Plano de Diretrizes para Conformidade à Lei Geral de Proteção de Dados Pessoais

Proteger, direito e dever

Brasília, junho de 2022

Versão 1.0

SECRETARIA EXECUTIVA MINISTÉRIO DA ECONOMIA
PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Ministério da Economia
Paulo Roberto Nunes Guedes
Ministro

Secretaria Executiva
Marcelo Pacheco dos Guaranys
Secretário-Executivo

Comitê Estratégico de Privacidade e Proteção de Dados Pessoais
Aleksey Lanter Cardoso (titular) e Rodrigo Otávio Póvoa Pullen Parente (suplente)
Bruno Silva da Silveira (titular) e Rogério Gabriel Nogalha de Lima (suplente)
Carlos Augusto Moreira Araújo (titular) e Luciana Silva Alves (suplente)
Juliano Brito da Justa Neves (titular) e Silvia Mikiko Tanji (suplente)
Diego Pederneiras Moraes Rocha (titular) e Renata Freire Martins (suplente)
Francisco Eduardo de Holanda Bessa (titular) e Thiago Mendes Rodrigues (suplente)
João Luis Rossi (titular) e Viviane Vecchi Mendes Muller (suplente)
Leonardo Rodrigo Ferreira (titular) e Loriza Andrade Vaz de Melo (suplente)
Luíza de Amorim Motta Deusdará (titular) e Etienne Lopes Ribeiro de Arruda (suplente)
Marcelo Pacheco dos Guaranys (titular)
Marta Juvina de Medeiros (titular)
Rafaelo Abritta (titular) e Juliano Cardoso Eleutério (suplente)
Vanessa Gonçalves Leite de Souza (titular) e Antônio Simões Branco Júnior (suplente)
Waldeir Machado da Silva (titular) e César Almeida de Meneses Silva (suplente)

Equipe Técnica de Elaboração
Coordenação-Geral de Proteção de Dados Pessoais – CGPDP/SE/ME

Proteger, direito e dever

Histórico de versões

Data	Versão	Descrição	Autor
13/06/2022	Minuta	Minuta do Plano de Diretrizes para Conformidade à LGPD	Equipe Técnica de Elaboração
21/06/2022	v1.0	Plano de Diretrizes para Conformidade à LGPD	Equipe Técnica de Elaboração

SUMÁRIO

1. Introdução

Este documento apresenta um plano estruturado de diretrizes para conformidade dos serviços e processos de trabalho do Ministério da Economia (ME) à Lei nº 13.709, de 14 de agosto 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – conforme entrega consignada na Resolução nº 8/2022 do Comitê Estratégico de Privacidade e Proteção de Dados Pessoais.

O ME, no exercício de suas funções institucionais, seja no provimento de serviços ao cidadão ou em suas tarefas administrativas, trata dados pessoais indispensáveis ao cumprimento de suas obrigações legais e necessários à execução de políticas públicas.

Neste contexto, o Órgão vem envidando esforços para realizar o inventário dos dados pessoais tratados em seus serviços e processos de trabalho, além de outras iniciativas institucionais com vistas à adequação à LGPD – a exemplo da instituição da Política de Proteção de Dados Pessoais[1] (Resolução CEPPDP nº 7/2022) e da Estrutura para Governança da Proteção de Dados Pessoais (Resolução CEPPDP nº 6/2022), da aprovação de Orientações para Elaboração de Termos de Uso e Avisos de Privacidade (Resolução CEPPDP nº 10/2022).

Este **Plano de Diretrizes para Conformidade à LGPD** é um dos instrumentos que demonstra o forte comprometimento com a temática de proteção de dados pessoais pelo Ministério da Economia.

1.1. Motivação

Considerando a relevância do tema, para além do disposto na Lei e o essencial respeito à privacidade dos titulares, esta seção tem como intuito destacar alguns normativos e orientações que impulsionaram a concepção deste Plano de Diretrizes para Conformidade à LGPD.

1.1.1. Proteção de dados pessoais como direito fundamental

A Emenda Constitucional nº 115[2] (EC115), promulgada em 10 de fevereiro de 2022 pelo Congresso Nacional, garantiu a inclusão da proteção de dados pessoais na categoria de direitos e garantias fundamentais da Constituição Federal de 1988.

1.1.2. Política de Proteção de Dados Pessoais do Ministério da Economia (Política)

Instituída pela Resolução CEPPDP nº 7/2022, a Política de Proteção de Dados Pessoais do Ministério da Economia dispõe, entre outros, sobre deveres e responsabilidades da Pasta, em especial:

---

[1] Disponível em https://extranet.economia.gov.br/lgpd/#legislação-lgpd. Acesso em 21 de junho de 2022.

[2] Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 13 de junho de 2022.

Art. 6º São deveres do Ministério da Economia, quando em exercício das atribuições típicas do controlador:
I - observar os fundamentos, princípios de proteção de dados e os deveres impostos ao controlador pela Lei nº 13.709, de 2018, e pela legislação correlata, ao decidir sobre um futuro tratamento ou realizá-lo;
Art. 7º São deveres do Ministério da Economia, quando em exercício das atribuições típicas do operador:
IV - observar os princípios definidos no art. 6º da LGPD e os deveres nela impostos ao operador, ao realizar o tratamento.

1.1.3. Programa de Privacidade e Segurança da Informação[3]

O Programa de Privacidade e Segurança da Informação (PPSI), da Secretaria de Governo Digital – SGD/SEDGG é constituído por um conjunto de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo das disciplinas de Governança, Pessoas, Metodologia, Tecnologia e Gestão de Maturidade, implementadas de forma concomitante, incremental e voltadas para aumento dos graus de maturidade e resiliência dos órgãos integrantes do SISP. O PPSI objetiva elevar o grau de maturidade, em termos de proteção de dados pessoais e ações de segurança da informação, dos órgãos integrantes do SISP, aumentando a proteção dos sistemas críticos de governo no ambiente cibernético.

1.2. Objetivos

Este documento tem como objetivo geral apresentar as diretrizes a serem consideradas pelas unidades organizacionais do ME a fim de adequarem os seus serviços e processos de trabalho à LGPD. Com a implementação deste Plano, pretende-se alcançar os seguintes objetivos específicos:

- adotar controles de segurança e privacidade adequados para o tratamento dos dados pessoais;
- adequar os processos de trabalho e serviços a fim de garantir os direitos dos titulares, proporcionando-lhes segurança jurídica;
- observar, na adequação à LGPD, os princípios do art. 6º da Lei, incluindo, mas não se limitando, a finalidade, adequação, transparência e necessidade;
- ter subsídios para o adequado tratamento de incidentes que possam acarretar danos aos titulares, incluindo a própria comunicação aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD);
- conscientizar as unidades, de forma subjacente, da importância da aplicação dos conceitos de privacidade por padrão e privacidade desde a concepção;
- oferecer maior consistência e qualidade aos dados pessoais custodiados pelo Ministério da Economia.

[3] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/PPSI. Acesso em 13 de junho de 2022.

1.3. Fatores críticos de sucesso

Os fatores críticos de sucesso (FCS) são direcionadores que garantirão resultados satisfatórios e competitivos para o sucesso de uma organização em busca de seus objetivos (Bullen & Rockart, 1981).

Assim, são necessários para conformidade com a LGPD os seguintes fatores críticos de sucesso:

- comprometimento da alta gestão: o principal fator crítico de sucesso de um programa de governança de privacidade é que a alta gestão do Órgão esteja ciente das ações necessárias à adequação e comprometa-se com seus resultados;
- engajamento da equipe: fortemente relacionado ao item anterior, compreende a cooperação e a participação ativa da equipe indicada (conforme informado em “3.1.1. Definição da Equipe e Responsabilidades") e a adesão às ações de desenvolvimento contidas no Plano de Capacitação e Conscientização em Proteção de Dados Pessoais, tornando-se um replicador da cultura de privacidade e proteção de dados pessoais e sensibilizando demais agentes públicos e colaboradores da unidade em relação à importância do tema na execução de seus processos de trabalho e serviços. Este engajamento e o sucesso da conformidade relacionam-se fortemente com a necessidade de delegar e explorar as competências da equipe e respectivos perfis de acordo com as atividades necessárias para a conformidade;
- criação de canais de comunicação da equipe: definir como a equipe irá comunicar-se para esclarecer dúvidas, apresentar o andamento das atividades e cooperar. Inclui, por exemplo, a definição de tecnologias e meios de comunicação, bem como a periodicidade;
- qualidade do inventário de dados pessoais: sendo a base para a adequação dos serviços e processos de trabalho, o inventário dos dados pessoais deve ser fidedigno, completo e organizado, para que assim seja possível realizar a análise dos riscos envolvidos e promover os decorrentes ajustes para conformidade;
- atualização do inventário dos dados pessoais: nesta perspectiva, vale destacar a necessidade de garantir a atualização do inventário dos dados pessoais relacionados aos serviços e processos de trabalho, informando casos de transferência de processo de trabalho ou serviço para outra unidade organizacional, a ocorrência de fusão ou cisão de processos, além da eventual extinção do processo ou serviço. Importa também manter a atualização dos dados dos servidores habilitados à ferramenta de Inventário de Dados Pessoais do Ministério da Economia (IDP-ME);
- acurácia no gerenciamento dos riscos técnicos e jurídicos do tratamento de dados pessoais: planejar e executar ações para aperfeiçoar os instrumentos utilizados em sua manutenção e proteção observando a implementação do Programa de Governança em Privacidade. Isto inclui, por exemplo, a adequação de contratos, a gestão do consentimento dos titulares de dados pessoais, a elaboração de termos de uso e avisos de privacidade, entre outros instrumentos;

- gestão de incidentes que envolvam dados pessoais: celeridade e comprometimento no tratamento das demandas decorrentes de notificações de incidentes que envolvam dados pessoais;
- conformidade normativa: observância das leis que versam sobre privacidade e proteção de dados pessoais, assim como das diretrizes, normativos e orientações expedidos pelo ME para a elaboração dos documentos e relatórios necessários à adequação à LGPD;
- apoio do Encarregado pelo tratamento de dados pessoais do Ministério da Economia: na etapa de planejamento de um novo processo de trabalho ou serviço que envolva dados pessoais, o Encarregado auxilia prestando orientações objetivando a privacidade desde a concepção.

1.4. Sobre o Projeto Piloto

Em observância ao deliberado pelo Comitê Estratégico de Privacidade e Proteção de Dados Pessoais em sua Sexta Reunião Ordinária, foi realizado, no período de 9 de maio a 3 de junho, o Projeto Piloto do Plano de Diretrizes para Conformidade à LGPD.

O conjunto de diretrizes contido no Projeto Piloto objetivou subsidiar unidades organizacionais do Ministério da Economia selecionadas[4] para elaborar planos de ação visando o planejamento da adequação de seus processos de trabalho e serviços que tratam dados pessoais à LGPD. As atividades do Projeto Piloto foram dirigidas e apoiadas pela Coordenação-Geral de Proteção de Dados Pessoais da Secretaria Executiva (CGPDP/SE).

A partir do esforço das unidades participantes do Projeto Piloto foi possível coletar informações relevantes a respeito de sua execução e oportunidades de melhoria que subsidiaram o aprimoramento deste Plano de Diretrizes para Conformidade à LGPD, inclusive com o aperfeiçoamento do item 1.3. Fatores críticos de sucesso.

[4] Participaram do projeto piloto o Conselho de Recursos do Sistema Financeiro Nacional e unidades das secretarias especiais de Desburocratização, Gestão e Governo Digital, de Produtividade e Competitividade e da Receita Federal do Brasil.

2. Definições

Algumas definições relevantes ao entendimento do conteúdo exposto neste Plano são dispostas a seguir. Sugere-se consultar a Política e a LGPD, caso algum termo seja necessário ao entendimento e não esteja contemplado nestas definições.

Aviso de privacidade: documento voltado aos titulares, que objetiva informar como os dados pessoais são tratados e para quais finalidades, quais os direitos dos titulares e como podem exercê-los, além de outras características que garantam ao titular a transparência em relação ao tratamento de seus dados pessoais, facilmente acessível e escrito em linguagem clara e simples, conforme disposto no art. 2º, inciso XVII da Política de Proteção de Dados Pessoais do Ministério da Economia (Resolução CEPPDP nº 7/2022);

GDPR ou **RGPD:** *General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

Segurança da informação: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Termo de uso: documento voltado aos titulares, que estabelece as regras e condições de uso de determinado serviço disponibilizado pelo ME, facilmente acessível e escrito em linguagem clara e simples, conforme disposto no art. 2º, inciso XVIII da Política de Proteção de Dados Pessoais do Ministério da Economia (Resolução CEPPDP nº 7/2022);

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (LGPD, art. 5º, inciso XV);

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (LGPD, art. 5º, inciso X);

Unidade responsável ou Unidade: unidade do ME gestora do serviço ofertado ao cidadão;

Usuário: pessoa física ou jurídica que pode fazer uso individual do serviço (Portaria SGD nº 548, de 24 de janeiro de 2022, art. 2º, inciso I);

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (LGPD, art. 5º, inciso XVI).

3. Plano de Diretrizes para Conformidade à LGPD

A seguir serão apresentadas as etapas e respectivas ações para conformidade dos processos de trabalho e dos serviços das unidades organizacionais à LGPD.

3.1. Preparação

Esta etapa tem como finalidade preparar as unidades para as atividades de conformidade à LGPD. Nela devem ser garantidos:

- o comprometimento da alta gestão;
- a definição da equipe que atuará na avaliação das diretrizes estabelecidas e no planejamento e execução do plano de conformidade, definindo as responsabilidades de cada ator envolvido;
- conhecimento e compreensão das estratégias definidas neste plano para registro das atividades de conformidade à LGPD, objetivando evidenciar o andamento das tarefas;
- a capacitação da(s) equipe(s) envolvida(s).

3.1.1. Definição da Equipe e Responsabilidades

Ainda neste escopo de mobilização inicial, a primeira atividade do gestor da unidade deverá ser a definição da equipe que atuará no planejamento e execução do plano de conformidade à LGPD. Na sequência, e considerando este Plano, recomenda-se a definição das responsabilidades de cada membro.

Esta definição de equipe e responsabilidades poderá ser realizada com foco na unidade organizacional ou ainda em observância aos serviços e processos de trabalho da unidade. Ou seja, a depender do tamanho e complexidade da unidade no que tange ao tratamento de dados pessoais e do conhecimento dos servidores quanto aos processos e serviços, o gestor da unidade pode entender ser mais relevante definir a equipe e suas responsabilidades para a unidade como um todo desde o início da adequação à LGPD ou, de modo alternativo, analisar cada um dos processos e realizar tais definições.

Considerando que o envolvimento e a priorização das tarefas de conformidade são condicionantes para o alcance dos objetivos deste Plano, além da necessidade de participação de diversos atores, é essencial a definição das responsabilidades de cada envolvido. Para isto, uma ferramenta amplamente adotada é a Matriz RACI (Responsável, Aprovador ou Autoridade, Consultado e Informado), também conhecida como Tabela RACI, onde são registrados os servidores que exercerão os seguintes papéis:

- R – Responsável: quem tem a responsabilidade pela realização da ação e pelas entregas;
- A – Aprovador ou Autoridade: quem tem autoridade para aprovação dos resultados das ações, acompanhando a execução e oferecendo suporte criativo;
- C – Consultado: especialista ou pessoa que detém informações essenciais para a execução das ações;

- I – Informado: pessoas que devem ser comunicadas sobre o progresso das ações.

A adoção da Matriz RACI pela unidade permite que cada integrante da equipe tenha ciência de suas atribuições, bem como propicia que o responsável pela unidade direcione o engajamento no processo.

3.1.2. Capacitação e Conscientização

No intuito de promover a compreensão necessária das equipes, recomenda-se a prévia realização do treinamento **Proteção de Dados Pessoais no Setor Público**, da Escola Virtual.Gov (EV.G.). Outro curso da EV.G que pode auxiliar na compreensão inicial da LGPD é o **Introdução à Lei Brasileira de Proteção de Dados Pessoais**.

Ainda, recomenda-se que as equipes que atuarão nas atividades de conformidade à LGPD tenham conhecimento do conteúdo dos seguintes materiais:

- Página de proteção de dados pessoais do Ministério da Economia[5]
- Política de Proteção de Dados Pessoais no âmbito do ME;
- Estrutura de governança de proteção de dados pessoais no âmbito do ME;
- Orientações para elaboração de termos de uso e avisos de privacidade;
- Guia Orientativo sobre Agentes de Tratamento e Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, da ANPD[6];
- Guia Inventário de dados pessoais e Oficina Inventário de dados pessoais[7];
- Guia de boas práticas LGPD, do Comitê Central de Governança de Dados[8];
- 1ª Semana de Proteção de Dados Pessoais gov.br[9].

3.1.3. Registro das ações

Desde o início das atividades de conformidade à LGPD, faz-se importante registrar todas as ações realizadas; por isso é elementar determinar os meios e as tecnologias a serem adotadas pela unidade a fim de centralizar os registros das tarefas.

Todas as informações podem ser oportunas para demonstração da conformidade do ME à LGPD. Por exemplo, é necessário determinar onde ficarão registrados a definição da equipe, as responsabilidades de cada envolvido, o inventário dos dados, as análises de riscos, as avaliações de legítimo interesse, os avisos de privacidade e demais questões que serão elucidadas no decorrer deste Plano.

---

[5] Disponível em https://extranet.economia.gov.br/lgpd/. Acesso em 21 de junho de 2022.

[6] Disponíveis em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 21 de junho de 2022.

[7] Disponíveis em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em 21 de junho de 2022.

[8] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd. Acesso em 21 de junho de 2022.

[9] Disponível em https://www.youtube.com/watch?v=Ai1m0LM8gIs. Acesso em 21 de junho de 2022.

Esta recomendação alinha-se com o princípio da responsabilidade e prestação de contas, conforme LGPD, art. 6º, inciso X:

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *(...)*
> *X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"*

Neste sentido, a Coordenação-Geral de Proteção de Dados Pessoais da Secretaria Executiva (CGPDP/SE), por meio deste Plano de Diretrizes, propõe a adoção do *Microsoft Planner* como ferramenta central para gestão do Plano de Conformidade à LGPD do Ministério da Economia, sendo oportuna tanto para o registro das atividades propostas quanto para gestão documental produzida em consequência das ações desenvolvidas. Informações detalhadas sobre tal proposta serão apresentadas no item 5.

3.2. Inventário dos dados pessoais

O registro das operações de tratamento de dados pessoais caracteriza o início das atividades práticas de adequação, sendo considerada a base para o correto andamento das demais atividades do plano (Blum, Vainzof, & Fabrett, 2020). Ou seja, para a conformidade do ME à LGPD, é essencial identificar quais os dados pessoais que são tratados em cada um dos processos de trabalho e serviços realizados em todas as unidades, e como ocorre este tratamento.

O Inventário de Dados Pessoais (IDP) deve refletir o caminho percorrido pelo dado pessoal dentro do Ministério, incluindo os processos e procedimentos pelos quais o dado transita.

3.2.1. Importância do IDP

A fim de destacar a relevância do registro das operações de tratamento de dados pessoais, BLUM et al. (2020) apresenta os seguintes motivos que justificam a construção de um IDP:

a) cumprimento do princípio da responsabilização e da prestação de contas: a fim de demonstrar sua responsabilização quanto às operações de tratamento, as organizações necessitam do IDP, ao menos, como instrumento para saber o que proteger;

b) para fins de fiscalização da ANPD: o IDP pode ser utilizado como um instrumento de fiscalização por parte da ANPD;

c) cumprimento do princípio da transparência: o IDP poderá servir de consulta para elaboração dos avisos de privacidade;

d) atendimento do direito à confirmação da existência de tratamento e direito ao acesso: na mesma perspectiva do item anterior, o IDP servirá de subsídio para

o atendimento destes direitos, facilitando a identificação do tratamento e demais informações relevantes para o processo de atendimento ao titular;

e) atribuição de base legal das operações de tratamento de dados pessoais: uma vez que o IDP contemplará os dados pessoais tratados, bem como a respectiva finalidade, faz-se oportuna a definição da base legal tendo como referência os arts. 7º, 11 e 14 da LGPD;

f) para adoção de medidas adequadas de proteção: o IDP também será fonte de insumos para determinar medidas técnicas e administrativas a serem empregadas pela organização, podendo inclusive, incrementar o inventário registrando os respectivos controles aplicados como evidência para prestação de contas;

g) para identificar tipos de dados envolvidos em uma operação de tratamento: o IDP registrará os tipos de dados tratados em cada operação, incluindo especialmente a existência de dados pessoais sensíveis, dados de crianças e adolescentes, ou ainda dados que, embora não classificados na LGPD, podem gerar riscos aos titulares, como dados financeiros, antecedentes criminais, entre outros. Desta forma, a organização identificará com maior facilidade o cumprimento de legislações correlatas, bem como de políticas, normas e procedimentos internos, além de poder considerar, por exemplo, a necessidade de análise aprofundada para determinar a necessidade de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD);

h) para criação de um plano de conformidade à LGPD orientado ao risco: assim como proposto neste Plano, o IDP será subsídio para determinar processos e serviços que possuem maior risco e que, por consequência, devem ser priorizados no planejamento para conformidade à LGPD.

O mapeamento de dados pessoais foi identificado por organizações europeias como o segundo maior risco de não conformidade entre as obrigações previstas no RGPD, ou Regulamento Geral de Proteção de Dados europeu. (IAPP-International Association of Privacy Professionals, 2017).

