PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

PRESIDÊNCIA DA REPÚBLICA[1]

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO

1. *Versão 3 • 31.03.2025*

SUMÁRIO

1. PROGRAMA

1.1 INTRODUÇÃO

A Lei n° 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. O objetivo desta legislação é proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Este programa é uma atualização do Programa de Governança em Privacidade da Presidência da República (PGP/PR), instituído pela Resolução CGD/PR nº 8, de 2 de setembro de 2021, em atendimento à Resolução CGD/PR nº 43, de 8 de outubro de 2024 e à Resolução nº 46, de 20 de maio de 2025.

O PGP/PR reflete o compromisso da Presidência da República (PR) com a conformidade às disposições da LGPD e o alinhamento às boas práticas de proteção de dados pessoais da Administração Pública Federal, em conformidade com o "Guia de elaboração de programa de governança em privacidade" (MGISP, 2024), promovendo segurança e transparência no tratamento de dados no âmbito institucional. Adicionalmente, o programa será atualizado periodicamente, conforme as necessidades do órgão ou para assegurar o alinhamento com as diretrizes da ANPD.

1.2 OBJETIVO

O PGP/PR tem como objetivo assegurar a proteção de dados pessoais e a privacidade dos cidadãos, em conformidade com a LGPD, ao longo de todas as etapas do tratamento de dados no âmbito institucional.

O programa promove a implementação de práticas de governança que atendem aos requisitos legais previstos no art. 50 da LGPD, garantindo o uso responsável e seguro das informações. Além disso, busca integrar políticas de proteção de dados à estrutura organizacional, fortalecendo a confiança, a transparência e o respeito à privacidade, tanto nas operações internas quanto na relação com a sociedade.

2. ETAPAS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

2.1 INÍCIO E PLANEJAMENTO

A etapa de início e planejamento estabelece as bases para a estruturação do PGP/PR, identificando informações e dados essenciais para garantir a conformidade com a LGPD e o fortalecimento das práticas institucionais de governança em privacidade.

Essa etapa organiza-se em marcos principais, como a nomeação de responsáveis, o mapeamento de dados pessoais e a análise da maturidade organizacional, preparando a instituição para os desafios do tratamento de dados pessoais e assegurando alinhamento às disposições legais.

2.1.1 NOMEAÇÃO DO ENCARREGADO

O Encarregado de Tratamento de Dados Pessoais (EDP) atua como o canal de comunicação entre a PR, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Os dados do EDP da Presidência da República são públicos e podem ser acessadosno sítio eletrônico pelo link: *https://www.gov.br/casacivil/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/dados-do-encarregado-pelo-tratamento-de-dados-pessoais-da-presidencia-da-republica-art-41-da-lgpd/*.

As principais atribuições do EDP da Presidência da República incluem:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da ANPD e adotar providências necessárias;
- orientar os funcionários e contratados sobre práticas relacionadas à proteção de dados pessoais;
- apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais, conforme determinado pelo art. 37 da LGPD;
- conduzir ou aconselhar a elaboração de relatórios de impacto à proteção de dados pessoais, conforme casos previstos pela LGPD;
- executar demais atribuições previstas em normas complementares ou determinadas pela Presidência da República.

2.1.2 ALINHAMENTO DE EXPECTATIVAS COM A ALTA ADMINISTRAÇÃO

O envolvimento da alta administração é essencial para consolidar o compromisso institucional com a proteção de dados pessoais. No âmbito da PR, o Comitê de Governança Digital e Segurança da Informação (CGD/PR), conforme competências estabelecidas pelo Decreto nº 10.433, de 20 de julho de 2020, desempenha um papel estratégico na aprovação e supervisão das políticas e ações do PGP/PR, garantindo que os objetivos estratégicos estejam alinhados às diretrizes da LGPD.

Esse alinhamento é promovido por meio de discussões estratégicas, acompanhamento das ações do programa e validação das prioridades estabelecidas para a implementação de práticas de governança em privacidade e segurança da informação.

