gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Guia de Elaboração de Programa de Governança em Privacidade

Programa de Privacidade e Segurança da Informação (PPSI)

Versão 2.3
Brasília, novembro de 2024

GUIA DE ELABORAÇÃO DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Loriza Andrade Vaz de Melo

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

Equipe Revisora – Versão 2.2

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Rafael da Silva Ribeiro

Rodrigo Duran Lima

Rogério Vinícius Matos Rocha

Equipe Revisora – Versão 2.3

Adriano de Andrade Moura

Anderson Souza de Araujo

Bruno Pierre Rodrigues de Sousa
Leonard Keyzo Yamaoka Batista
Rafael da Silva Ribeiro
Rogério Vinícius Matos Rocha

Histórico de versões

Data	Versão	Descrição	Autor
05/09/2020	1.0	Primeira versão do Guia de Programa de Governança em Privacidade.	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão
31/01/2024	2.1	Atualização para a incorporação das Medidas 21.4 e 21.6 do Guia do Framework do PPSI.	Equipe Técnica de Revisão
19/03/2024	2.2	Atualização para inclusão de referência a Ferramenta do Framework como auxílio ao diagnóstico de maturidade e ao monitoramento de performance.	Equipe Técnica de Revisão
22/11/2024	2.3	Atualização para adequação com a Resolução CD/ANPD Nº 18, de 16 de julho de 2024.	Equipe Técnica de Revisão

Sumário

1 Aviso preliminar e agradecimentos

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de um Programa de Governança em Privacidade, em atendimento ao previsto no art. 50 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve, no âmbito de suas competências, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Adicionalmente, a Elaboração de um Programa de Governança em Privacidade visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO), do National Institute of Standards and Technology (NIST) e de Autoridades de Proteção de Dados. Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Ressaltamos ainda, que a adoção deste guia não dispensa as instituições da Administração Pública Federal de observar e considerar as diretrizes estabelecidas pela Autoridade Nacional

de Proteção de Dados (ANPD), pelo Gabinete de Segurança Institucional (GSI), pela Lei Geral de Proteção de Dados (LGPD) e outras normas vigentes.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

2 Introdução

Na administração pública, a governança em privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que os órgãos e entidades precisam prover para conquistar a confiança dos servidores e dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade. Um Programa de Governança em Privacidade (PGP) captura e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

Nesse sentido, este Guia orienta a elaboração de um Programa de Governança em Privacidade por órgãos e entidades da Administração Pública Federal (APF) direta, autárquica e fundacional.

O Controle 21 do Guia do Framework de Privacidade e Segurança da Informação, estabelece que:

Controle 21: Governança – A governança em privacidade estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos de impacto à privacidade e melhorias contínuas na maturidade.

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção de medidas do Controle 21 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 21 que estão contempladas por este Guia são: 21.1, 21.2, 21.4, 21.6, 21.7, 21.9.

O gerenciamento de segurança e risco, bem como seus respectivos responsáveis, encontram, cada vez mais, requisitos complexos e restritivos a serem cumpridos para se ter, assim, uma efetiva governança em privacidade e manuseio de dados pessoais ao longo de seu ciclo de vida. Uma implementação ampla e inclusiva de um Programa de Governança em Privacidade é necessária para gerenciar riscos, em ascensão, nas mais variadas áreas. Aumentar a confiança de todas as partes interessadas necessita que os gestores do gerenciamento de segurança e risco ampliem tanto a frequência quanto a amplitude da comunicação, para assim assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

As orientações relativas à elaboração do Programa de Governança em Privacidade foram estruturadas em duas seções:

- A primeira destaca sua composição; e

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 10/09/2024.

- A segunda trata sobre suas etapas e como elaborá-las.

3 Programa de Governança em Privacidade

3.1 O que é

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º sobre as características mínimas de um Programa de Governança em Privacidade – PGP, conforme apresentado na Figura 1:

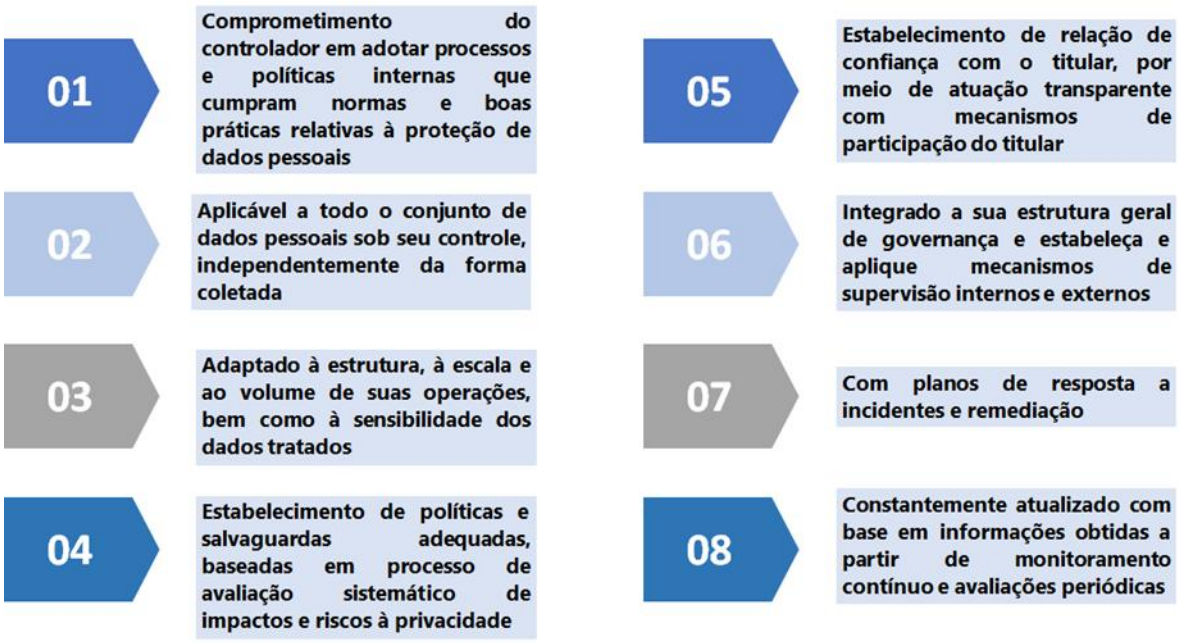

Figura 1 - Características Mínimas de um Programa de Governança em Privacidade na LGPD

Diante das características de um Programa de Governança em Privacidade – PGP apresentadas pela LGPD é necessário também destacar seus principais atores:

- No papel central, por sua importância, tem-se o titular, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso II do art. 2º da Lei Geral de Proteção de Dados);
- A seguir, o controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da Lei Geral de Proteção de Dados). O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador;
- O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da Lei Geral de Proteção de Dados). Ambos, controlador e operador, recebem a nomeação de "agentes de tratamento" (inciso IX do art. 5º da Lei Geral de Proteção de Dados);
- O encarregado corresponde a uma pessoa natural inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer - DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas

também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VIII do art. 5º da Lei Geral de Proteção de Dados);

- finalmente, a Autoridade Nacional de Proteção de Dados - ANPD tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados.

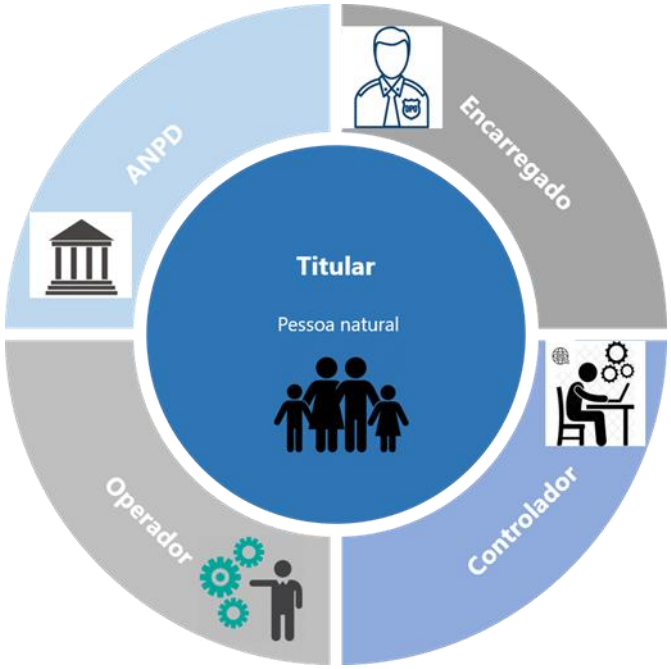

Figura 2 - Atores da LGPD

Vale ressaltar que, ao contrário de um projeto, que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade. Pode-se, entretanto, criar projetos para se alcançar objetivos do programa. Na criação de projetos para se alcançar objetivos do programa, deve-se selecionar a metodologia mais adequada a realidade institucional. Após a escolha da metodologia é necessário definir:

- os objetivos, as metas e os indicadores;
- os líderes responsáveis por cada frente de atuação do projeto (interação com o cidadão, operações de TI, segurança, jurídico, operadores, entre outros); e
- canais de comunicação com os líderes, cidadãos, com os operadores e também com a Autoridade Nacional de Proteção de Dados - ANPD.

Por fim, recomenda-se ainda criar modelos padronizados para obtenção de respostas que subsidiarão reportes para a alta administração.

3.2 Estruturação

A estrutura do PGP apresentada neste documento é inspirada no ciclo PDCA (Plan, Do, Check e Act) bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para

controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

O programa foi estruturado nas seguintes etapas, conforme Figura 3, e serão descritas e detalhadas no próximo capítulo:

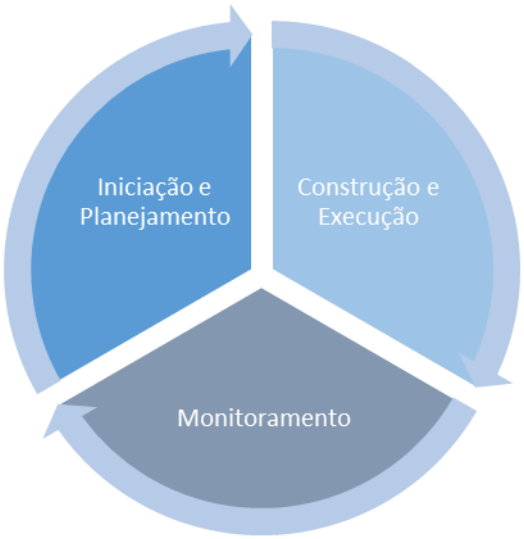

Figura 3 - Etapas do Programa de Governança em Privacidade – PGP

4 Etapas do Programa de Governança em Privacidade

4.1 Iniciação e Planejamento:

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Com isso em mente, essa etapa é constituída pelos marcos apresentados na Figura 4, que serão detalhados a seguir.

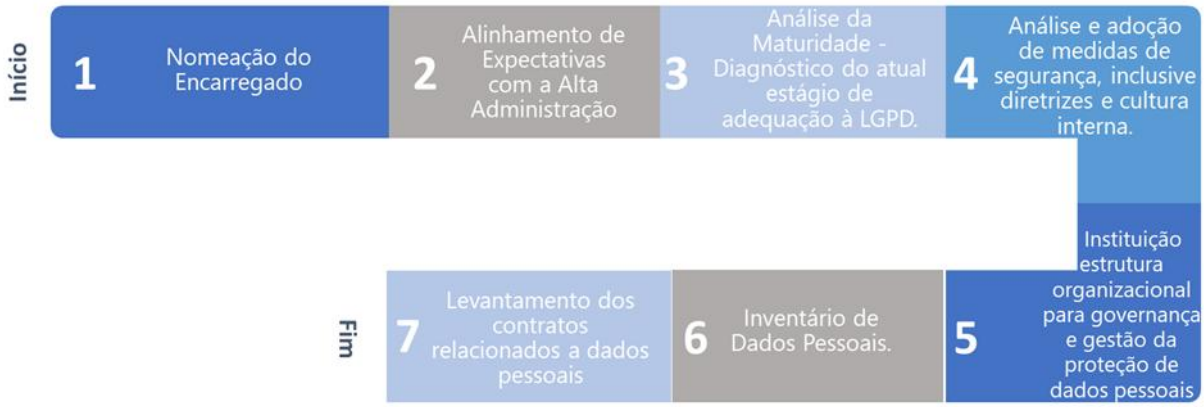

Figura 4 - Marcos da Etapa de Iniciação e Planejamento

Recomenda-se que o início seja dado pela nomeação do encarregado com ampla divulgação de tal ato para os colaboradores internos e demais interessados de acordo com os procedimentos de comunicação do órgão. O encarregado conduzirá a instituição no que diz respeito ao Programa de Governança em Privacidade, em conjunto com o Comitê de Governança Digital, instituído conforme o Art. 2º do Decreto nº 10.332, de 28 de abril de 2020[2]. De acordo com o referido decreto, o encarregado é um dos membros do Comitê de Governança Digital do respectivo órgão, que tem como objetivo deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação.

O início também deve incluir a criação de uma estrutura organizacional para compor o conhecimento de dados pessoais em toda a entidade ou órgão, além de supervisionar as três etapas de ações executadas na criação e manutenção do Programa de Governança em Privacidade.

4.1.1 O Encarregado

De acordo com o Art. 5º 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 ANPD. É importante salientar que o encarregado deve ser capaz de comunicar-se com os

[2] Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10332.htm>

titulares e com a ANPD, de forma clara e precisa e em língua portuguesa. Sua indicação precisa ocorrer logo no início do PGP e deve ser realizada por meio de ato formal do agente de tratamento. Entende-se por ato formal, de acordo com a Art. 3º, § 1º da RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024, documento escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do agente de tratamento em designar como encarregado uma pessoa natural ou jurídica e que constem as formas de atuação e atividades a serem desempenhadas.

A LGPD não distingue se o encarregado deve ser pessoa física ou jurídica e se deve ser um funcionário da organização ou um agente externo, porém, conforme o Art. 5º da RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024, as pessoas jurídicas de direito público referidas no art. 1º, parágrafo único, da Lei nº 12.527, de 18 de novembro de 2011, ou seja, a União, os Estados, o Distrito Federal e os Municípios, deverão indicar encarregado quando realizarem operações de tratamento de dados pessoais, recaindo a indicação, preferencialmente, sobre servidores ou empregados públicos detentores de reputação ilibada. A indicação, nesse caso em específico, deverá ser publicada em Diário Oficial da União, do Estado, do Distrito Federal ou do Município, a depender da esfera de atuação do agente de tratamento. Dessa forma, considerando as boas práticas internacionais e a RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024, o encarregado poderá ser tanto uma pessoa natural, integrante do quadro organizacional ou agente externo quanto uma pessoa jurídica.

É importante que sejam considerados alguns requisitos para o desempenho da função de encarregado e cabe ao agente de tratamento estabelecer as qualificações profissionais necessárias para o desempenho das atribuições do encarregado, considerando seus conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto, o volume e o risco das operações de tratamento realizadas.

Além disso, com base em inspiração resultante de pesquisa realizada em publicações associadas à General Data Protection Regulation (GDPR)[3][4] recomenda-se que também sejam considerados para designação do encarregado os requisitos listados na Figura 5.

[3] Article 29 Data Protection Working Party WP 243 revi.01 The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data

[4] The DPO Handbook Guidance seção 2.5.3

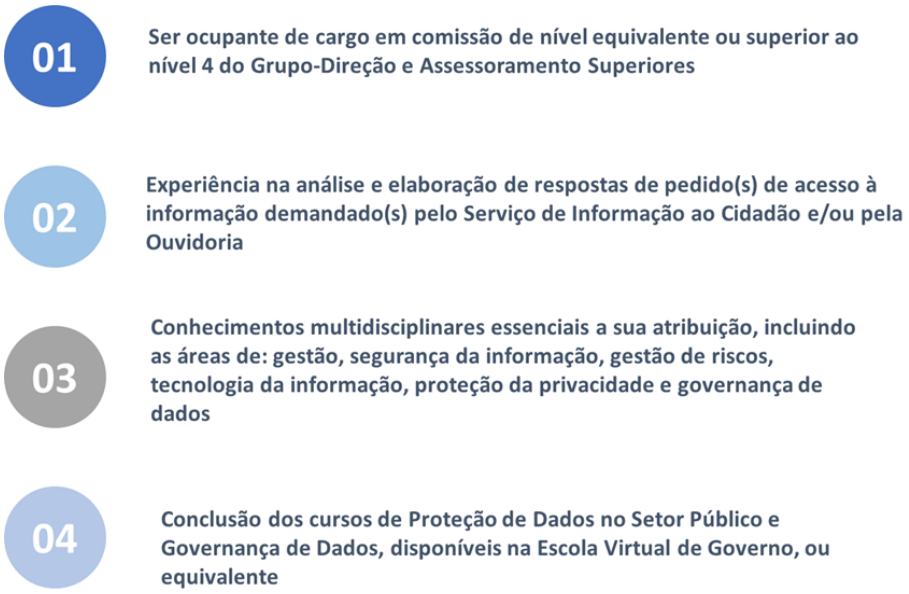

Figura 5 - Requisitos para designação do encarregado

Dentre as suas principais atribuições, podemos citar:

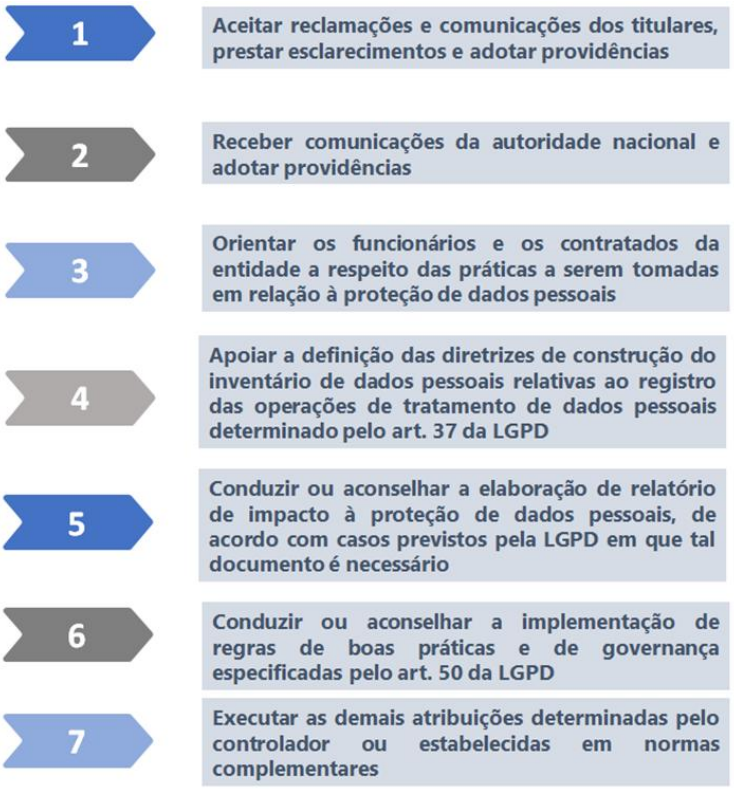

Figura 6 - Competências do encarregado na LGPD[5]

[5] Item 5 da Figura 5: conforme seção 2.5.2.2 do Guia de Boas Prática LGPD

É importante salientar que ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento de informações pertinentes, adotando providencias como encaminhar internamente a demanda para as unidades competentes, fornecer orientação e assistência necessárias ao agente de tratamento e, indicar o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

Observa-se também que não poderão consistir em obstáculos para o exercício dos direitos dos titulares ou para o atendimento às comunicações da ANPD as ausências, impedimentos e vacâncias do encarregado. Nessas situações, sua função deve ser exercida por um substituto formalmente designado.

Cabe, ainda, ao encarregado, prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de:

- registro e comunicação de incidente de segurança;
- registro das operações de tratamento de dados pessoais;
- relatório de impacto à proteção de dados pessoais;
- mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
- 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;
- processos e políticas internas que assegurem o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, e dos regulamentos e orientações da ANPD;
- instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
- transferências internacionais de dados;
- regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 14 de agosto de 2018;
- produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e
- outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

O desempenho das atividades e atribuições do encarregado não o conferem a responsabilidade, perante a ANPD, pela conformidade do tratamento dos dados pessoais realizado pelo controlador. O agente de tratamento é o responsável pela conformidade do tratamento dos dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018.

Além disso, o encarregado pode acumular funções e atuar para mais de um agente de tratamento, desde que consiga atender plenamente suas atribuições para cada agente de tratamento e desde que não exista conflito de interesse, devendo o agente de tratamento, se atentar para que o encarregado não exerça atividades que possam configurar conflito de interesse.

O encarregado deve atuar com ética, integridade e autonomia técnica, evitando qualquer situação que possa configurar um conflito de interesse. É essencial que ele mantenha uma postura ética e íntegra em todas as suas atividades, garantindo a confiança e a transparência no tratamento de dados pessoais. Portanto, também é obrigação do encarregado declarar ao agente de tratamento qualquer situação que possa configurar conflito de interesse. Essas e outras especificidades sobre conflito de interesse podem ser verificados na seção III da Resolução CD/ANPD Nº18.

Com vistas ao que foi apresentado e considerando as boas práticas, é importante que os órgãos da Administração Pública assegurem ao encarregado recursos adequados para realização de suas atividades, que podem incluir:

- Uma estrutura organizacional suficiente (instalações, equipamentos e pessoal) para governança e gestão da proteção de dados pessoais, conforme o porte da instituição;
- Autonomia, independência e tempo hábil, livre de interferências indevidas, para determinar a aplicação de recursos e ações necessárias para o cumprimento das funções relativas ao tratamento de dados pessoais realizados pelo órgão;
- acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.
- Acesso necessário, bem como o pronto apoio das unidades administrativas (Recursos Humanos, Jurídico, TI, Segurança etc.) no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais;
- Amplo acesso a estrutura organizacional, para investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas;
- Contínuo aperfeiçoamento por meio de treinamentos e capacitações realizadas nas áreas de segurança da informação e proteção de dados pessoais.

É válido destacar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões relacionadas a tratamento de dados pessoais na instituição.

Diante da nítida importância do encarregado para a implementação da LGPD e, consequentemente, para o PGP, a seguir é apresentada uma proposta de tópicos a serem abordados, analisados e tratados pelo encarregado. É recomendado que o trabalho a ser

executado pelo encarregado também seja dividido em etapas e os seguintes passos são sugeridos:

Encarregado - Etapa de Iniciação e Planejamento

• Alinhamento de expectativas entre o encarregado e a alta direção do órgão;
• Apresentação, para as secretarias do órgão (secretários, diretores e coordenadores), do papel exercido pelo encarregado como relevante e influenciador;
  ○ Como o encarregado pode servir e agregar valor ao órgão, dado o disposto na LGPD;
  ○ Confirmar e garantir aos servidores do órgão que, enquanto representante interno da ANPD, seu papel deve ser uma assistência de grande valor e não um obstáculo;
• Priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de compliance do órgão;
  ○ Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações;
  ○ Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais serviços que utilizam dados pessoais do órgão.
• Alcance de credibilidade e valor entre os dirigentes do órgão;
• Apresentação de minuta de política de privacidade aos dirigentes do órgão, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;
• Instituição, em conjunto com o Comitê de Governança Digital do órgão ou entidade, e coordenação de uma:
  ○ Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais.
• Projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário para, no mínimo, os próximos 12 meses, bem como a associação e o relacionamento aos pontos de atenção listados;
• Neste início sugere-se concentrar em poucos assuntos, balanceando entre as áreas de maior risco e as mais simples do órgão, quanto a privacidade dos dados. Por exemplo, alternar entre o projeto com maior risco, no que envolve dados pessoais, e uma campanha de sensibilização para os servidores.

Quadro 1: Encarregado - Etapa de Iniciação e Planejamento

4.1.2 Alinhamento de Expectativas com a Alta Administração

Ao longo da etapa de Iniciação e Planejamento é importante ainda alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas. É importante destacar que o alinhamento com a Alta administração e a priorização de ações urgentes guiam o estabelecimento da cultura de proteção de dados na instituição.

4.1.3 Maturidade da Organização

Outro ponto a se analisar é a maturidade da organização, observando fatores como a rastreabilidade de dados - estruturando-os e descrevendo as informações tratadas em cada sistema -, a comunicação com o cidadão e a transparência (elaborando, por exemplo, a política de privacidade e termos de uso de serviços, bem como a comunicação sobre o uso de cookies). Como ferramenta para a análise da maturidade, a Secretaria de Governo Digital (SGD), por meio do Programa de Privacidade e Segurança da Informação (PPSI), no capítulo 7 do Guia do Framework de Privacidade e Segurança da Informação[6], provê uma ferramenta que auxilia no diagnóstico de maturidade do órgão quanto a adoção dos controles de privacidade e segurança da informação, trazendo subsídios para a formalização e cálculo de um índice de maturidade. A maturidade tem foco na avaliação e gestão do nível de proteção no que diz respeito a Privacidade e Segurança da Informação. Os mecanismos para medir este nível de proteção são constituídos pelos índices de maturidade em Privacidade e Segurança da Informação do órgão, que o subsidiarão na implementação e monitoramento dos controles e medidas de Privacidade e Segurança da Informação. O capítulo 6 do Guia do Framework de Privacidade e Segurança da Informação fornece detalhes sobre as etapas necessárias para realizar avaliações de capacidade e de maturidade para obtenção dos indicadores de maturidade em privacidade (iPriv) e em segurança da informação (iSeg) da sua organização. Além de retratar o nível de conformidade em Privacidade e Segurança da Informação quanto aos normativos previstos no escopo do Guia do Framework, o índice de maturidade é também utilizado como um índice de performance e será apresentado na etapa de Monitoramento do PGP, item 4.3.1 deste Guia.

4.1.4 Medidas de Segurança

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas.

Nesse cenário, uma das ferramentas que podem auxiliar na construção do PGP como um todo é o Guia de Boas Práticas da LGPD. Com o objetivo de fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para

[6] https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/manual_ferramenta_framework.pdf

as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD, o Comitê Central de Governança de Dados (CCGD) instituído pelo Decreto 10.046, de 9 de outubro de 2019, publicou o Guia para propor caminhos que levem à sustentabilidade das ações de proteção aos dados pessoais para um país que hoje se projeta como uma potência na transformação digital de governo.

4.1.5 Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais

Recomenda-se ainda, como suporte para a estrutura do PGP, assim como para a realização das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da instituição. Como referência e sugestão de estruturação, a Portaria da Anatel nº 1.197, de 25 de agosto de 2020[7] apresenta, entre outras informações, as competências de um Escritório de Apoio a Proteção de Dados, que representa, com êxito, a estrutura recomendada

4.1.6 Inventário de Dados Pessoais

Para obter um mapeamento dos dados pessoais utilizados pelo órgão, recomenda-se a realização de um inventário de dados, especialmente dos dados pessoais. Conforme o Guia de Elaboração de Inventário de Dados Pessoais, o Inventário de Dados Pessoais representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

No Guia de Elaboração de Inventário de Dados Pessoais, a Secretaria de Governo Digital (SGD) propõe aos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) um modelo simplificado de inventário de dados pessoais, baseado nas metodologias adotadas pela ANPD e também por várias agências estrangeiras de tratamento de dados pessoais , visando identificar as operações de tratamento de dados pessoais realizadas pela instituição no papel de controlador (LGPD, art. 5º, VI). 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.

[7] Disponível em < https:www.in.gov.br/en/web/dou/-/portaria-n-1.197-de-25-de-agosto-de-2020-274640686>

4.1.7 Levantamento de Contratos relacionados a Dados Pessoais

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de um cruzamento 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.

4.2 Construção e Execução

Além do texto apresentado na LGPD, pode-se inferir da ABNT ISO/TR 18638:2019 que, considerando os órgãos da Administração Pública Federal (APF), um PGP deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes.

Assim, na etapa de construção de um programa de governança em privacidade, deve-se considerar os pontos de atenção listados na Figura 7.

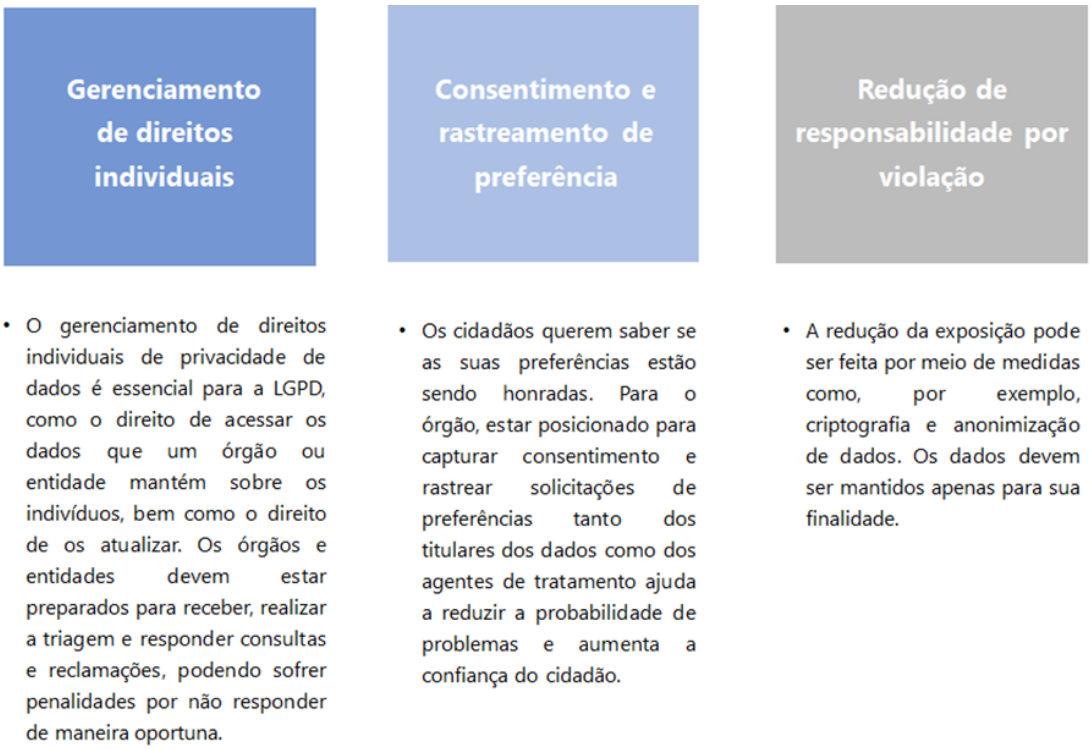

Figura 7 - Considerações da Etapa de Construção e Execução

Logo, neste capítulo, os marcos a serem alcançados na etapa de Construção e Execução, apresentados na Figura 8, serão descritos e detalhados.

Figura 8 - Marcos da Etapa de Construção e Execução

4.2.1 Políticas e práticas para proteção da privacidade do cidadão

Na construção de um PGP devem ser especificadas políticas e práticas para proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais são conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. Além disso, deve ser prevista a comunicação dessas políticas e procedimentos operacionais relacionados à proteção de dados pessoais às partes interessadas internas e externas.

Tal comunicação deve ser feita de acordo com os diversos canais de comunicação da instituição, os quais poderão incluir, não se limitando a:

- Aplicativos de mensagens, como Teams e WhatsApp;
- E-mail;
- Ferramentas de videoconferência;
- Extranet;
- Intranet;
- Sítio eletrônico da Instituição;
- Sistema Eletrônico de Informações;
- Telefone.

Além das políticas e práticas, na Administração Pública, papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos cidadãos em relação aos seus direitos quanto à privacidade da informação.

Informações como a finalidade do órgão ou entidade e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, realizado na etapa de Iniciação e Planejamento, são úteis na construção das operações de tratamento. Tais informações auxiliam na determinação dos detalhes do ciclo de vida dos dados pessoais, por exemplo a finalidade do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

4.2.2 Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design)

A promoção de uma cultura de segurança e proteção de dados deve ser tratada na etapa de construção de um PGP com o intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. As informações do PGP devem ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis. Capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção (privacy by design) 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, tal privacidade 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.

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

É ainda na etapa de Construção e Execução do PGP que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os 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 risco.

O Guia de Boas Práticas da LGPD, em sua seção 2.5 apresenta orientações no sentido de auxiliar os órgãos e entidades a elaborar um RIPD.

4.2.4 Medidas e Política de Segurança da Informação e Política de Privacidade

Ainda na etapa de Construção e Execução do PGP, tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos. Desse modo, torna-se fundamental o desenvolvimento de uma política de segurança da informação da instituição, conforme a Instrução Normativa n. 1 de 27 de maio de 2020 , do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), bem como de uma política de privacidade de dados. 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 ser implementadas na etapa de Construção do programa de governança em privacidade. Segurança desde a Concepção (security by design) e a importância de se tomar medidas preventivas precisam ser consideradas, bem como a gestão dos riscos, a gestão de incidentes e a violação dos dados.

Por fim, mas não menos importante, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, do ponto de vista da Administração Pública, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

4.2.5 Adequação Cláusulas Contratuais

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento, é importante rever os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que a Administração Pública revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados em seu art. 6º. Como um dos princípios listados é a transparência, torna-se essencial que o contrato apresente 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.

4.2.6 Termo de Uso e Política de Privacidade

Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade, publicado pela SGD, Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele. Isto posto, a Política de Privacidade faz parte do Termo de Uso e consiste na prestação de informações ao titular sobre o tratamento dos dados pessoais e a privacidade fornecida.

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.

A Política de Privacidade 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.

O Termo de Uso e Política de Privacidade 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.

4.2.7 O Encarregado

Segundo o artigo 16 da RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024cabe ao encarregado prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação de processos e políticas internas que assegurem o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, dos regulamentos e orientações da ANPD, além de seguir as regras de boas práticas, de governança e do programa de governança em privacidade, nos termos do art. 50 da mesma lei.

Recomenda-se que o encarregado, na etapa de Construção/Execução, realize as atividades apresentadas no quadro a seguir.

Encarregado - Etapa de Construção e Execução
• Implementação do plano de ação elaborado e detalhado na etapa de Planejamento; • Demonstração, para os dirigentes do órgão, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos servidores. • Se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes e secretarias do órgão. • Estabelecimento e manutenção de documentação relacionada à LGPD e aos dados pessoais tratados no órgão, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais. • Definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador, suporte e nunca um obstáculo.

Quadro 2 – Encarregado – Etapa de Construção e Execução

4.3 Monitoramento:

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para os órgãos e entidades manterem PGP a longo prazo. Assim sendo, esta última etapa do PGP

aborda aspectos, detalhados nas próximas seções, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados. A Figura 9 apresenta os marcos da Etapa de Monitoramento, que serão apresentados a seguir.

Figura 9 - Marcos da Etapa Monitoramento

4.3.1 Indicadores de Performance

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no programa de governança em privacidade assim como o status de outras iniciativas de privacidade. Recomenda-se o uso dos indicadores de Maturidade por Controle (iMC), de Maturidade de Privacidade (iPriv) e de Maturidade de Segurança da Informação (iSeg) – presentes no Capítulo 6 do Guia do Framework de Privacidade e Segurança da Informação. Além disso, recomenda-se ainda indicadores mais específicos, tais como:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- 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 conscientização em privacidade e segurança da informação: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;
- Índice de ativos institucionais e de software inventariados: quantidade de ativos institucionais e de software inventariados / quantidade de ativos do órgão * 100.

4.3.2 Gestão de Incidentes

É importante incluir nesta etapa do PGP um processo de Gestão de Incidentes, que conte com um planejamento de resposta a incidentes adequado à LGPD e que registre os incidentes de segurança da informação e de privacidade ocorridos, armazenando informações como: 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 mitigá-los a fim de evitar reincidências.

É válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou o órgão contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pelo órgão contratante.

É recomendado ainda que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

4.3.3 Análise e Reporte de Resultados

O reporte de resultados também é indicado na etapa de monitoramento para demonstrar o valor do PGP à alta administração. Mostrar a evolução das ações e resultados obtidos, bem como o papel da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados.

4.3.4 O Encarregado

A Resolução CD/ANPD Nº 18 traz em seu artigo 16 e inciso IV que o encarregado deve prestar assistência e orientar o agente de tratamento na elaboração, definição e implementação de mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais.

O encarregado, dado seu papel de articulação, exerce função fundamental nessa etapa, conforme apontado no quadro a seguir:

Encarregado - Etapa de Monitoramento
• Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do programa de governança em privacidade; • Divulgação dos resultados entre as diversas áreas do órgão - estabelecimento de uma estrutura de divulgação de resultados para a alta direção dos órgãos e entidades.

Quadro 3 – Encarregado – Etapa de Monitoramento

A incorporação de todos os passos apresentados nas 3 etapas, listados na Figura 10, em um PGP ajudará a garantir que o programa abordará os regulamentos de privacidade de dados e ajudará a criar a confiança do cidadão titular dos dados por meio da demonstração do cuidado com seus dados pessoais e sua privacidade.

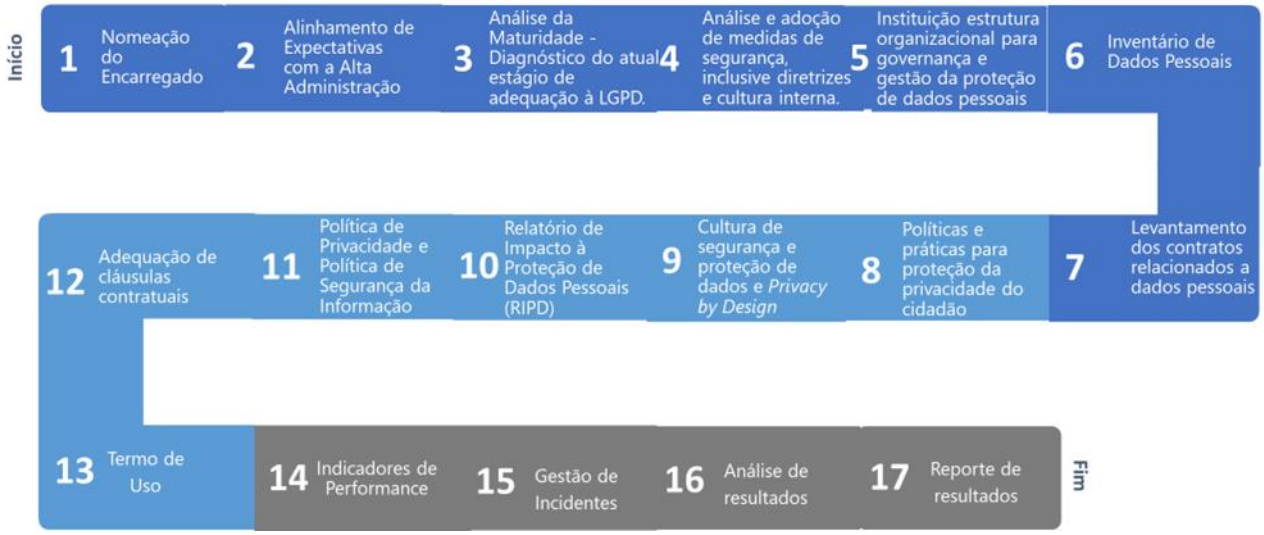

Figura 10 - Passos das Etapas do Programa de Governança em Privacidade

5 Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. **Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.**

_____. ABNT NBR ISO/IEC 27001:2013. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**.

_____. ABNT NBR ISO/IEC 27005:2011. **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.**

_____. ABNT NBR ISO/IEC 27701:2019. **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação-Requisitos e diretrizes.**

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/TR 18638:2019- **Informática em saúde — Orientações sobre educação da privacidade das informações em saúde em organizações de assistência à saúde.**

ARTICLE 29 DATA PROTECTION WORKING PARTY. WP29 guidelines on the Data Protection Officer requirement in the GDPR. 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>. Acesso em: 10 set. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 set. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD Nº 18, de 16 de julho de 2024.** Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074> Acesso em: 10 set. 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: 10 set. 2024.

IBM RATIONAL UNIFIED PROCESS**. Um processo proprietário de Engenharia de software. IBM, 2003.**

GARTNER GROUP. **The Privacy Officer's First 100 Days. 2018**. Disponível em: <https://www.gartner.com/en>. Acesso em: 10 set. 2024.

KORFF, Douwe; GEORGES, Marie. **The DPO Handbook: Guidance for data protection officers in the public and quase-public sectors on how to ensure compliance with the european union general data protection regulation. Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. 2019.** Disponível em: <https://ssrn.com/abstract=3428957>. Acesso em: 10 set. 2024.

PROJECT MANAGEMENT INSTITUTE. **Um Guia de Conhecimento em Gerenciamento de Projetos. Guia PMBOK 5a edição. Project Management Institute, 2013.**

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação.** Novembro 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 10 set. 2024.

6 Anexo I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Guia de Elaboração de Programa de Governança em Privacidade.

Mudanças da Versão 2.3

Primeiramente, ressalta-se que as mudanças dessa versão em comparação a anterior visam um alinhamento com a publicação da Resolução CD/ANPD Nº 18, de 16 de julho de 2024, a qual aprova o regulamento sobre a atuação do encarregado pelo tratamento dos dados pessoais.

Foram realizados ajustes nas subseções 4.1.1, 4.2.7 e 4.3.4 do presente guia, para adequação com a referida Resolução, em pontos específicos sobre o encarregado como: indicação, suas características, quem pode ser, suas atividades e atribuições, conflitos de interesses, seu papel na etapa de construção e execução do PGP bem como na etapa de monitoramento.

Mudanças da Versão 2.2

Foram realizados ajustes nas subseções 4.1.3 e 4.3.1 para inclusão de referência a Ferramenta do Framework do PPSI para auxiliar no diagnóstico de maturidade do órgão quanto a Privacidade e Segurança da Informação e no cálculo do índice de performance na etapa de monitoramento do PGP.

Mudanças da Versão 2.1

Foram realizados ajustes nas subseções 4.1.1 e 4.2.1 para que contemplem as ideias trazidas nas medidas 21.4 e 21.6 do Controle 21 do Guia do Framework de Privacidade e Segurança da Informação.

Mudanças da Versão 2.0

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação do mesmo com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Elaboração de Programa de Governança em Privacidade.

Dentre os ajustes pontuais, cumpre destacar atualização da seção 4.2.6 a fim de contemplar a definição de Política de Privacidade e aperfeiçoar o esclarecimento sobre o que é Termo de Uso.