3.2.2. Conteúdo Mínimo do IDP

Ainda que a LGPD não estabeleça de maneira direta o conteúdo mínimo do IDP, tal qual faz o RGPD em seu art. 30 (1) e (2), analisando a LGPD e compreendendo as obrigações e direitos dos titulares, é possível definir que as informações apresentadas na Tabela 1 são oportunas de constar neste registro:

Dispositivo da LGPD	Conteúdo Mínimo
Art. 6º, X	Identificação do responsável pelo preenchimento
Art. 9º, I a V	Finalidade específica do tratamento determinada pelo controlador
	Forma do tratamento

	Duração do tratamento
	Identificação do controlador, inclusive as informações de contato
	Informações acerca do uso compartilhado de dados pelo controlador e a finalidade do compartilhamento
Arts. 7º, 11 e 14	Identificar qual a base legal atribuída a cada operação, se controlador
Capítulo V	Informações relacionadas à transferência internacional, se houver
Art. 48, §1º, I e II	Descrição da natureza dos dados pessoais afetados
	Informações sobre os titulares envolvidos (categoria dos titulares)
Arts. 46 e 48, §1º, III	Medidas de segurança, técnicas e administrativas utilizadas para a proteção dos dados, observados os segredos comercial e industrial

Tabela 1 – Conteúdo Mínimo do IDP
Fonte: Adaptado de (Blum, Vainzof, & Fabrett, 2020)

As informações sobre as operações de tratamento de dados possibilitam o melhor conhecimento dos dados pessoais tratados pelo ME e assim viabilizam as etapas seguintes propostas neste Plano de Diretrizes para Conformidade à LGPD. Entre os conteúdos mencionados, tendo como referência o *GDPR Enforcement Tracker*[10] – que contém uma lista e uma visão geral das multas e penalidades que as autoridades de proteção de dados europeias aplicaram com fundamento no RGPD –, dois deles merecem atenção especial: a identificação da base legal e a definição de medidas de segurança.

De acordo com o *GDPR Enforcement Tracker*, historicamente, "base legal insuficiente para o processamento de dados" é um dos principais tipos de violações, seja pela soma monetária das multas aplicadas ou pelo número de ocorrências.

No que tange à definição de bases legais, no âmbito do ME é importante ressaltar o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, da ANPD. O documento destaca que "uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável". Nesse sentido, considerando as peculiaridades do tratamento de dados pelo Poder Público, o guia se limita a discutir as bases legais de consentimento, legítimo interesse, cumprimento de obrigação legal e regulatória e execução de políticas públicas.

3.2.3. IDP-ME: ferramenta de IDP do Ministério da Economia

[10] Disponível em https://www.enforcementtracker.com/?insights. Acesso em 13 de junho de 2022.

A Secretaria Executiva do ME disponibilizou uma ferramenta denominada **Inventário de Dados Pessoais do Ministério da Economia** (IDP-ME), que tem por finalidade viabilizar o registro das informações relativas às operações de tratamento de dados pessoais realizadas no âmbito da Pasta, quer o tratamento ocorra em meio físico ou digital. Cabe ressaltar que a ferramenta não viabiliza o mapeamento do processo de trabalho ou serviço, mas sim o registro, pela unidade responsável, dos dados pessoais neles tratados.

De modo a reforçar o mencionado anteriormente, ao descrever fontes de treinamento para conformidade à LGPD, destaca-se que o IDP-ME é norteado pelo Guia de Elaboração de Inventário de Dados Pessoais[11] e sua respectiva Oficina de Inventário de Dados Pessoais[12], que orientam como realizar o levantamento e o registro dos dados pessoais tratados em âmbito institucional, descrevendo quais as informações são relevantes constar no inventário. Neste mesmo contexto, os seguintes documentos publicados pela ANPD foram relevantes como referência ao IDP-ME: o Guia Orientativo sobre Agentes de Tratamento e o Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público.

Em um esforço para elaboração de um registro de dados pessoais fidedigno à realidade, completo, estruturado de forma organizada e detalhada, ao inventariar as atividades de tratamento de dados pessoais associadas aos processos de trabalho e serviços das unidades do ME, é importante destacar os seguintes pontos:

- cada item registrado deve considerar a complexidade do fluxo dos dados e ponderar sobre a possibilidade de segmentar o item em dois ou mais registros. Por exemplo: um serviço de atendimento ao cidadão pode ser realizado de diferentes formas, seja no meio presencial ou *on-line*, e, não obstante, possuir diferentes canais de solicitação. Desta forma, é possível que o fluxo de dados pessoais em cada um destes canais seja consideravelmente diferente, sendo recomendado então o registro dessa atividade em dois ou mais itens no inventário;
- o inventário de dados pessoais no IDP-ME, relacionado ao serviço ou processo de trabalho, deverá ser delimitado pela fronteira da responsabilidade da unidade. Ou seja, caso o serviço percorra diferentes unidades do ME, cada unidade deverá registrar no seu respectivo inventário os dados pessoais tratados, o fluxo informacional e as demais informações – exclusivamente no que tange à sua atuação ou responsabilidade perante o serviço ou processo de trabalho;
- o foco do inventário é nos processos de trabalho e serviços da unidade. É comum no início das atividades de inventário ocorrer a identificação com base nas tecnologias e sistemas em geral, no entanto, para esta finalidade será proposto um

[11] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf. Acesso em 21 de junho de 2022.

[12] Disponível em https://www.youtube.com/watch?v=UBAohlUAB0U. Acesso em 21 de junho de 2022.

inventário distinto, de tecnologias. Os sistemas são habilitadores dos processos e serviços, sendo recomendada apenas a sua indicação no inventário; portanto, o foco é sempre o processo de trabalho ou serviço realizado pela unidade;

- a revisão dos processos e serviços mapeados por colaboradores distintos, tal como ocorre em revisão por pares, é uma importante ferramenta a ser considerada pelas unidades, objetivando avaliar e aprimorar a qualidade do inventário de dados pessoais realizado.

Destaca-se que as informações sobre o inventário de dados pessoais devem ser inseridas no IDP-ME por servidor da unidade responsável pelo processo ou serviço.

Considerando o IDP como ponto de partida das ações para conformidade na perspectiva prática, destaca-se que o registro das operações de tratamento de dados pessoais é uma atividade que deve ser constantemente revista e atualizada, visto ser comum a ocorrência de mudanças nas operações de tratamento. Como consequência, a necessidade de manutenção do IDP é aplicável para todas as demais ações de conformidade à LGPD, incluindo a atividade prévia de definição de equipe e respectivas responsabilidades.

3.3. Definição dos processos de trabalho ou serviços prioritários

A depender da unidade organizacional do ME, considerando a quantidade e a complexidade dos processos e serviços, bem como a experiência e a quantidade de horas disponíveis da equipe para executar as análises e adequações necessárias, faz-se relevante o estabelecimento de critérios para priorização dos processos e serviços a serem inclusos no Plano de Conformidade à LGPD da unidade.

Com isto, sugere-se que as seguintes ponderações sejam feitas:

- em um primeiro momento, a depender da experiência dos envolvidos na conformidade à LGPD, pode ser mais oportuno iniciar por processos mais simples, objetivando o ganho de maturidade durante a conformidade, compreendendo e superando os desafios gradativamente;
- na sequência, e de forma mais relevante aos objetivos de adequação, recomenda-se que sejam priorizados os processos ou serviços de maior risco, tendo como parâmetros para estimativa de risco os seguintes critérios:
  - escopo do serviço (local, regional, nacional ou global);
  - número estimado do público-alvo (titulares);
  - categorias de dados pessoais tratados (dados de identificação, contato, financeiros, dados técnicos, dados sensíveis, entre outros);
  - quantidade de tipos de dados pessoais tratados;

- formato da coleta dos dados pessoais (diretamente do titular, por terceiros, reuso de dados já coletados pelo ME, dados tornados públicos pelo titular);
- se há combinação de bases de dados diferentes;
- se há tecnologias emergentes ou inovadoras como: inteligência artificial, *blockchain*, realidade aumentada, entre outras;
- se há tratamento de dados de crianças e/ou adolescentes, bem como de idosos e demais vulneráveis;
- se há tratamento de dados sensíveis;
- quantidade de eventuais operadores envolvidos;
- ocorrência de transferência internacional.

Com isto, após a conclusão do inventário dos dados pessoais dos serviços e processos de trabalho e a definição de quais serão priorizados para a adequação, deverá ser realizada a análise de conformidade.

3.4. Análise de conformidade - avaliação dos princípios

A fim de estabelecer uma estratégia para análise de conformidade à LGPD, para cada um dos processos de trabalho e serviços registrados no IDP-ME deverão ser avaliados os princípios dispostos no art. 6º da LGPD.

A seguir são destacados cada um dos princípios, ilustrando os principais pontos de atenção no que tange à sua aplicação nas atividades de conformidade à LGPD.

Ainda tendo como referência o *GDPR Enforcement Tracker*, é possível identificar que a "não conformidade com os princípios gerais de processamento de dados" é um dos principais tipos de violações. Em abril de 2022, esta infração foi registrada em primeiro lugar em termos de soma monetária das multas aplicadas e em segundo pelo número de ocorrências.

3.4.1. Princípio da Finalidade

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *I - finalidade: realização do tratamento para propósitos* ***legítimos, específicos, explícitos*** *e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*

O princípio da finalidade determina que o motivo da coleta dos dados pessoais seja compatível com o objetivo final do tratamento dos dados, visando minimizar o risco de uso secundário sem o conhecimento por parte do titular. Ou seja, a utilização do dado estará associada ao motivo que originou a sua coleta (Maldonado & Blum, 2019).

Para este fim, a LGPD relaciona três conceitos ao princípio da finalidade (Article 29 Working Party, 2013):

- legítimo: este conceito vai além de uma simples definição de uma das bases legais para tratamento dos dados pessoais. Também se estende a outras áreas do direito e deve ser interpretado no contexto do processamento. Este requisito de legitimidade significa que as finalidades devem estar "de acordo com a lei", no sentido mais amplo;
- específico: os objetivos do tratamento dos dados devem ser precisos e totalmente identificados para determinar se o processamento está dentro do propósito apresentado, assim como permitir que a legitimidade possa ser avaliada e que as medidas de segurança sejam determinadas. Neste sentido, o controlador deve considerar cuidadosamente para qual finalidade ou finalidades os dados pessoais serão tratados e não deve coletar dados pessoais que não sejam necessários, adequados ou relevantes para a finalidade ou finalidades a que se destinam. Além disso, é necessária atenção especial ao nível de detalhamento do propósito, uma vez que um propósito vago ou geral, como, por exemplo, "melhorar a experiência dos usuários", "fins de marketing", "fins de segurança de TI" ou "pesquisa futura" normalmente não atendem aos critérios de especificidade;
- explícito: o motivo do tratamento deve ser claramente revelado, explicado ou expresso a fim de garantir que todos os envolvidos tenham o mesmo entendimento inequívoco da sua finalidade, independentemente de qualquer diversidade cultural ou linguística. O objetivo final deste requisito é garantir que os propósitos sejam especificados sem imprecisão ou ambiguidade quanto ao seu significado ou intenção. A especificação das finalidades deve, em particular, ser expressa de forma a ser entendida da mesma forma não apenas pelo controlador (incluindo todos os funcionários relevantes) e quaisquer processadores terceiros, mas também pelas autoridades de proteção de dados e os titulares dos dados. Perante os titulares, tal requisito deve ser atendido o mais tardar no momento em que ocorre a coleta dos dados pessoais. Formas de atender este conceito incluem, por exemplo, descrever as finalidades em um aviso fornecido aos titulares de dados, em uma notificação fornecida à ANPD ou internamente nas informações fornecidas ao Encarregado.

Importante destacar que, na hipótese em que o consentimento seja a base legal utilizada, caso ocorram mudanças na finalidade do tratamento não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento.

Desta forma, o ME deverá identificar e avaliar se as finalidades descritas no IDP-ME estão de acordo com este princípio e seus conceitos. Essencial que a análise realizada seja registrada, incluindo justificativas, ponderações, responsáveis pela análise e datas.

3.4.2. Princípio da Adequação

LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

O princípio da adequação aborda o procedimento realizado para alcançar a finalidade pretendida, impedindo que o informado ao titular ou por ele consentido para uma finalidade específica sofra, durante o tratamento, uma utilização diversa, não esperada (Blum, Vainzof, & Fabrett, 2020), (Bioni, et al., 2021).

Assim, faz-se necessário que o ME verifique o tratamento que está sendo realizado com o dado pessoal coletado, a fim de garantir consistência com a finalidade do caso concreto apresentado ao titular.

3.4.3. Princípio da Necessidade

LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

O princípio da necessidade enaltece a legalidade como inerente ao tratamento de dados pessoais e promove uma prática voltada à racionalização dos dados coletados para os imprescindíveis, aos que sejam estritamente necessários ao alcance de determinada finalidade. Ou seja, este princípio está diretamente associado à minimização dos dados (Maldonado & Blum, 2019).

Observar tais limitações é ação tão relevante quanto identificar previamente ao tratamento: a proporcionalidade do tratamento com os riscos aos direitos dos titulares, se a finalidade poderia ser atingida sem a utilização de dados pessoais, quais seriam e qual volume de dados são realmente imprescindíveis ao tratamento, apontando para a possibilidade de elaboração do RIPD.

Para adequar-se ao princípio da necessidade o ME deve revisar o processo de trabalho ou serviço, identificar viabilidade, realizar minimização da coleta dos dados pessoais, avaliar procedimento quanto aos dados extras coletados e atualizar o processo de trabalho ou serviço na ferramenta IDP-ME.

3.4.4. Princípio do Livre Acesso

LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

Ao decidir realizar o tratamento de dados, defina antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (Comitê Central de Governança de Dados, 2020).

Para garantir aos titulares o direito de consulta sobre a forma e o tratamento, além da integralidade de seus dados pessoais, é preciso que o Ministério da Economia registre tal tratamento, e mantenha-o atualizado.

3.4.5. Princípio da Qualidade dos Dados

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *(...)*
> *V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*

O princípio da qualidade dos dados assegura que os titulares terão acesso a informações confiáveis, para que possam exercer da melhor forma possível a autodeterminação informativa (Hoepers, et al., 2020). Para tal, faz-se imprescindível que o Ministério da Economia garanta que os dados pessoais estejam corretos e atualizados, e que relacionem-se fidedignamente ao titular.

A busca por dados de qualidade, incluindo a modernização de processos de trabalho ou serviços, propicia sua interoperabilidade, que é a capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados (Decreto nº 10.046, de 9 de outubro de 2019, art. 2º, inciso XVIII).

3.4.6. Princípio da Transparência

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *(...)*
> *VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*

Ao traçar a necessidade de comunicação da LGPD com os normativos que tutelam a transparência de dados e o controle social, o Tribunal de Contas do Estado do Rio Grande do Sul destaca (Cravo, Ramos, & Gonçalves da Cunda, 2021):

> *"A temática lança luzes ao cotejo entre o direito ao acesso à informação e transparência e o direito à privacidade, uma vez que a Lei de Acesso à Informação e a Lei de Responsabilidade Fiscal tratam o sigilo como exceção, a LGPD tem, como diretriz, a proteção à privacidade. Mais recentemente, a Lei nº 14.129/2021 deixa bem claro, em seu art. 29, § 1º, que "na promoção da transparência ativa de dados, o poder público*

deverá observar como requisito a observância da publicidade das bases de dados não pessoais como preceito geral e o sigilo como exceção".

A transparência repercute em confiança perante o titular de dados pessoais e a sociedade se fortalece ao vivenciar este princípio. Estar comprometido com o dever de informar, buscar no diálogo a eliminação de qualquer tipo de ambiguidade gera boa reputação, mais inovação e competitividade global (Bioni, et al., 2021).

Para construir uma reputação lastreada em oferecer mais transparência ao uso dos dados, o ME tem o dever, alinhado às diretrizes de governança, de assumir a responsabilidade de proteger os dados pessoais, respeitando o direito à oposição, à intimidade e à privacidade de seus servidores, demais agentes públicos e colaboradores, além dos titulares dos dados pessoais custodiados por meio de processos de trabalho ou serviços da Pasta.

3.4.7. Princípio da Segurança

LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Na mesma perspectiva das bases legais inadequadas, de acordo com o *GDPR Enforcement Tracker*, historicamente, "medidas técnicas e organizacionais insuficientes para garantir a segurança da informação" é um dos principais tipos de violações, seja pela soma monetária das multas aplicadas ou pelo número de ocorrências.

A segurança dos dados pessoais apresenta-se na LGPD dispondo que os agentes de tratamento devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de eventuais violações. Não há dúvidas de que a segurança da informação é fator essencial para conformidade com a LGPD, visto que uma violação de dados pessoais é um fator crítico, pois coloca em risco os direitos dos titulares e prejudica a imagem do Órgão.

Conforme identificado pelo *GDPR Enforcement Tracker*, nestes casos a probabilidade e o impacto de sanções administrativas e responsabilização civis são maiores. Cabe salientar também que, em caso de violações de segurança, tanto o controlador como o operador que deixar de adotar as medidas de segurança adequadas podem responder pelos danos decorrentes (Maldonado & Blum, 2019).

Estas medidas devem ser observadas desde a fase de concepção do projeto, processo ou serviço, devendo atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei e nas demais normas regulamentares. Portanto, é importante ter como referência as normas produzidas pelo

Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República, com especial atenção às Normas Complementares[13], as quais tratam tópicos como:

- Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR);
- Diretrizes para Implementação de Controles de Acesso;
- Diretrizes para Gerenciamento de Incidentes em Redes Computacionais;
- Diretrizes e orientações básicas para o uso de dispositivos móveis;
- Diretrizes para o Desenvolvimento e Obtenção de Software Seguro;
- Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes;
- Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes.

O controlador também tem a responsabilidade de instruir o operador quanto às medidas técnicas e organizacionais para o tratamento dos dados pessoais.

Destaca-se que a segurança deve ser proporcional ao risco do tratamento; por conseguinte, é importante aplicar metodologias para avaliação de riscos como as propostas pela ABNT NBR ISO/IEC 27005:2011 ou pelo *Center for Internet Security Risk Assessment Method* (CIS RAM). Seguindo esta perspectiva, a SGD/SEDGG/ME elaborou o Guia de Avaliação de Riscos de Segurança e Privacidade, as respectivas Oficina Dirigida de Avaliação de Riscos e ferramenta para auxiliar na avaliação dos riscos de segurança e privacidade. O material tem como objetivo "fornecer aos responsáveis pelo tratamento de dados pessoais no órgão ou entidade uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição".

O Guia de Avaliação de Riscos de Segurança e Privacidade se alinha com os controles propostos no Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis[14], no Guia de Requisitos Mínimos de Segurança e Privacidade para APIs[6], no Guia de Segurança em Aplicações Web[6] e, especialmente, no Guia de Framework de Segurança[6], elaborados pela SGD/SEDGG. Importante fazer uma menção a algumas das principais referências neste âmbito, as quais também foram consideradas na elaboração dos referidos materiais:

- *Center for Internet Security* (CIS) – com destaque ao CISControls e ao CIS RAM;
- NIST e sua série de publicações especiais NIST SP-800, bem como o NIST *Privacy Framework*[15]*;*
- ENISA - Agência da União Europeia para a Cibersegurança;

[13] Disponível em https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao. Acesso em 13 de junho de 2022.
[14] Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em 13 de junho de 2022.
[15] Disponível em https://www.nist.gov/system/files/documents/2021/09/02/NIST.CSWP_.01162020pt.pdf. Acesso em 13 de junho de 2022.

- OWASP - *Open Web Application Security Project;*
- Normas da família ISO 27000;
- *Secure Controls Framework* (SCF).

Para fins de conformidade com este princípio, tendo como orientação os referidos guias, as unidades do ME devem avaliar o nível de risco aos quais seus serviços e processos de trabalho estão suscetíveis e identificar as medidas técnicas a serem aplicadas, neste caso com auxílio da área responsável pelas tecnologias que suportam a atividade de tratamento, além das medidas administrativas de segurança.

É recomendado, por fim, que para as atividades que apresentarem nível de risco considerável seja elaborado o RIPD ou Relatório de Impacto para a Proteção de Dados Pessoais (LGPD, art. 5º, XVII, art. 10, art. 32 e art. 38), tendo como referência o Guia, a Oficina e o modelo também propostos pela SGD/SEDGG[14]. Alinhado com o princípio de responsabilização e prestação de contas, a ser apresentado na sequência, é essencial que tal avaliação de risco e os respectivos controles sejam registrados.

3.4.8. Princípio da Prevenção

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *(...)*
> *VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*

A LGPD é uma legislação baseada em riscos; logo, o princípio da prevenção estabelece que os riscos devem ser mitigados anteriormente ao tratamento. Ou seja, a Lei determina que os agentes de tratamento, desde a concepção de suas iniciativas que incluam tratamento de dados pessoais, avaliem os riscos e adotem medidas efetivas para garantir a proteção dos dados pessoais, o respeito à privacidade e à legalidade do tratamento.

A prevenção esperada neste princípio tem como base o conceito *Privacy by Design* (PbD), de Ann Cavoukian (Cavoukian, 2009), pelo qual a proteção à privacidade advém da trilogia: (i) sistemas de tecnologia informação; (ii) práticas negociais responsáveis; e (iii) design físico e infraestrutura de rede. Para atingir seus objetivos, o PbD é pautado em sete conceitos fundamentais:

1. **Proativo e não reativo; preventivo e não corretivo** – o primeiro princípio do PbD refere-se justamente à adoção de postura preventiva e de medidas proativas e não reativas, de modo a evitar ou minimizar a probabilidade de incidentes de violação à privacidade;
2. **Privacidade por padrão** - a privacidade e a proteção dos dados pessoais devem ser preservadas por padrão, ou seja, sem a necessidade de configurações por parte dos titulares;
3. **Privacidade incorporada na concepção** – a privacidade deve ser incorporada em todas as iniciativas desde a sua concepção, e não em momento posterior, seja

no andamento ou com a atividade em produção. A privacidade deve ser componente essencial desde a etapa de concepção de novos projetos, serviços ou processos de trabalho;

4. **Funcionalidade total** - os interesses e objetivos envolvidos devem ser satisfeitos, gerando um benefício mútuo aos titulares e à organização, evitando falsas dicotomias que levem à mitigação de direitos;
5. **Segurança de ponta a ponta** – a prevenção e as medidas de segurança, e a decorrente análise de riscos, devem ser aplicadas desde o princípio e estender-se para todo o ciclo de vida (processamento, compartilhamento, arquivamento, destruição, entre outros) dos dados tratados, ou seja, de ponta a ponta;
6. **Visibilidade e transparência** – o princípio da transparência previsto no art. 6º da LGPD deve ser assegurado desde a concepção para que todos os envolvidos sejam informados de forma suficientemente transparente acerca das atividades de tratamento de dados pessoais; e
7. **Respeito pela privacidade do usuário** – determina que os agentes de tratamento respeitem a privacidade dos usuários.

Dessa forma, recomenda-se que as unidades do ME verifiquem o atendimento de cada conceito fundamental proposto por Ann Cavoukian, bem como mantenham documentadas tais análises. De forma semelhante, sempre que considerar pertinente, consulte o Encarregado de maneira formal e mantenha este registro, assim como os demais, de maneira organizada e centralizada – para fins de demonstração de conformidade.

3.4.9. Princípio da Não Discriminação

LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

A atuação do ME deve promover equilíbrio nas relações entre titular de dados pessoais e Estado, garantir a não exclusão de grupos vulneráveis, promover seu trânsito social, sem preconceitos, inibir danos pela utilização de sistemas de decisão automatizados que possam motivar questionamentos e dificultar responsabilização e, acima de tudo, ter sua contestação facilitada (Bioni, et al., 2021).

Revisitar processos de trabalho ou serviços sob risco discriminatório para convergir preceitos legais com a finalidade do tratamento pode, ao passo das decisões automatizadas, motivar a inclusão de humanos no processo de tomada de decisão (*Human-in-the-loop*) como também, proporcionar o exercício do dever de informar, convalidando todos os princípios que regem a LGPD e inaugurando assim importantes salvaguardas para o titular de dados pessoais.

3.4.10. Princípio da Responsabilização e Prestação de Contas

> *LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *(...)*
> *X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

O princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia (Comitê Central de Governança de Dados, 2020).

Para tanto, ações de desenvolvimento voltadas a agentes públicos em exercício no Ministério da Economia vêm sendo aplicadas com o objetivo de conscientizar, treinar e educar quanto à temática de proteção de dados pessoais, de modo a viabilizar a compreensão dos princípios da proteção de dados pessoais e dos ditames da LGPD, boas práticas, comportamentos mais seguros, prevenção de riscos e contenção de danos aos titulares de dados pessoais.

4. Implementação prática do Plano

A CGPDP/SE fornecerá às unidades do ME, via ferramenta *Microsoft Planner*, um projeto-modelo contemplando ações pré-definidas com vistas à conformidade à LGPD. Dessa forma, a unidade organizacional responsável pelo processo de trabalho e serviços poderá realizar a gestão centralizada dos procedimentos de conformidade, propondo novas ações ou ajustando aquelas previamente contempladas no projeto-modelo.

Para tanto, e a partir do projeto-modelo, algumas informações deverão ser mantidas atualizadas, na ferramenta *Microsoft Planner,* pelas unidades organizacionais cujos processos de trabalho e serviços estejam inventariados no IDP-ME, a exemplo de:

- previsão de data inicial e final de execução de cada ação;
- prioridade e responsável pela ação;
- requisitos/recursos necessários para execução da ação, incluindo custos envolvidos, os quais podem ser inseridos enquanto “comentários” na ação;
- pendências – requisitos de recursos não disponíveis atualmente, os quais também podem ser inseridos como “comentários”;
- progresso da ação – não iniciada, em andamento e concluída.

Cada um dos projetos gerados a partir do projeto-modelo será parte integrante do **Programa de Conformidade à LGDP do Ministério da Economia**, ilustrado na Figura 1.

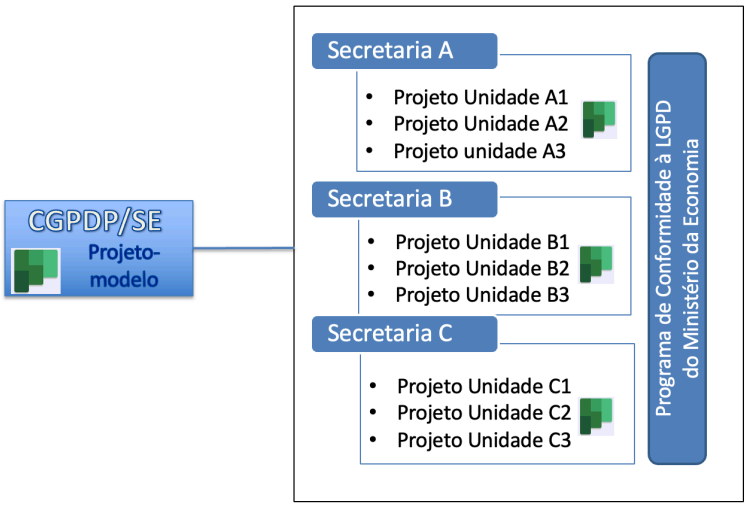

Figura 1 – Uso do projeto-modelo para criação dos projetos pelas unidades organizacionais

5. Acompanhamento e avaliação do Plano

A execução dos projetos de conformidade à LGPD pelas unidades organizacionais será apoiada e assistida pela Coordenação-Geral de Proteção de Dados Pessoais da Secretaria Executiva e pelo Encarregado pelo tratamento de dados pessoais do Ministério da Economia.

Serão realizadas reuniões preparatórias no decorrer do mês de julho com as unidades organizacionais que registraram as operações de tratamento de dados pessoais no IDP-ME objetivando apresentar o projeto-modelo elaborado na ferramenta *Microsoft Planner*, de modo que a CGPDP/SE instrua os passos necessários para que as unidades possam criar seus projetos de conformidade à LGPD – conforme agenda individual a ser acordada pela CGPDP/SE com cada uma das unidades.

Em continuidade às reuniões preparatórias, a partir do mês de agosto a CGPDP/SE realizará reuniões mensais de ponto de controle para acompanhar o andamento das atividades de conformidade à LGPD nas unidades, assim como para esclarecimento de dúvidas surgidas a partir do planejamento e da execução das atividades do projeto – desde que os temas sejam de competência da CGPDP/SE.

Desta forma, pretende-se manter atualizado o progresso do **Programa de Conformidade à LGPD**, viabilizando assim o conhecimento do cenário geral acerca do desempenho do Programa no Órgão, além de possibilitar apresentar mais assertivamente eventuais respostas aos órgãos de controle e à Autoridade Nacional de Proteção de Dados a respeito da adequação à Lei.

Ademais, como forma de avaliação da efetividade deste Plano, registram-se algumas possíveis métricas de conformidade à LGPD a serem empregadas para avaliação do desempenho das atividades propostas:

- comprometimento da alta administração
  - foram alocados servidores para as tarefas?

- as tarefas estão sendo executadas no decorrer do tempo?
- número de treinamentos realizados pelos servidores que compõem a equipe de conformidade da unidade.

- número de processos de trabalho e serviços com avaliação dos princípios da LGPD concluída
- número de processos de trabalho e serviços adequados à Lei

A sintese do Programa de Conformidade à LGPD do Ministério da Economia está ilustrada na Figura 2.

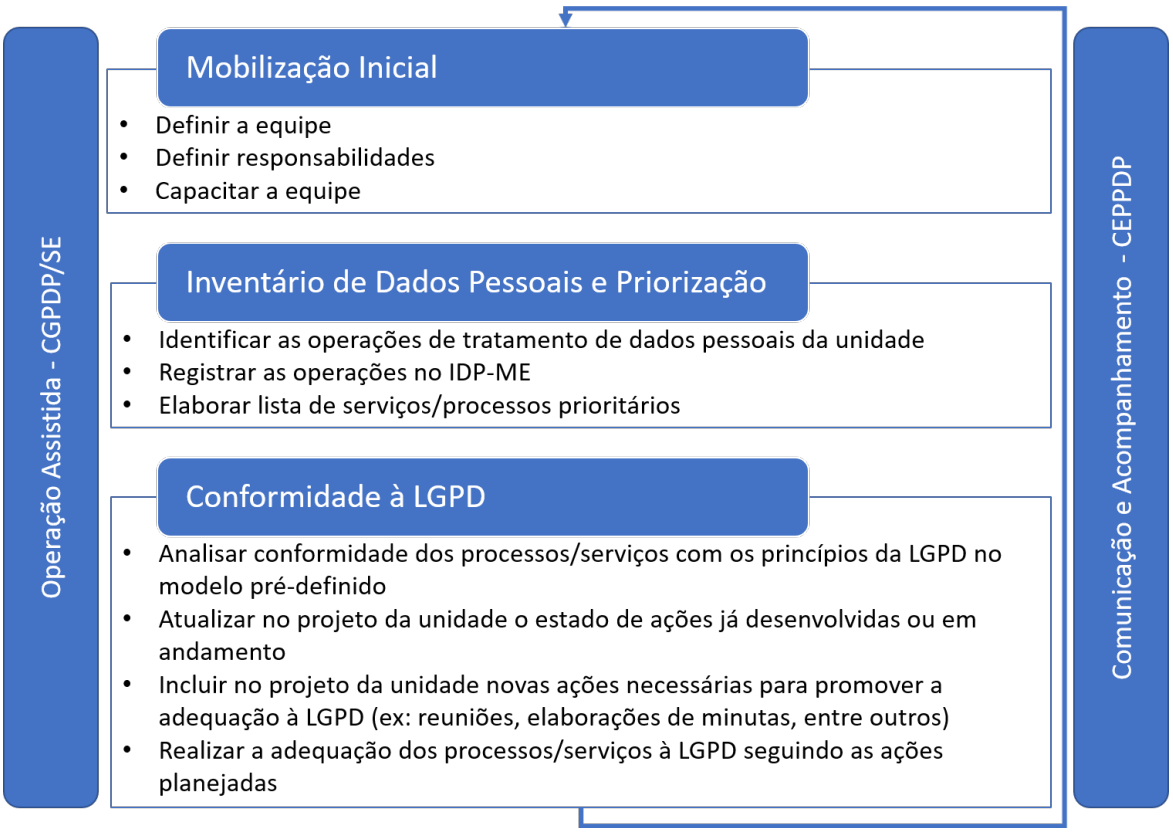

Figura 2 – Programa de Conformidade à LGPD do Ministério da Economia

6. Considerações finais

Tendo em vista a necessidade de adequação dos serviços e processos de trabalho do ME à LGPD, este documento apresenta uma proposta de diretrizes para conformidade à referida Lei.

Desde o princípio foi destacada a importância dos registros das ações bem como a responsabilização pelas atividades de conformidade por meio da recomendação de elaboração de uma matriz RACI. Na sequência foram apresentadas as diretrizes – as quais se baseiam nos princípios da LGPD – para conformidade dos serviços e processos à LGPD, por meio de atividades propostas a serem desenvolvidas no âmbito das unidades do ME. Tais atividades culminarão na elaboração de um Plano de Conformidade, o qual será devidamente apoiado e acompanhado pela Coordenação-Geral de Proteção de Dados Pessoais da Secretaria Executiva. O acompanhamento também será realizado na perspectiva do Plano de Entregas do CEPPDP para o ano de 2022 (Resolução CEPPDP nº 8/2022).

Desta forma, fica estabelecido o Plano de Diretrizes para Conformidade à LGPD, que será aplicado em todos os serviços e processos de trabalho no âmbito do ME.

7. Referências bibliográficas

Article 29 Working Party. (2 de Abril de 2013). *Opinion 03/2013 on purpose limitation.* Acesso em 08 de Abril de 2022, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Bioni, B., Mendes, L. S., Martins, P., Rielli, M. M., Monteiro, R. L., Ribeiro, M. M., . . . Zanatta, R. A. (2021). Proteção de Dados - Contexto, Narrativas e Elementos Fundantes. São Paulo.

Blum, R. O., Vainzof, R., & Fabrett, H. (2020). *Data Protection Officer (Encarregado).* Revista dos Tribunais.

Bullen, C. V., & Rockart, J. F. (1981). A primer on critical success factors. *Massachusetts Institute of Technology (MIT) - Sloan School of Management*.

Cavoukian, A. (2009). *Privacy by Design - The 7 Foundational Principles.* Ontario, Canada: Information and Privacy Commissioner.

Comitê Central de Governança de Dados. (2020). *Guia de Boas Práticas - LGPD.*

Cravo, D. C., Ramos, R., & Gonçalves da Cunda, D. Z. (2021). Lei Geral de Proteção de Dados e o Poder Público. Porto Alegre.

Hoepers, F., Roth, G., Rocha, G., Haag, L. D., Cavalcanti, R. d., Paiva, S. M., . . . Bernardi, V. (2020). Lei Geral de Proteção de Dados Pessoais - Estudo direcionado e comentado da Lei Geral de Proteção de Dados - Artigo a Artigo. Porto Alegre.

IAPP-International Association of Privacy Professionals. (2017). *Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation.* IAPP. Fonte: https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf

Maldonado, V. N., & Blum, R. O. (2019). *LGPD: Lei geral de proteção de dados: comentada.* São Paulo: Revista dos Tribunais.

Visite a página de Proteção de Dados Pessoais https://extranet.economia.gov.br/lgpd/

e a página do Comitê Estratégico de Privacidade e Proteção de Dados Pessoais https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca

Proteger, direito e dever.