2.1.3 MATURIDADE DA ORGANIZAÇÃO

O diagnóstico do nível de maturidade da Presidência da República em relação à adequação à LGPD foi realizado com base no framework do Programa de Privacidade e Segurança da Informação (PPSI), desenvolvido pelo Ministério da Gestão e da Inovação (MGI). Esse diagnóstico considerou os controles específicos de privacidade (iPRIV) para mensuração da conformidade com a legislação e a implementação das boas práticas de proteção de dados.

Os resultados da avaliação fornecem uma visão ampla sobre as práticas institucionais relacionadas à proteção de dados pessoais, destacando áreas de excelência e oportunidades de aprimoramento. O Framework PPSI continuará sendo utilizado como ferramenta estratégica para monitoramento e planejamento contínuos, apoiando a implementação de ações alinhadas às necessidades institucionais e às diretrizes da LGPD.

2.1.4 MEDIDAS DE SEGURANÇA

A proteção de dados pessoais é um pilar essencial do PGP/PR, assegurando conformidade com a LGPD e prevenindo acessos não autorizados, além de mitigar riscos acidentais ou ilícitos que possam comprometer a integridade, confidencialidade e disponibilidade dos dados.

De acordo com o art. 46 da LGPD, os agentes de tratamento devem implementar medidas técnicas e administrativas desde a concepção até a execução dos serviços ou produtos, garantindo que a segurança e a proteção dos dados sejam incorporadas desde as fases iniciais. Essas diretrizes serão aprofundadas no item 2.2.2, que trata da Cultura de Segurança e Proteção de Dados e Privacidades desde a concepção.

No âmbito da Presidência da República, as principais medidas de segurança incluem:

- alinhamento normativo, consistindo em revisão e aprimoramento contínuos das diretrizes de segurança, seguindo orientações da ANPD e do Gabinete de Segurança Institucional (GSI).
- proteção tecnológica, que se refere à implementação de ferramentas avançadas de criptografia e controle de acesso para garantir a segurança durante todas as fases do tratamento de dados pessoais.
- gestão de incidentes, por meio do desenvolvimento e atualização de um Plano de Resposta a Incidentes, com ações rápidas e coordenadas para minimizar impactos em caso de violações de dados;
- diretrizes institucionais, que consistem na promoção de uma política de segurança da informação abrangente, incluindo orientações específicas para proteção de dados pessoais;
- capacitação de servidores, promovendo treinamentos contínuos para conscientizar os colaboradores sobre as diretrizes de proteção de dados, práticas de segurança da informação e prevenção de incidentes, garantindo que todos compreendam seus papéis e responsabilidades no tratamento de dados pessoais.

2.1.5 ESTRUTURA ORGANIZACIONAL PARA GOVERNANÇA E GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS

A governança da proteção de dados na PR é composta por instâncias estratégicas e operacionais que garantem a implementação do PGP/PR e o cumprimento da LGPD.

O Comitê de Governança Digital e Segurança da Informação (CGD/PR) é responsável pelas diretrizes e decisões estratégicas sobre o tratamento de dados pessoais. Complementarmente, há uma instância colegiada de proteção de dados, que promove a articulação entre as unidades organizacionais para a aplicação das políticas institucionais.

Todas as unidades da PR, gestores e colaboradores têm a responsabilidade de assegurar a conformidade com a LGPD, garantindo que suas atividades e processos estejam alinhados às normas e às boas práticas de proteção de dados.

2.1.6 INVENTÁRIO DE DADOS PESSOAIS

O inventário de dados pessoais (IDP) é uma ferramenta essencial para mapear e documentar as operações de tratamento de dados pessoais realizadas pela PR, conforme o art. 37 da LGPD. Ele oferece uma visão abrangente do ciclo de vida dos dados pessoais, desde a coleta até a eliminação, possibilitando a identificação de riscos, áreas críticas e oportunidades de melhoria.

O IDP será elaborado e atualizado com base no modelo proposto pelo Guia de Elaboração de Inventário de Dados Pessoais, publicado pela Secretaria de Governo Digital (SGD). Esse modelo poderá ser ajustado para incorporar novos campos ou atender às necessidades específicas da PR, assegurando alinhamento às melhores práticas e a conformidade com a LGPD.

As informações registradas no IDP devem incluir, no mínimo:

- os atores envolvidos, identificando os agentes de tratamento e o encarregado de tratamento de dados pessoais;
- a finalidade do tratamento dos dados pessoais;
- a hipótese legal, ou seja, a base jurídica para o tratamento, conforme os arts. 7º e 11 da LGPD;
- a previsão legal, que consiste na regulamentação que embasa o tratamento;
- os dados pessoais tratados, contendo o detalhamento dos dados pessoais e sensíveis utilizados;
- as categorias de titulares, representando a classificação dos titulares dos dados;
- o tempo de retenção, ou seja, o prazo pelo qual os dados são armazenados;
- as instituições com as quais os dados são compartilhados;
- a identificação de transferências de dados para fora do país, conforme o art. 33 da LGPD; e
- as medidas de segurança, ou seja, os controles técnicos e administrativos atualmente adotados.

Além de garantir a conformidade com a LGPD, o IDP servirá como base para:

- avaliações de impacto, para identificar vulnerabilidades e planejar ações mitigadoras;
- monitoramento e auditoria, para assegurar que as operações de tratamento estejam em conformidade com os princípios legais; e
- elaboração de políticas internas, para promover a transparência e fortalecer a governança de dados pessoais.

2.1.7 LEVANTAMENTO DE CONTRATOS RELACIONADOS A DADOS PESSOAIS

O levantamento de contratos relacionados ao tratamento de dados pessoais é uma etapa fundamental para assegurar a conformidade contratual com a LGPD e reforçar a governança em privacidade. Esse processo consiste em mapear os contratos vigentes e correlacioná-los aos serviços identificados no Inventário de Dados Pessoais (IDP), com foco na análise de aspectos como coleta, transferência, armazenamento e processamento de dados pessoais.

Além disso, a adequação dos contratos existentes e a inclusão de cláusulas específicas para proteção de dados em futuros instrumentos contratuais são essenciais para mitigar riscos e garantir a transparência no tratamento de dados pessoais. Essa análise deve incluir:

- a definição de responsabilidades, contendo uma delimitação clara entre controladores e operadores;
- a finalidade do tratamento, com a garantia de que os dados sejam utilizados exclusivamente para os fins previstos contratualmente;
- as medidas de segurança, por meio do estabelecimento de controles técnicos e administrativos para proteção dos dados;
- a notificação de incidentes, prevendo obrigações para informar qualquer incidente relacionado ao tratamento de dados pessoais; e
- a observância de requisitos para compartilhamento e transferência internacional de dados, conforme o art. 33 da LGPD.

2.2 CONSTRUÇÃO E EXECUÇÃO

A etapa de construção e execução é dedicada à implementação prática das ações planejadas para assegurar a conformidade com a LGPD. Nessa fase, o foco está em operacionalizar as iniciativas definidas, integrando-as à estrutura institucional e promovendo a proteção efetiva dos dados pessoais tratados pela PR.

Os marcos dessa etapa abrangem medidas específicas que visam fortalecer a governança em privacidade e garantir a aplicação dos princípios legais no tratamento de dados pessoais.

2.2.1 POLÍTICAS E PRÁTICAS PARA PROTEÇÃO DA PRIVACIDADE DO CIDADÃO

O PGP/PR estabelece diretrizes para garantir que o tratamento de dados pessoais seja conduzido de maneira transparente, segura e em conformidade com a LGPD. O foco dessa etapa é assegurar que a proteção da privacidade dos cidadãos seja incorporada nas atividades institucionais da PR, de acordo com o que estabelece a Política de Segurança da Informação da Presidência da República (POSIN/PR). As práticas incluem:

- a promoção de uma cultura de privacidade e segurança por meio de ações educativas junto aos servidores e colaboradores;
- o desenvolvimento de documentos normativos que detalhem as responsabilidades e os procedimentos relacionados ao tratamento de dados pessoais, como Avisos de Privacidade e Termos de Uso;
- a comunicação clara e acessível das práticas de proteção de dados por meio de canais institucionais.

2.2.2 CULTURA DE SEGURANÇA E PROTEÇÃO DE DADOS E PRIVACIDADE DESDE A CONCEPÇÃO

A consolidação de uma cultura de segurança e proteção de dados é essencial para a efetividade do PGP/PR. Para isso, é necessário estabelecer iniciativas contínuas de conscientização e treinamento, promovendo o entendimento das responsabilidades e das boas práticas relacionadas ao tratamento de dados pessoais em todos os níveis da PR.

Entre os pilares dessa cultura está o conceito de Proteção de Dados e Privacidade desde a Concepção, que determina que a privacidade e a segurança da informação devem ser incorporadas desde a fase inicial e ao longo de todo o ciclo de vida de sistemas, processos e serviços. Isso significa que as diretrizes de proteção de dados não devem ser adicionadas posteriormente, mas sim embutidas desde o desenvolvimento dos processos institucionais.

De acordo com o Guia de Boas Práticas da LGPD, essa abordagem se fundamenta em sete princípios essenciais:

- Proatividade e prevenção: antecipação de riscos e implementação de medidas preventivas para evitar incidentes de segurança.
- Privacidade como padrão: garantia de que os dados pessoais sejam protegidos automaticamente, sem necessidade de ação adicional por parte do titular.
- Integração ao projeto: a proteção de dados deve ser um elemento essencial dos processos e tecnologias, e não um complemento.
- Funcionalidade completa: a implementação de segurança deve coexistir com a plena funcionalidade dos serviços, sem comprometer sua eficiência.
- Proteção ao longo do ciclo de vida: desde a coleta até a eliminação dos dados, assegurando integridade, segurança e conformidade.
- Visibilidade e transparência: processos claros, auditáveis e de fácil compreensão, garantindo a confiança no tratamento dos dados.
- Respeito à privacidade do usuário: adoção de práticas que priorizem a proteção dos direitos dos titulares de dados pessoais.

Para viabilizar a implementação desses princípios na PR, serão adotadas campanhas de comunicação interna, treinamentos contínuos, disseminação de manuais e uso de ferramentas institucionais voltadas à segurança da informação. Adicionalmente, a capacitação de servidores e colaboradores será promovida para garantir que todos compreendam seus papéis e responsabilidades no tratamento de dados pessoais, fortalecendo, assim, uma cultura organizacional que valorize a privacidade e a segurança desde a concepção.

2.2.3 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um instrumento fundamental para documentar e avaliar os riscos associados ao tratamento de dados pessoais, assegurando conformidade com a LGPD e mitigando possíveis impactos aos direitos e liberdades fundamentais dos titulares. O controlador é o responsável por sua elaboração, devendo adotá-lo sempre que houver tratamento de alto risco, conforme definido pelo regulamento da ANPD.O RIPD deve conter informações detalhadas sobre o tratamento de dados pessoais, incluindo a identificação dos agentes de tratamento, a descrição dos dados coletados e suas finalidades, as bases legais aplicáveis, a análise dos riscos envolvidos e as medidas adotadas para mitigação de impactos. Além disso, deve documentar consultas realizadas com partes

interessadas e assegurar que o tratamento de dados atenda aos princípios da necessidade e proporcionalidade, evitando excessos no uso das informações.

Para garantir uniformidade e alinhamento com as melhores práticas, a PR adotará o modelo de RIPD proposto pelo Guia de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais, publicado pela Secretaria de Governo Digital (SGD). Esse modelo estabelece um roteiro padronizado para a construção do documento, permitindo que sejam avaliadas todas as etapas do tratamento de dados de forma estruturada e transparente.

O RIPD não é de publicação obrigatória, mas pode ser disponibilizado parcialmente caso necessário, respeitando a proteção de informações sensíveis. Sua versão completa será encaminhada à ANPD apenas mediante solicitação. Além disso, o relatório deve ser revisado periodicamente, especialmente quando houver mudanças significativas no tratamento de dados, como a adoção de novas tecnologias, alteração na base legal, ampliação da coleta de informações ou ocorrência de incidentes de segurança que exijam reavaliação das práticas institucionais.

2.2.4 MEDIDAS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E POLÍTICA DE PRIVACIDADE

A PR adota um conjunto de políticas institucionais voltadas à segurança da informação, como a política de controle de acesso e a política de backup e recuperação de dados, que são fundamentais para garantir a integridade e a disponibilidade das informações institucionais. Essas políticas, respaldadas por resoluções do Comitê de Governança Digital e Segurança da Informação (CGD/PR), são desenvolvidas em conformidade com normativos nacionais, incluindo a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

A Política de Segurança da Informação da Presidência da República (POSIN/PR) estabelece diretrizes estratégicas para a proteção da informação e governança de dados no âmbito da PR, alinhando as práticas adotadas às exigências da Lei Geral de Proteção de Dados (LGPD). A POSIN/PR também incorpora as diretrizes da Política de Privacidade, consolidando as normas e responsabilidades relacionadas ao tratamento de dados pessoais.

A estrutura e as diretrizes da POSIN/PR foram elaboradas considerando as recomendações e parâmetros estabelecidos pelo Modelo de Política de Segurança da Informação e pelo Modelo de Política de Proteção de Dados Pessoais, ambos desenvolvidos pelo Ministério da Gestão e da Inovação em 2024, visando garantir alinhamento às melhores práticas e normas aplicáveis à Administração Pública Federal.

2.2.5 ADEQUAÇÃO DE CLÁUSULAS CONTRATUAIS

A adequação de cláusulas contratuais no âmbito da Presidência da República é uma etapa crucial para assegurar que todos os instrumentos jurídicos que impliquem o tratamento de dados pessoais estejam em conformidade com os princípios e requisitos da LGPD. Essa iniciativa inclui contratos, convênios e outros documentos que regulem relações jurídicas com terceiros, envolvendo o compartilhamento, armazenamento ou processamento de dados pessoais.

Esse processo está diretamente vinculado ao Inventário de Dados Pessoais (IDP) e ao levantamento de contratos relacionados a dados pessoais, realizados na etapa de planejamento do Programa de Governança em Privacidade. O objetivo é garantir a proteção e segurança

dos dados tratados, alinhando os instrumentos contratuais ao princípio da transparência e aos demais princípios definidos no art. 6º da LGPD.

Nos contratos, devem ser consideradas cláusulas que tratem, de forma clara e objetiva, aspectos como:

- responsabilidades do controlador e operador no tratamento dos dados;
- critérios para coleta, uso, armazenamento e eliminação dos dados;
- direitos dos titulares, incluindo acesso, correção, revogação de consentimento e eliminação dos dados;
- medidas de segurança implementadas para proteção dos dados, incluindo requisitos de auditoria e governança;
- comunicação à Administração sobre eventuais subcontratações ou suboperadores que tratem os dados pessoais;
- obrigação de notificação imediata em caso de incidentes envolvendo dados pessoais.

2.2.6 TERMO DE USO E POLÍTICA DE PRIVACIDADE

O Termo de Uso e a Política de Privacidade da PR são documentos essenciais para garantir a transparência, a clareza e a conformidade das atividades de tratamento de dados pessoais realizadas no âmbito dos serviços públicos oferecidos. Em consonância com o Guia de Elaboração de Termo de Uso e Política de Privacidade, publicado pela SGD, ambos os instrumentos visam estabelecer os direitos e as responsabilidades dos usuários e da Administração Pública no contexto do tratamento de dados pessoais.

O Termo de Uso detalha as condições e as regras aplicáveis à utilização dos serviços disponibilizados pela PR, apresentando uma descrição clara das suas finalidades, bem como os deveres do controlador e do titular dos dados. Já a Política de Privacidade é um documento complementar que descreve como os dados pessoais são coletados, armazenados, processados e protegidos, assegurando o cumprimento dos princípios dispostos no artigo 6º da LGPD.

Ambos os documentos deverão abordar tópicos essenciais, tais como:

- aceitação dos termos e condições;
- definições e arcabouço legal;
- finalidades do tratamento de dados pessoais;
- direitos dos titulares, incluindo acesso, correção e eliminação de dados;
- medidas de segurança e proteção adotadas;
- responsabilidades dos usuários e da PR no uso dos serviços;
- alterações nos termos de uso e políticas aplicáveis; e
- informações de contato para esclarecimentos e solicitações.

A PR adotará uma abordagem proativa, promovendo a atualização periódica desses documentos, para assegurar que as informações neles contidas estejam alinhadas às melhores práticas de governança e às exigências legais. Além disso, serão disponibilizados em locais de destaque nos canais institucionais, facilitando o acesso do cidadão e reforçando o compromisso com a transparência e a proteção de dados pessoais.

2.2.7 O ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS

O Encarregado de Dados Pessoais desempenha um papel essencial na execução do Programa de Governança em Privacidade da Presidência da República, garantindo o cumprimento da LGPD e das regulamentações da ANPD. Na etapa de Construção e Execução, suas principais responsabilidades incluem:

- implementar o plano de ação definido na etapa de Planejamento, assegurando a conformidade das atividades com as metas estabelecidas;
- reportar regularmente aos dirigentes da PR os avanços e resultados alcançados nas iniciativas de proteção de dados pessoais;
- atualizar e manter a documentação relativa ao tratamento de dados pessoais, abrangendo políticas, inventários, incidentes e registros de atividades planejadas e executadas; e
- estabelecer mecanismos de comunicação interna que garantam transparência e eficiência na troca de informações e na gestão de incidentes.

2.3 MONITORAMENTO

2.3.1 INDICADORES DE PERFORMANCE

Os indicadores de performance desempenham um papel fundamental no monitoramento e na avaliação do PGP/PR, permitindo a identificação de lacunas e a mensuração do progresso na implementação das ações planejadas.

Inicialmente, a PR adotará os indicadores sugeridos pelo Guia do Framework de Privacidade e Segurança da Informação, que são obrigatórios para aferir a maturidade e eficiência das práticas em privacidade e segurança. Entre os principais indicadores a serem utilizados, destacam-se:

- o índice de maturidade por controle (iMC). Avaliação da eficácia de controles específicos implementados no âmbito do PGP;
- o índice de maturidade de privacidade (iPriv). Mensuração do nível de conformidade e governança em privacidade dentro da instituição; e
- o índice de maturidade de segurança da informação (iSeg). Análise da robustez das medidas de segurança adotadas, garantindo proteção contra riscos e ameaças.

Além dos indicadores de maturidade, o PGP/PR poderá incluir, em etapas subsequentes, indicadores mais específicos e alinhados às suas necessidades institucionais. Contudo, para a fase inicial do monitoramento, a prioridade será a análise e acompanhamento dos índices acima citados, dado o alinhamento com as diretrizes previstas no Framework de Privacidade e Segurança da Informação.

Essa abordagem inicial permitirá uma avaliação estruturada e consistente da evolução do PGP, ao mesmo tempo em que fornece subsídios para o planejamento de ações futuras, com base nos resultados monitorados.

2.3.2 GESTÃO DE INCIDENTES

A gestão de incidentes é essencial para mitigar riscos associados ao tratamento de dados pessoais e garantir conformidade com a LGPD. Esse processo deve incluir a criação de um planejamento para resposta a incidentes, registro detalhado dos eventos e implementação de procedimentos operacionais que assegurem a detecção, tratamento e mitigação de riscos.

É fundamental que os incidentes de segurança e privacidade sejam registrados, documentando informações como descrição do incidente, sistemas e dados envolvidos, riscos associados e medidas corretivas adotadas. O planejamento deve prever também um fluxo claro de comunicação para informar incidentes às autoridades fiscalizadoras e aos titulares dos dados, conforme o disposto no artigo 48 da LGPD.

A capacitação contínua dos servidores e colaboradores deve ser priorizada, promovendo a conscientização sobre as responsabilidades no tratamento de dados pessoais e fortalecendo a resposta institucional a incidentes de segurança.

2.3.3 ANÁLISE E REPORTE DE RESULTADOS

A análise e o reporte dos resultados do PGP/PR são fundamentais para avaliar o progresso das ações implementadas e reforçar a cultura de privacidade na Presidência da República. Esse processo envolve a consolidação e apresentação de indicadores-chave, como os índices de maturidade em privacidade e segurança da informação, o número de serviços com dados pessoais inventariados e os treinamentos realizados.

Os resultados obtidos serão avaliados regularmente com base em relatórios de monitoramento, possibilitando identificar lacunas, mensurar a eficácia das medidas adotadas e propor ajustes necessários. As informações consolidadas serão apresentadas à alta administração, assegurando que as decisões estratégicas sejam fundamentadas em evidências e promovam a melhoria contínua das práticas de proteção de dados.

2.3.4 O ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS

Na etapa de monitoramento, o encarregado de dados pessoais desempenha um papel estratégico, assegurando a supervisão contínua das atividades relacionadas à privacidade e proteção de dados. Em conformidade com o art. 16, inciso IV, da Resolução CD/ANPD nº 18, suas responsabilidades incluem:

- o gerenciamento de métricas, estabelecendo e monitorando indicadores de desempenho que auxiliem no acompanhamento das ações do Programa de Governança em Privacidade.
- a divulgação de resultados, promovendo a comunicação clara dos resultados obtidos, por meio de uma estrutura de divulgação voltada à alta direção e às áreas envolvidas, garantindo que as informações sejam utilizadas para embasar decisões estratégicas.
- a mitigação de riscos, apoiando na implementação de mecanismos internos que assegurem a mitigação de riscos associados ao tratamento de dados pessoais.

3. REFERÊNCIAS

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

BRASIL. Decreto nº 10.433, de 20 de julho de 2020. Dispõe sobre a governança digital no âmbito da administração pública federal e institui o Comitê de Governança Digital e Segurança da Informação da Presidência da República. Disponível em: *http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10433.htm*

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Comitê de Governança Digital e Segurança da Informação. Resolução nº 29, de 21 de julho de 2022. Institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República (POSITEC/PR). Brasília: Presidência da República, 2022. Disponível em: *https://www.gov.br/planalto/pt-br/acesso-a-informacao/acoes-e-programas/governanca/comite-de-governanca-digital-e-seguranca-da-informacao-da-presidencia-da-republica/legislacao-e-normas/resolucoes-2022/resolucao-n-29-de-21-de-julho-de-2022.pdf*

BRASIL. Secretaria de Governo Digital. Guia de Elaboração de Programa de Governança em Privacidade (PPSI). Brasília: Ministério da Gestão e da Inovação, 2021. Disponível em: *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf*

BRASIL. Secretaria de Governo Digital. Guia de Elaboração de Inventário de Dados Pessoais. Brasília: Ministério da Gestão e da Inovação, 2022. Disponível em: *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf*

BRASIL. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação (PPSI). Brasília: Ministério da Gestão e da Inovação, 2023. Disponível em: *https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/ppsi/manual_ferramenta_framework.pdf*

BRASIL. Secretaria de Governo Digital. Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos. Brasília: Ministério da Gestão e Inovação, 2022. Disponível em: *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf*

BRASIL. Secretaria de Governo Digital. Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília: Ministério da Gestão e Inovação, 2023. Disponível em: *https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_template_ripd.docx*

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo para atuação do encarregado pelo tratamento de dados pessoais. Brasília: ANPD, 2022. Disponível em: *https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_da_atuacao_do_encarregado_anpd.pdf/@@download/file*

4. 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. Métricas 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, visando a 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.

4.1 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 da 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 da 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.*

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO