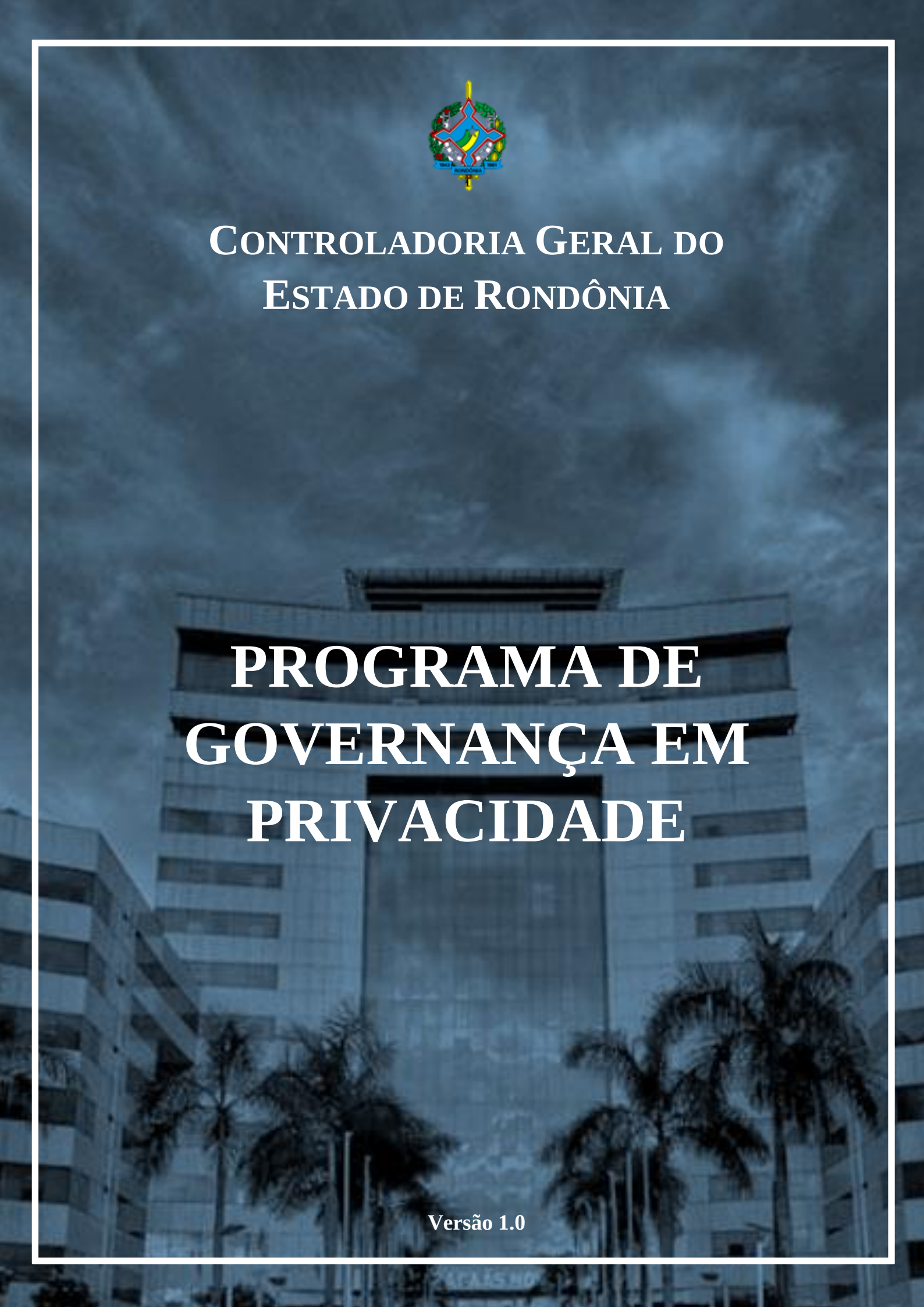


CONTROLADORIA GERAL DO ESTADO DE RONDÔNIA

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Versão 1.0

CONTROLADOR-GERAL DO ESTADO

Francisco Lopes Fernandes Netto

COORDENADOR TÉCNICO

Rodrigo Cesar Silva Moreira

EQUIPE TÉCNICA DE ELABORAÇÃO

Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados Pessoais

Ádrian Breno Cavalcante do Nascimento

Alan Negri Feitosa

Alessandra Nunes Silva

Cíntia da Silva Rodrigues Costa

Fagna da Silva Paiva

Franklin Ribeiro

Henrique Ferreira Guimarães

Jeferson Leal Maia

Juscélia Nunes dos Santos

Pablo Jean Vivan

Rodrigo Cesar Silva Moreira

Ronaldo Aparecido Avanzi

SUMÁRIO

1. APRESENTAÇÃO

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), dispõe sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica, de direito público ou privado, abrangendo inclusive o tratamento realizado nos meios digitais, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com características extraterritoriais e de interesse nacional, a LGPD regula toda operação realizada com o uso de dados pessoais, configurando relevante marco legislativo a determinar a atuação de agentes públicos e privados em matéria de tratamento e utilização dos dados que detêm em razão das atribuições e serviços que exercem. Estando ali previstos os critérios para a guarda, armazenamento e divulgação de informações de origem privada, o dever de preservação e proteção desses dados, bem como sanções resultantes da transgressão de suas regras.

E quando analisada a matéria sob o enfoque da Administração Pública, o art. 23, da LGPD, determina que o tratamento de dados "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

Outrossim, determina a Lei que o tratamento de informações deva ser realizado para propósitos específicos, explícitos e informados ao titular. Modificada a finalidade, caberá ao ente dizê-lo ao titular, fazendo-se necessário novo consentimento.

Observa-se que alguns fundamentos trazidos pela norma já são utilizados como parâmetros para a atuação do Poder Público, a saber: os princípios da legalidade, da impessoalidade, da moralidade administrativa, da publicidade (art. 37, caput, da Constituição Federal de 1988).

Visando orientar a adequação das organizações às novas regras estabelecidas, a LGPD estabeleceu princípios norteadores no tratamento de dados, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6˚ da LGPD).

Traz, ainda, seção específica referente à formulação de regras de boas práticas e de governança a serem observadas pelos envolvidos no tratamento de dados, estabelecendo no inciso I, § 2°, I, do art. 50, que "o controlador poderá implementar programa de governança em privacidade", o qual deverá no mínimo:

a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) contar com planos de resposta a incidentes e remediação; e

h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

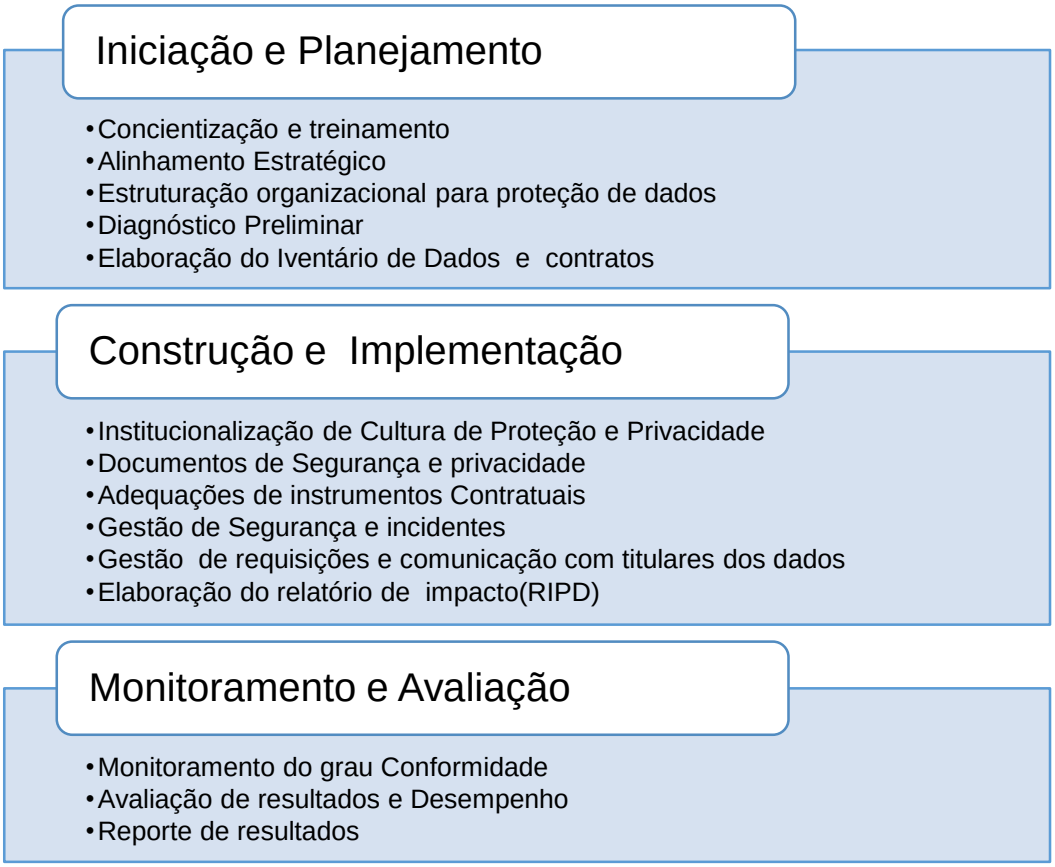
Nesse sentido, a elaboração do presente Programa de Governança em Privacidade da Controladoria Geral do Estado (PGP-CGE), tem por objetivo definir as estratégias e ações necessárias para que a Controladoria promova as adequações e permaneça em conformidade com as diretrizes estabelecidas pela LGPD, buscando garantir a proteção de dados e a privacidade em todas as etapas dos seus processos de trabalho.

Para elaboração deste Programa seguiu-se as instruções dispostas no *Guia De Elaboração de Programa de Governança em Privacidade*[1] do Governo Federal, adaptando-

[1] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf

as à realidade e necessidade desta CGE, estruturando-o com as fases consideradas basilares para o processo de adequação, quais sejam – iniciação e planejamento, construção e implementação, monitoramento e avaliação –, e estabelecendo os marcos de maior relevância de cada etapa. Ressalta-se que as ações apresentadas não são terminantes e não devem ser consideradas em sequência, sendo sua execução adaptada à realidade e priorização de acordo com a sua natureza/relevância e as especificidades da Controladoria.

Figura 1 - Etapas e ações do Programa de Governança em Privacidade CGE/RO



2. AÇÕES INICIAIS E PLANEJAMENTO

2.1. Conscientização e Capacitação

A Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) é a primeira legislação do Brasil que trata especificamente do uso de dados pessoais. Com ela surgiram algumas obrigações e sanções impostas à pessoa jurídica de direito público ou privado, tornando necessária a adoção de várias medidas que busquem atender aspectos de conformidade com a Lei.

Tendo em conta que o tema é relativamente novo para as instituições, o conhecimento e internalização dos conceitos, obrigações e sanções trazidos pelo normativo é essencial e deve alcançar toda a organização e seus parceiros, para conscientização da necessidade de implementação de boas práticas de segurança e privacidade de dados e das implicações da inconformidade no tratamento de dados.

Neste sentido, deve a CGE desenvolver sistemática institucionalizada de conscientização organizacional em segurança da informação, sendo primordial o comprometimento da alta administração no processo, mostrando a importância da LGPD e sua aplicabilidade prática, buscando institucionalizar a cultura de segurança da informação e privacidade de dados (*privacy by design* e *privacy by default*).

A LGPD traz explicitamente no art. 50, §2º, I, "a", que o PGP deve demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, o que pode ser fomentado através das campanhas de conscientização e treinamentos.

Logo, recomenda-se inicialmente executar o diagnóstico preliminar incluindo todos os colaboradores da CGE para aferição do grau de conhecimento da organização relacionado à aplicação da LGPD, iniciando-se em seguida campanhas de conscientização de nivelamento sobre o tema, seguido de capacitações quanto às melhores práticas e à política de privacidade e proteção de dados em meios físicos e digitais.

As ações de capacitações, treinamentos e conscientização devem ser desenvolvidas continuamente e podem ser conduzidos por: membros da Comissão Multidisciplinar, pelo Encarregado de Dados, por representantes externos convidados para este fim e/ou por terceiros contratados (especializados) para capacitações específicas conforme necessidade da CGE.

Métodos de treinamento e conscientização podem variar e incluem cursos de capacitação presenciais, *e-learning*, reuniões de equipe, boletins informativos, informações no portal eletrônico, entre outros materiais pedagógicos julgados pertinentes.

A avaliação do grau de conhecimento dos colaboradores da CGE relacionado ao tema deverá estar inclusa no monitoramento anual a ser realizado pela Comissão Multidisciplinar, pelo encarregado de dados e ou pela Gerência de Monitoramento – GGRM.

2.2. Alinhamento Estratégico

A participação da alta administração, representando o compromisso e o papel do controlador, é crucial para a efetividade das ações relacionadas ao cumprimento das obrigações estipuladas pela LGPD, cabendo a essa o exemplo, condução e supervisão para o desenvolvimento, implementação e operação do Programa de Privacidade.

Importa destacar que o alinhamento estratégico com a alta gestão é essencial na definição e priorização de ações referentes ao tratamento de dados pessoais, na busca do comprometimento de toda a organização no processo de adequação, e para o sucesso do trabalho a ser executado pelo Encarregado, e pela estrutura de governança em privacidade, devendo estes estar envolvidos nas decisões relativas aos projetos e recursos, treinamento, entre outras relacionadas ao tema.

2.3. Estrutura Organizacional

Entendendo a transdisciplinaridade da lei em voga, que alcança todas as unidades internas da CGE, e os requisitos para tratamento de dados pelo poder público, observa-se

a necessidade de estruturação da organização para suporte ao planejamento, execução e monitoramento da conformidade deste órgão ao disposto na LGPD.

2.3.1. Do Encarregado de Dados

De acordo com inciso III, do art. 23 da LGPD, o Encarregado de Dados ou DPO é figura de natureza obrigatória em instituições públicas, que deve estar envolvido em todas as questões de proteção de dados pessoais da instituição, deve contar com suporte e acesso a recursos adequados para cumprir suas funções e manter suas habilidades e conhecimentos técnicos.

Nos termos da LGPD, as principais atribuições do Encarregado são:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Entretanto, observa-se que a LGPD estabelece que a Autoridade Nacional de Proteção de Dados – ANPD – poderá estabelecer normas complementares sobre a definição e as atribuições do Encarregado, e as melhores práticas internacionais indicam que o Encarregado pode assumir um papel mais central no apoio à conformidade do controlador representado.

No âmbito da Controladoria Geral do Estado, o Encarregado pelo Tratamento de Dados, além das atribuições definidas pela Portaria nº 103 de 07 de junho de 2021, em especial a de "conduzir a implementação de regras de boas práticas e de governança especificadas no art. 50 da LGPD, enfatizando-se o Programa de Governança em Privacidade (PGP)" será responsável por:

e) monitorar a conformidade à LGPD, incluindo o gerenciamento de atividades internas de adequação, sugerir treinamento de pessoal e realização de pareceres internos; e

f) elaborar/fornecer aconselhamento sobre o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) e monitorar o seu desempenho.

O Encarregado de Dados contará com os membros da Comissão Multidisciplinar que irão auxiliá-lo a realizar suas atividades, nos procedimentos de implementação de ações e sustentação da conformidade da Controladoria Geral à LGPD.

2.3.2. Da Comissão Multidisciplinar de Implementação da Lei Geral de Proteção de Dados

Por meio da Portaria nº 104 de 07 de junho de 2021, a CGE instituiu Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados, composta por representantes de áreas estratégicas da CGE, com a finalidade de definir e implementar estratégias de atuação preventiva nas frentes de segurança da informação e privacidade de dados, bem como fomentar a cultura de proteção de dados visando sobretudo avançar no processo de adequação da CGE à LGPD, com competências para:

- ✓ Elaborar o plano de ação e Programa de Governança em Privacidade (PGP) para a CGE;
- ✓ Propor ações e diretrizes voltadas ao tratamento e proteção de dados pessoais;
- ✓ Planejar e acompanhar a execução de medidas para adequação à Lei Geral de Proteção de Dados, no âmbito da CGE;
- ✓ Acompanhar e convalidar o mapeamento de dados pessoais, no âmbito da CGE;
- ✓ Estabelecer os responsáveis pela execução, levantamento, gestão de riscos e análise do inventário de dados;
- ✓ Convalidar o plano de comunicação institucional sobre procedimento de proteção e privacidade de dados;
- ✓ Opinar sobre investimentos e aquisições de soluções direcionadas exclusivamente à conformidade da CGE à LGPD; e
- ✓ Apoiar o Encarregado da Proteção de Dados na aplicação de procedimentos institucionais referente à segurança e privacidade de dados e monitorar os resultados.

Integram a Comissão Multidisciplinar: a Diretoria Executiva – DIREX, o Encarregado de Dados e representantes da Assessoria de TI, Transparência e Prevenção da Corrupção – ASTIPC; Gerência Administrativa e Financeira – GAF; Gerência de Análise e Certificação de Contas – GACC; Gerência de Fiscalização e Auditoria Interna – GFAI; e Gerência de Gestão de Risco e Monitoramento – GGRM.

A seguir, a divisão de competências, levando em consideração o desenvolvimento da adequação desta Controladoria:

Quadro 1 - Atores e suas responsabilidades na implementação do Programa de Governança e Privacidade da CGE

Atores	Responsabilidades
Controlador-CGE	Adequação da CGE à LGPD, além de priorizar e monitorar as ações a serem implementadas
Unidades Internas da CGE	Inventariar os dados e adequar os processos pelos quais são responsáveis pelo tratamento à LGPD, com apoio do Encarregado e da Comissão Multidiciplinar.
Encarregado	Intermediar a comunicação entre a CGE e a ANPD, e titulares dos dados e demais responsabilidades definidas na LGPD e Portaria nº 103 de 07 de junho de 2021
Comissão Multidiciplinar	Propor ações e diretrizes voltadas ao tratamento e proteção de dados pessoais, bem como auxiliar na execução e monitoramento dos procedimentos de adequação à LGPD e demais competências definidas na Portaria 104 de junho de 2021

2.4. Diagnóstico Inicial

No marco inicial de adequação da LGPD, é imperiosa a análise da organização, em termos de estrutura, atribuições e competências legais e administrativas para compreensão das atividades executadas pela CGE, bem como a visualização clara do seu papel institucional enquanto órgão central de controle interno do poder executivo.

As competências, atribuições e finalidades da Controladoria Geral foram estabelecidas no art. 111 da Lei Complementar nº 965/2017 e Decreto nº 23.277 de outubro de 2018, atribuindo à CGE enquanto Órgão Central de Controle Interno as funções de:

fiscalização dos sistemas contábil, financeiro, orçamentário e operacional do Estado, das Entidades da Administração Direta e Indireta, dos Fundos Estaduais e das Fundações instituídas ou mantidas pelo Poder Executivo, quanto aos aspectos de legalidade, legitimidade e economicidade, aplicação das subvenções e outras transferências, regularidade da receita e despesa e renúncias de receitas, por meio de inspeções, auditorias ou outro instrumento de controle.

Atentando para a realidade organizacional, é recomendada a realização de uma avaliação diagnóstica que demostre o grau de maturidade da unidade atinente ao tratamento de dados pessoais, o que permitirá a definição de ações e metas a serem desenvolvidas para alcance da adequação à LGPD. Para isso, pode-se lançar mão da utilização de ferramentas online disponíveis, a exemplo do Diagnóstico de Maturidade de Privacidade para Adequação à LGPD[2], desenvolvida pela Secretaria de Governo Digital do Ministério da Economia (SGD).

A realização dos diagnósticos em relação ao grau de maturidade de conformidade da unidade à LGPD é imprescindível para a identificação do estágio de conformidade em que a unidade se encontra, em relação às boas práticas de privacidade já aplicadas e da necessidade de ampliação da conscientização dos agentes públicos em relação ao assunto.

A par das necessidades dessas ações, em setembro de 2020, a Comissão Multidisciplinar de Implementação e Adequação da LGPD realizou o diagnóstico para mensuração do índice de maturidade da CGE, utilizando-se da ferramenta retrocitada, o qual apresentou índice de maturidade inicial, possibilitando a priorização das ações necessárias para entrada em conformidade com a LGPD. O cálculo do índice de adequação desta Controladoria à LGPD está demonstrado no quadro abaixo:

[2] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-privacidade-lgpd

Quadro 2 - Nível de Adequação da CGE à LGPD

Eixo\Nível de Adequação	Inicial 0,00 a 0,29	Básico 0,30 a 0,49	Intermediário 0,50 a 0,69	Em aprimoramento 0,70 a 0,89	Aprimorado 0,90 a 1,00
Governança			0,67		
Conformidade Legal e Respeito aos Princípios		0,30			
Transparência e Direitos do Titular		0,46			
Rastreabilidade	0,20				
Adequação de Contratos e de Relações com Parceiros	0,20				
Segurança da Informação	0,20				
Violação de Dados		0,44			
Índice geral		0,36			

Fonte: Adaptado do Diagnóstico da Cultura Organizacional e do Grau de Maturidade da CGE à LGPD

Não obstante, foi realizado diagnóstico acerca da cultura organizacional por meio de questionário com dez perguntas aplicado a todos os servidores da CGE. Dentre os questionamentos, destaca-se o relacionado à participação dos servidores em capacitação em LGPD, que gerou um índice de 57,7%. No entanto, embora somente um pouco mais da metade dos servidores tenham sido capacitados, 98,7% deles conseguiram definir o que são dados pessoais.

Os diagnósticos colaboram para o direcionamento de esforços e a priorização das ações necessárias para construção da conformidade à Lei Geral de Proteção de Dados, devendo ser realizados periodicamente de forma a atuar como um índice de performance e incorporados aos Relatórios de Monitoramento reportados ao Controlador-Geral (CGE).

2.5. Inventário De Dados Pessoais – IDP

O Inventário de Dados Pessoais (IDP) é exigência da LGPD, conforme determina seu art. 37, "o controlador e o operador devem manter registro de operações de tratamento de dados pessoais que realizarem".

Nesse contexto, o IDP deve representar o mapeamento dos processos, sistemas e serviços com registro das operações de tratamento, sendo fundamental para

identificação de como os dados são coletados, tratados e descartados, além da visualização sobre o compartilhamento de dados, bases legais e finalidade do tratamento. Ademais, o IDP pode ser base para elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) – instrumento fundamental para avaliação da conformidade do tratamento de dados e análise do controlador quanto às medidas, salvaguardas e mecanismos de mitigação de riscos adotados, e identificação de lacunas (*Gap Analysis*) no tratamento de dados pessoais – etapa em que são estudadas brechas na adequação, ou seja, quais processos e ferramentas podem abrir margem para possíveis penalidades na LGPD.

Recomenda-se que tal instrumento deverá descrever informações tais como:

Atores envolvidos	Agentes de tratamento/Encarregado de Dados
Processo/sistema/serviço	Identificação do processo/sistema e/ou serviço para o qual coleta-se os dados
Dados coletados	Especificação dos dados coletados, ex. nome, CPF, endereço
Hipótese	Conforme arts. 7º e 11 da LGPD
Previsão legal	Instrumento legal do tratamento
Finalidade	Finalidade do tratamento dos dados
Categoria dos titulares dos dados pessoais	Especificar quanto à categoria dos dados (dados pessoais, dados sensíveis)
Tempo de retenção dos dados pessoais	Informações do tempo em que os dados serão armazenados/retidos
Compartilhamento	Informações quanto ao compartilhamento dos dados com outras entidades
Transferência internacional	Informar quanto à existência de compartilhamento do dado (art. 33 da LGPD)
Medidas de segurança	Informações quanto às medidas de segurança atualmente adotadas para proteção dos dados

Quanto à metodologia utilizada para realizar o IDP, sugere-se que seja adotado o mapeamento por processo/serviço, ou seja, a identificação dos dados tratados no âmbito do processo ou serviço. O Encarregado, com apoio da Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados, será responsável pela condução da realização do IDP, o qual deve ser elaborado com base no *Guia de Elaboração de Inventário de Dados Pessoais da SGD/ME*[3].

As atividades de mapeamento dos serviços, processos e sistemas para elaboração do IDP deverão ser realizadas pela gerência responsável pelo serviço/processo de negócio, com observância ao disposto no guia supracitado. Os registros devem ser mantidos atualizados com periodicidade mínima anual.

2.5.1. Levantamento de contratos relacionados a Dados Pessoais

Concomitante à elaboração do Inventário de Dados, deverá ser realizado o levantamento e a análise dos contratos formalizados entre CGE e terceiros que, de alguma forma, realizem tratamento e/ou compartilhamento de dados pessoais, com vistas a promover a adequação para cumprimento dos dispositivos da LGPD por todos os envolvidos no tratamento de dados, singularmente pelo controlador e pelo operador.

Da mesma maneira que os serviços, processos e sistemas, os contratos que coletem, transfiram e processem dados pessoais devem ser incluídos nos relatórios de gestão de riscos, para a análise de possíveis e necessárias implementações de cláusulas que assegurem a proteção dos dados pessoais.

2.5.2. Relatório de Gestão de Risco

O estágio da gestão de risco deverá ser iniciado após a elaboração do IDP e tem como objetivo a avaliação das informações do inventário, identificando as lacunas de

[3] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf

segurança da informação e de privacidade sobre os dados tratados, demonstrando, aos setores do processo/serviço e tomadores de decisão, onde se encontram os riscos de privacidade dos processos e o impacto dimensionado, com orientações para adequação e propostas de ações de mitigação desses.

Nesse contexto, os relatórios de gestão de riscos devem identificar os riscos inerentes aos tratamentos de dados realizados no âmbito da CGE e apresentar orientações e proposições de medidas mitigadoras, bem como estabelecer prazos para adequação, quando for o caso.

As recomendações apontadas no relatório de gestão de riscos deverão ser monitoradas pelo Encarregado de Dados em conjunto com a GGRM, para acompanhamento da implementação das medidas, devendo as unidades internas serem devidamente notificadas quanto aos resultados dos relatórios e dos prazos para implementação das medidas sugeridas.

3. CONSTRUÇÃO E EXECUÇÃO

3.1. Proteção de Dados e Privacidade desde a Concepção (*Privacy by design*)

O art. 46, da LGPD, dispõe que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Portanto, sendo a CGE custodiante e responsável pelo tratamento de dados pessoais coletados e processados por meio dos serviços internos e externos que oferece, possui a obrigação de assegurar a proteção desses dados.

Considerando que existe diversas formas para implementação dessas medidas, a CGE buscará adotar metodologias de implementação de medidas proativas, como *Privacy by design* (Privacidade desde a concepção), de forma que novos projetos e serviços

garantam a privacidade desde seu início, impedindo esforços e gastos exacerbados de última hora.

A ideia de *Privacy by design* (Privacidade desde a concepção) traduz-se na implementação de conceitos e medidas de privacidade e proteção de dados desde o início dos projetos, serviços e/ou processos.

O *Privacy by Design* considera 7 (sete) princípios que o formam:

- **Proatividade e Prevenção** - caracterizada por medidas proativas, ou seja, antecipa e evita eventos invasivos de privacidade antes que eles aconteçam.
- **Privacidade como Padrão (Privacy by Default) -** busca garantir que dados pessoais sejam protegidos automaticamente sem qualquer ação por parte do titular, pois ela já estará embutida no sistema, por padrão.
- **Privacidade incorporada ao projeto (design)** - objetiva que a privacidade se torne um componente da função a ser entregue, sendo parte integrante do sistema.
- **Funcionalidade total** – busca garantir todos os legítimos interesses e objetivos.
- **Segurança e proteção de ponta a ponta** - a privacidade deve ser protegida ao longo de todo ciclo de vida do tratamento dos dados em questão.
- **Visibilidade e Transparência** – por serem valores essenciais para o estabelecimento de responsabilidade e confiança, preza pela responsabilização, transparência e conformidade.
- **Respeito pela privacidade do usuário** - exige respeito aos direitos dos titulares dos dados pessoais.

Nesse sentido, os conceitos de privacy by design (privacidade desde a concepção) devem ser incorporados à cultura organizacional da CGE, buscando sua implementação desde a concepção até a execução de todo projeto, processo ou serviço desenvolvido pela unidade, com vistas a garantir governança e proteção dos dados pessoais do usuário.

Para isso, a mudança da cultura na concepção de projetos é essencial, sendo fundamental que a CGE, por meio da Comissão Multidisciplinar, promova ações voltadas a incorporar o Privacy by Design na cultura organizacional.

3.2. Documentos de Privacidade

A elaboração de documentos com vistas a estabelecer as diretrizes, medidas técnicas e administrativas para proteção de dados é etapa essencial no processo de conformidade da unidade à LGPD e tem por objetivo, além de prover a segurança e a privacidade dos dados, o cumprimento dos quesitos elencados no art. 50, § 1º, I, "a" e "d", que dispõe que o controlador deve demonstrar comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; e estabelecer políticas e salvaguardas adequadas.

3.2.1. Da Política de Privacidade

A Política de Privacidade tem por objetivo estabelecer as diretrizes da CGE para resguardo e uso de dados pessoais que venham a ser tratados em suas atividades e aplicações (sítios, sistemas ou aplicativos para dispositivos móveis), tendo como referência a Lei Geral de Proteção de Dados Pessoais, entre outras normas nacionais e internacionais relativas à privacidade e à proteção de dados pessoais, com especial atenção à *General Data Protection Regulation* e à ISO/IEC 27001.

A Política de Privacidade de Dados é um documento endereçado ao usuário, que esclarece papéis e responsabilidades, a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas, e que busca atender aos princípios da transparência, do livre acesso e da prestação de contas previstos no art. 6º da LGPD.

Nesse sentido, é instrumento que esclarece o dever do controlador e os direitos do titular, bem como a necessidade e a finalidade da coleta e tratamento dos dados, e as medidas empregadas para que a privacidade e confidencialidade dos dados prestados seja

garantida de forma eficiente e seguindo os princípios, como: a finalidade, a adequação, a necessidade, dentre outros dispostos na LGPD e citados no *Guia de Elaboração de Termo de Uso e Política de Privacidade Para Serviços Públicos*[4].

A elaboração e implementação da Política de Privacidade, como já mencionado, tem fundamento no inciso VI do art. 6º da LGPD, que consiste no princípio da transparência, o qual garante aos titulares: informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento dos dados pessoais.

A Política de Privacidade da Controladoria Geral do Estado de Rondônia será elaborada pela Comissão Multidisciplinar com revisão do setor de tecnologia e do Encarregado de Dados, e deve contemplar no mínimo as seguintes informações:

- Informação sobre a CGE como entidade responsável pelo tratamento;
- Especificar os dados pessoais tratados e respectivas finalidades do tratamento, incluindo-se dados não informados pelo usuário (exemplo: IP, localização, etc.), quando aplicável;
- Fundamento legal do tratamento;
- Prazo de retenção dos dados pessoais;
- Informações de contato do encarregado de proteção de dados;
- Canais de atendimento ao titular e a forma como são atendidos os direitos do titular, informando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento;
- Informações quanto à existência de compartilhamento de dados com terceiros e qual a finalidade (quando aplicável);
- Se há transferência internacional de dados (quando aplicável);
- Proteção de dados de menores de idade, se for o caso; e
- Proteção de dados sensíveis.

[4] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf

3.2.2. Termos de Uso

O Termo de Uso é um documento de caráter vinculativo que estabelece as regras e condições de uso de determinado serviço fornecido pela organização. Destaca-se que esse documento pode ser específico de cada serviço ou, ainda, geral, devendo esse último relacionar todos os serviços aos quais o mesmo é aplicado, de forma a conscientizar o titular dos dados quanto aos serviços que utilizam seus dados e quais dados são utilizados em cada serviço.

Quando da aceitação do Termo de Uso pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nesse, sendo essencial a transparência dessa informação ao titular dos dados e de observação obrigatória da unidade quanto às responsabilidades, às condições e às regras aplicáveis a ele, referente às atividades de tratamento desses dados, observando os princípios dispostos no art. 6º da LGPD.

Os Termos de Uso aplicáveis aos serviços da CGE serão elaborados observando-se o *Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços Públicos*[5], e periodicamente atualizado, de forma a refletir, de modo claro e preciso, a realidade concernente ao tratamento dos dados coletados, que comumente serão utilizados pelo órgão no exercício de suas competências legais.

3.2.3. Da Política de Segurança

A Política de Segurança da Informação (PSI) consiste na instituição de normas para utilização de recursos de Tecnologia da Informação, para gestão de ativos, de classificação de informações, de gerenciamento de acessos, de gestão de operação de Tecnologia da Informação, de desenvolvimento seguro e de gerenciamento de riscos de Tecnologia da Informação.

É sobretudo instrumento para gerir os riscos da ocorrência de eventos que possam causar danos às pessoas, ao patrimônio e às informações, prevenindo-os ou, pelo menos, reduzindo-os a níveis mínimos aceitáveis e minorar os impactos de situações anormais de funcionamento que afetem a confidencialidade, disponibilidade, integridade, legalidade e

[5] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf

autenticidade das informações, caso ocorram. Em suma é instrumento que estabelece medidas de segurança, técnicas 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, conforme disposto no art. 46 da LGPD.

A Política de Segurança da Informação será elaborada pela Assessoria de Tecnologia da Informação com apoio da Comissão Multidisciplinar e aprovado pelo Controlador-Geral, com observância aos normativos e boas práticas de segurança de informação existentes, estabelecendo diretrizes, responsabilidades, competências e medidas técnicas e administrativas de segurança da informação, sendo de observância obrigatória por todos os servidores e parceiros da CGE.

3.3. Adequação de instrumentos contratuais

Esta é a etapa de adequação dos instrumentos contratuais – contratos, convênios, termos e congêneres –, documentos essenciais para a relação entre entidades e parceiros, os quais também devem ser objeto de conformidade à LGPD, com objetivo de respeitar a norma protetiva voltada aos titulares cujos dados pessoais são tratados na relação contratual.

O art. 42 da LGPD estabelece a obrigação para o controlador e operador de reparação de dano causado decorrente da violação à legislação. Não obstante, o inciso I do art. 42 da LGPD dispõe que "*o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei*".

Nesse sentido, a adequação dos instrumentos contratuais, com inclusão de cláusulas específicas sobre a proteção de dados pessoais, perpassa a fase de levantamentos e análise dos instrumentos que impliquem no tratamento de dados pessoais, mapeados na etapa de Iniciação e Planejamento, e deve abordar tantos contratos existentes quanto os novos a serem firmados.

Em suma, deve a CGE, à luz da LGPD e demais instrumentos legais, estabelecer cláusulas com regras de proteção e privacidade de dados a serem observados pelas partes, bem como procedimentos a serem implementados em caso de incidente de dados pessoais, com planos de respostas e remediação estruturados.

A padronização de cláusulas contratuais de conformidade à LGPD é de responsabilidade da GAF, que contará com apoio da Comissão Multidisciplinar e, julgando necessário, pode a CGE realizar consultar à Procuradoria Jurídica do Estado - PGE, tendo em vista as competências desta, em especial as insculpidas no inciso II, do art. 3º da Lei Complementar nº 620 de 2011.

3.4. Da Gestão de Incidentes

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e a liberdade dos titulares dos dados pessoais[6].

O inciso I, § 2º, do art. 50 da LGPD, dispõe que deve ser implementado um programa de governança em privacidade que conte com planos de resposta a incidentes e remediação. O art. 48 da mesma Lei determina que é obrigação do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Logo, é imperioso a implementação de medidas de gestão de incidentes de segurança concernentes a violação de dados pessoais, essencialmente estabelecer o Plano de Resposta a Incidentes que deve contemplar, entre outros, o registro do evento de incidente, as ações primárias de mitigação do impacto, as medidas técnicas e administrativas de segurança a serem adotadas e os atores responsáveis pelas ações, além

[6] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

da identificação dos demais interessados a serem cientificados quando da ocorrência do evento, em especial a comunicação apropriada e tempestiva à Autoridade Nacional de Dados Pessoais – ANDP – e aos titulares afetados.

Assim, o Processo de Gestão de Incidentes deve ter a capacidade de preservação do máximo de evidências do incidente e de todas as medidas adotadas a partir da sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, o comprometimento da CGE e toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

A Comissão Multidisciplinar com apoio do encarregado de dados será responsável pela elaboração do plano de resposta a incidentes, o qual deverá ser revisado pela Assessoria de Tecnologia e aprovado pela Diretoria executiva da CGE. Ademais deverá ser amplamente divulgado para todos os servidores, no sentido de demonstrar as medidas que deverão ser adotadas no caso de incidente de segurança envolvendo a violação de dados pessoais.

3.5. Gestão de Requisições e Comunicação com o Titular

A LGPD dispõe em seu art. 18 que "o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição" especificando entre outros os direitos a:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados.

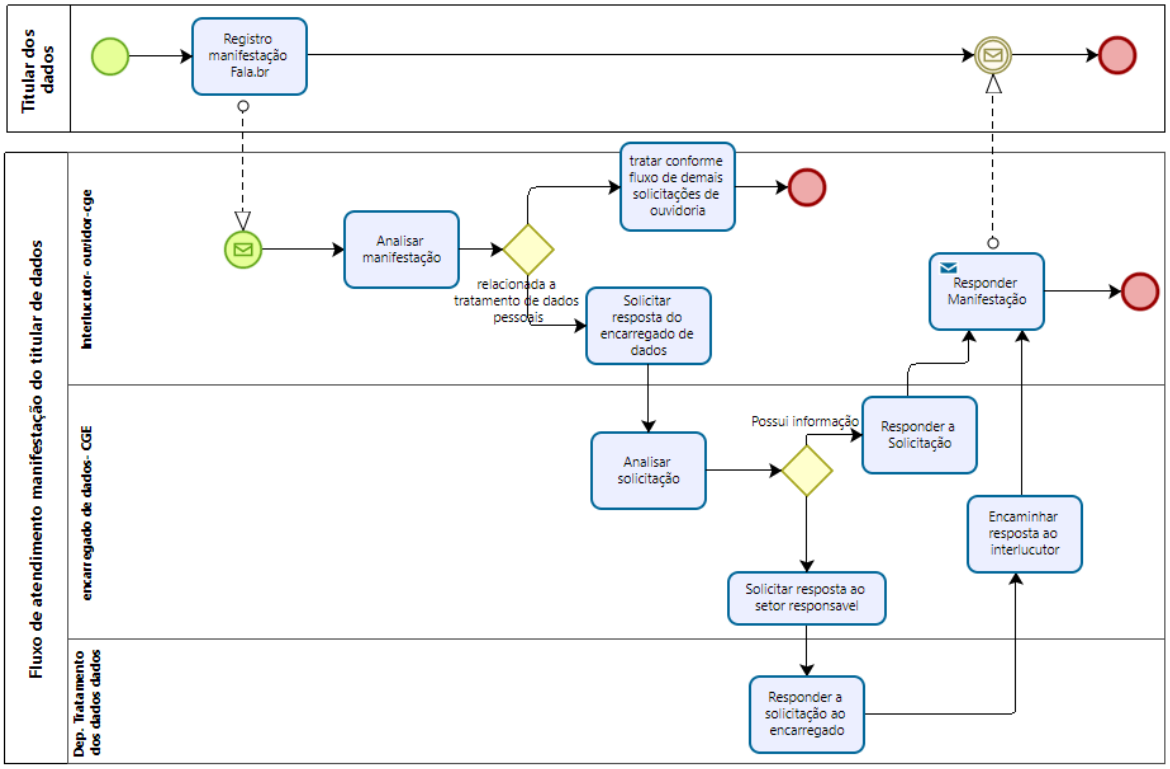
Além disso, o mesmo artigo prevê que o titular exercerá seus direitos mediante requerimento expresso dele próprio ou de representante legalmente constituído, a agente de tratamento (art. 18, § 3º, LGPD).

Para conformidade do requisito mencionado, a CGE adotará a plataforma Fala.BR Rondônia, administrada pela Ouvidoria Geral do Estado de Rondônia, como o meio de comunicação entre a CGE e os titulares de dados pessoais, pelo qual os titulares poderão

registrar as solicitações relacionadas ao tratamento de dados pessoais, bem como receber resposta a sua demanda.

No âmbito da CGE, o Encarregado de Dados é o responsável pelo recebimento e análise preliminar das solicitações, cujo processo de atendimento seguirá preferencialmente o fluxo abaixo:

Fluxo de atendimento de requisições



Concernente aos prazos para tramitação e resposta aos demandantes de requisições afetas ao tratamento de dados pessoais, a CGE observará ao disposto na Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) e na Lei nº 13.460/2017 (Código de Defesa dos Usuários de Serviços Públicos) ou de norma correlata, salvo disposição específica na LGPD.

3.6. Relatório de Impacto de Proteção de Dados (RIPD)

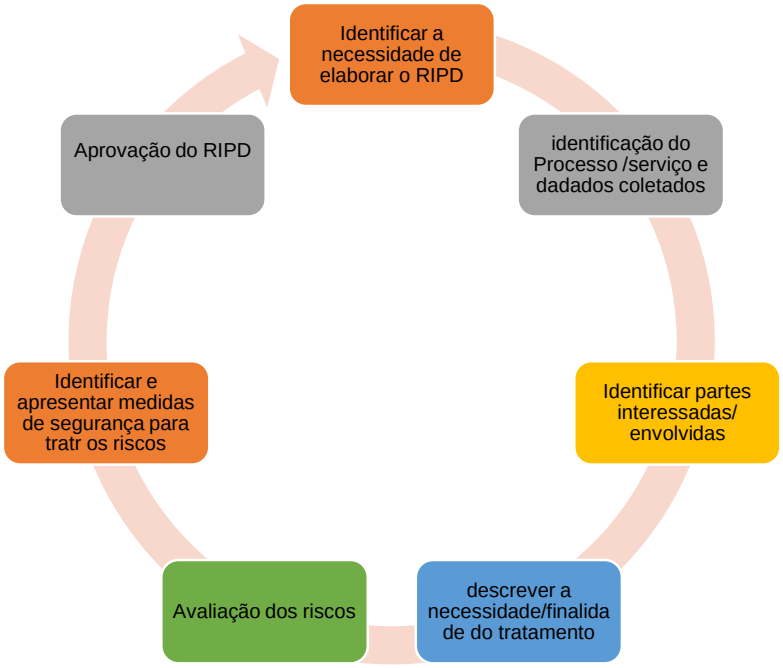
Trata-se de documento elaborado com a finalidade de identificação e análise de riscos à privacidade de dados pessoais em processos/serviços – pelos quais dados pessoais são coletados, tratados, compartilhados –, que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

O RIPD é abordado no inciso XVII, do art. 5º da LGPD, como " documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Nesse contexto, considera-se que nem toda atividade enseja a necessidade de um RIPD. Assim, na CGE deve ser considerada a elaboração do RIPD nos casos em que for observado que o serviço, processo ou projeto que de alguma forma realize tratamento de dados pessoais e apresente potencial de gerar risco às liberdades civis e aos direitos fundamentais do titular, ou ainda, quando solicitado pela ANPD, conforme art. 38 da LGPD, e pelo Encarregado, devendo contemplar no mínimo a descrição dos processos/serviços de tratamento de dados pessoais, os tipos de dados coletados, a metodologia utilizada para coleta e para garantia da segurança das informações e análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A elaboração do RIPD é de responsabilidade do titular da unidade dona do processo/serviço, que contará com o apoio da Comissão Multidisciplinar e da Gerência de Riscos na confecção do documento, quando observado tal necessidade, podendo lançar mão da utilização do *Guia de Elaboração RIPD*[7] disponibilizado pelo Governo Federal, observando-se no mínimo as etapas disposta abaixo:

[7] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx



4. MONITORAMENTO e AVALIAÇÃO

4.1. Monitoramento

O monitoramento consiste na adoção de ações pela CGE a fim de verificar se as medidas implementadas estão de acordo com o instituído no PGP e as recomendações emitidas nos relatórios de gestão de riscos ou com o RIPD, e se aquelas medidas foram suficientes para conformidade do tratamento de dados à LGPD e para solucionar a situação apontada nos relatórios como inadequada frente aos critérios adotados.

A GGRM, com apoio do Encarregado de Dados, é a unidade responsável pelo monitoramento e avaliação, cabendo às unidades internas a responsabilidade de zelar pelo cumprimento das recomendações emitidas pela GGRM. Nas situações em que a GGRM concluir que as recomendações de adequação não foram atendidas, deve comunicar a questão à Comissão Multidisciplinar e à alta administração. Antes da discussão com a alta administração, a GGRM deve avaliar a conveniência de fazer interlocução com as áreas responsáveis pelo risco em questão para compartilhar suas preocupações, conhecer a perspectiva dos gestores envolvidos e orientá-los quanto à resposta aos riscos.

4.2. Avaliação e Indicadores de Performance

Avaliação é o processo que deve buscar identificar o grau de conformidade da CGE à luz da LGPD. Nesse sentido, a GGRM, com apoio do Encarregado de Dados, deve dispor de ferramentas e métodos para aferição das medidas de proteção da privacidade já implementadas, a fim de verificar a evolução das unidades no processo de adequação dos serviços e sistemas, bem como se as medidas adotadas são suficientes e atendem aos requisitos de proteção dos dados.

De acordo com *Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal – MOT 2017*[8], indicador de performance: trata-se de um número, percentagem ou razão que mede um aspecto do desempenho, com o objetivo de comparar esta medida com metas preestabelecidas.

À vista disso, a avaliação deve se basear nos resultados de indicadores que devem sobretudo buscar identificar o grau de aderência e conformidade da CGE com a LGPD, devendo ser realizado no mínimo anualmente, e contemplar a avaliação dos indicadores abaixo:

Índice de maturidade da CGE – deverá ser realizado por meio do Diagnóstico de Adequação à LGPD[9];

Índice de conscientização organizacional referente à LGPD – poderá ser mensurado por meio de questionários elaborados e aplicados na fase de diagnóstico inicial;

Percentual de conformidade de serviços/processos/sistemas;

Número de requisições de titulares de dados;

Número de registro de incidentes (violação de dados) afetos a dados pessoais;

[8]Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-1.pdf
[9]Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-deadequacao-a-lgpd

4.3. Reporte de Resultados

Trata-se da comunicação dos achados/resultados de monitoramento e relatórios de avaliações a todas as unidades da CGE interessadas e à alta administração, que servirá de subsídio na tomada de decisão.

Os resultados dos monitoramentos que, por ventura, contemplarem recomendações e determinações de adoção de medidas técnicas e administrativas de proteção de dados pessoais em processos, serviços e sistemas, devem ser encaminhados prioritariamente às unidades responsáveis pelo serviço/sistema, com ciência da Comissão Multidisciplinar e Diretoria Executiva. O relatório de monitoramento deve contemplar, no mínimo:

a) o escopo delimitado e período de monitoramento;

b) a identificação do objeto;

c) as lacunas (gaps) encontradas que possam colocar em risco a privacidade do titular dos dados e/ou limitar o processo de adequação (conforme objeto);

c) as oportunidades de melhoria identificadas;

d) proposição de ações corretivas, e/ou atualização se for o caso;

e) identificação das ações já implementadas/em atraso e das não iniciadas;

f) recomendações para melhoria dos processos de adequação.

Os resultados das avaliações anuais, cujo objetivo é a aferição do grau de aderência da CGE à LGPD, devem ser reportados à Comissão Multidisciplinar, à alta administração e a todas as unidades administrativas da CGE. Essa comunicação tem por finalidade promover e reforçar o patrocínio da alta administração em relação às ações necessárias para evolução e aprimoramento da conformidade. As comunicações devem contemplar, no mínimo:

a) o escopo e período da avaliação;

b) o nível de conformidade da CGE, de acordo com a escala adotada;

c) os resultados aferidos por meio dos indicadores;

d) conclusão com apresentação dos resultados gerais e, se for o caso, recomendações para melhorias.

Por fim, ressalta-se a importância desses controles serem postos em prática, pois têm o objetivo de subsidiar a alta administração na tomada de decisão e direcionamento das ações, e, sobretudo, monitorar as atividades da organização, com o intuito de detectar tempestivamente as lacunas que necessitam de ações de correção ou incremento, suscitando mais qualidade e melhoria contínua na atuação da gestão.

REFERÊNCIAS

BRASIL. **Guia de boas práticas**. Lei Geral de Proteção de Dados Pessoais (LGPD). Comitê Central de Governança Digital. Versão 2. Brasília: ago. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

BRASIL. **Guia de elaboração de inventário de dados pessoais**. Ministério da Economia. Secretaria de Governo Digital (SGD). Versão 1.1. Brasília: abr. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf.

BRASIL. **Guia de elaboração de programa de governança em privacidade**. Ministério da Economia. Secretaria de Governo Digital (SGD). Versão 1.O. Brasília: out. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf.

BRASIL. **Guia de elaboração de termo de uso e política de privacidade para Serviços públicos**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: set. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf.

BRASIL. **Instrução Normativa nº 1, de 27 de maio de 2020.** Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Presidência da República/Gabinete de Segurança Institucional. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215

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. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Presidência da República/Gabinete de Segurança Institucional. Disponível em: in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663.

BRASIL. **Programa de Governança em Privacidade da ENAP.** Comitê de Governança Digital - CGD. Versão 1.0. Brasília: Jul. 2021 Disponível em: https://repositorio.enap.gov.br/bitstream/1/6480/1/Programa%20de%20Governan%c3%a7a%20em%20Privacidade%20da%20Enap_PGP-Enap.pdf.

BRASIL. **Programa de Governança em Privacidade do MCOM.** Ministério das Comunicações. Disponível em: https://www.gov.br/mcom/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/programa-de-governanca-em-privacidade/ProgramadeGovernanaemPrivacidadedoMCaLGPD_mcom.pdf.

RONDÔNIA. **Programa de Governança em Privacidade da Superintendência Estadual de Tecnologia da Informação e Comunicação**. Versão 1.0. Rondônia: Jul. 2021. Disponível em: http://wiki.setic.ro.gov.br/lib/exe/fetch.php?media=playground:programa_de_governanca_em_privacidade_da_setic.pdf.