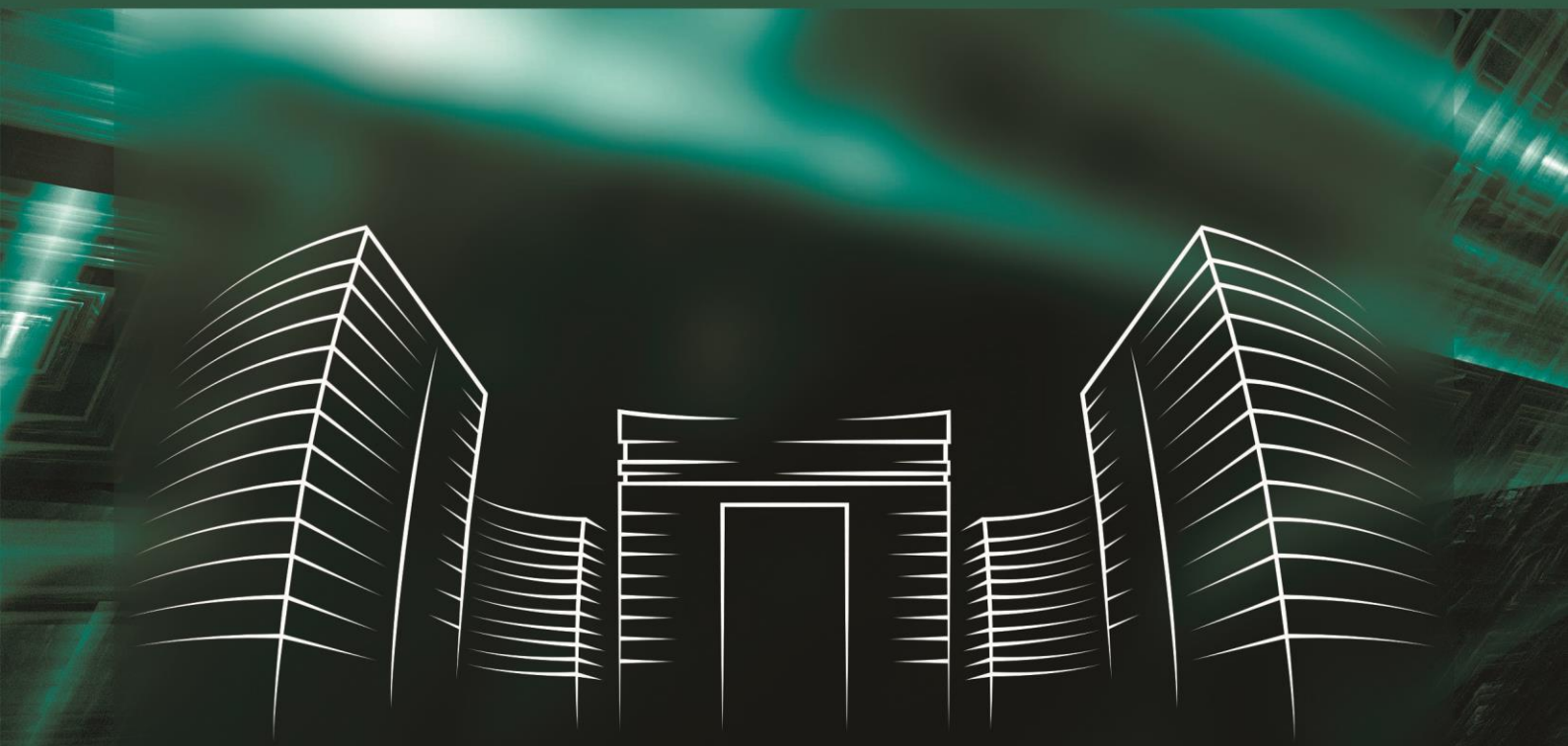
SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE



2021

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE DA SETIC

SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire

Superintendente

DIRETORIA TÉCNICA DA SETIC

Maico Moreira da Silva

Diretor Técnico

Elaboração

Tiago Lopes de Aguiar

Encarregado pelo Tratamento de Dados Pessoais

Revisão

Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD)

Maico Moreira da Silva

Tiago Lopes de Aguiar

Frederico Nakahara Silva

Gabriel Carrijo Bento Teixeira

Leonardo Courinos Lima da Silva

Janderson de Castro Thomaz

Tiago de Novais Silveira

David Lucas da Silva Ferreira

Histórico de Versões

Data	Versão	Descrição	Autoria
21/07/2021	1.0	Primeira versão do Programa de Privacidade da SETIC.	Tiago Lopes de Aguiar

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CGPD	Comitê Gestor de Privacidade e Proteção de Dados Pessoais
CI	Controle Interno
CSIRT	*Computer Security Incident Response Team* - Grupo de Resposta a Incidentes de Segurança
COGE	Coordenadoria de Gestão Estratégica da SETIC
CPSI	Comissão Permanente de Segurança da Informação da SETIC
IDP	Inventário de Dados Pessoais
LAI	Lei de Acesso à Informação - Lei nº 12.527/2011
LC	Lei Complementar
LGPD	Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018
MCOM	Ministério das Comunicações
OGE	Ouvidoria-Geral do Estado de Rondônia
PCI	Programa de Capacitação Institucional da SETIC
PGP	Programa de Governança em Privacidade
PSI	Política de Segurança da Informação
RIPD	Relatório de Impacto de Proteção de Dados Pessoais
SEI	Sistema Eletrônico de Informações
SETIC	Superintendência Estadual de Tecnologia da Informação e Comunicação do Governo do Estado de Rondônia
SGD	Secretaria de Governo Digital do Ministério da Economia
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

SUMÁRIO EXECUTIVO

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

Como bem esclarecido no art. 23, LGPD, a administração pública, no tratamento de dados pessoais, deverá atender "sua finalidade pública, na persecução do interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". Deve ainda informar as hipóteses em que realiza o tratamento de tais dados, fornecendo informações sobre a previsão legal, finalidade, procedimentos e práticas utilizadas, bem como indicar um encarregado pelo tratamento desses dados.

Nesse sentido, a LGPD constitui marco importante para os órgãos da administração pública, sejam municipais, estaduais ou federais, pois devem cumprir com seus ditames. Dentre suas características, destaca-se a transdisciplinaridade, pois permeia os mais variados órgãos e departamentos na administração pública, cujo tratamento de dados pessoais pode envolver diferentes titulares, desde os próprios servidores até usuários dos serviços públicos.

Dessa forma, o Programa de Governança em Privacidade (PGP) da Superintendência Estadual de Tecnologia da Informação e Comunicação do Governo do Estado de Rondônia (SETIC) tem por objetivo apresentar ações permanentes de conformidade com a LGPD e diretrizes correlatas. O PGP visa promover a entrada em conformidade e a execução de ações de melhoria contínua no que diz respeito ao cumprimento das diretrizes estabelecidas pela LGPD, apresentando estratégias e ações necessárias para que a SETIC entre, e se mantenha, em conformidade com a LGPD.

O roteiro deste PGP foi desenvolvido com base nas exigências da LGPD, em normas de boas práticas, experiências de especialistas na área, guias operacionais do Governo Federal e em orientações e consultorias da Gartner, considerando, sobretudo, as peculiaridades da SETIC.

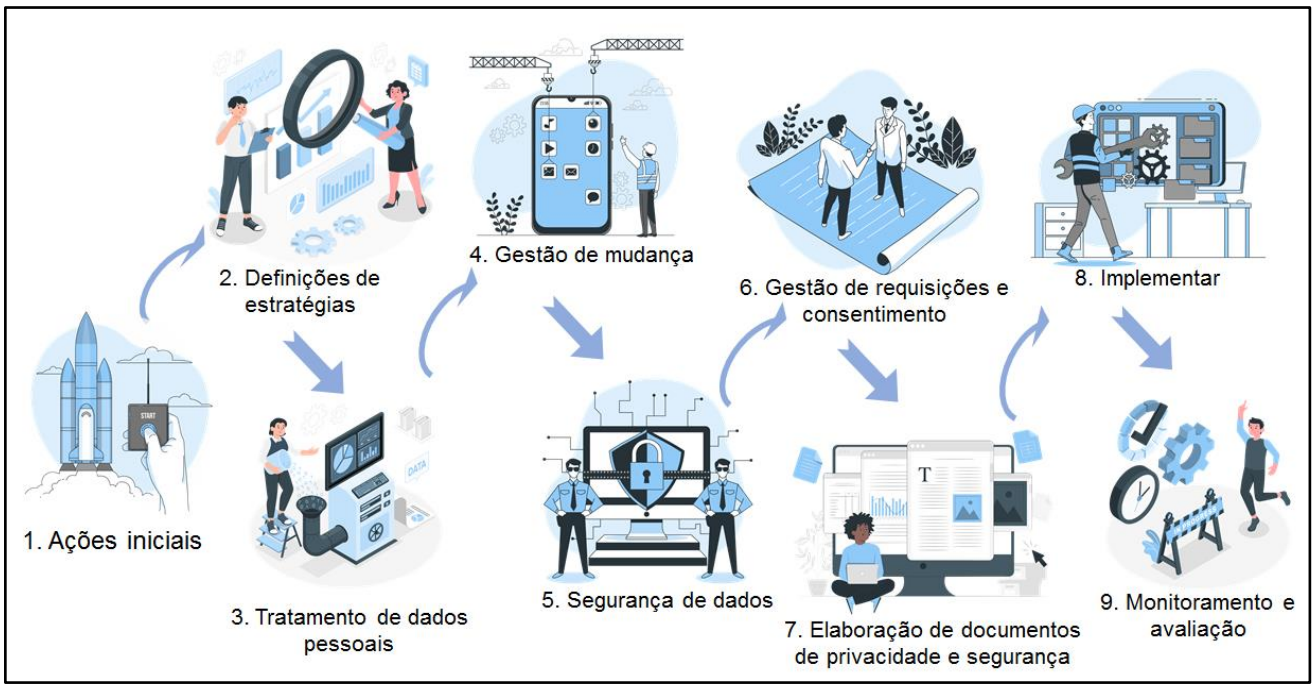
Nesse sentido, a SETIC buscará formular regras de boas práticas e de governança incluindo a adoção de normas de segurança e padrões técnicos visando a conformidade com a LGPD e normas correlatas.

Com intuito de desenvolver as estratégias e ações deste PGP, buscando facilitar sua compreensão, abordagem e aplicabilidade, foram desenvolvidos, de forma didática e dicotômica, 9 (nove) estágios, considerados essenciais para sua implementação e continuidade:

1. Ações iniciais;
2. Definições de estratégias;
3. Tratamento de dados;
4. Gestão de mudança;
5. Segurança de dados pessoais;
6. Gestão de requisições e consentimento;
7. Elaboração de documentos de privacidade e segurança;
8. Implementação; e
9. Monitoramento e avaliação.

Tais estágios serão devidamente abordados no decorrer deste PGP, apresentando-se abaixo uma figura que as resume de forma ilustrativa:

Figura 1 - Passos para implementação do PGP.

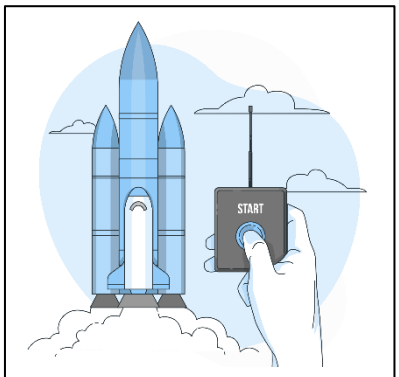


Fonte: StorySet, com adaptações (2021).

1 AÇÕES INICIAIS

1.1 Requisitos do Programa de Governança em Privacidade (PGP)

O Programa de Governança em Privacidade (PGP) da Superintendência Estadual de Tecnologia da Informação e Comunicação do Governo do Estado de Rondônia (SETIC) deve atender aos requisitos mínimos elencados no art. 50, § 2º, I, LGPD:



Fonte: StorySet (2021)

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. estabelecer diretrizes e regras que possam ser aplicáveis 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. ser um instrumento que inspira 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.

Portanto, para a implementação bem sucedida do PGP, a SETIC deverá promover mudanças e se adequar para que alcance tais requisitos, iniciando com diagnóstico inicial, nomeação do Encarregado pelo Tratamento de Dados Pessoais,

vinculação de competências ao Controle Interno (CI) e instituição do Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD).

1.2 Diagnóstico inicial

O diagnóstico inicial deve se dar a partir do levantamento de informações relativas à SETIC, evidenciando-se sua organização, estrutura e atribuições. De posse dessas informações, há uma melhor compreensão sobre o seu atual cenário (realidade organizacional) de maturidade quanto à conformidade com a LGPD.

Nesse diapasão, destaca-se que a SETIC é órgão autônomo, que se subordina diretamente ao Governador do Estado de Rondônia, conforme art. 89, I, “d”, da Lei Complementar nº 965, de 20 de dezembro de 2017, de Rondônia.

A SETIC é “órgão de nível estratégico e tático, responsável por exercer a coordenação, supervisão, orientação técnica e controle, em nível central, das atividades de Tecnologia da Informação e Comunicação (TIC) e transformação digital dos órgãos da Administração Pública Estadual Direta e Indireta”, conforme *caput* do art. 114-A, Lei Complementar nº 965/2017.

Dessa forma, a principal atividade da SETIC está relacionada com “conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios” (parágrafo único, art. 114-A, LC 968/2017).

Destaca-se que, para atendimento de suas finalidades, a SETIC conta com uma estrutura interna, destacando-se os seguintes departamentos: Administrativo e Financeiro; Infraestrutura e Serviços; Segurança da Informação; Desenvolvimento de Sistemas; Análise e Gestão de Dados; e Gestão e Estratégia. Cada qual com suas peculiaridades quanto ao tratamento de dados pessoais, atuando de forma conjunta e em sincronia para cumprir com as atribuições da SETIC.

Assim, torna-se imperioso que haja articulação entre os departamentos, objetivando dar os primeiros passos em direção à conformidade com a LGPD, nivelando as informações e enfatizando-se tal importância.

Após esse nivelamento, estando claro o alcance da conformidade com a LGPD dentro das atribuições da SETIC, deverá ser realizada a primeira avaliação diagnóstica, objetivando mensurar seu nível de maturidade com a LGPD. Diversas são as ferramentas disponíveis para tal, sugerindo-se seguir as diretrizes do **Guia**

de Conformidade: Lei Geral de Proteção de Dados Pessoais[1] da própria SETIC, que apresenta uma ferramenta *online* desenvolvida pela Secretaria de Governo Digital do Ministério da Economia (SGD).

Tal ferramenta deve avaliar a situação do Órgão, atribuindo-lhe nível de maturidade no que diz respeito ao tratamento de dados pessoais, permitindo traçar ações e metas com intuito de concentrar esforços para uma melhor adequação à LGPD.

1.3 Encarregado pelo Tratamento de Dados Pessoais

O encarregado pelo tratamento de dados pessoais, conforme explicita o inciso art. 5º, VIII, LGPD, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, titulares e Autoridade Nacional de Proteção de Dados (ANPD).

A nomeação do encarregado é requisito para que o poder público possa realizar o tratamento de dados pessoais, conforme explicitado no art. 23, III, e caput do art. 41, ambos da LGPD, devendo ser indicado pela figura do controlador.

Vale ressaltar que também é mandatória a divulgação pública da identidade e informações de contato do encarregado, atendendo os requisitos da clareza e objetividade, preferencialmente no sítio eletrônico do controlador, conforme ditames do § 1º, art. 41, LGPD.

O encarregado deve ter autonomia e independência para executar suas atribuições, sugerindo-se, inclusive, que tenha acesso direto à autoridade máxima do órgão. No **Guia de Elaboração de Programa de Governança em Privacidade**[2], da Secretaria de Governo Digital (SGD), verifica-se alguns atributos importantes quanto ao encarregado:

- Independência para determinar a aplicação de recursos e as ações necessárias;
- Amplo acesso a estrutura organizacional;
- Pronto apoio das unidades administrativas;
- Investigar os níveis de conformidade (diagnóstico);

[1] Disponível em: https://data.portal.sistemas.ro.gov.br/2021/06/Guia-de-Conformidade-LGPD-SETIC-versao-1.0.pdf. Acesso em: 21 jun. 2021, p. 12.
[2] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Acesso em: 16 mar. 2021, p. 10-14.

- Instruir os responsáveis pelos riscos a corrigir as lacunas encontradas;
- Apoio da alta administração;
- Autonomia e independência funcional.

Além das atribuições legais do Encarregado pelo Tratamento de Dados Pessoais, elencadas no art. 41, § 2º, LGPD, deve ainda, no âmbito da SETIC:

1. assessorar os responsáveis pelo tratamento de dados pessoais na emissão de relatórios de impacto à proteção de dados pessoais;
2. monitorar a conformidade das atividades de tratamento de dados pessoais com a regulamentação e as normas vigentes;
3. recomendar as salvaguardas para mitigar quaisquer riscos aos direitos dos titulares de dados pessoais tratados pela SETIC, inclusive salvaguardas técnicas e medidas organizacionais; e
4. 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).

A escolha do encarregado pelo tratamento de dados pessoais deve levar em conta seus conhecimentos multidisciplinares nas áreas de: gestão, legislação, tecnologia da informação, segurança da informação, governança de dados etc.

O Encarregado deve estar envolvido em todas as questões relativas à privacidade e proteção de dados pessoais na SETIC, tendo acesso a todas as operações de tratamento institucionais, podendo-se firmar compromisso de sigilo e confidencialidade sobre os dados e informações acessadas.

No âmbito da SETIC, o Encarregado estará vinculado ao Controle Interno, objetivando elidir possíveis conflitos de interesses, inclusive possuindo poderes relativos a ações de auditoria e monitoramento no que diz respeito às atividades relacionadas ao tratamento de dados pessoais. Deverá contar com o Controle Interno que lhe prestará apoio na execução de suas atividades, além de fazer parte do Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD).

1.4 Controle Interno (CI)

O Controle Interno (CI) promoverá as ações, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, voltadas à conformidade da SETIC para com a LGPD, normas complementares e conexas, atuando em nível tático e operacional, subsidiando o Encarregado na execução de suas atividades.

A incorporação de tais ações ao CI objetiva elidir possíveis conflitos de interesses e exercer atividades de auditoria e monitoramento quanto à conformidade com a LGPD.

O CI e o Encarregado deverão proporcionar melhor alinhamento estratégico da Alta Gestão e do CGPD para com as atividades relativas ao tratamento de dados pessoais, principalmente por considerar a transdisciplinaridade da Lei em voga, que alcança todas as coordenadorias, departamentos e setores da SETIC.

1.5 Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD)

O Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD), de caráter permanente, tem por finalidade assessorar a SETIC nas atividades relacionadas à privacidade e proteção de dados pessoais. Possui cunho estratégico e tático.

Considerando a transdisciplinaridade da LGPD, deverá ser composto por equipe multidisciplinar, devendo fazer parte: Diretor Técnico, Encarregado pelo Tratamento de Dados Pessoais e líderes de cada área técnica da SETIC.

Pelo fato de o comitê ser multidisciplinar, no que diz respeito a sua composição, se torna importante o desenvolvimento de treinamentos objetivando o nivelamento quanto ao conhecimento, atribuições e funcionamento.

Os membros do comitê não só deverão representar as áreas de negócio da SETIC, mas deverão ser seus líderes, pois detêm conhecimentos em nível estratégico, tático e operacional do funcionamento de seu departamento/setor. Tais membros também desempenharão papel importante na mudança cultural da organização, pois serão considerados verdadeiros influenciadores quanto ao adequado tratamento de dados pessoais, servindo de referências para seus liderados. Além disso, os líderes terão poder de voto em deliberações que se

referem ao tratamento de dados pessoais, fazendo parte das decisões e diretrizes que o órgão deverá seguir em busca da conformidade com a LGPD.

2 ESTRATÉGIA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

2.1 Objetivo e importância do PGP

Fonte: StorySet (2021)

O Programa de Governança em Privacidade da SETIC (PGP) tem por objetivo promover ações permanentes que proporcionem a conformidade da SETIC com a LGPD e normas correlatas. Visa a manutenção, adaptação, criação e execução de políticas, processos e procedimentos buscando a melhoria contínua no que diz respeito ao cumprimento das diretrizes estabelecidas pela LGPD por meio de estratégias e ações necessárias para que a SETIC entre, e se mantenha, em conformidade.

Importante destacar que a SETIC, como órgão da administração pública do Estado de Rondônia, deve cumprir com as determinações legais, não sendo diferente no que diz respeito à LGPD. Deve se atentar aos princípios elencados na própria LGPD, em seu art. 6º: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas; bem como aos fundamentos da disciplina da proteção de dados pessoais, destacas em seu art. 2º: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nesse sentido, todos os departamentos e setores da SETIC devem se atentar ao cumprimento das diretrizes da LGPD, agindo como unidade e colaborando para com a mudança cultural e promoção da conformidade, devendo haver conscientização e comprometimento entre os servidores públicos, clientes, parceiros, fornecedores, prestadores de serviço e demais envolvidos, responsáveis pelas decisões ou realização do tratamento de dados pessoais no âmbito da SETIC.

Vale ressaltar que a SETIC representa o Governo do Estado de Rondônia, sendo este o controlador de direito. Entretanto, a SETIC desempenha funções típicas de controlador, por força da desconcentração administrativa.

Destaca-se que o controlador é “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI, LGPD), já o operador é “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (art. 5º, VII, LGPD). Portanto, a SETIC também poderá ser caracterizada como operadora, dependendo de sua atuação quanto ao tratamento de dados pessoais.

2.2 Modelo de Governança

O PGP contará com ações permanentes que proporcionem a conformidade da SETIC com a LGPD e normas correlatas, podendo, a SETIC, implementar projetos para desenvolver tais ações.

Os projetos deverão ser desenvolvidos observando as necessidades organizacionais e adotando metodologias compatíveis com a realidade da SETIC. Dentre seus requisitos, os projetos deverão contemplar, no mínimo: objetivo geral, objetivos específicos, justificativa, metas, público alvo, indicadores, custos (quando houver), metodologia e líderes responsáveis por cada frente de atuação.

O desenvolvimento e a execução dos projetos relativos à privacidade e proteção de dados pessoais deverá ser realizada pelo Encarregado e CI, com apoio da Coordenadoria de Gestão Estratégica (COGE) da SETIC, que serão responsáveis pelos devidos registros em sistema próprio para gestão deste PGP e dos projetos correlatos.

O CGPD desenvolverá ações de cunho estratégico e tático, já o CI, desenvolverá ações em nível tático e operacional, ambos devem agir em sincronia, dentro de suas competências, objetivando atender as necessidades da SETIC no que diz respeito à conformidade com a LGPD.

Segue figura que ilustra os níveis de atuação do CGPD e do CI:

Figura 2 - Pirâmide dos níveis de atuação do CGPD e CI.

Fonte: Próprio autor (2021).

A responsabilidade de cada um dos colegiados encontra-se na tabela abaixo:

Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD)	**Controle Interno (CI)**
a) Assessorar a SETIC nas atividades relacionadas à privacidade e proteção de dados pessoais; b) Colaborar com a elaboração, implementação e manutenção do Programa de Governança em Privacidade (PGP); c) Facilitar a promoção cultural de privacidade e proteção de dados pessoais; d) Avaliar processos e procedimentos que envolvam o tratamento e proteção de dados pessoais; e) Propor ações e diretrizes voltadas ao tratamento e proteção de dados pessoais; f) Acompanhar as investigações e avaliações de incidentes de segurança da informação que envolvam dados pessoais; g) Notificar a Comissão Permanente de Segurança da Informação (CPSI) da	a. Subsidiar o Encarregado pelo Tratamento de Dados Pessoais na execução de suas atividades; b. Colaborar com o Encarregado na implementação do Programa de Governança em Privacidade (PGP); c. Agir em conjunto com o Encarregado para receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; d. Contribuir com o Encarregado para receber comunicações da Autoridade Nacional e adotar providências; e. Orientar, em conjunto com o Encarregado, os servidores e os contratados da SETIC a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; f. Apoiar o Encarregado no assessoramento aos responsáveis pelo tratamento de dados pessoais na emissão de relatórios de impacto à

SETIC sobre eventuais incidentes de segurança da informação envolvendo dados pessoais, quando vier a ter conhecimento; h) Manifestar-se sobre qualquer matéria relativa à privacidade e proteção de dados pessoais; i) Deliberar sobre propostas de medidas destinadas à privacidade e proteção de dados pessoais; j) Solicitar a colaboração de outros órgãos quando de ações voltadas à privacidade e proteção de dados pessoais; k) Propor a expedição de normativas e recomendações necessárias ao exercício de suas competências; l) Acompanhar as ações relativas à execução de suas deliberações; m) Propor ações voltadas ao seu aperfeiçoamento, com vistas ao cumprimento das disposições da Lei nº 13.709, de 14 de agosto de 2018; n) Auxiliar o Encarregado pelo tratamento de dados pessoais no cumprimento de suas competências; o) Manifestar-se sobre a aquisição de produtos ou serviços destinados a promover a privacidade e proteção de dados pessoais; p) Receber e apreciar propostas que versem sobre adoção de medidas que visem a promoção da privacidade e proteção de dados pessoais no âmbito da SETIC; q) Emitir opiniões e pareceres sobre os Relatórios de Impacto de Proteção de Dados Pessoais (RIPD), inclusive sobre sua metodologia de elaboração; r) Incentivar a realização do Inventário de	proteção de dados pessoais; g. Monitorar, em conjunto com o Encarregado, a conformidade das atividades de tratamento de dados pessoais com a regulamentação e as normas vigentes; h. Colaborar com o Encarregado na recomendação das salvaguardas para mitigar quaisquer riscos aos direitos dos titulares de dados pessoais tratados pela SETIC, inclusive salvaguardas técnicas e medidas organizacionais; i. Auxiliar o Encarregado na implementação de regras de boas práticas e de governança; j. Contribuir com o Encarregado na realização do Inventário de Dados Pessoais (IDP); k. Promover campanhas de conscientização e publicidade, bem como treinamentos e o desenvolvimento de pessoal, no que diz respeito ao adequado tratamento de dados pessoais no âmbito da SETIC; l. Executar as demais atribuições determinadas pela SETIC ou estabelecidas em normas complementares relativas ao tratamento de dados pessoais.

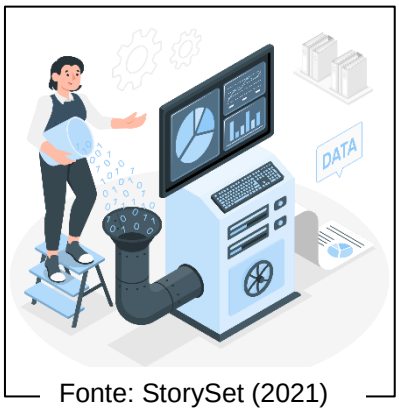
Dados Pessoais (IDP); s) propor diretrizes para execução de atividades sob responsabilidade do Controle Interno (CI) e do Encarregado.	

Todos os documentos e comunicações relativos a ações de conformidade com a LGPD deverão ser registrados em sistema eletrônico, Documentos Sistemas (https://documentos.sistemas.ro.gov.br/shelves/lgpd) e Sistema Eletrônico de Informações - SEI (https://sei.sistemas.ro.gov.br/), ou no que vier a substituí-los.

3 TRATAMENTO DE DADOS PESSOAIS

3.1 Tratamento de dados pessoais pelo Poder Público

A LGPD constitui marco importante para os órgãos da administração pública, sejam municipais, estaduais ou federais, pois devem cumprir com seus ditames. Dentre as características da LGPD, destaca-se a transdisciplinaridade, pois permeia os mais variados órgãos e departamentos na administração pública, cujo tratamento de dados pessoais pode envolver diferentes titulares, desde os próprios servidores até usuários dos serviços públicos.



Fonte: StorySet (2021)

O tratamento de dados pessoais realizado pelo Poder Público, conforme art. 23, LGPD, deve atender “sua finalidade pública, na persecução do interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, informando inclusive as hipóteses em que realiza o tratamento de tais dados, fornecendo informações sobre a previsão legal, finalidade, procedimentos e práticas utilizadas.

Portanto, a SETIC, como parte integrante da administração pública do Governo do Estado de Rondônia, objetivando entrar em conformidade com a LGPD, agindo com responsabilidade e transparência, deve se atentar às suas competências, procurando executar ações que objetivem cumprir com as exigências relativas ao tratamento de dados pessoais.

Para isso, há necessidade de se realizar um inventário e mapeamento de todos os dados pessoais que são tratados no âmbito da SETIC, avaliando-se serviços e processos de negócios sob o aspecto da LGPD, procurando, na sequência, corrigir eventuais desvios e traçar ações para resolver ou mitigar as lacunas encontradas.

3.2 Inventário de Dados Pessoais (IDP)

O Inventário de Dados Pessoais (IDP) contempla uma das exigências da LGPD, mais especificamente em seu art. 37, quando determina que “o controlador e

o operador devem manter registro de operações de tratamento de dados pessoais que realizarem". Além disso, visa subsidiar a elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) e outras ações necessárias, como a identificação de lacunas frente às exigências da LGPD ou de outras normas.

O objetivo é realizar o levantamento das ações que o órgão desenvolve com dados pessoais, delimitando-se o escopo das operações de tratamento de dados pessoais, abrangendo, no mínimo: identificação dos agentes de tratamento; as fases do ciclo de vida do tratamento; descrição do fluxo do tratamento; hipótese legal de tratamento; finalidade e previsão legal do tratamento; quais dados são tratados; categoria dos titulares; informações sobre compartilhamento; classificação das medidas de segurança; informações sobre transferência internacional; e informações sobre contratos, termos ou congêneres que estejam correlatos com o tratamento.

A metodologia utilizada para realizar o IDP é a *top-down*, iniciando-se a análise pelos serviços/processos, e não pelo dado propriamente dito. O Encarregado, com apoio do CI e do CGPD, será responsável pela condução da realização do IDP, devendo seguir as orientações do **Guia de Elaboração de Inventário de Dados Pessoais**[3] da Secretaria de Governo Digital (SGD), do Ministério da Economia, Governo Federal, considerando as peculiaridades da SETIC, não descartando-se o uso de ferramentas de *software* para realização do mapeamento (*data mapping*) e descoberta (*data discovery*) de dados pessoais. Ao final, a SETIC terá os registros das operações de tratamento de dados pessoais considerando cada serviço/processo existente na organização. O IDP deverá ser realizado pelos responsáveis do serviço/processo de negócio, ou seja, por seus donos, com o apoio do CI.

Destaca-se que é importante sempre manter tais registros atualizados, por isso deve-se estabelecer um ciclo de periodicidade para revisão. Portanto, todos os departamentos e setores da SETIC devem revisar o IDP a cada ano, e sempre que houver mudança no ciclo de tratamento de dados pessoais do serviço/processo relacionado.

[3] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf. Acesso em: 17 mar. 2021, p. 6.

Atendendo ao princípio da transparência, elencado no art. 6º, VI, LGPD, o IDP de cada serviço ou processo de negócio deverá ser público, sendo disponibilizado no sítio eletrônico da SETIC.

3.3 Parecer diagnóstico do IDP

O parecer diagnóstico deve ser realizado com base no IDP, caracterizando-se pela sua avaliação e validação, apreciando-se todos os quesitos indicados no *template*(formulário de inventário). Deve ser realizado pelo Encarregado, com apoio do CI e do CGPD.

Por meio dessa ação, o Encarregado deverá identificar os serviços/processos de negócios que precisam se adequar à LGPD, bem como as lacunas (*gaps*) existentes, recomendando soluções para resolvê-las ou mitigá-las.

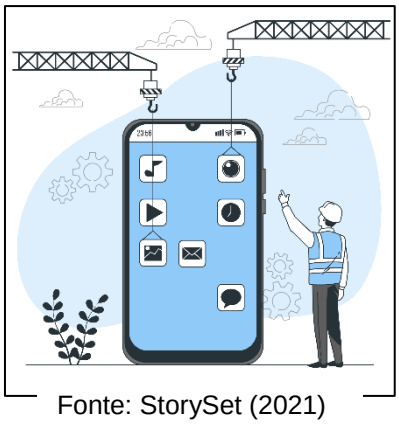
É o momento para realizar a avaliação crítica sobre todas as operações de tratamento de dados pessoais que são realizadas pelo órgão. Tais informações subsidiarão a realização de ações visando a adequação da SETIC à LGPD. Além disso, também deverão ser providenciados dados estatísticos sobre a quantidade de dados pessoais e dados pessoais sensíveis que são tratados e sobre as hipóteses de tratamento que respaldam as ações da SETIC.

O Encarregado e o CI deverão se articular com cada departamento ou setor da SETIC, responsáveis pelo serviço ou processo de negócio, com intuito de informar sobre os resultados do parecer diagnóstico de seus respectivos inventários, registrando notificações e apontamentos sobre tratamento inadequado e/ou excessivo, bem como sobre a existência de lacunas.

4 GESTÃO DE MUDANÇA

4.1 Privacidade desde a concepção (*Privacyby Design*)

Existem diferentes formas de gerir mudanças em ambientes organizacionais. Considerando o contexto da SETIC, bem como suas peculiaridades, adotará planos de ação objetivando implementar a privacidade desde a concepção de serviços e processos de negócio, além de promover, sistematicamente, campanhas de conscientização e publicidade, bem como treinamento e desenvolvimento relacionados com as diretrizes da LGPD.



Fonte: StorySet (2021)

A privacidade desde a concepção, conhecida como *Privacyby Design*,consiste em desenvolver projetos, produtos ou serviços já inserindo medidas de privacidade desde sua construção.

No art. 46, § 2º, LGPD, determina-se que os agentes de tratamento (controlador e operador) devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, sendo que tais medidas devem ser observadas desde a fase de concepção do produto ou do serviço até sua execução.

O *Privacyby Design* possui 7 (sete) princípios, sendo estes:

1. Proatividade e prevenção;
2. *Privacyby Default* (privacidade como padrão);
3. Privacidade incorporada ao *design*, pois deve ser incorporado ao desenvolvimento e à arquitetura de sistemas de TIC, bem como em práticas de negócios e quaisquer produtos e serviços desenhados;
4. Funcionalidade total, pois busca acomodar todos os legítimos interesses e objetivos;
5. Segurança de ponta a ponta, uma vez que integra todas as fases do ciclo de vida do tratamento de dados pessoais;
6. Visibilidade e transparência, que preza pela diligência e pela conformidade; e
7. Respeito pela privacidade do usuário.

Nesse sentido, o Encarregado e o CI, com apoio do CGDP, deverão promover ações voltadas à incorporar o *Privacyby Design* na cultura organizacional da SETIC, desde a concepção até a execução de serviços, processos e produtos, no âmbito de suas competências. Tal implementação deverá ocorrer de forma progressiva, com a realização de campanha de conscientização e publicidade, bem como por meio da realização de treinamento e desenvolvimento contínuo.

4.2 Campanha de conscientização e publicidade

A instituição de uma campanha de conscientização e publicidade é uma ação que visa principalmente a mudança cultural quanto ao tratamento de dados pessoais, uma vez que a LGPD é transdisciplinar e deve ser cumprida no decorrer de todo o ciclo de vida do tratamento de dados pessoais.

No mais, na própria LGPD (art. 50, I, “a”) se verifica 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 poderá ser incentivado por meio da campanha de conscientização e publicidade.

A campanha deverá ser promovida pelo CI com apoio do CGPD, por meio de *folders*, *banners*, cartilhas, manuais de conduta, gamificação, vídeos, entrevistas, páginas *web*, *e-mail*, boletins informativos, folhetos, slogan etc., todos de cunho informacional, procurando promover a conscientização dos próprios servidores que atuam em nome da SETIC, dos clientes, parceiros, fornecedores, prestadores de serviço e demais envolvidos, sobre a importância e responsabilidade de todos no processo de entrada e permanência em conformidade com a LGPD.

Deverá ainda, a campanha, ser continuamente desenvolvida e procurar informar sobre a aplicabilidade de normas correlatas à LGPD, políticas relacionadas, consequências em decorrência de suas violações e informar sobre canais para sanar dúvidas e receber reclamações e denúncias.

4.3 Treinamento e desenvolvimento

O treinamento e desenvolvimento consistem em ações objetivando o nivelamento e constante aperfeiçoamento dos servidores que atuam em nome da SETIC, objetivando difundir boas práticas no que diz respeito à conformidade com a LGPD. É uma necessidade, considerando a transdisciplinaridade da Lei, que permeia os mais variados setores e departamentos de uma organização.

O art. 50, I, "a", LGPD, explicita 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 poderá ser incentivado por meio de programas de treinamento e desenvolvimento.

O treinamento e desenvolvimento poderá ser realizado por meio de cursos, palestras, eventos, congressos, *workshops*, oficinas etc., utilizando-se inclusive das ações que a SETIC já disponibiliza, como a SIXFIRE, SETICAST, Programa de Capacitação Institucional (PCI) e SETICEXPLICA.

Além do treinamento e desenvolvimento em nível institucional, procurando alinhar o conhecimento sobre LGPD, a SETIC também poderá custear ações específicas voltadas aos membros do CI e do CGPD, com intuito de se aprofundarem nos conhecimentos relativos à privacidade e proteção de dados pessoais, buscando facilitar a execução de suas atribuições e promovendo melhorias no que diz respeito à conformidade com a LGPD.

O treinamento e desenvolvimento será promovido pelo CI com apoio do CGPD, podendo contar com representantes internos ou externos à SETIC, devendo ser desenvolvidos continuamente.

4.4 Revisão de contratos e instrumentos congêneres

A adequação e revisão dos atuais contratos com terceiros deve ser realizada objetivando o cumprimento dos dispositivos da LGPD, tanto pelo controlador quanto pelo operador, e demais envolvidos no tratamento de dados pessoais.

Nesse sentido, deve-se procurar atender principalmente aos princípios da adequação, responsabilização e prestação de contas, elencados no art. 6º, LGDP, buscando cumprir com a compatibilidade entre o tratamento e as finalidades

elencadas em contrato, bem como com a observância e o cumprimento de normas de proteção de dados pessoais pelos envolvidos no ciclo de tratamento.

A LGPD, em seu artigo 42, caput, determina que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados pessoais é do controlador ou operador. Inclusive há previsão (art. 42, I, LGPD) de responsabilidade solidária do operador quando este não cumprir com suas obrigações legais e com instruções lícitas do controlador.

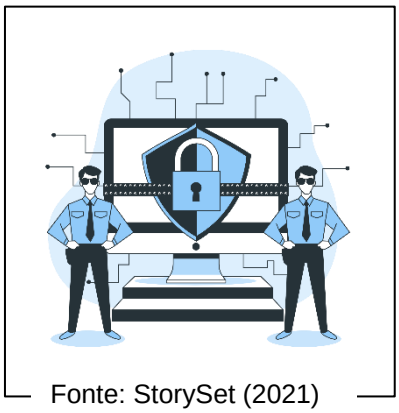
Dessa forma, torna-se imperioso que todos os contratos, termos, convênios e congêneres estejam adequados à LGPD e normas complementares, prevendo cláusulas específicas sobre proteção de dados pessoais, destacando-se ainda a necessidade de realizar diligências junto aos parceiros para validação de cumprimento das exigências da LGPD (*DueDiligence*).

Os gestores de contratos deverão se atentar à necessidade de atualização destes que estão sob sua responsabilidade, agindo em sincronia com o CI e com o Jurídico, que promoverão ações de conscientização no âmbito de todos os departamentos e setores da SETIC.

5 SEGURANÇA DE DADOS

5.1 Gestão de vulnerabilidades

A gestão de vulnerabilidades objetiva a realização de monitoramento e aplicação de resolução/mitigação de eventuais falhas existentes em sistemas inseridos no contexto do órgão. Procura prevenir a exploração de tais vulnerabilidades, identificando e aplicando soluções pontuais.



Fonte: StorySet (2021)

A SETIC deve reforçar as ações de gestão de vulnerabilidades, procurando cumprir com a abordagem contida no caput do art. 50, LGPD, que determina que tanto o controlador quanto o operador devem formular regras de boas práticas e de governança que estabeleçam mecanismos internos de supervisão e de mitigação de riscos.

A análise de vulnerabilidades deve ser realizada periodicamente, registrando e notificando os envolvidos, orientando-os quanto ao seu uso, manutenção e desenvolvimento.

Nesse contexto, a SETIC deve adotar mecanismos de monitoramento proativo no que diz respeito aos eventos de segurança.

Não obstante, tal ação também visa o atendimento do previsto no *caput* do art. 46 da LGPD, determinando 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”.

5.2 Gestão de incidentes de violação de dados pessoais

Considerando as diretrizes da LGPD, é importante frisar que o controlador deverá comunicar à ANPD, bem como ao titular, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, inteligência do *caput*, art. 48, LGPD.

Já o art. 48, § 1º, estabelece que tal comunicação deverá ser realizada em prazo razoável, contendo no mínimo: a descrição da natureza dos dados pessoais afetados; informações sobre os titulares envolvidos; e indicação das medidas técnicas e de segurança utilizadas para proteção dos dados.

Dessa forma, torna-se imperiosa a implementação de uma gestão de incidentes de violação de dados pessoais, abrangendo a criação de: um CSIRT (*Computer Security Incident Response Team* - Grupo de Resposta a Incidentes de Segurança); de procedimentos para apuração de incidentes; de gestão de auditoria e logs; e plano de respostas e comunicação de incidentes.

Com tais ações, a SETIC também estará cumprindo com as determinações contidas no art. 50, § 2º, I, "g", LGPD, que consiste na abordagem de planos de respostas a incidentes e remediações no Programa de Governança em Privacidade (PGP).

A SETIC também deverá promover o registro das ações adotadas para solucionar os incidentes que envolvam violação de dados pessoais, bem como registrar tais incidentes, tornando-se importante o estabelecimento de responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes que envolvam violação de dados pessoais.

5.3 Avaliação de riscos de segurança e de privacidade

A avaliação de riscos de segurança e de privacidade deve ocorrer com base nos Relatórios de Impacto de Proteção de Dados (RIPD), que dependem da realização do Inventário de Dados Pessoais (IDP).

Risco, conforme "Glossário de Segurança da Informação" (Portaria nº 93, de 26 de setembro de 2019), consiste num "potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização". Já a avaliação de riscos consiste no "processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco".

A avaliação de riscos objetiva classificar os riscos envoltos dos ativos, neste caso os dados pessoais dos titulares, e possibilitar a implementação de ações voltadas à mitigação, resolução ou transferência do risco.

Não obstante, a SETIC deve cumprir com a abordagem contida no caput do art. 50, LGPD, que determina que tanto o controlador quanto o operador deverão formular regras de boas práticas e de governança que estabeleçam mecanismos internos de supervisão e de mitigação de riscos.

Classificar os riscos envoltos dos ativos, neste caso os dados pessoais dos titulares, e possibilitar a implementação de ações voltadas à mitigação, resolução ou transferência do risco.

6 GESTÃO DE REQUISIÇÕES E CONSENTIMENTO

6.1 Sistema para gerir requisições e consentimento de titulares

Fonte: StorySet (2021)

De acordo com o art. 18 da LGPD, o titular tem direito a obter do controlador, em relação aos seus dados pessoais, a qualquer momento e mediante requisição: a confirmação da existência de tratamento; o acesso aos dados; a correção de dados; a anonimização, bloqueio ou eliminação de dados; a portabilidade dos dados a outro fornecedor de serviço ou produtos; a eliminação dos dados pessoais tratados com o consentimento do titular; a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e a revogação do consentimento.

O titular também tem direito à revisão de decisões automatizadas (art. 20, LGPD).

Sobretudo, destaca-se que o titular exercerá seus direitos mediante requerimento expresso dele próprio ou de representante legalmente constituído, a agente de tratamento (art. 18, § 2º, LGPD).

Segundo Viviane Maldonado, “A gestão é sim algo complexo, mas a preparação inicia com o agente de tratamento elencando e organizando tudo aquilo que seja necessário para se conseguir responder ao titular. A gestão das requisições passará basicamente por três aspectos, que devem acontecer ao mesmo tempo. Primeiro, por processos, com canal para receber as demandas e desenhados a partir da realidade de cada empresa. Segundo, por treinamentos, para toda a pirâmide da organização. E terceiro, mas não menos importante, é preciso facilitar para o titular”.

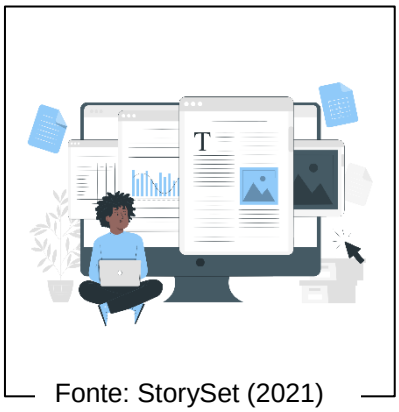
Nesse sentido, as manifestações do titular deverão ser efetivadas por meio do **Fala.BR Rondônia** da Ouvidoria-Geral do Estado de Rondônia - OGE, que serão, por sua vez, direcionadas ao Encarregado e ao CI para atendimento.

Os prazos para tramitação das requisições serão os mesmos da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), da Lei nº 13.460/2017 (Código de

Defesa dos Usuários de Serviços Públicos) ou de norma correlata, salvo disposição específica na LGPD.

7 ELABORAÇÃO DE DOCUMENTOS DE PRIVACIDADE E SEGURANÇA

7.1 Política de privacidade



Fonte: StorySet (2021)

A Política de Privacidade, conforme **Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços Públicos**[4], tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas. Para isso, o serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares seja garantida de forma eficiente e como os princípios elencados no art. 6º, LGPD, são atendidos.

O art. 6º, que trata dos princípios da LGPD, traz em seu inciso VI o princípio da transparência, o qual consiste em “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”, justificando a implementação da Política de Privacidade.

Ademais, o caput do art. 50 da LGPD versa que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam, dentre outros, regime de funcionamento, normas de segurança e outros aspectos relacionados ao tratamento de dados pessoais, reforçando a ideia da implementação da Política de Privacidade.

O Encarregado, com o apoio do CI e do CGPD, será responsável pela elaboração da Política de Privacidade.

7.2 Termo de uso

[4] 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/governanca-de-dados/ GuiaTermoUso.pdf. Acesso em: 6 jun. 2021, p. 24.

O Termo de Uso, conforme **Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços Públicos**[5] (SGD, 2020, p. 6), é um documento que estabelece as regras e condições de uso de determinado serviço. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele.

O art. 6º, que trata dos princípios da LGPD, traz em seu inciso VI o princípio da transparência, o qual consiste em "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial", justificando a implementação do Termo de Uso.

Ademais, o caput do art. 50 da LGPD versa que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam, dentre outros, regime de funcionamento, normas de segurança e outros aspectos relacionados ao tratamento de dados pessoais, reforçando a ideia da implementação da Termo de Uso.

7.3 Política de segurança

Política de Segurança da Informação (PSI), conforme "Glossário de Segurança da Informação" (Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República), consiste num documento contendo um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação.

Conforme descreve o art. 46 da LGPD: "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".

A adoção de uma PSI também cumpre com os quesitos elencados no art. 50, § 1º, I, "a" e "d", especificando que o controlador deve demonstrar comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma

[5] Ibid., p. 6.

abrangente, de normas e boas práticas relativas à proteção de dados pessoais; e estabelecer políticas e salvaguardas adequadas.

Dessa forma, a implementação de uma PSI procura prevenir danos ao andamento do negócio e padronizar procedimentos, além de prever e mensurar respostas a incidentes. A longo prazo, isso pode resultar na redução de custos com incidentes de TIC.

A PSI deve estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis, devendo conter, além dos objetivos, princípios e requisitos do documento, as seguintes normatizações: responsabilidades dos servidores; responsabilidades da área de TIC; informações ligadas à logística da implementação da TIC no órgão; tecnologias de defesa contra ciberataques; política de treinamento aos colaboradores dentre outras.

No âmbito da SETIC a Política de Segurança da Informação (PSI) foi instituída pela Portaria nº 97, de 09 de junho de 2021.

7.4 Relatório de Impacto de Proteção de Dados (RIPD)

De acordo com o art. 5º, XVII, LGPD, o Relatório de Impacto de Proteção de Dados (RIPD) consiste em “documentação 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”.

Ademais, ao longo da LGPD, o RIPD é abordado em diferentes vertentes. No art. 4º, § 3º, a ANPD deverá solicitá-lo aos responsáveis elencados no rol de exceções do art. 4º, III. No art. 10, § 3º, a ANPD poderá solicitá-lo quando do tratamento com fundamento no legítimo interesse. No art. 32, a ANPD poderá solicitar sua publicação e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público. No art. 38, a ANPD poderá determinar ao controlador sua elaboração referente a operações de tratamento de dados pessoais.

O RIPD deve abordar, por exemplo, a análise dos riscos à privacidade e proteção de dados pessoais no que diz respeito ao tratamento, considerando cada serviço/processo de negócio que demandarem tal necessidade.

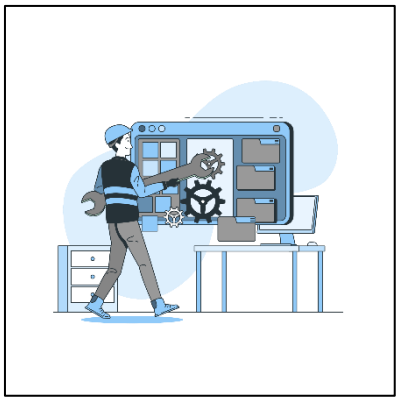
No que diz respeito às etapas de construção do RIPD, deve-se abordar no mínimo:

- a realização da análise preliminar do serviço/processo de negócio, identificando a real necessidade de se elaborá-lo;
- a realização ou revisão do IDP do serviço/processo negócio;
- a análise do risco e desenvolvimento do plano de tratamento;
- o desenvolvimento de relatório e publicação do mesmo.

O RIPD deverá ser realizado pelos responsáveis do serviço/processo de negócio, ou seja, por seus donos, com o apoio do CI.

8 IMPLEMENTAÇÃO

Após devidamente estruturado, o PGP deverá ser adotado por toda a SETIC, devendo, os departamentos e setores, cumprirem com o previsto nos documentos de privacidade e segurança atendendo os preceitos da LGPD e normas correlatas, no que diz respeito ao adequado tratamento de dados pessoais.



Fonte: StorySet (2021)

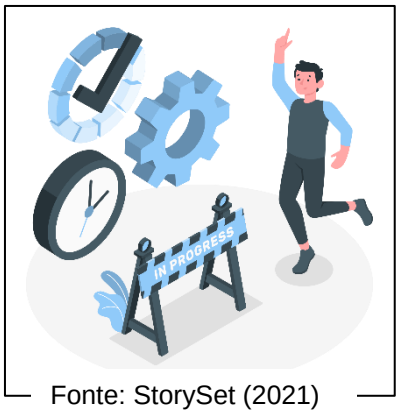
Deve ainda, ser tornado público, estando disponível no sítio eletrônico da SETIC, dando-se ampla divulgação, principalmente aos servidores públicos, clientes, parceiros, fornecedores, prestadores de serviço e demais interessados.

Salienta-se, inclusive, que o PGP se trata de documento dinâmico, devendo evoluir de acordo com mudanças legais, regulatórias e demais normativas relacionadas ao tratamento de dados pessoais, considerando inclusive novas tecnologias, bem como os serviços e processos de negócios no contexto da SETIC.

9 MONITORAMENTO E AVALIAÇÃO

9.1 Instrumentos de monitoramento

A implementação do PGP deverá ser monitorada, objetivando sua manutenção e aplicação de melhorias em busca de sua efetividade. Tal ação visa a garantia do cumprimento de seu objetivo, bem como de ações norteadoras para sua execução.



Fonte: StorySet (2021)

Tal monitoramento deverá ser constante, sendo conduzido pelo Encarregado e pelo CI com apoio do CGPD, destacando-se as seguintes atividades:

- a criação e utilização de métricas; e
- a instituição de canal para contatar encarregado e realizar denúncias;
- auditoria.

Destaca-se ainda que este PGP deverá ser revisado a cada 2 (dois) anos, ou quando for necessário, dependendo da análise prévia do Encarregado, CI e CGPD.

9.2 Criação e utilização de métricas

As métricas possibilitam mensurar, monitorar e gerir as estratégias visando a entrada e permanência da SETIC em conformidade com a LGPD. Elas apresentam informações sobre quais estratégias devem ser continuadas, aperfeiçoadas ou até mesmo abandonadas.

Conforme o **Programa de Governança em Privacidade do Ministério das Comunicações**[6], as métricas são ferramentas que facilitam a tomada de decisões estratégicas e a prestação de contas. São obtidas mediante a coleta, análise e relatório de dados. Para serem eficientes, devem ser objetivas, mensuráveis, relevantes e claramente definidas, além de alinhadas com o objetivo específico do PGP. O ciclo de vida da métrica envolve a identificação da audiência a que as

[6] BRASIL. **Programa de Governança em Privacidade do MCOM**. Ministério das Comunicações. Disponível em: https://www.gov.br/mcom/pt-br/composicao/secretaria-executiva-novo/planejamento-e-tecnologia-da-informacao/programa-de-governanca-em-privacidade/ProgramadeGovernanaemPrivacidadedoMCaLGPD_mcom.pdf. Acesso em: 6 jun. 2021, p. 17.

métricas se destinam, seleção das métricas relevantes, definição dos responsáveis por sua mensuração, coleta e análise da métrica.

São essenciais pois apontam os reais resultados de investimentos, sejam em gestão de pessoas, otimização de processos, redução de gastos, aumento da produtividade dentre outros.

A SETIC adotará, para mensuração de índice de maturidade, o **Diagnóstico de Adequação à LGPD**[7], disponível pelo Governo Federal, por intermédio da Secretaria de Governo Digital (SGD). Trata-se de questionário que, após respondido, apresenta índice de maturidade, possibilitando a priorização das ações necessárias para entrada em conformidade com a LGPD. O diagnóstico traz consigo o índice de maturidade e seu nível de adequação correspondente, conforme Figura abaixo:

Figura 3 - Índice e nível de adequação à LGPD.

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em aprimoramento
0,90 a 1,00	Aprimorado

Fonte: Secretaria de Governo Digital (SGD) do Ministério da Economia (2021).

Destaca-se que esse diagnóstico deverá ser realizado com periodicidade, comparando-se os resultados com intuito de avaliar o progresso da SETIC em busca da conformidade. Os resultados das avaliações deverão ser publicados no sítio eletrônico da SETIC.

Além disso, seguem exemplos de outras métricas que poderão ser adotadas:

- percentual de treinamentos concluídos;
- porcentagem de conformidade de sistemas;
- número de requisições de titulares de dados;
- número de incidentes de segurança/vazamento de dados etc.

9.3 Canal para contatar encarregado e realizar denúncias

[7] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd. Acesso em: 16 mar. 2021.

A institucionalização de canal para contatar o encarregado, bem como para registro de denúncias, pressupõem ação voltada à auditoria e ao monitoramento no que diz respeito à conformidade do tratamento de dados pessoais perante a LGPD e o cumprimento dos princípios elencados no art. 6º da referida Lei.

O art. 5º, VIII, LGPD, contém a definição de encarregado, que consiste: “Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD”. Ademais, o art. 50, § 2º, I, alínea “e”, esclarece que no Programa de Governança em Privacidade (PGP) tem o “objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular”.

O caráter da denúncia anônima busca proteger a identidade da pessoa do denunciante, evitando perseguições e retaliações.

Portanto, para cumprir tais apontamentos deve-se instituir canal de comunicação para contar o encarregado, bem como para apuração de eventuais desvios.

Nesse sentido, as requisições e denúncias deverão ser efetivadas por meio do **Fala.BR Rondônia** da Ouvidoria-Geral do Estado de Rondônia - OGE, que serão, por sua vez, direcionadas ao Encarregado e ao CI para atendimento.

9.4 Auditoria

A auditoria consiste em ações que buscam avaliar e evidenciar o cumprimento das diretivas fornecidas pelo PGP, devendo ter como abrangência toda a SETIC, limitando-se ao tratamento de dados pessoais e demais normas correlatas.

Deverá ser realizada pelo CI com apoio do CGPD, apontando ações que deverão ser diligenciadas para corrigir eventuais inadequações.

Poderá ser realizada de forma proativa (com intuito de validar o adequado tratamento de dados pessoais e cumprimentos de normas correlatas) ou reativa (tal como o recebimento de denúncia acerca do inadequado tratamento de dados pessoais).

É possível também que a SETIC utilize auditoria por terceiros independentes, realizada por instituições de consultoria especializada ou autoridades de supervisão, como a ANPD.

Para cada auditoria deverá ser emitido parecer conclusivo apontando todas as nuances relativas à LGPD, observado o serviço ou processo de negócio.

REFERÊNCIAS

BRASIL. **Guia de boas práticas**: Lei Geral de Proteção de Dados Pessoais (LGPD). Comitê Central de Governança Digital. Versão 2. Brasília: ago. 2020.

BRASIL. **Guia de elaboração de inventário de dados pessoais**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: abr. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia_inventario_dados_pessoais.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Guia de elaboração de programa de governança em privacidade**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: out. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Aceso em: 6 jun. 2021.

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/governanca-de-dados/ GuiaTermoUso.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. ANPD. Brasília: mai. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em 28 mar. 2021.

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/ L13709compilado.htm. Acesso em: 28 mar. 2021.

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: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em 6 jun. 2021.

BRASIL. **Programa de Governança em Privacidade do MCOM**. Ministério das Comunicações. Disponível em: https://www.gov.br/mcom/pt-br/composicao/secretaria-executiva-novo/planejamento-e-tecnologia-da-informacao/programa-de-governanca-em-privacidade/ ProgramadeGovernanaemPrivacidadedoMCaLGPD_mcom.pdf. Acesso em: 6 jun. 2021.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CRESPO, Marcelo Xavier de Freitas. **Compliance no Direito Digital**. São Paulo: Thomson Reuters Brasil, v. 3, 2020.

MALDONADO, Viviane Nóbrega. LGPD: **Lei Geral de Proteção de Dados Pessoais**: manual de implementação. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane. SERPRO Notícias e Artigos. **O titular e a gestão de seus direitos**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/ titular-gestao-direitos-lgpd/. Acesso em: 6 jun. 2021.
OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

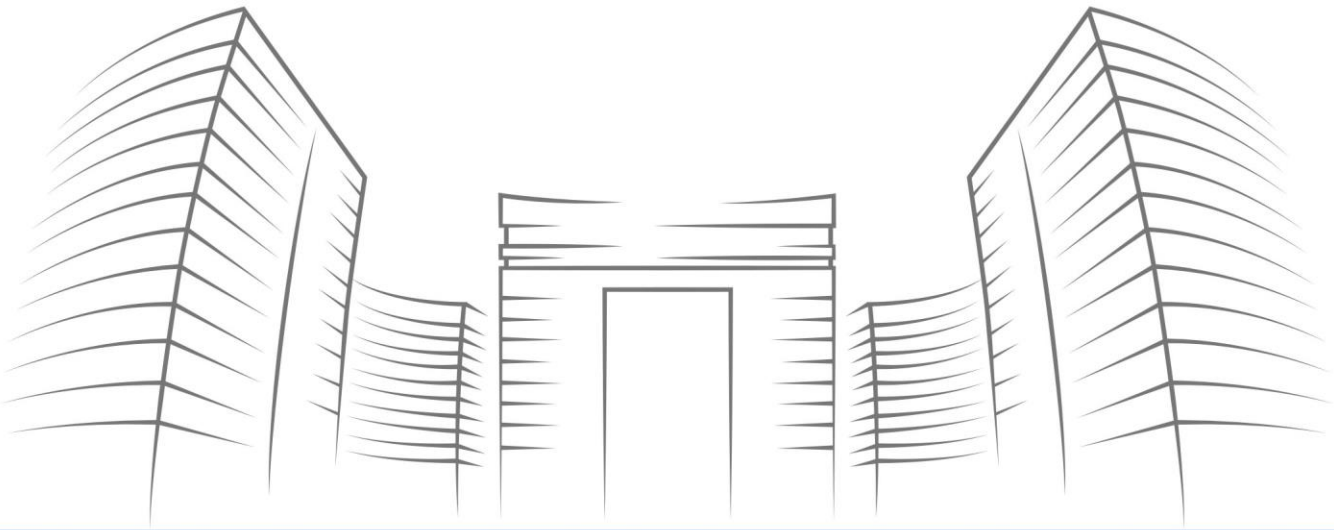
PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

POZZO, Augusto Neves Dal. MARTINS, Ricardo Marcondes. **LGPD e administração pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

SETIC
Superintendência Estadual de
Tecnologia da Informação e Comunicação

Governo do Estado de
RONDÔNIA

Wiki.SETIC | *Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC*
wiki.setic.ro.gov.br



setic.ro.gov.br
@setic.rondonia

Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470