NOVO PLANO DE PROTEÇÃO DE DADOS

PRESIDÊNCIA DA REPÚBLICA[1]

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO

1. *Versão 3 • 11.06.2025*

LUIZ INÁCIO LULA DA SILVA
Presidente da República

GERALDO ALCKMIN
Vice-Presidente da República

RUI COSTA
Ministro de Estado Chefe da Casa Civil

MARCIO COSTA MACEDO
Ministro de Estado Chefe da Secretaria-Geral

GENERAL AMARO
Ministro de Estado Chefe do Gabinete de Segurança Institucional

MARCO AURELIO SANTANA RIBEIRO
Chefe do Gabinete Pessoal do Presidente da República

CELSO LUIZ NUNES AMORIM
Assessor-Chefe da Assessoria Especial do Presidente da República

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO

FICHA TÉCNICA

COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DA PRESIDÊNCIA DA REPÚBLICA

Secretário-Executivo da Casa Civil da Presidência da República

Secretário-Executivo da Secretaria de Relações Institucionais da Presidência da República

Secretário-Executivo da Secretaria-Geral da Presidência da República

Secretário-Executivo do Gabinete de Segurança Institucional da Presidência da República

Secretário-Executivo da Secretaria de Comunicação Social da Presidência da República

Chefe do Gabinete Pessoal do Presidente da República

Assessor-Chefe da Assessoria Especial do Presidente da República

Chefe de Gabinete do Vice-Presidente da República

Secretário de Administração da Casa Civil da Presidência da República

Coordenador do Subcomitê de Segurança da Informação da Presidência da República

Coordenador do Subcomitê Técnico de Soluções Tecnológicas da Presidência da República

Diretor de Tecnologia da Secretaria de Administração da Casa Civil da Presidência da República

EQUIPE DE ELABORAÇÃO DO PLANO

Grupo de Trabalho constituído pela Resolução nº 43, de 08 de outubro de 2024

Secretaria de Controle Interno da Casa Civil da Presidência da República
Titular: Aline Veloso dos Passos
Substituto: Túlio Kenzo Uema

Casa Civil da Presidência da República
Titular: Erica de Lima Gallindo
Substituto: Gabifran Coelho de Souza

Secretaria de Relações Institucionais da Presidência da República
Titular: Thaís Brito Faria Maciel
Substituto: Nelci dos Santos

Secretaria-Geral da Presidência da República
Titular: Fernanda Gomes Pedrosa
Substituto: Sonia Aguiar Cruz Riascos

Gabinete de Segurança Institucional da Presidência da República
Titular: Edésio César Farias dos Santos
Substituto: Elise Sueli Pereira Gonçalves

Secretaria de Comunicação Social da Presidência da República
Titular: Samara Mariana de Castro
Substituto: Marina Silva Meira

Gabinete Pessoal do Presidente da República
Titular: Jeter Ribeiro de Souza
Substituto: Roridan Penido Duarte

Vice-Presidência da República
Titular: Aline de Souza Ribeiro
Substituto: José Maria de Sá Freire Sobrinho

Secretaria de Administração
Titular: Ana Gabriela Carvalho Rodrigues do Nascimento
Substituto: João Francisco da Mota Junior

COLABORADORES

Mariana Barreto Ribeiro - Secretaria de Controle Interno da Casa Civil da Presidência da República
Sarita de Paula Pereira Cavalcante - Secretaria de Relações Institucionais da Presidência da República
Fernando Marques Borges - Gabinete de Segurança Institucional da Presidência da República
Erik Marques Alves Branco - Gabinete de Segurança Institucional da Presidência da República
Roberta Battisti Pereira - Secretaria de Comunicação Social da Presidência da República
Daniel Mascarenhas Sampaio de Farias - Secretaria de Comunicação Social da Presidência da República
Gustavo Henrique Moreira Alvares da Silva - Vice-Presidência da República

SUMÁRIO

1. APRESENTAÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), é responsável por regular as atividades de coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o intuito de proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da pessoa natural. Além disso, essa lei possibilita um contexto de segurança jurídica por meio da padronização de regulamentos e práticas referentes à proteção de dados pessoais de todos aqueles que se encontram em território brasileiro.

Faz-se válido registrar que, embora, no Brasil, já existissem normas esparsas com o intuito de estabelecer diretrizes para a proteção de dados, essa foi a primeira lei brasileira específica e abrangente sobre o assunto. Com o seu advento, é possível a qualquer pessoa ter conhecimento sobre o processo de tratamento de seus dados pessoais: quais dados serão coletados, como e se serão compartilhados e qual a finalidade da coleta. Ainda, o indivíduo é capaz de, dentre outras ações, revogar a autorização de uso concedida, transferir dados para outro fornecedor de serviços e solicitar acesso, exclusão, explicações ou até mesmo correção de seus dados pessoais.

A definição de dados pessoais está disposta na própria legislação, que também esclarece que alguns deles precisam de atenção e cuidado maiores, como dados pessoais sensíveis e dados sobre crianças e adolescentes. Ademais, impende destacar que a LGPD é aplicável, conforme dispõe seu art. 3º, "a qualquer operação de tratamento realizada por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", e as normas gerais nela previstas "devem ser observadas pela União, Estados, Distrito Federal e Municípios".

A fiscalização acerca do cumprimento da LGPD, a edição de regulamentos e procedimentos sobre proteção de dados pessoais, e a deliberação, na esfera administrativa, sobre a interpretação da lei, suas competências e casos omissos, são algumas das atribuições a cargo da Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, a quem incumbe, nos termos legais, "zelar pela proteção dos dados pessoais", e, assim, proteger e fortalecer os direitos dos titulares dos dados.

No âmbito da Presidência da República (PR), para a implementação da LGPD, foi divulgado, em março de 2022, o Plano de Proteção de Dados, com a previsão de 7 (sete) ações: 1) Campanha de Conscientização; 2) Diagnóstico das Necessidades de Adequação da Presidência da República à LGPD; 3) Elaboração de Inventário de Dados Pessoais; 4) Elaboração de Termo de Uso e Política de Privacidade; 5) Análise de Risco de Segurança de Privacidade; 6) Adequação de Contratos Administrativos e Instrumentos Congêneres; e 7) Relatório de Impacto à Proteção de Dados Pessoais.

Em 2024, o Comitê de Governança Digital e Segurança da Informação (CGD/PR), com o fito de aprimorar os procedimentos atinentes à LGPD nos órgãos que compõem à PR, decidiu pela composição de Grupo de Trabalho, o qual foi instituído pela Resolução nº 43, de 8 de outubro, integrado por representantes da Casa Civil, Secretaria de Relações Institucionais, Secretaria-Geral, Gabinete de Segurança Institucional, Secretaria de Comunicação Social, Gabinete Pessoal do Presidente da República e Vice-Presidência da República, sob a coordenação da Secretaria de Controle Interno, com os seguintes objetivos:

I. elaborar proposta de atualização do Programa de Governança em Privacidade da Presidência da República e da Vice-Presidência da República, objeto da Resolução CGD/PR nº 8, de 2 de setembro de 2021, visando seu alinhamento à Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI);

II. propor novo Plano de Proteção de Dados da Presidência da República e da Vice-Presidência da República;

III. formular diagnóstico sobre o modelo de gestão da LGPD adotado no âmbito dos órgãos que integram a Presidência da República e da Vice-Presidência da República, o que inclui a definição de papéis e responsabilidades de cada órgão; e

IV. elaborar proposta de Plano de Capacitação em Privacidade para servidores dos órgãos da PR e VPR.

É importante destacar que a adequação das organizações à LGPD envolve uma transformação cultural que deve atingir os níveis estratégico, tático e operacional. Nesse contexto, este novo plano objetiva fortalecer as diretrizes estratégicas e operacionais da LGPD nos órgãos que compõem a Presidência e a Vice-Presidência da República, com foco na disseminação de boas práticas e na conscientização de servidores e colaboradores sobre a importância da privacidade e da proteção de dados pessoais em seus processos de trabalho, promovendo, assim, a integração e padronização das medidas de proteção de dados nos diversos órgãos que compõem a Presidência da República.

2. NOVO PLANO DE PROTEÇÃO DE DADOS DA PRESIDÊNCIA DA REPÚBLICA

O novo Plano de Proteção de Dados busca aprimorar as ações já estabelecidas e em caráter contínuo, além de implementar novas iniciativas alinhadas às orientações mais recentes dos órgãos competentes. As seguintes ações estão sendo propostas:

a) Estabelecimento de diretrizes para atualização e manutenção do inventário de dados pessoais;

b) Apresentação de uma metodologia para diagnóstico das necessidades de adequação à LGPD;

c) Instituição de procedimentos de resposta a vazamentos de dados pessoais; e

d) Adoção de um Programa de Capacitação Contínua em LGPD.

No que se refere ao **inventário de dados pessoais,** o grupo de trabalho (GT) propõe diretrizes para sua atualização e manutenção, e detalha os tipos de dados mantidos e sua relação com os processos de trabalho das unidades responsáveis. Essa iniciativa segue as orientações do Guia Operacional para Inventário de Dados do Ministério da Gestão e Inovação em Serviços Públicos (MGI), atualizado em 2023, e inclui a criação de um formulário eletrônico padronizado, a ser disponibilizado a todas as unidades da Presidência por meio de um sistema informatizado. A ferramenta permitirá inventariar os sistemas e seus respectivos dados pessoais, além de consolidar as informações de forma eficiente.

A segunda ação refere-se à adoção de uma **metodologia para diagnóstico das necessidades de adequação à LGPD,** fundamentada nas diretrizes de Privacidade e Segurança da Informação (PPSI) estabelecidas pela Portaria SGD/MGI nº 852, de 28 de março de 2023. O objetivo é identificar quais informações e dados precisam ser avaliados para determinar o estágio de adequação à LGPD na Presidência da República. Os órgãos deverão adotar o Framework de Privacidade e Segurança da Informação, composto por controles, metodologias e ferramentas de apoio voltados para a implementação das melhores práticas de privacidade, segurança da informação e proteção de dados. Esse modelo baseia-se em valores como maturidade, resiliência, efetividade, colaboração e inteligência.

Outra ação essencial proposta neste plano é a criação de **procedimentos de resposta a vazamentos de dados pessoais.** Esses procedimentos visam garantir que, em caso de comprometimento da segurança e da privacidade dos dados pessoais, a organização adote as medidas necessárias para mitigar os danos causados e garantir a conformidade com a legislação de proteção de dados. Essa ação padroniza os fluxos a serem seguidos e as providências a serem tomadas em situações como erro humano, roubo ou perda de dispositivos, exposição de dados por acessos indevidos, compartilhamento não autorizado ou incidentes cibernéticos.

Por fim, o fortalecimento da cultura de proteção de dados pessoais será impulsionado pelo Programa de Capacitação Contínua em LGPD, que visa capacitar os servidores da PR em questões de segurança e privacidade. Esse programa será baseado em quatro pilares: conscientização permanente (comunicações rápidas, impactantes e educativas), treinamento contínuo e autoinstrucional (cursos acessíveis e flexíveis para os servidores), treinamentos avançados sob demanda (capacitações especializadas e personalizadas) e treinamentos não convencionais (aprendizado prático e imersivo com ferramentas de simulações realistas).

3. AÇÃO 1

ELABORAÇÃO/ATUALIZAÇÃO/MANUTENÇÃO DO INVENTÁRIO DE DADOS PESSOAIS DA PRESIDÊNCIA DA REPÚBLICA

O Inventário de Dados Pessoais (IDP) é um recurso utilizado para identificar e registrar todas as informações pessoais que uma organização coleta, utiliza, armazena e compartilha. Esse documento descreve, de forma detalhada, os tipos de dados mantidos e seu uso especificamente, os métodos e locais de armazenamento, além de indicar com quem essas informações são compartilhadas.

O Inventário de Dados Pessoais da Presidência da República tem por objetivo documentar as operações de Tratamento de Dados Pessoais realizadas pelos órgãos que compõem a PR (SG, SRI, GSI, SECOM, CC, VPR, e GPPR) durante a execução de seus processos de trabalho, alinhando-se ao disposto no art. 37 da Lei Geral de Proteção de Dados (LGPD): ***"o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".***

Segundo a Autoridade Nacional de Proteção de Dados (ANPD), esse instrumento demonstra o compromisso da Administração Pública em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relacionadas à Proteção de Dados Pessoais.

A elaboração do Inventário de Dados Pessoais é um marco importante para a realização das próximas etapas de implementação do Plano de Proteção de Dados Pessoais da Presidência da República, que busca alinhar os processos de trabalho e práticas dos órgãos à LGPD.

Além disso, a elaboração desse inventário conta com o apoio do Comitê de Dados Pessoais da Presidência da República. Esse documento será complementado periodicamente à medida que os órgãos realizem a identificação das operações de Tratamento de Dados Pessoais em seus processos de trabalho.

3.1 ETAPAS SUGERIDAS PARA ELABORAÇÃO/ATUALIZAÇÃO/MANUTENÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

TÍTULO DA AÇÃO	ETAPAS SUGERIDAS	RESPONSÁVEIS	PRAZO
Inventário de Dados Pessoais	**1.** *Elaboração e envio de ofício via SEI, solicitando indicação dos pontos focais de cada órgão/unidade da Presidência e VPR*	*Encarregado da Presidência da República*	*15 dias para indicação a partir da data de aprovação do plano*
	2. *Preenchimento do Sistema de Inventário de Dados da Presidência da República*	*Pontos focais indicados via ofício*	*3 meses para o preenchimento do sistema após a conclusão do item 1*
	3. *Consolidação das respostas das UORGs no Relatório de Inventário de Dados da PR*	*Subcomitê de Dados Pessoais da PR (CISET/CC e os 7 órgãos da PR - SG, SRI, GSI, SECOM, CC, VPR e GPPR)*	*2 meses para a consolidação no Relatório após a conclusão do item 2*
	4. *Manutenção e atualização do Inventário de Dados da Presidência da República*	*Pontos focais indicados via ofício*	*Semestralmente*

3.2 PREENCHIMENTO DO SISTEMA DE INVENTÁRIO DE DADOS DA PRESIDÊNCIA DA REPÚBLICA

O Inventário de Dados Pessoais (IDP) objetiva catalogar informações fundamentais sobre o tratamento de dados pessoais na organização.

Para orientar esse processo nos órgãos da Administração Pública Federal, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) atualizou em 2023 o Guia Operacional para Inventário de Dados com orientações procedimentais e planilha modelo que indicam as informações básicas que podem compor o inventário.

O Inventário de Dados Pessoais (IDP) contém o registro das operações de tratamento dos dados pessoais realizados pela instituição (art. 37 da LGPD). De uma forma geral, esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

- Atores envolvidos (agentes de tratamento e o encarregado);
- Finalidade (o que a instituição faz com o dado pessoal);
- Hipótese (Art. 7º e 11 da LGPD);
- Previsão legal;
- Dados pessoais tratados pela instituição;
- Categoria dos titulares dos dados pessoais;
- Tempo de retenção dos dados pessoais;
- Instituições com as quais os dados pessoais são compartilhados;
- Transferência internacional de dados (Art. 33 da LGPD); e
- Medidas de segurança atualmente adotadas.

O Ministério da Gestão e Inovação em Serviços Públicos (MGI) estruturou um modelo de inventário em formato de planilha eletrônica, disponível no link ***https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx***

O referido modelo de inventário é utilizado como referência para o Inventário de Dados Pessoais dos órgãos da Presidência da República e da Vice-Presidência da República. Neste sentido, durante as atividades para proposição do presente Plano de Proteção de Dados da PR, foi desenvolvida como forma de inovação a solução tecnológica ***https://inventario.presidencia.gov.br/***, adaptada com base no modelo estruturado pelo MGI, para auxiliar os órgãos integrantes da PR e VPR na realização do inventário. Ela permite o registro dos sistemas computacionais e das operações de tratamento de dados sob custódia da Presidência da República, com o intuito de gerar maior controle, transparência e segurança no processamento dessas informações. Além de atender às exigências da LGPD, esse inventário também apoia o cumprimento de normativos vigentes relacionados à privacidade e à Segurança da Informação, fortalecendo a governança e a proteção dos dados no âmbito da Presidência.

Para a primeira fase de elaboração do inventário, foi priorizada a realização de Inventários de Dados Pessoais relacionados aos Inventários de Sistemas Computacionais e Dados. Em fases futuras, será avaliada a expansão considerando processos e serviços da Presidência da República.

O preenchimento do Sistema de Inventário ocorrerá em duas partes:

a) Todas as unidades organizacionais (UORGs) deverão informar se são ou não controladoras de sistemas computacionais ou proprietárias de informações de dados pessoais armazenados em qualquer tipo de sistema.

b) Nos casos de respostas positivas, essas UORGs devem preencher as informações solicitadas no inventário de sistemas e dados pessoais.

Dada a natureza evolutiva dos processos organizacionais, o IDP deverá ser revisado e atualizado de forma contínua e sempre que haja mudanças nas estruturas dos órgãos, alterações nos fluxos de tratamento de dados ou na legislação aplicável. Essa atualização contínua garante que o inventário reflita a realidade da organização, o que permite um mapeamento preciso dos riscos e a adoção de medidas de segurança e conformidade adequadas.

3.3 CONSOLIDAÇÃO DAS RESPOSTAS DAS UNIDADES ORGANIZACIONAIS DA PRESIDÊNCIA DA REPÚBLICA NO RELATÓRIO INTEGRADO DE INVENTÁRIO DE DADOS

O Inventário de Dados Pessoais das unidades organizacionais (UORGs) da Presidência da República deverá ser consolidado para compor repositório único e permitir a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a avaliação de riscos na proteção de dados pessoais.

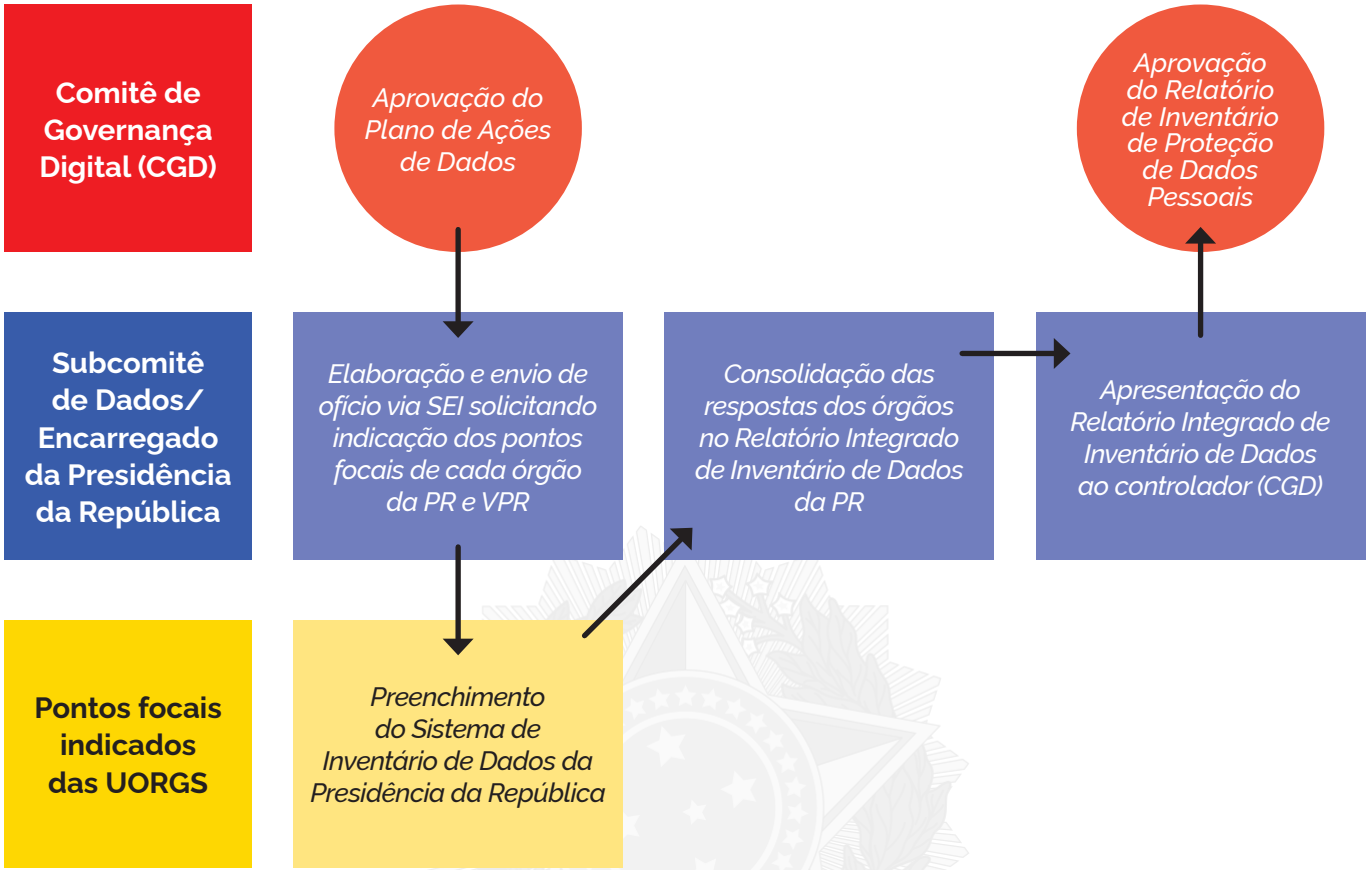
O sistema do inventário de dados possibilita a extração de relatórios, o que facilita a análise e o gerenciamento das informações pessoais coletadas.

Além disso, o Subcomitê de Dados Pessoais/Encarregado, analisará os relatórios extraídos de cada UORG e consolidará apenas um documento, o Relatório Integrado de Inventário de Dados da Presidência da República, que assegurará uma visão abrangente e integrada das informações e será submetido ao controlador para aprovação. O Relatório Integrado de Inventário de Dados da Presidência da República será elaborado com periodicidade anual.

3.4 FLUXOGRAMA DO INVENTÁRIO DE DADOS PESSOAIS DA PRESIDÊNCIA DA REPÚBLICA

O fluxograma foi desenvolvido para facilitar o entendimento do processo de elaboração/atualização/manutenção do Inventário de Dados Pessoais. Essa representação visual ajuda a identificar claramente as fases do processo, os envolvidos, as responsabilidades e os fluxos de informação, o que promove uma gestão mais eficiente.

FLUXOGRAMA • INVENTÁRIO DE DADOS PESSOAIS



4. AÇÃO 2

DIAGNÓSTICO DAS NECESSIDADES DE ADEQUAÇÃO DA PRESIDÊNCIA DA REPÚBLICA À LGPD

Esta ação busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos para identificar o atual estágio de adequação à LGPD pelos órgãos integrantes da PR e da VPR, por meio de metodologia estabelecida pelo Ministério da Gestão e da Inovação em Serviços Públicos.

4.1 METODOLOGIA ADOTADA PARA O DIAGNÓSTICO

A metodologia utilizada pela Presidência da República seguiu as diretrizes do **Programa de Privacidade e Segurança da Informação (PPSI),** instituído pela Portaria SGD/MGI nº 852, de 28 de março de 2023. Conforme o disposto no art. 8º da referida portaria, os órgãos e as entidades deverão adotar o Framework de Privacidade e Segurança da Informação, de responsabilidade da Estrutura de Governança de cada órgão e entidade.

Nesse contexto, com o objetivo de avaliar e mensurar o grau de maturidade dos órgãos da PR e da VPR, o Grupo de Trabalho sobre LGPD (GT - LGPD) respondeu ao questionário de privacidade, disponibilizado pela Secretaria de Governo Digital do Ministério da Gestão e Inovação em Serviços Públicos (SGD/MGI), em atendimento ao referido Framework, conforme disponível no link: ***ferramenta_framework_ppsi_v7_ciclo_4.xlsx.***

4.2 RESPOSTA AO QUESTIONÁRIO DA SGD DO MGI

Os representantes dos órgãos integrantes da Presidência da República no GT-LGPD ficaram responsáveis por consolidar as respostas do questionário e mapear as evidências correspondentes, em alguns casos.

Os resultados obtidos a partir das respostas do questionário permitiram identificar o nível de maturidade dos órgãos, possibilitando a detecção de lacunas, desafios e oportunidades relacionadas à conformidade com a LGPD.

4.3 ANÁLISE DOS RESULTADOS E ÍNDICE DE MATURIDADE

A partir dos dados do questionário, foi obtido um índice de maturidade que possibilitará aos órgãos da Presidência da República detectar as principais lacunas. Esse índice ainda indicará a direção dos esforços que deverão ser aplicados e priorizará ações que necessitam ser tomadas para adequação às obrigações presentes na LGPD, compondo, assim, o conjunto das medidas para adequação à legislação.

Desse modo, os resultados apresentados foram utilizados como subsídios para elaboração do Plano de Ações de Proteção de Dados Pessoais da Presidência da República, incluindo a definição de papéis e responsabilidades de cada órgão.

4.3.1 Capacidade e Maturidade

Os mecanismos para medir o grau de maturidade são constituídos pelos índices de maturidade em privacidade e segurança da informação do órgão, que o subsidiarão na implementação e monitoramento de controles e medidas de privacidade e segurança cibernética.

Para expressar o desempenho quanto ao atendimento dos controles previstos no Framework, propõe-se realizar avaliações de capacidade e de maturidade para obtenção dos indicadores de maturidade em privacidade (iPriv) e em segurança da informação (iSeg) da Presidência da República.

A avaliação de maturidade consiste nas seguintes etapas:
1. Implementação: Avaliação e seleção do nível de implementação por medida.
2. Capacidade: Avaliação e seleção do nível de capacidade por controle.
3. Maturidade: Obtenção do nível de maturidade por controle.
4. iSeg & iPriv: Obtenção do índice de maturidade em segurança (iSeg) e do índice de maturidade em privacidade (iPriv) com base nas respostas fornecidas em relação à adoção das medidas de cada controle.

Os resultados obtidos formam a base para a elaboração de planos de ação e estratégias futuras, o que garante a evolução contínua da PR rumo à plena conformidade com a LGPD.

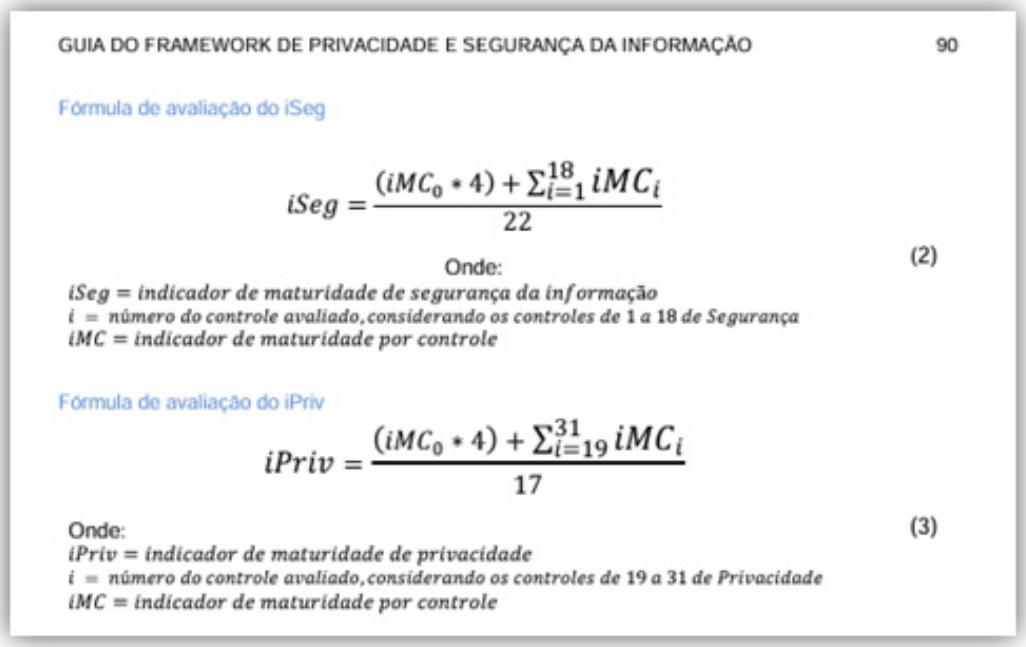
4.3.2 Obtenção do nível de maturidade por controle

A maturidade é obtida por meio da relação entre a avaliação quantitativa e a qualitativa, ou seja, considerando os níveis de implementação atribuídos às medidas e os níveis de capacidade atribuídos aos controles.

A fórmula do Indicador de Maturidade por Controle (iMC), conforme descrito na página 89 do Guia do Framework de Privacidade e Segurança da Informação, está em alinhamento ao estabelecido na Ferramenta do Framework disponibilizada aos órgãos para diagnóstico e avaliação da maturidade em Privacidade e Segurança da Informação.

4.3.3 Obtenção do iSeg e/ou iPriv

Após calculada a maturidade de todos os controles de segurança da informação ou de privacidade, os valores dos indicadores de maturidade por controle devem ser aplicados às fórmulas a seguir:



GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO 90

Fórmula de avaliação do iSeg

$$iSeg = \frac{(iMC_0 * 4) + \sum_{i=1}^{18} iMC_i}{22} \quad (2)$$

Onde:

iSeg = indicador de maturidade de segurança da informação
i = número do controle avaliado, considerando os controles de 1 a 18 de Segurança
iMC = indicador de maturidade por controle

Fórmula de avaliação do iPriv

$$iPriv = \frac{(iMC_0 * 4) + \sum_{i=19}^{31} iMC_i}{17} \quad (3)$$

Onde:

iPriv = indicador de maturidade de privacidade
i = número do controle avaliado, considerando os controles de 19 a 31 de Privacidade
iMC = indicador de maturidade por controle

Fonte: *Guia do Framework de Privacidade e Segurança da Informação, página 90.*

Destaca-se que o MGI disponibiliza ferramenta que automatiza a implementação desse Framework, inclusive os cálculos de maturidade.

O diagnóstico evidencia a necessidade de a Presidência da República e a Vice-Presidência da República adotarem medidas estruturadas e coordenadas para garantir a conformidade à LGPD. O uso do índice de maturidade de Privacidade - iPriv como ferramenta de monitoramento permitirá uma evolução consistente na proteção de dados, assegurando a confiança do cidadão nos serviços públicos digitais.

A mensuração do índice de maturidade de Privacidade – iPriv, no âmbito da PR e VPR, será feita a cada semestre, conforme ciclo avaliativo do Framework estipulado pelo MGI.

4.4 RESPONSÁVEIS PELA EXECUÇÃO E A AVALIAÇÃO DO FRAMEWORK

Para privacidade, o Encarregado pelo Tratamento de Dados Pessoais é quem atua na condução da avaliação, que deve contar com o apoio do Gestor de Segurança da Informação e do Gestor de TI.

Após a avaliação do Framework, recomenda-se a identificação dos instrumentos normativos aplicáveis à PR e à VPR, especialmente aqueles relacionados à Segurança da Informação e Privacidade, de modo a alinhar suas diretrizes à proteção de dados pessoais.

4.5 FERRAMENTA DE ACOMPANHAMENTO DA IMPLEMENTAÇÃO DO FRAMEWORK

Com a finalidade de facilitar a aplicação e acompanhamento da implementação do Framework de Privacidade e Segurança da Informação, a SGD/MGI desenvolveu uma ferramenta em formato de planilha na qual poderão ser obtidos e acompanhados indicadores de maturidade de privacidade e segurança da informação do órgão mediante preenchimento de diagnósticos.

Para verificar a evolução do cumprimento da legislação por parte dos órgãos da PR e VPR em relação à adequação à LGPD, a Subsecretaria de Gestão da Informação da Secretaria-Executiva da Casa Civil da Presidência da República desenvolveu uma solução tecnológica, com base na planilha disponibilizada pela SGD/MGI, para aumentar a eficiência na tomada de decisões no âmbito da Presidência da República.

4.6 PRODUÇÃO DO RELATÓRIO DE RECOMENDAÇÕES PARA ADERÊNCIA E CONFORMIDADE DA PR À LGPD

Para garantir a aderência da PR à LGPD, recomenda-se a consulta ao Guia de Boas Práticas da Secretaria de Governo Digital do MGI, disponível em: ***https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos.***

O Guia do Framework de Privacidade e Segurança da Informação, elaborado pela SGD/MGI, direcionado à Administração Pública Federal, difunde as melhores práticas em privacidade e proteção de dados, alinhadas à PNSI (Decreto nº 9.637/2018), à LGPD e demais normativos vigentes.

5. AÇÃO 3

RESPOSTA A VAZAMENTO DE DADOS PESSOAIS

O processo de tratamento de dados pessoais consiste na coleta, no armazenamento, no uso, no compartilhamento, na atualização, na retenção e na eliminação de tais dados. Ao longo de cada uma dessas fases, podem ocorrer falhas que resultam no vazamento de dados pessoais sob a custódia das organizações. Essas falhas podem ser causadas de forma intencional, acidental, sistêmica, fraudulenta ou por ação externa.

Cada tipo de evento exige que as organizações adotem práticas rigorosas de proteção de dados, O que inclui a implementação de tecnologias de segurança, políticas de treinamento para colaboradores e monitoramento contínuo. A conscientização e a proteção proativa são essenciais para minimizar os riscos de comprometimentos dessa natureza.

Este plano de ação foi desenvolvido para garantir que a PR esteja preparada para responder de forma ágil e eficiente a incidentes cibernéticos que envolvam dados pessoais, o que reforça a segurança da informação e a proteção dos dados sensíveis.

5.1 TIPOS DE VAZAMENTOS DE DADOS PESSOAIS

A terminologia de "Vazamento de Dados" refere-se à transmissão não autorizada de informações de uma organização para um destino ou receptor externo, que pode ocorrer tanto eletronicamente quanto fisicamente, o que compromete a segurança e a privacidade das informações. No caso de dados pessoais, podem ocorrer os seguintes tipos de vazamentos de dados: erro humano (falhas de atenção, negligência, falta de treinamento ou processos inadequados); roubo ou perda (extravio de dispositivos físicos ou transporte/armazenamento de forma inadequada); exposição de dados (informações sensíveis acessadas, visualizadas ou compartilhadas inadvertidamente por pessoas não autorizadas); compartilhamento de dados (acesso a qualquer categoria de dados sem autorização do titular, venda, utilização, divulgação ou compartilhamento desses dados com terceiros); incidente cibernético (ataque bem-sucedido realizado por agentes mal-intencionados).

Incidentes envolvendo dados pessoais representam um evento adverso que compromete sua confidencialidade e podem, também, afetar sua integridade ou disponibilidade. O vazamento de dados pessoais pode ocorrer de maneira acidental ou voluntária, o que resulta em divulgação, alteração, perda ou acesso não autorizado a esses dados.

5.2. PROCESSO DE TRATAMENTO DE INCIDENTES ENVOLVENDO VAZAMENTO DE DADOS PESSOAIS

A seguir são descritas as fases para o tratamento do incidente e as notificações decorrentes que envolvem dados pessoais no contexto dos órgãos da Presidência da República (PR), com vistas a garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Segurança da Informação (PNSI) e a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

O objetivo é garantir que, em caso de incidente cibernético envolvendo dados pessoais, as ações sejam tomadas de forma coordenada e as notificações sejam realizadas de maneira eficiente à Autoridade Nacional de Proteção de Dados (ANPD), aos agentes de tratamento de dados e aos titulares dos dados.

5.2.1 FASE 1: TRIAGEM E NOTIFICAÇÃO INICIAL

A primeira fase é voltada à realização da identificação e triagem inicial do incidente e notificação das partes envolvidas.

Conforme apresentado inicialmente, a identificação de um vazamento de dados pessoais pode ocorrer por diferentes fontes, incluindo membros da organização, titulares dos dados, terceiros, operador de dados ou em decorrência de um ataque cibernético. Independentemente da origem, a notificação deve ser imediata e seguir um fluxo bem definido para garantir a contenção e mitigação dos impactos do incidente.

A) Vazamento identificado pela própria organização

Quando um servidor da organização identifica um possível vazamento de dados pessoais, ele deve registrar todas as informações relevantes, como local do vazamento, tipo de dado comprometido, data e hora do evento. O incidente deve ser comunicado ao Encarregado de Dados Pessoais (EDP), que o informará ao controlador de dados, que acionará as áreas responsáveis pela custódia ou tratamento dos dados afetados.

O EDP, quando determinado pelo controlador de dados, deve providenciar a notificação preliminar à ANPD utilizando o formulário oficial, conforme exigido pela legislação vigente.

B) Vazamento identificado pelo titular dos dados

Se um titular perceber que seus dados pessoais foram vazados dentro da organização, ele deve registrar uma reclamação formal por meio do canal de contato do EDP, que deve estar publicamente disponível na página institucional. O EDP encaminhará a reclamação ao Gestor de Dados, que verificará a existência do vazamento junto às áreas responsáveis. Caso seja confirmada a exposição indevida de dados críticos, medidas imediatas devem ser tomadas, incluindo identificação da origem, bloqueio do acesso e correção da falha.

C) Vazamento identificado por terceiros

Quando terceiros (como parceiros, órgãos reguladores ou cidadãos comuns) identificam um vazamento de dados pessoais, devem registrar formalmente a denúncia e encaminhá-la ao EDP, por meio do canal de comunicação disponibilizado no sítio da Presidência da República, ou ainda pelo Fala.BR.

D) Vazamento identificado pelo Operador de Dados

Quando o Operador de Dados identificar indícios de vazamento de dados sob sua custódia ou tratamento, ele deverá comunicá-los imediatamente ao controlador de dados, por meio do canal previamente estabelecido em contrato. Na comunicação deve haver informações claras sobre a natureza do incidente, os dados potencialmente comprometidos, data e hora do evento, além de medidas emergenciais adotadas.

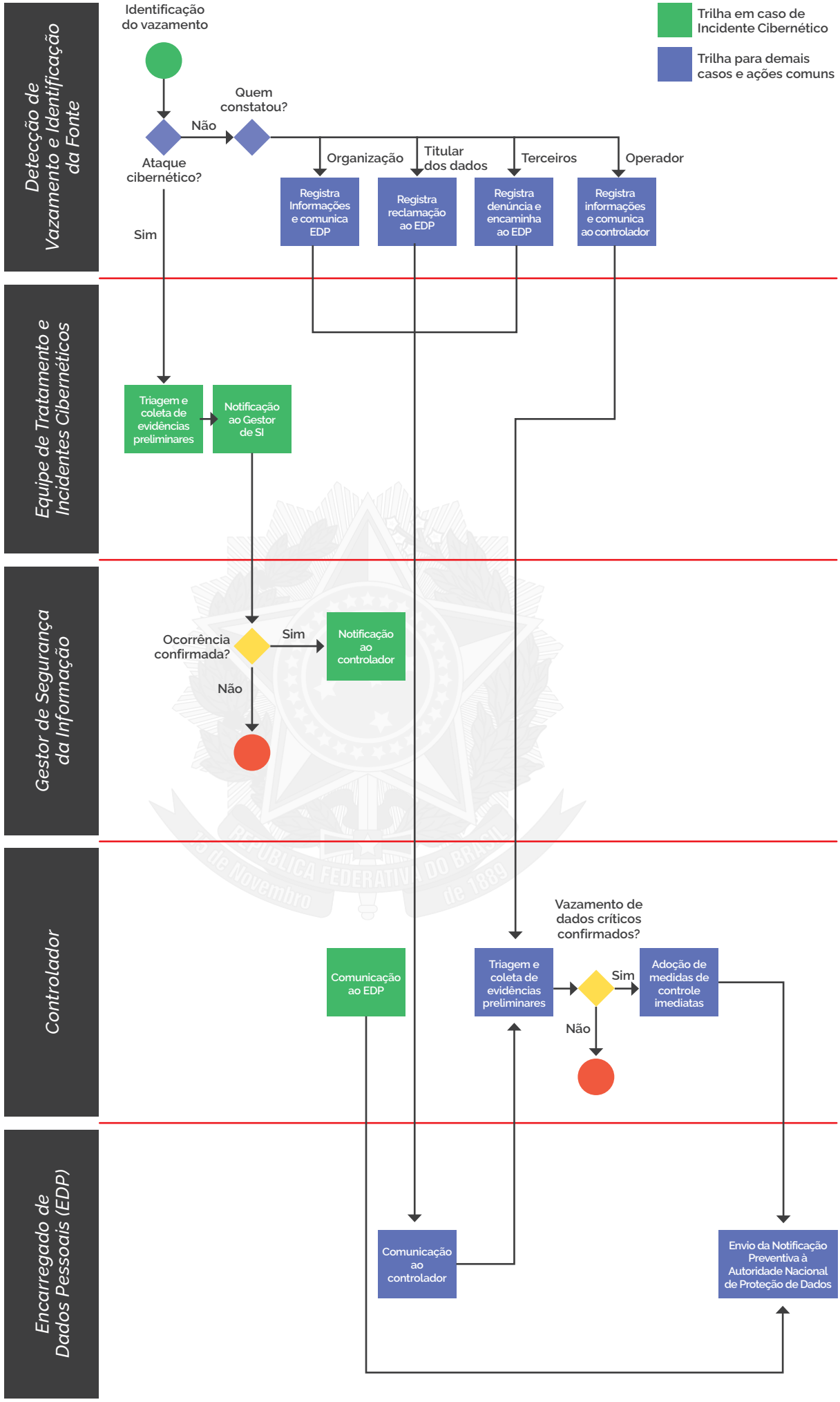
Após o recebimento da notificação, cabe ao controlador acionar o EDP e definir a necessidade de notificação preliminar à ANPD. O operador deve manter total cooperação com o controlador e fornecer registros, evidências e demais informações que auxiliem na contenção do incidente e na mitigação dos riscos aos titulares dos dados.

E) Vazamento de dados pessoais decorrente de ataque cibernético

No caso de um incidente cibernético, a Equipe de Tratamento e Resposta a Incidentes (ETIR), vinculada ao Departamento de Tecnologia (DITEC), é responsável pela identificação inicial do vazamento. A equipe deve coletar evidências sobre o incidente e notificar imediatamente o Gestor de Segurança da Informação. No caso de confirmação do incidente, o Gestor comunicará o controlador de dados que, por sua vez, comunicará o EDP.

Em qualquer um dos casos, a notificação à ANPD deve ocorrer imediatamente após a identificação do incidente, mesmo sem informações detalhadas. Essa notificação inicial é realizada pelo EDP, conforme determina o art. 48 da LGPD.

FASE 1 • TRIAGEM E NOTIFICAÇÃO INICIAL



5.2.3 FASE 2: COMPLEMENTAÇÃO DA NOTIFICAÇÃO INICIAL

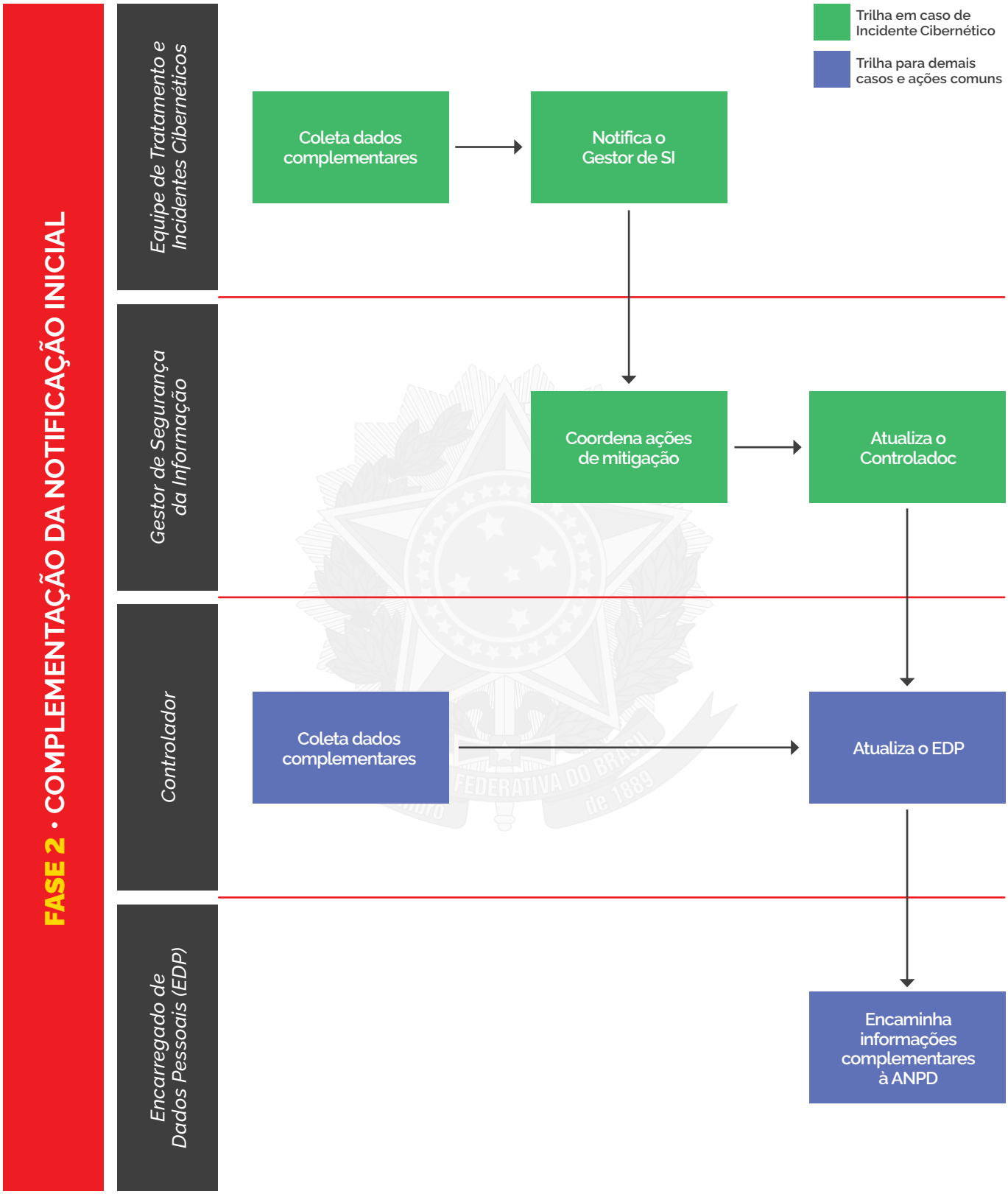
Nessa fase, o controlador busca investigar a extensão do vazamento, identifica causas, impactos, executa medidas emergenciais e encaminha à ANPD, via EDP, as informações complementares, o que garante que o órgão regulador tenha uma visão detalhada da situação.

Especificamente no caso de vazamento por incidente cibernético, é a ETIR Planalto a responsável pela coleta das informações adicionais para detalhar o incidente. Esses dados são enviados ao Gestor de Segurança da Informação, que coordena ações internas para mitigação do incidente e mantém o controlador atualizado.

Da mesma forma que existe um processo de controle de informações e evidências de casos tratados pela ETIR Planalto, o controlador de dados também deve gerenciar essas referências.

Assim, é necessário que o controlador mantenha um repositório centralizado de arquivos, onde as informações complementares devem ser armazenadas, de modo a permitir a rastreabilidade dos casos tratados, e ainda servir de base para eventual análise de lições aprendidas ou auditorias. Para isso, o controlador deve recomendar ao EDP a utilização do SUPER/SEI para registro de processos enviados à ANPD, além de manter pastas específicas para cada caso no servidor de arquivos da PR.

Se houver risco significativo aos direitos dos titulares, a ANPD deve ser notificada dentro do prazo de 72 horas, conforme exigido pela LGPD.


FASE 2 • COMPLEMENTAÇÃO DA NOTIFICAÇÃO INICIAL
Equipe de Tratamento e Incidentes Cibernéticos
Gestor de Segurança da Informação
Controlador
Encarregado de Dados Pessoais (EDP)
Trilha em caso de Incidente Cibernético
Trilha para demais casos e ações comuns
Coleta dados complementares
Notifica o Gestor de SI
Coordena ações de mitigação
Atualiza o Controladoc
Coleta dados complementares
Atualiza o EDP
Encaminha informações complementares à ANPD

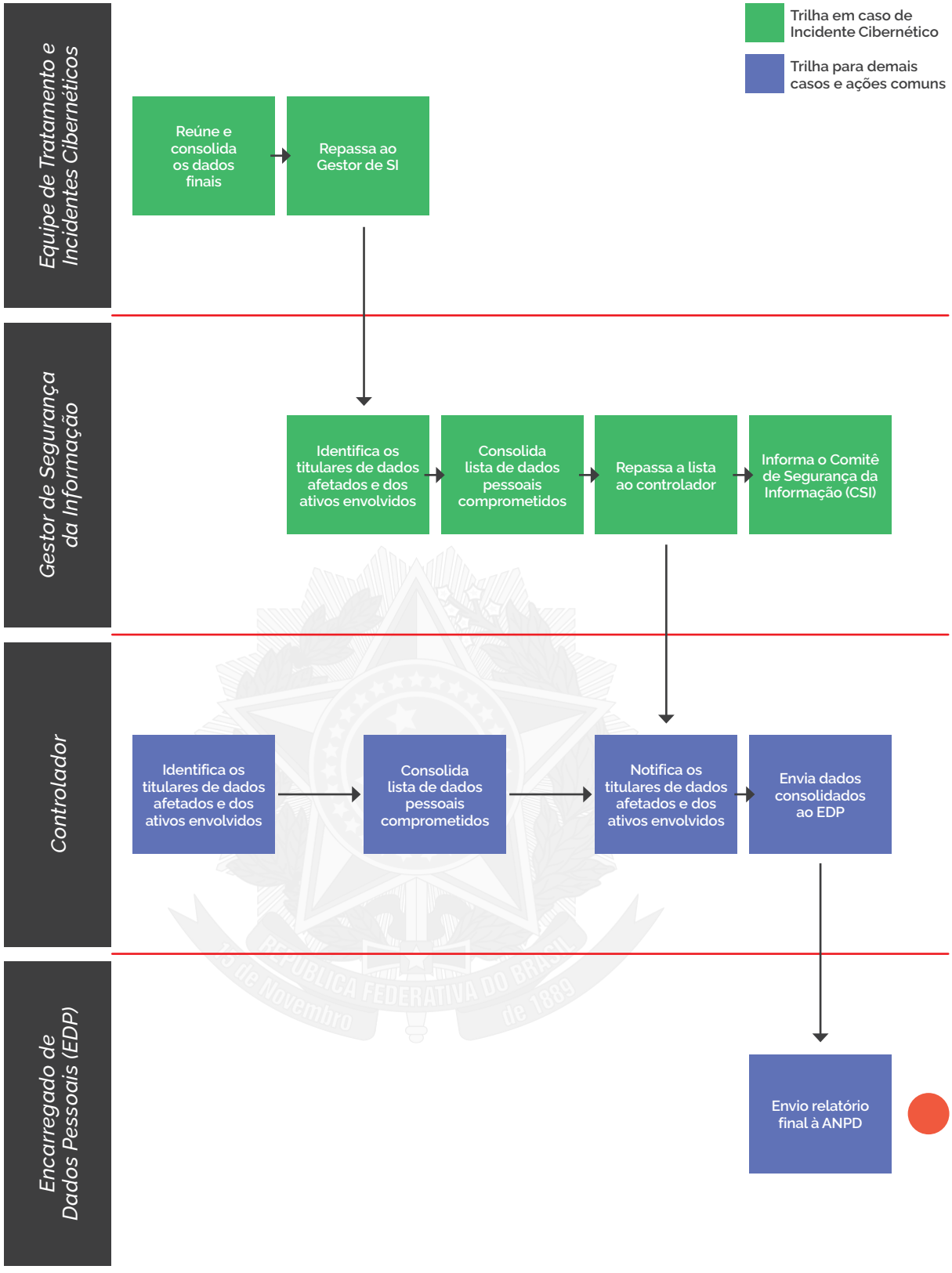
5.2.4 FASE 3: CONSOLIDAÇÃO DOS DADOS E NOTIFICAÇÃO FINAL

Na última fase, todas as informações sobre o incidente são consolidadas e os titulares dos dados vazados são identificados. O controlador de dados é responsável pela notificação final aos titulares dos dados comprometidos, e informa-os sobre o incidente, os riscos e as medidas adotadas.

O meio para notificação do titular dos dados comprometidos será definido pelo controlador de dados a partir das informações apresentadas pelo proprietário do ativo envolvido. Caso a notificação individual não seja viável, excepcionalmente poderão ser utilizados meios coletivos, como publicações em sítios institucionais ou redes sociais.

Uma vez que o vazamento tenha ocorrido por ataque cibernético, a ETIR Planalto reúne os dados do incidente, que incluem origem, impacto e medidas de mitigação. O Gestor de Tecnologia da Informação e Comunicações (Gestor de TIC) identifica os titulares dos dados comprometidos e os responsáveis pelos ativos envolvidos. Em seguida, o Gestor de Segurança da Informação analisa as informações recebidas e coordena as ações finais para mitigar riscos.

FASE 3 • COMPLEMENTAÇÃO DA NOTIFICAÇÃO INICIAL



EM QUALQUER UMA DAS SITUAÇÕES, A ANPD DEVE RECEBER O RELATÓRIO FINAL SOBRE O INCIDENTE NO PRAZO DE 20 DIAS ÚTEIS, CONFORME DETERMINADO PELA LEGISLAÇÃO VIGENTE.

5.3 CONSIDERAÇÕES FINAIS

Alguns documentos são fundamentais para identificar tratamentos que exigem avaliação de impacto e garantem transparência, segurança e governança na proteção de dados. O primeiro é o Inventário de Dados Pessoais (IDP) que, quando atualizado, é essencial, pois permite mapear os dados pessoais tratados e identificar o proprietário do ativo envolvido para determinar sua origem, o que agiliza a comunicação com o titular dos dados comprometidos.

O segundo é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no art. 38 da LGPD, que fornece uma análise prévia e detalhada sobre os riscos associados ao tratamento desses dados, bem como as medidas de mitigação adotadas pela organização.

Por fim, nota-se que a adoção de boas práticas e a clareza nas notificações ao órgão regulador, aos gestores e aos titulares de dados são fundamentais para minimizar os impactos do vazamento e garantir a proteção dos direitos dos titulares dos dados pessoais.

5. AÇÃO 4

PROGRAMA DE CAPACITAÇÃO CONTÍNUA EM LGPD

No intuito de conscientizar os servidores acerca da importância do assunto, foi elaborado um Programa de Capacitação Contínua em Proteção de Dados. O objetivo desse programa é fortalecer a governança e promover uma cultura organizacional de proteção e privacidade de dados pessoais, de forma a padronizar práticas adequadas e em conformidade com a LGPD, por meio de conteúdos e treinamentos disponibilizados.

6. REFERÊNCIAS

BRASIL. Guia de Resposta a Incidentes de Segurança. Programa de Privacidade e Segurança da Informação (PPSI). Versão 3.3. Brasília, julho de 2024. BRASIL. Instrução Normativa nº 1, de 27 de maio de 2020. Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2020. Disponível em: *https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215* - Acesso em: 7 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: *https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm* Acesso em: 28 fev. 2025.

BRASIL. Presidência da República. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: *https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm* - Acesso em: 7 mar. 2025.

CCGD (2020) - Guia de Boas Práticas LGPD. COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. Guia de Boas Práticas LGPD. Abril 2020. *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf* - Acesso em 16/12/2024.

BRASIL (2018) - Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm* - Acesso em 16/12/2024.

MGI (2023) - Guia de Elaboração de Inventário de Dados Pessoais atualizado pelo Ministério da Gestão e da Inovação em Serviços Públicos. *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf* - Acesso em 16/12/2024.

8. GLOSSÁRIO

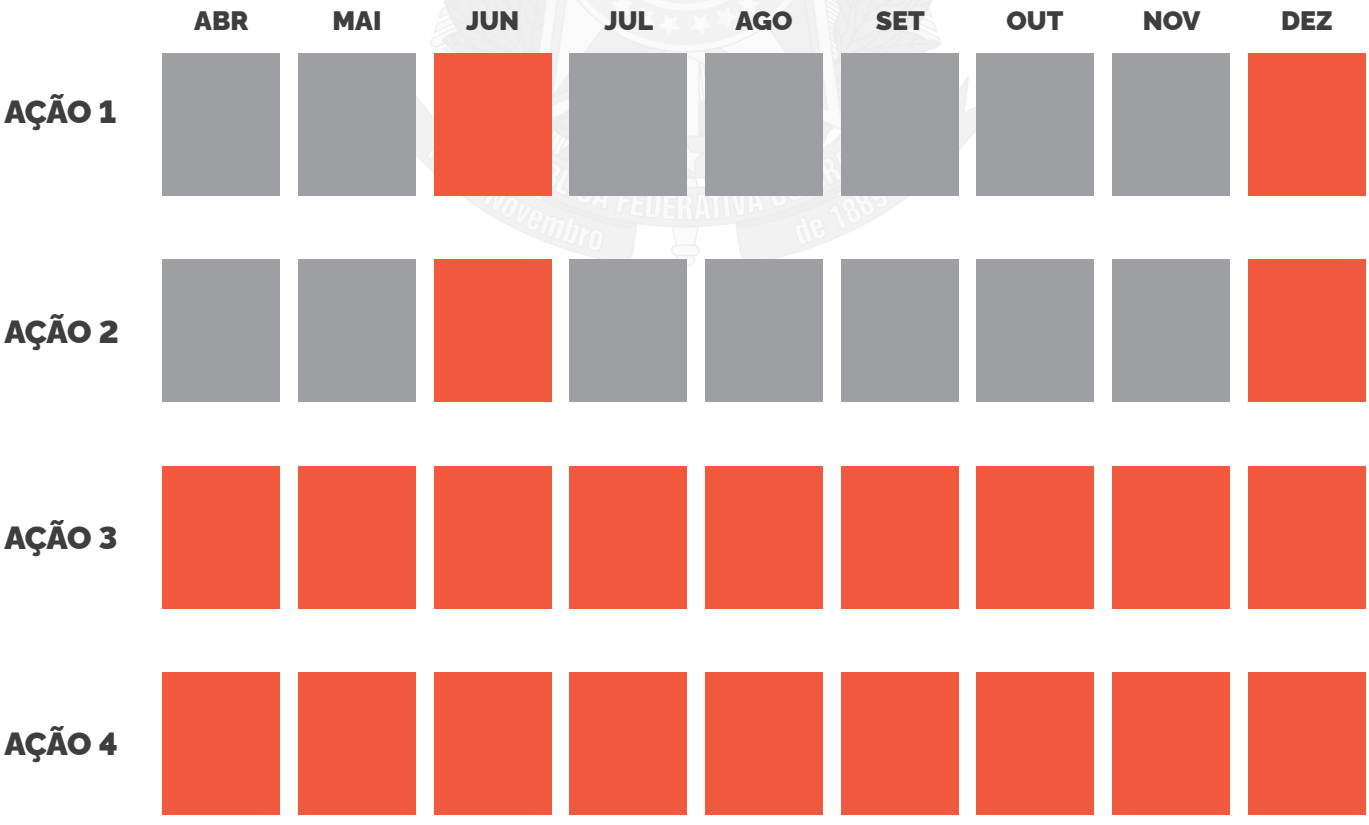
- **ANPD (Autoridade Nacional de Proteção de Dados):** Órgão regulador da LGPD.
- **CGD/PR (Comitê de Governança Digital e Segurança da Informação da Presidência da República):** Comitê que supervisiona o programa PGP/PR.
- **CSA Control Self-Assessment (Autoavaliação de Controles):** Metodologia utilizada para a autoavaliação da conformidade com a LGPD.
- **Controlador:** Pessoa física ou jurídica que determina a finalidade e os meios do tratamento de dados pessoais.
- **Encarregado de Dados Pessoais - EDP:** Responsável pela garantia da conformidade com a LGPD dentro da organização.
- **GT-LGPD:** Grupo de Trabalho Lei Geral de Proteção de Dados Pessoais. Grupo formado para adequação à LGPD na Presidência da República, integrado pelos órgãos: Casa Civil, GSI, SRI, SECOM, SA, SG, GPPR, VPR.
- **IDP (Inventário de Dados Pessoais):** Ferramenta para mapear e documentar as operações de tratamento de dados.
- **iMC:** Indicador de Maturidade por Controle. Indicador de desempenho do Framework PPSI.
- **iPriv:** Índice de Maturidade em Privacidade. Métrica para avaliar o nível de maturidade em privacidade.
- **iPRIV:** Controles específicos de privacidade (do Framework PPSI).
- **iSeg:** Índice de Maturidade em Segurança da Informação. Métricas para avaliar o nível de maturidade em segurança da informação.
- **Intermediação entre a Sociedade e a ANPD:** A lei estabelece que há uma função de intermediação entre a sociedade e a Autoridade Nacional de Proteção de Dados (ANPD) e o controlador, com vistas à proteção dos dados pessoais.
- **LGPD (Lei Geral de Proteção de Dados):** Lei nº 13.709/2018.
- **PPSI:** Programa de Privacidade e Segurança da Informação. Framework do Ministério da Gestão e da Inovação para avaliar e melhorar a privacidade e a segurança da informação em órgãos públicos.
- **PGP/PR (Programa de Governança em Privacidade da Presidência da República):** Programa descrito nos documentos.
- **POSIN/PR (Política de Segurança da Informação da Presidência da República):** Política de segurança da informação.
- **Proprietário da Informação:** De acordo com o GSI, refere-se à entidade que detém a titularidade dos dados e é responsável por sua gestão.
- **Operador:** Pessoa física ou jurídica que trata dados pessoais em nome do controlador.
- **RIPD (Relatório de Impacto à Proteção de Dados Pessoais):** Instrumento para avaliar os riscos associados ao tratamento de dados.
- **SGD/MGI:** Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos. Órgão responsável pela elaboração e disseminação de diretrizes em governança digital.
- **TCU:** Tribunal de Contas da União. Órgão de controle externo do governo federal brasileiro.
- **Usuários de Informação:** Refere-se aos indivíduos ou entidades que acessam e utilizam a informação tratada.

8.1 LISTA DE SIGLAS E ABREVIATURAS:

- **ANPD:** *Autoridade Nacional de Proteção de Dados*
- **CC:** *Casa Civil*
- **CGD/PR: C***omitê de Governança Digital e Segurança da Informação da Presidência da República*
- **DITEC:** *Diretoria de Tecnologia da Presidência da República*
- **GSI:** *Gabinete de Segurança Institucional da Presidência da República*
- **GPPR:** *Gabinete Pessoal do Presidente da República*
- **LGPD:** *Lei Geral de Proteção de Dados*
- **MGI:** *Ministério da Gestão e Inovação em Serviços Públicos*
- **iMC:** *Indicador de Maturidade por Controle (do Framework PPSI)*
- **iPriv:** *Índice de Maturidade em Privacidade (do Framework PPSI)*
- **iPRIV:** *Controles específicos de privacidade (do Framework PPSI)*
- **iSeg:** *Índice de Maturidade em Segurança da Informação (do Framework PPSI)*
- **IDP:** *Inventário de Dados Pessoais*
- **PGP/PR:** *Programa de Governança em Privacidade da Presidência da República*
- **POSIN/PR:** *Política de Segurança da Informação da Presidência da República*
- **PPSI:** *Programa de Privacidade e Segurança da Informação*
- **SG:** *Secretaria-Geral da Presidência da República*
- **SGD:** *Secretaria de Governo Digital do Ministério da Gestão e Inovação*
- **SECOM:** *Secretaria de Comunicação Social da Presidência da República*
- **SRI:** *Secretaria de Relações Institucionais da Presidência da República*
- **TCU:** *Tribunal de Contas da União*
- **VPR:** *Vice-Presidência da República*

9. CRONOGRAMA DE EXECUÇÃO

AÇÃO 1 Elaboração/Atualização/Manutenção do Inventário de Dados Pessoais da Presidência da República	**PRAZO** Setembro 2025 **Prazo de manutenção:** semestralmente (junho e dezembro)
AÇÃO 2 Diagnóstico das Necessidades de Adequação da Presidência da República à LGPD	**PRAZO** Semestralmente (junho e dezembro)
AÇÃO 3 Resposta a Vazamento de Dados Pessoais	**PRAZO** sob demanda (depende se existir vazamentos)
AÇÃO 4 Programa de Capacitação Contínua em LGPD	**PRAZO** Todos os meses (contínuo)




GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO