PORTARIA Nº 457 DE 26 DE MAIO DE 2022

DOE 101 | Pág. 16 | 01.06.2022

Instituir o Programa de Governança de Proteção de Dados no âmbito da Procuradoria Geral do Estado de Rondônia.

O PROCURADOR-GERAL DO ESTADO DE RONDÔNIA, no uso de suas atribuições legais, especialmente as previstas no artigo 23, da Lei Complementar Estadual nº 620, de 20 de junho de 2011, com a redação da Lei Complementar Estadual nº 1.106, de 12 de novembro de 2021;

CONSIDERADO o art. 11, inciso I da Complementar Estadual nº 620, de 20 de junho de 2011;

CONSIDERANDO a Lei n. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO a aprovação pelo Comitê Gestor de Proteção de Dados do Programa de Governança em Privacidade e Proteção de Dados Pessoais em reunião realizada no dia 25 de maio de 2022 na sede da Procuradoria-Geral do Estado.

Art. 1º Instituir o Programa de Governança de Proteção de Dados no âmbito da Procuradoria-Geral do Estado de Rondônia inserido no anexo I deste resolução.

Art. 2º Esta resolução entra em vigor na data de sua publicação.

Maxwel Mota de Andrade

Procurador-Geral do Estado

Fábio de Sousa Santos

ANEXO I

1. ROTEIRO DE IMPLEMENTAÇÃO

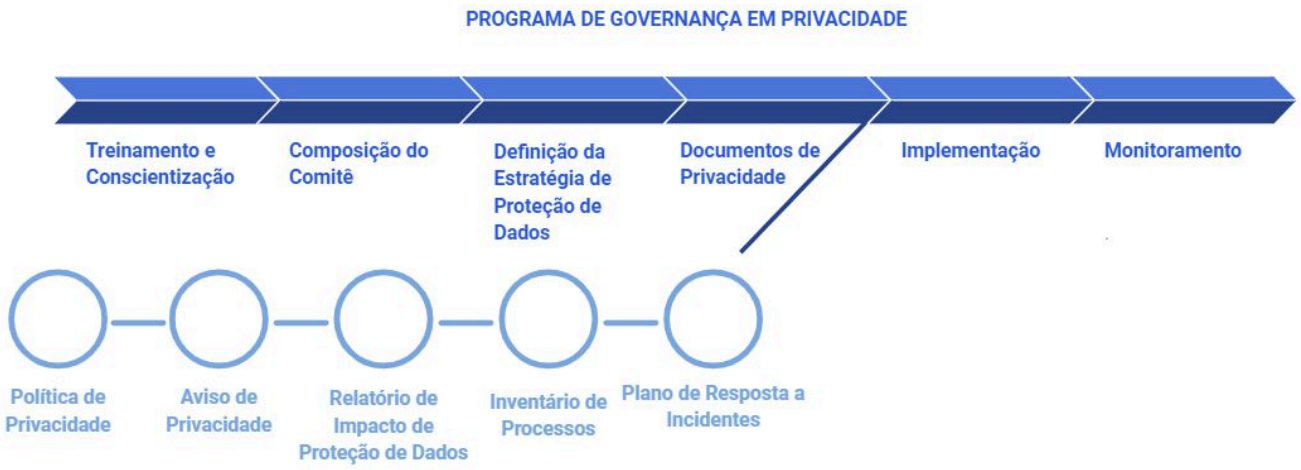
O presente documento apresenta, de forma sucinta, um roteiro de atividades que devem ser realizadas para a implementação de um Programa de Governança em Privacidade, em conformidade com o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n. 13.709, de 14 de agosto de 2018) e o decreto estadual nº 26.451, de 4 de outubro de 2021.

O roteiro é baseado em boas práticas da indústria e em modelos internacionais, mas leva em consideração a estrutura organizacional da Procuradoria-Geral do Estado de Rondônia (PGE-RO) de forma a conhecer o contexto jurídico normativo em que a PGE-RO desempenha suas atividades institucionais e realiza o tratamento de dados pessoais, para a realização de um Programa de Governança em Privacidade destacam-se, como essenciais, as seguintes atividades:

ETAPA	PRAZO
Composição do Comitê de Proteção de Dados Pessoais e da Equipe de Proteção de Dados Pessoais	Cumprido
Avaliação da Realidade Organizacional (Diagnóstico)	30 dias após aprovação do Programa de Governança em proteção de dados
Definição da Estratégia de Proteção de Dados Pessoais	30 dias após realização do diagnóstico
Elaboração dos Documentos de Privacidade	30 dias após realização da Estratégia de Proteção de Dados Pessoais
Treinamento e Conscientização	Início 30 dias após realização dos Documentos de Privacidade, todavia serão realizados de forma contínua
Plano de Resposta a Incidentes de Segurança da Informação e Privacidade	60 dias após início dos Treinamentos e Conscientização
Monitoramento do Programa de Governança em Privacidade (Avaliação)	Realizado de forma contínua

O presente documento apresenta proposta de Programa de Governança em Privacidade, que

deverá ser validado e complementado pelo Comitê de Proteção de Dados da PGE/RO. A figura a seguir apresentada resume as atividades que contemplam o Programa de Governança em Privacidade e suas sub-atividades, que serão descritas ao longo deste documento.



2. ATIVIDADES DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

O Programa de Governança em Privacidade guia uma instituição para a conformidade com leis e regulamentos de privacidade e proteção de dados pessoais, apoiando objetivos e metas mais amplas da organização. Conforme o art. 50, I, da LGPD, deve, no mínimo:

- 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;
- ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- ter o objetivo de estabelecer relação de confiança com o titular de dados, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- estar integrado à estrutura geral de governança da instituição, além de estabelecer e aplicar mecanismos desupervisão internos e externos;
- contar com planos de resposta a incidentes e remediação;
- ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

A seguir detalham-se as atividades consideradas essenciais para a realização de um Programa de Governança em Privacidade.

É importante frisar que algumas dessas atividades ocorrerão em paralelo e se repetirão ao longo de várias etapas. Por exemplo, atividades de treinamento e de conscientização devem ocorrer em todas as fases do plano em que se detecte a necessidade de nivelamento organizacional sobre noções de privacidade e proteção de dados pessoais (ou conhecimentos mais especializados, a depender da área).

Outro exemplo é o das atividades de monitoramento, que permanecerão após a implementação do Programa de Governança em Privacidade, para garantir seu aprimoramento contínuo.

2.1. TREINAMENTO E CONSCIENTIZAÇÃO

Para que um Programa de Governança em Privacidade seja corretamente implementado, é essencial que toda a instituição esteja bem alinhada. A melhor forma de fazer isso é a partir de programas de treinamento e conscientização do corpo funcional. Campanhas de treinamento e comunicação devem informar leis e políticas aplicáveis e as consequências por violá-las, identificar possíveis violações, explicar como abordar reclamações, e incluir procedimentos de denúncia.

Com relação à Procuradoria-Geral do Estado de Rondônia, enquanto conhecimentos gerais sobre a política de privacidade devem ser comunicados para todas as equipes, algumas funções podem necessitar de capacitações específicas e mais especializadas, a saber:

- A Gestão de Pessoas deve ser informada sobre procedimentos administrativos para tratar dados pessoais do corpo funcional durante todo o ciclo de vida dos dados;
- A Tecnologia da Informação deve ser capacitada para a implementação de medidas técnicas de segurança que protejam os dados pessoais tratados no âmbito da instituição;
- A Ouvidoria deve ser preparada para receber solicitações e reclamações de titulares de dados, com respeito a seus direitos e eventuais vazamentos de dados;
- A Comunicação Social deve compreender bem o Programa de Governança em Privacidade para que possa traduzi-lo em campanhas de conscientização para o resto do corpo funcional, trabalhando em conjunto com o Encarregado de Proteção de Dados.

Métodos de treinamento e conscientização podem variar e incluem cursos de capacitação presenciais, e-learning, reuniões de equipe, boletins informativos, e-mails, pôsteres, folhetos, slogan e informações no portal eletrônico.

Os treinamentos podem ser conduzidos por representantes internos ou externos à instituição, de acordo com as diretrizes definidas pelo Comitê de Proteção de Dados Pessoais. Contudo, treinamentos podem ser necessários antes mesmo da composição do Comitê, ou na sua fase inicial de constituição, para orientá-lo em como deverá realizar suas atribuições. Neste caso, deve-se selecionar servidores com conhecimentos em Privacidade e Proteção de Dados para instruir a alta administração sobre o tema.

Uma vez composto o Comitê e a Equipe de Proteção de Dados Pessoais, treinamentos deverão ser realizados ao longo de todo o Programa de Governança em Privacidade, conforme se identifiquem necessidades de capacitação geral ou específicas.

Campanhas de conscientização deverão ser continuamente desenvolvidas pela área de Comunicação Social com apoio da Equipe de Proteção de Dados Pessoais para desenvolver a cultura da privacidade dentro da instituição.

2.2. 2 - COMPOSIÇÃO DO COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS E DA EQUIPE DE PROTEÇÃO DE DADOS PESSOAIS.

O Comitê de Proteção de Dados Pessoais reúne os principais interessados que lideram e que são responsáveis por atividades de tratamento de dados pessoais relevantes da instituição. Para sua composição, deve-se considerar representantes das unidades organizacionais que tratam dados pessoais internos e externos à instituição. O Comitê também irá propor diretrizes para as atividades a serem executadas pela Equipe de Proteção de Dados Pessoais, tais como a elaboração dos documentos de privacidade.

No contexto da Procuradoria-Geral do Estado de Rondônia, em primeira análise sobre que áreas estratégicas irão possuir representantes no comitê são:

I - Secretário(a)-Geral da Procuradoria-Geral do Estado de Rondônia;

II - Encarregado de Proteção de Dados Pessoais;

III - Diretor(a) de Tecnologia da Informação;

IV - Controlador(a) Interno(a);

V - Ouvidor(a) da Procuradoria-Geral do Estado de Rondônia;

VI - Assessor de Segurança Institucional;

VII - Coordenador do Escritório de Projetos;

VIII - 1 (um) representante designado pela da Corregedoria da Procuradoria-Geral do Estado de Rondônia;

IX - 1 (um) servidor(a) da carreira de apoio;

X - 1 (um) Procurador(a) do Estado não ocupante do cargo disposto no inciso I.

O Encarregado é figura de natureza obrigatória em instituições públicas, conforme o inciso III, do art. 23 da LGPD. Ele deve estar envolvido em todas as questões de proteção de dados pessoais da instituição e necessita ter suporte e acesso a recursos adequados para cumprir suas funções de trabalho e para manter suas habilidades e conhecimentos técnicos.

As boas práticas recomendam que o Encarregado seja independente para exercer suas atividades livre de influências internas ou externas que ponham em risco a proteção de dados pessoais. Além disso, ele deve ter uma linha de contato direta com o Comitê, acesso a todas as operações de tratamento de dados pessoais institucionais e um compromisso de sigilo e confidencialidade sobre os dados e informações acessadas.

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 servidores 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.

A LGPD estabelece que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado.

Por outro lado, observa-se que as melhores práticas internacionais indicam que o Encarregado pode assumir um papel mais central no apoio à conformidade do Controlador que ele representa, incluindo:

I) monitorar a conformidade à LGPD, incluindo o gerenciamento de atividades internas de proteção de dados

pessoais, treinamento de pessoal e realização de auditorias internas; e

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

Os demais integrantes da Equipe de Proteção de Dados Pessoais irão auxiliá-lo a realizar suas atividades, assim como outras tarefas essenciais para o correto funcionamento do Programa de Governança em Privacidade.

3. DEFINIÇÃO DA ESTRATÉGIA DE PROTEÇÃO DE DADOS PESSOAIS

O Comitê deve definir a Estratégia de Proteção de Dados Pessoais, que define a missão, visão e objetivos da instituição em relação à privacidade e à proteção de dados pessoais. Em seguida, atividades para atingir os objetivos estratégicos deverão ser listadas.

A Estratégia deve prever a(s) área(s) responsáveis pela implementação do Programa de Governança em Privacidade e definir como se dará o monitoramento do projeto de implementação. Deve, também, ser capaz de refletir quais as posições da instituição enquanto agente de tratamento de dados pessoais, ou seja, em que contextos ela é controladora de dados (LGPD, art. 5º, VI) e em que contextos ela é operadora de dados (LGPD, art. 5º, VII). Para tal, a Estratégia deverá considerar, em linhas gerais, as principais finalidades de tratamento de dados da instituição.

Além disso, a Estratégia deve contemplar o Modelo de Governança, que especifica como deveres e responsabilidades são distribuídos entre diferentes partes interessadas e explicita as regras e procedimentos para a tomada de decisões em assuntos relacionados à privacidade e proteção de dados pessoais. Cabe ao Comitê de Proteção de Dados Pessoais definir o modelo de governança a ser utilizado.

Observações importantes para a estruturação de um modelo de governança são:

a) Envolver lideranças de áreas estratégicas, que tomam decisões institucionais;

b) Envolver unidades interessadas, que lidam diretamente com dados pessoais internos e ou externos à instituição;

c) Estruturar mecanismos de comunicação e colaboração entre as partes interessadas;

Considerando a estrutura organizacional da Procuradoria-Geral do Estado, áreas cujas lideranças devem estar diretamente envolvidas com a estruturação do modelo de governança são:

I - Gabinete

II - Secretaria-Geral

III - Tecnologia da Informação

IV - Controle Interno

V - Ouvidoria

VI - Recursos Humanos

Modelos de governança podem ser centralizados (top-down), descentralizados (bottom-up) ou híbridos. Neste último, valores principiológicos são definidos pelo Comitê de Proteção de Dados Pessoais e informados às unidades, que definem seus próprios métodos de operacionalizar essas diretrizes.

No caso da PGE/RO, recomenda-se a adoção do modelo centralizado, que utiliza um mesmo conjunto de recursos para todas as unidades da organização, elaborando diretrizes e produzindo os documentos de privacidade a partir do Comitê.

4. AVALIAÇÃO DA REALIDADE ORGANIZACIONAL

A realidade organizacional é uma fotografia da situação da instituição em um determinado momento. Este diagnóstico é realizado pela Equipe de Proteção de Dados Pessoais a partir das diretrizes definidas pelo Comitê de Proteção de Dados Pessoais.

No que diz respeito à proteção de dados pessoais, isso significa identificar o escopo das operações de tratamento de dados, incluindo quais dados são tratados, como são tratados, por que são tratados, quem é responsável pelo tratamento e por quanto tempo são armazenados.

Em seguida, devem ser identificadas lacunas que serão preenchidas para garantir a correta adequação à LGPD.

Desse modo, a avaliação da realidade organizacional pode ser realizada através do mapeamento de dados pessoais e do Gap analysis.

- Que categorias de dados pessoais são tratadas?
- Qual a finalidade do tratamento?
- Qual o contexto do tratamento?
- Qual a origem e destino dos dados pessoais?
- Qual o volume de dados pessoais armazenados?
- Por quanto tempo os dados pessoais são armazenados?
- Qual o formato dos dados? Estão armazenados de forma estruturada ou não estruturada?
- Com quem os dados pessoais são compartilhados (interna e externamente)?
- Existe transferência internacional de dados?

Ferramentas comumente utilizadas para o mapeamento são planilhas, software de Governança, Risco e Conformidade (GRC) e/ou software desenvolvido internamente.

5. GAP ANALYSIS

A segunda etapa para análise da realidade organizacional é entender qual a situação do atual gerenciamento de privacidade e proteção de dados pessoais frente às legislações aplicáveis, identificando as lacunas legais.

No contexto brasileiro, a principal norma aplicável é a LGPD, porém, a depender das atividades da instituição, deve-se também considerar a aplicação de normas setoriais e de leis estrangeiras, como o regulamento europeu – RGPD. Neste documento, será dado foco apenas aos requisitos da LGPD.

Essa análise permite identificar quais lacunas existem para a correta adequação às legislações aplicáveis.

As operações de tratamento devem ser identificadas e avaliadas ao longo de toda a instituição, e uma boa prática é a realização de sessões assess-and-coach, onde, ao mesmo tempo em que riscos e deficiências são identificados, recomendações são oferecidas sobre como saná-los. De forma similar ao inventário de dados, planilhas que identificam práticas vigentes também são bastante importantes.

Algumas das perguntas que esse segundo mapeamento pode contemplar são:

- Qual a base legal para o tratamento dos dados pessoais (art. 7º da LGPD)?
- Existem dados pessoais sensíveis sendo tratados (art. 11º)? Se sim, quais as bases legais e quais as medidas de segurança para sua proteção adicional?
- Existem dados pessoais de crianças e adolescentes sendo tratados (art. 14º)? Há necessidade de consentimento parental? Quais as medidas para confirmar a obtenção desse consentimento?
- Quais os procedimentos para eliminação de dados pessoais? Quais as exceções legais aplicáveis para armazenamento de dados além do período pré- estabelecido (art. 16)?
- Quais os procedimentos que permitam aos titulares de dados serem informados e exercerem seus direitos (art. 18)?
- As regras para tratamento de dados pessoais pelo poder público são cumpridas (arts. 23 a 27)?

- Há operações de transferência internacional de dados pessoais? Se sim, para onde são enviados, quais as entidades envolvidas, qual o procedimento? Qual a base legal para a transferência internacional (art. 33)?
- Existe registro das operações de tratamento de dados pessoais? Como esse registro é atualizado (art. 37)?
- Foi realizada uma análise de riscos preliminar das operações de tratamento? Há necessidade de elaboração de um Relatório de Impacto de Proteção de Dados (art. 38)? Este relatório foi elaborado?
- Existe encarregado de proteção de dados pessoais? Quais suas competências (art. 41)?
- Quais medidas de segurança, técnicas e administrativas são adotadas para proteger os dados pessoais de acessos não autorizados e outras situações acidentais ou ilícitas - destruição, perda, alteração, comunicação, tratamento inadequado

É importante que o comitê gestor participe do procedimento de gap analysis para garantir que obrigações legais da LGPD e outras leis aplicáveis sejam cumpridas.

6. DOCUMENTOS

Além das atividades anteriormente descritas, o Programa de Governança em Privacidade também envolve a elaboração de políticas e procedimentos que garantam a correta adequação a legislações de proteção de dados pessoais, tais como a LGPD. Neste roteiro, os seguintes documentos são destacados:

I - política de privacidade, de uso interno;

II - aviso de privacidade, para usuários externos;

III - inventário de contratos, convênios e ajustes com terceiros

IV - relatório de impacto de proteção de dados - RIPD;

V - plano de resposta a incidentes.

Estes documentos devem ser produzidos pelo Encarregado de Proteção de Dados Pessoais, de acordo com as diretrizes definidas pelo Comitê de Proteção de Dados Pessoais.

Contudo, RIPDs devem refletir realidades específicas das unidades organizacionais que estejam conduzindo um processo ou projeto de tratamento de dados que justifique a elaboração deste documento.

Deste modo, um RIPD deverá ser produzido pela área técnica competente e revisado pelo Encarregado de Proteção de Dados Pessoais. Uma vez elaborados, os documentos de privacidade deverão ser submetidos para avaliação do Comitê de Proteção de Dados Pessoais.

6.1. POLÍTICA DE PRIVACIDADE

A política de privacidade é um documento interno dirigido a servidores e eventuais terceiros que forneçam produtos e serviços para a instituição (contratados). No caso da Procuradoria-Geral do Estado, isso significa tanto a equipe de servidores efetivos, comissionados e terceirizados, assim como toda e qualquer organização que venha a prestar serviços ou fornecer produtos mediante licitação ou contratação direta.

Este documento deve informar como dados pessoais serão tratados, armazenados e transmitidos para atender as necessidades organizacionais e legislações aplicáveis, definindo todos os

aspectos relativos à proteção de dados, incluindo como o aviso de privacidade será formado, se necessário, e o que ele conterá.

A política de privacidade deve ser considerada por toda a instituição – do mais alto nível de governança institucional até às equipes operacionais. Deve ser compreensível, acessível a todos os funcionários, abrangente, conciso, orientado para a prática, mensurável e testável.

Seus principais componentes são:

I - Objetivo: porque a política existe e metas a serem alcançadas;

II - Escopo: que recursos (pessoas, processos e tecnologias) a política protege;

III - Responsabilidades: quais papéis são responsáveis por quais atividades relacionadas à proteção de dados, incluindo líderes, gerentes, demais funcionários e terceiros;

IV - Conformidade: estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos complementares (ex. política de controle de acesso) e regime de sanções disciplinares por desrespeito à política de privacidade.

6.2. INVENTÁRIO DE CONTRATOS, CONVÊNIOS E AJUSTES COM TERCEIROS

O Inventário de Contratos, Convênios e Ajustes com Terceiros é um catálogo de todos os instrumentos de contrato, convênios ou ajustes diversos. Trata-se de instrumento essencial para operacionalizar a gestão e a governança das atividades de tratamento de dados pessoais, especialmente diante da necessidade de monitorar a vigência e a conformidade destes instrumentos com os termos da legislação que disciplina a questão.

Enquanto não for publicada a Política de Privacidade e Proteção de Dados, a gestão do Inventário de Contratos, Convênios e Ajustes será coordenada pelo Encarregado pelo Tratamento de Dados Pessoais, e a manutenção será de responsabilidade dos fiscais designados para cada instrumento, aos quais caberá manter atualizadas as informações pertinentes.

6.3. AVISO DE PRIVACIDADE

O aviso de privacidade é uma comunicação externa para titulares de dados que não componham a instituição, descrevendo como esta coleta usa, compartilha, retém e divulga suas informações pessoais com base na política de privacidade da organização. O seu objetivo é permitir que o indivíduo tome decisões informadas sobre o uso de seus dados pessoais pela instituição. É corriqueiro que os avisos sejam chamados de “políticas de privacidade”, pois este se tornou o termo usual para as informações disponibilizadas em portais eletrônicos de uma instituição.

No caso da Procuradoria-Geral do Estado, deve-se verificar se o aviso de privacidade será necessário, baseado nos usuários externos que se comunicam com a instituição, seja por telefone, email, website, etc.

Uma vez confirmada a sua necessidade, deve-se decidir a melhor forma de manifestar esse aviso. Uma boa prática é a implementação de notificação por camadas: uma notificação geral de quais dados estão sendo coletados e para quais finalidades e informando que maiores detalhes podem ser acessados em um local específico (como por exemplo, o website institucional). Essa notificação geral pode e deve ser informada por qualquer canal de contato (telefone, portal web, aplicativos, e-mail), nos casos em que seja relevante.

6.4. RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS

O Relatório de Impacto de Proteção de Dados - RIPD, é uma análise dos riscos à proteção de

dados associados ao tratamento de dados pessoais em relação a um determinado projeto, produto ou serviço. O RIPD também deve sugerir ou fornecer ações corretivas ou mitigações necessárias para evitar ou mitigar esses riscos.

Nem toda atividade enseja a necessidade de um RIPD e a LGPD deixou em aberto para a autoridade supervisora, a ANPD, determinar hipóteses em que este relatório seria necessário. Contudo, uma boa prática é conduzir o RIPD sempre que determinado projeto desenvolvido tenha o potencial de altos riscos para os direitos e liberdades dos indivíduos.

Conquanto acredita-se que a ANPD irá fornecer orientações para a elaboração de um RIPD, já existem diversos guias de como conduzi-lo, muitos deles produzidos por Autoridades de Proteção de Dados, tais como a Information Commissioner's Office – ICO, do Reino Unido e a francesa Commission Nationale de l'Informatique et des Libertés – CNIL.

Outra importante referência para a condução de uma RIPD é a ISO 29134. A seguir, descreve-se brevemente as etapas previstas nesta ISO:

I - Análise preliminar: conduzir uma análise preliminar de riscos, para determinar se o RIPD é

necessário. Se for concluído por existência de atividades de alto- risco, a elaboração do RIPD deve ser conduzida;

II - Preparação do RIPD: coleta de informações sobre as operações de tratamento. O inventário de dados pessoais e o gap analysis são dois procedimentos importantes nessa etapa preparatória.

III - Elaboração do RIPD: identificar o escopo do tratamento, determinar os requisitos de proteção de dados relevantes (princípios, bases legais, direitos dos titulares, transferências internacionais, etc.), acessar o risco (identificação, análise e avaliação do risco) e elaborar o plano tratamento do risco (medidas técnicas e administrativas security by design e privacy by design).

IV - Monitoramento do RIPD: preparar e publicar o relatório, implementar o plano de tratamento de risco, revisar o relatório.

6.5. PLANO DE RESPOSTA A INCIDENTES

Por mais cuidadosa que seja uma instituição, ela sempre estará sujeita a riscos inerentes à sua atividade, o que inclui riscos de vazamento de dados. A existência de um plano de respostas a incidentes (PRI) robusto é o diferencial para que a organização esteja preparada para lidar com vazamentos de dados, garantindo a proteção dos dados de titulares e evitando sanções administrativas.

O PRI deve fornecer instruções que auxiliem a identificar se um determinado incidente de segurança é também um vazamento de dados, ou seja, se o incidente detectado acarreta risco ou dano relevante aos titulares de dados. Caso positivo, as regras da LGPD se aplicarão, o que inclui obrigações de comunicação à autoridade nacional e aos titulares de dados sobre o incidente (art. 48).

Algumas das informações que um PRI deve conter são:

I - instruções para garantir o sigilo de informações sensíveis quanto ao vazamento;

II - definição de funções e responsabilidades de unidades organizacionais durante o vazamento;

III - escalonamento de possíveis problemas e relato de atividades suspeitas;

IV - classificações de gravidade de incidentes;

V - orientações para comunicações externas (por exemplo, com reguladores, fornecedores de

serviços,

seguradoras, titulares, etc).

6.6. IMPLEMENTAÇÃO DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Uma vez estruturado e aprovado o Programa de Governança em Privacidade este deve ser implementado por todas as unidades organizacionais, de acordo com as instruções estabelecidas nos documentos de privacidade. Aqui é importante que o Encarregado de Dados, conduza todos os esforços para garantir que as políticas e procedimentos estabelecidos sejam corretamente aplicados pelo resto da equipe funcional.

O gerenciamento do ciclo de vida dos dados deve possuir todos os processos, padrões e funções bem definidos e registrados. Recursos devem ser disponibilizados que garantam, entre outras atividades, o respeito aos princípios da LGPD, a confirmação das bases legais para tratamento de dados, garantia dos direitos dos titulares de dados, implementação de medidas de segurança e de procedimentos de retenção e eliminação de dados pessoais, limitações de acesso e compartilhamento, realização de tratamento de dados internacionais, gerenciamento de terceiros e notificações sobre vazamento de dados.

Dentre as atividades supramencionadas, destaca-se aqui o conceito de privacy by design, a ideia de que medidas técnicas e administrativas de privacidade e proteção de dados devem ser implementadas desde a concepção do desenvolvimento de um sistema.

Esse paradigma ressalta ao menos três valores:

a) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema;

b) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente, e;

c) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos. Alguns exemplos de medidas técnicas e organizacionais privacy by design incluem:

- uso de criptografia para proteção de bases de dados e meios de comunicação;
- minimização e pseudonimização de bases de dados;
- controle de acesso baseado em funções;
- mecanismo de respostas a requisições e reclamações dos titulares de dados;
- plano de respostas a incidentes e remediação de segurança e privacidade;
- segurança física;
- políticas de privacidade para aquisição de produtos/serviços;
- políticas de gerenciamento da segurança da informação;
- política de retenção e eliminação de dados pessoais.

Duas práticas importantes a serem implementadas são os mecanismos de respostas a requisições e reclamações dos titulares de dados e a incidentes de segurança e privacidade.

Estes mecanismos têm como objetivo respeitar os direitos dos titulares de dados previstos na LGPD e preparar-se para cenários indesejados de vazamento de dados, identificando que áreas deverão ser envolvidas para conter o dano, informar as partes interessadas relevantes (ex. ANPD e titulares de dados) e lidar com responsabilizações judiciais.

7. MÉTRICAS

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 objetivos específicos do Programa de Governança em Privacidade.

O ciclo de vida da métrica envolve a identificação da audiência a que as métricas se destinam, seleção das métricas relevantes, definição dos responsáveis por sua mensuração, coleta e análise da métrica.

Um bom Programa de Governança em Privacidade define quais métricas serão coletadas de acordo com os objetivos do Programa e a audiência destinada. Métricas comumente utilizadas são análises de comportamento estatístico, retorno de investimento (Return On Investment – ROI) e resiliência do negócio. Outra métrica recomendada é o estabelecimento de um modelo de maturidade da privacidade (Privacy Maturity Model), que permite identificar quão evoluído está o Programa de uma determinada instituição.

Outros exemplos de métricas específicas para os mais variados fins do Programa incluem:

- Número de treinamentos realizados / percentual de equipe treinada;
- Percentual de treinamentos concluídos;
- Porcentagem de conformidade de sistemas
- Número de requisições de titulares de dados;
- Número de reclamações de titulares de dados;
- Número de incidentes de segurança / vazamento de dados;
- Tempo médio entre incidentes;
- Tempo médio para recuperação;
- Porcentagem de existência de planos de resposta;

A Equipe de Proteção de Dados Pessoais, na figura do Encarregado, é responsável por reportar as métricas para o Comitê de Proteção de Dados, de modo que decisões estratégicas possam ser tomadas.

8. CONCLUSÃO

Enquanto este roteiro não aborda todas as minúcias referentes à estruturação de um Programa de Governança em Privacidade, ele fornece etapas importantes que precisam ser cumpridas para garantir que uma instituição atenda às principais obrigações da LGPD.

Com isso a Procuradoria-Geral do Estado poderá garantir a implementação de um Programa de Governança em Privacidade, em observância à norma e o respeito aos titulares de dados.