas as categorias utilizadas no período avaliado.
nº CategoriasUtilizadas – representa o total de categorias utilizadas no período avaliado.

2.3.2 Categorias de Indicadores

2.3.2.1 Indicadores de Conformidade – iCatConf

Os Indicadores da Categoria de Conformidade (*iCatConf*) serão calculados, preferencialmente, com base em metodologia utilizada por órgãos centrais ou de controle. Para o primeiro ciclo de avaliação a proposta é a de

utilização dos indicadores utilizados pela Secretaria de Governo Digital para avaliação do Programa em Privacidade e Segurança da Informação (PPSI), conforme metodologia constante do Guia do Framework de Privacidade e Segurança da Informação (disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_framework_psi.pdf) e do índice de adequação à LGPD medido pelo Tribunal de Contas da União (TCU) no âmbito do Acórdão nº 1.384/2022 TCU-Plenário (metodologia disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm).

Ambos os indicadores iniciais propostos acima, atendem ao requisito de retorno de valores entre 0 (zero) e 1 (um) descritas no item 2.3.1.1, porém precisam ser ajustadas para se adequar as regras do item 2.3.1.2. Segue abaixo fórmula de ajuste que poderá ser utilizada em categorias com mais de um indicador como no caso proposto:

$$iCatConf = \frac{\sum iAferidos\ na\ Categoria}{nº\ Indicadores\ Aferidos}$$

Legenda: *iCatConf* - indicador da Categoria de Conformidade.

Segue abaixo exemplo de cálculo do *iCatConf*, considerando a utilização do iPriv-SGD (PPSI-SGD) e do iLGPD-TCU:

$$iCatConf = \frac{iPriv{-}SGD + iLGPD{-}TCU}{2}$$

Legenda: *iCatConf* - indicador da Categoria de Conformidade.
iPriv-SGD – indicador de Privacidade calculado no âmbito do PPSI-SGD.
iLGPD-TCU – indicador de adequação à LGPD proposto pelo TCU.

2.3.2.2 Indicadores de Normatização - iNormPDP

A categoria especial de **indicadores de normatização** contempla as atividades que estejam necessariamente relacionadas à expedição de normas pelo

Comitê de Proteção de Dados Pessoais (PDP). Dessa forma, Portarias, Resoluções, Programas, Planos, Políticas, Orientações e quaisquer outras formas de normas que exigem deliberação do CPDP serão classificadas nesta categoria.

Nessa linha, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iNormPDP	Indicador de Normatização de Ações de Proteção de Dados Pessoais	Número de ações de normatização realizadas dividido pelo número de ações previstas no período avaliado

2.3.2.3 Indicadores de Documentação - iDocPDP

Os **indicadores de documentação** são classificados com uma categoria especial e contempla as atividades de documentação, registro ou padronização que não estejam relacionadas à expedição de normas pelo Comitê de Proteção de Dados Pessoais (PDP). Dessa forma, a criação de formulários padrão no SEI, a realização e documentação dos inventários e até a elaboração de um Aviso de Privacidade, por exemplo, podem ser classificadas nessa categoria.

Foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iDocPDP	Indicador de Ações de Documentação na área de Proteção de Dados Pessoais	Número de ações de documentação realizadas dividido pelo número de ações previstas no período avaliado

2.3.2.4 Indicadores de Execução - iExePDP

A categoria de **indicadores de execução** é classificada como uma categoria especial, para os fins do método proposto, por contemplar um grande número de atividades as quais, em conjunto com as categorias especiais de

normatização e documentação, englobam todas as ações constantes no Plano do PGP-MGI.

São classificadas como ações de execução, as ações que não estiverem enquadradas na categoria especial de documentação e de normatização. Nessa linha, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iExePDP	Indicador de Execução de Ações de Proteção de Dados Pessoais	Número de ações executadas dividido pelo número de ações previstas no período avaliado

2.3.2.5 Indicadores de Contratação - iContPDP

A categoria de **indicadores de contratação** foi inicialmente associada a atividades relacionadas à área de proteção de dados pessoais que envolvam a necessidade de contratação para a consecução da atividade final pretendida. Como exemplo, pode-se citar o caso de contratação de cursos especializados para capacitação de gestores, membros e curadores de dados pessoais. Nessa linha, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iContPDP	Indicador de Contratação relacionada à Proteção de Dados Pessoais	Número de ações de contratações realizadas dividido pelo número de ações previstas no período avaliado

2.3.2.6 Indicadores de Governança de Dados Pessoais - iGDP

A categoria de **indicadores de governança de dados pessoais** foi inicialmente relacionada a atividades que envolvam a criação de sistema

tecnológico, ou processos de suporte para a correta gestão do ciclo de vida dos dados pessoais dentro do MGI. Nessa linha, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iGDP	Indicador de Governança de Dados Pessoais	Número de ações de governança de dados pessoais realizadas dividido pelo número de ações previstas no período avaliado

Além do indicar acima, cabe listar alguns indicadores propostos pela SGD no Guia do Framework de Privacidade e Segurança da Informação como inspiração para futuras medições:

- **Índice de serviços com dados pessoais inventariados:** número de serviços com dados pessoais inventariados / número de serviços com dados pessoais do órgão * 100;
- **Índice de serviços com termo de uso elaborado:** quantidade de serviços com termo de uso elaborado / quantidade de serviços do órgão * 100;
- **Índice de serviços com RIPD elaborado**: quantidade de serviços com RIPD elaborado / quantidade de serviços do órgão * 100;
- **Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço:** quantidade de controles de segurança e privacidade implementados para um determinado serviço / quantidade total de controles de segurança e privacidade identificados para o serviço * 100**.**

2.3.2.7 Indicadores de Capacitação - iCapPDP

A categoria de **indicadores de capacitação** foi inicialmente relacionada a atividades capacitação, treinamento e desenvolvimento de pessoas relacionadas à área de privacidade e proteção de dados pessoais. Nessa linha, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iCapPDP	Indicador de Capacitação em Proteção de Dados Pessoais	Número de ações de capacitação realizadas dividido pela quantidade de ações previstas no período avaliado

Além do indicador acima, podem ser criados indicadores para treinamentos específicos, conforme exemplo indicado pela SGD no Guia do Framework de Privacidade e Segurança da Informação:

- **Índice de conscientização em segurança:** quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100.

2.3.2.8 Indicadores de Monitoramento - iMonitorPDP

A categoria de **indicadores de monitoramento de dados pessoais** está relacionada a ações que envolvam o monitoramento reativo e proativo de incidentes e o registro de ações. Nessa categoria, também serão classificadas as ações para monitoramento do próprio PGP, bem como as atividades relacionadas ao processo de Gestão de Incidentes descrito na seção 2.3.3. Dessa forma, foi proposto o seguinte indicador:

Sigla	Nome	Cálculo
iMonitorPDP	Indicador de Monitoramento de Proteção de Dados Pessoais	Número de ações de monitoramento realizadas dividido pela quantidade de ações previstas no período avaliado

Como inspiração para futuras criações de indicadores nesta categoria, cabe listar um indicador proposto pela SGD no Guia do Framework de Privacidade e Segurança da Informação:

- **Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais.**

2.3.2.9 Indicadores de Performance - iPerfPDP

No primeiro ciclo de avaliação do PGP não estão sendo propostos indicadores de performance para avaliação, tendo em vista necessidade de maior

maturidade para a implementação dessa categoria. De qualquer forma, entende-se como desejável um indicador que consiga expressar de forma numérica uma situação de adiantamento de entrega ou de atraso.

2.3.3 Gestão de Incidentes

A elaboração do processo de Gestão de Incidentes abrange o registro dos incidentes de segurança da informação e de privacidade ocorridos e onde serão armazenadas as informações relativas ao ocorrido, incluindo a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente; e as medidas tomadas para mitigação, a fim de evitar reincidências.

O Plano de Ações do PGP-2024-2025 prevê a elaboração de um Plano de Resposta a Incidentes com a definição de processo de comunicação de incidente à ANPD.

2.3.4 Análise e Reporte de Resultados

O monitoramento semestral será elaborado sob coordenação da Secretaria-Executiva do Comitê de Proteção de Dados Pessoais (CPDP) e será apresentado em reunião ordinária do CPDP, momento no qual será discutida a necessidade de revisão do plano, bem como ações de mitigação para resultados encontrados.

A fim de reforçar e fortalecer a cultura de privacidade dos dados, bem como demonstrar o papel da privacidade para o cidadão, o MGI irá elaborar mecanismos para divulgar a evolução das ações e resultados obtidos.

2.4 Conclusão

Com as diretrizes, processos e metodologias apresentadas neste Programa de Governança em Privacidade, espera-se que o MGI avance na difusão do tema de Proteção de Dados Pessoais para seu corpo interno de servidores e colaboradores, bem como para os órgãos vinculados e parceiros ao MGI, com especial destaque ao ColaboraGov, tendo em vista os serviços relacionados à área de tecnologia da informação, prestados pela Secretaria de Serviços Compartilhados (SSC) no âmbito do ColaboraGov, o qual, no momento da elaboração do presente programa, já conta com 13 ministérios atendidos. Sob a ótica da LGPD, a prestação de serviços de tecnologia da informação, que envolva o tratamento de dados pessoais em nome dos ministérios controladores, classifica o MGI como operador de dados pessoais, portanto, o presente programa também possui o intuito de ampliar o relacionamento com as equipes de proteção de dados pessoais dos ministérios demandantes.

Por fim, vale ressaltar que o objetivo final do presente programa é prover aos titulares de dados pessoais tratados pelo MGI maior transparência, segurança e garantia de direitos.

2.5 Referências Bibliográficas

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 14 ago. 2018 c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 mar. 2023.

BRASIL. ANPD, Autoridade Nacional de Proteção de Dados. Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, jun. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 19 fev. 2024.

BRASIL. MGI, Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Elaboração de Programa de Governança em Privacidade. Brasília, DF, jan. 2024.

Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/guia_programa_governanca_privacidade.pdf>. Acesso em: 19 fev. 2024.

BRASIL. MGI. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria MGI nº 7.601, de 24 de novembro de 2023. Institui o Comitê de Proteção de Dados Pessoais no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-mgi-n-7.601-de-24-de-novembro-de-2023-525938325>. Acesso em: 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Portaria nº 218, de 19 de maio de 2020. Institui a Política de Segurança da Informação do Ministério da Economia. 20 mai. 2020 a. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-218-de-19-de-maio-de-2020-257605466>. Acesso em: 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Orientações para elaboração de Termos de Uso e Avisos de Privacidade. abr. 2022 a. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/documentos-do-ceppdp/OrientacoesParaElaboracaoDeTermosDeUsoAvisosDePrivacidadev1.1.pdf>. Acesso em: 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Portaria ME nº 2.800, de 1º de abril de 2022. Altera a Portaria nº 218, de 19 de maio de 2020, que institui a Política de Segurança da Informação do Ministério da Economia. 04 abr. 2022 b. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/arquivos/documentos-cesi/portarias-cesi/portaria-me-no-2-800-de-1o-de-abril-de-2022/@@download/file. Acesso em: 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução CEPPDP/ME nº 6, de 22 de fevereiro de 2022. Dispõe sobre a estrutura de governança de proteção de dados pessoais no âmbito do Ministério da Economia. 22 fev. 2022 c. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucao-no-6-ceppdp-22-02-22>. Acesso em 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução CEPPDP-ME nº 07, de 22 de fevereiro de 2022. Aprova a Política de Proteção de Dados Pessoais no âmbito do Ministério da Economia. 22 fev. 2022 d. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucao-no-7-ceppdp-22-02-22>. Acesso em 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução CEPPDP/ME nº 10, de 23 de maio de 2022. Aprova as Orientações para Elaboração de Termos de Uso e Avisos de Privacidade no âmbito do Ministério da Economia. 24 mai. 2022 e. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucaoceppdpn10-2022.pdf>. Acesso em 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução CEPPDP/ME nº 13, de 23 de novembro de 2022. Altera a Política de Proteção de Dados Pessoais no âmbito do Ministério da Economia. 23 nov. 2022 f. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-

ceppdp/resolucoes-ceppdp/resolucaoceppdp-13-2022.pdf>. Acesso em 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução CEPPDP/ME nº 14, de 24 de novembro de 2022. Aprova as orientações para análise da necessidade de elaboração de relatório de impacto à proteção de dados pessoais. 24 nov. 2022 g. Disponível em: < https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucaoceppdp-14-2022.pdf>. Acesso em 19 fev. 2024.

BRASIL. ME. Ministério da Economia. Resolução Conjunta CEPPDP/ME e CRTCI/ME nº 1, de 24 de novembro de 2022. Estabelece diretrizes para a gestão de riscos à proteção de dados pessoais no âmbito do Ministério da Economia. 24 nov. 2022 h. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucaoconjuntaceppdpcrtci-1-2022.pdf>. Acesso em 19 fev. 2024.

BRASIL. TCU. Tribunal de Contas da União. Acórdão nº 1.384/2022. Plenário. Relator: Ministro Augusto Nardes. Sessão de 15/6/2022. Diário Oficial da União, Brasília, DF, 15 jun. 2022. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 19 fev. 2024.

BRASIL. CGGD. Comitê Central de Governança de Dados - CCGD. Guia de Boas Práticas LGPD. Ago. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias/guia_lgpd.pdf>. Acesso em: 19 fev. 2024.

Cavoukian, Ann. *Privacy by Design*: The 7 Foundational Principles. August, 2009. Disponível em:

<https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf>. Acesso em: 13 jan. 2020.