Diário Oficial do Estado de Rondônia nº 64
Disponibilização: 04/04/2025
Publicação: 04/04/2025

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

RESOLUÇÃO N. 24/2025/IPERON-DIREX

Instituir o Programa de Governança de Proteção de Dados no âmbito do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia.

O **PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA**, no uso de suas atribuições que lhe confere o Decreto de 29 de março de 2023, publicado no DOE/RO nº 59, de 29 de março de 2023;

CONSIDERANDO as atribuições definidas no artigo 94 da Lei Complementar nº 1.100, de 18/10/2021;

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 o Decreto Estadual nº 26.451, de 4 de outubro de 2021, que dispõe sobre a adoção de medidas para aplicação da Lei Federal n° 13.709 /18, em especial seu art. 6º, que remete ao inciso I do § 2° do art. 50 da Lei Federal n° 13.709, de 2018;

CONSIDERANDO a aprovação do Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados – CMSIPD (0037732207, 0052553360) e alterações;

CONSIDERANDO as deliberações contidas na na 1ª Reunião Ordinária da Diretoria Executiva do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon de 27/1/2025 (0057208533);

RESOLVE:

Art. 1º Aprovar e instituir, na forma do Anexo Único, o Programa de Governança de Proteção de Dados no âmbito do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia.

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

Porto Velho, 3 de abril de 2025.

TIAGO CORDEIRO NOGUEIRA
Presidente do Iperon

ANEXO ÚNICO

PROGRAMA DE GOVERNANÇA DE PROTEÇÃO DE DADOS

APRESENTAÇÃO

O presente documento apresenta um roteiro de atividades que devem ser realizadas para a implementação do **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). O roteiro é baseado em boas práticas em modelos corporativos de órgãos públicos e sedimentado nos requisitos mínimos previstos na lei supramencionada, leva em consideração, por óbvio, a estrutura organizacional do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia, de forma a construir uma lista de atividades que se adeque à realidade deste Instituto.

Para a realização de um Programa de Governança em Privacidade destacam-se, como essenciais, as seguintes atividades:

1. Composição do Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados Pessoais;

1.1. Comissão Tática e Operacional de Adequação à LGPD;

2. Avaliação da Realidade Organizacional, por meio de diagnóstico;

3. Definição da Estratégia de Proteção de Dados Pessoais;

4. Treinamento e Conscientização;

5. Elaboração dos Documentos de Privacidade:

5.1. Politica de privacidade;

5.2. Aviso de privacidade;

5.3. Inventário de dados pessoais;

5.4. Relatório de impacto de proteção de dados;

5.5. Plano de resposta a incidentes de segurança da informação e privacidade;

6. Implementação do Programa de Governança em Privacidade;

7. Monitoramento do Programa de Governança em Privacidade.

O presente documento apresenta o Programa de Governança em Privacidade, que deverá **ser validado** e complementado pelo **Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados.**

1. 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 amplos da organização, conforme inciso I do § 2° do art. 50 da Lei Federal n° 13.709, de 2018, deve, no mínimo:

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

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

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

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

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

f) Estar integrado à estrutura geral de governança da instituição, além de estabelecer e aplicar 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.

Consubstanciado no requerido pelo normativo acima citado as atividades consideradas essenciais para a realização de um Programa de Governança em Privacidade serão detalhados. 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.

1.1. Composição do Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados Pessoais

O Comitê de Segurança da Informação e 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 do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia, em primeira análise as áreas estratégicas irão possuir representantes no comitê, portanto será composto pelo Encarregado de Proteção de Dados, Ouvidor do Instituto, 1 (um) representante do gabinete-alta administração, 1(um) representante da Diretoria de Previdência; 1 (um) representante da Diretoria Administrativa, 1 (um) representante da Diretoria de Tecnologia. As competências voltadas para segurança da informação serão distintas daquela direcionadas para a Proteção de Dados Pessoais e Sensíveis.

O Encarregado é figura de natureza obrigatória em instituições públicas, conforme o inciso III, do art. 23 da Lei 13.709/18, regulamentado pela Resolução RESOLUÇÃO CD/ANPD Nº 18, de 16 de julho de 2024. 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.

As demais atribuições do encarregado estão regulamentadas na Resolução CD/ANPD Nº18 https://sedu.es.gov.br/Media/sedu/pdf%20e%20Arquivos/Resolu%C3%A7%C3%A3o%20CD-ANPD%20N%C2%BA%202024-18%20-%20Regulamento%20sobre%20Atua%C3%A7%C3%A3o%20do%20Encarregado.pdf. 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.

2. AVALIAÇÃO DA REALIDADE ORGANIZACIONAL

A realidade organizacional é uma fotografia da situação da instituição em um determinado momento. Este diagnóstico é realizado pela **Comissão Tática e Operacional de Adequação à LGPD,** instituída temporariamente (Portaria 290 (0019681121) e será conduzida a partir das diretrizes definidas pelo Comitê de Proteção de Dados Pessoais, Portaria 288 0019653289.

No que diz respeito à proteção de dados pessoais, isso significa identificar o escopo das operações de tratamento de dados, visando adequar o Instituto de Previdência do Estado de Rondônia à Lei Geral de Proteção de Dados Pessoais com apresentação de um **Relatório Operacional de Adequação do Instituto de Previdência do Estado de Rondônia à Lei Geral de Proteção de Dados Pessoais** Relatório 0022275933.

3. DEFINIÇÃO DA ESTRATÉGIA DE PROTEÇÃO DE DADOS PESSOAIS

A **Comissão Tática e Operacional de Adequação à LGPD** 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 seu relatório. Em seguida, atividades para atingir os objetivos estratégicos deverão ser listadas. A Estratégia deve prever a(s) área(s) ou servidores responsáveis pela implementação das atividades listadas no relatório e neste 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 Multidisciplinar de Segurança da Informação e Proteção de Dados - CMSIPD

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; e

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

Considerando a estrutura organizacional do Iperon áreas cujas lideranças devem estar diretamente envolvidas com a estruturação do modelo de governança são:

a) Gabinete;

b) Diretoria de Previdência, Diretoria Administrativa e Diretoria de Tecnologia e Informação;

c) Ouvidoria; e

d) Controle Interno.

Modelos de governança podem ser centralizados (*top-down*), descentralizados (*bottom-up*) ou híbridos. Neste último, valores principiológicos são definidos pelo Comitê Multidisciplinar de Proteção de Dados Pessoais e informados às unidades, que definem seus próprios métodos de operacionalizar essas diretrizes. No caso do Iperon, 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 Multidisciplinar de Segurança da Informação e Proteção de Dados. A exceção seria para a elaboração de Relatórios de Impacto à Proteção de Dados - RIPDs, que, devido à sua natureza, devem ser produzidos pelas áreas finalísticas a partir de diretrizes definidas pelo Comitê.

3.1. Gap AnaLysis

Uma etapa para análise da realidade Institucional 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. Neste documento, será dado foco apenas aos requisitos da LGPD. 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 e o questionário abaixo pode direcionar o mapeamento, vejamos:

a) Qual a base legal para o tratamento dos dados pessoais (art. 7º da LGPD)?

b) Existem dados pessoais sensíveis sendo tratados (art. 11º)? Se sim, quais as bases legais e quais as medidas de segurança para sua proteção adicional?

c) 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?

d) Quais os procedimentos para eliminação de dados pessoais? Quais as exceções legais aplicáveis para armazenamento de dados além do período pré- estabelecido (art. 16)?

e) Quais os procedimentos que permitam aos titulares de dados serem informados e

exercerem seus direitos (art. 18)?

f) As regras para tratamento de dados pessoais pelo Poder Público são cumpridas (arts. 23 a27)?

g) 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)?

h) Existe registro das operações de tratamento de dados pessoais? Como esse registro é atualizado (art. 37)?

i) 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?

j) Existe encarregado de proteção de dados pessoais? Quais suas competências (art. 41)?

k) 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.

4. 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 ao Iperon, enquanto conhecimentos gerais a política de privacidade deve ser comunicada a todas as equipes, algumas funções podem necessitar de capacitações específicas e mais especializadas, a saber:

a) 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;

b) 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;

c) A Ouvidoria deve ser preparada para receber solicitações e reclamações de titulares de dados, com respeito a seus direitos e eventuais vazamentos de dados; e

d) 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.

Métodos de treinamento e conscientização podem variar e incluem cursos de capacitação presenciais, reuniões de equipe, boletins informativos, e-mails, pôsteres, 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 Multidisciplinar de Segurança da Informação e Proteção de Dados. 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 Multidisciplinar de Segurança da Informação e Proteção de Dados, 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 do Comitê Multidisciplinar de segurança da Informação e Proteção de Dados Pessoais para desenvolver a cultura da privacidade dentro da instituição.

5. ELABORAÇÃO DOS DOCUMENTOS DE PRIVACIDADE

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 Lei Geral de Proteção de Dados. Neste roteiro, os seguintes documentos são destacados:

a) Política de privacidade, de uso interno;

b) Aviso de privacidade, para usuários externos;

c) Inventário de dados;

d) Relatório de impacto de proteção de dados - RIPD; e

e) Plano de resposta a incidentes.

Estes documentos em sua maioria devem ser produzidos pelo Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados, e submetido a aprovação da alta administração. Contudo, IDPs e 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, tanto o IDP quanto o RIPD deverá ser produzido pela área técnica competente e revisado pelo Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados Pessoais. Ferramentas comumente utilizadas para o mapeamento/IDP são planilhas, software de Governança, Risco e Conformidade (GRC) e/ou software desenvolvido internamente.

5.1. 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 do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia 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 as equipes operacionais. Deve ser compreensível, acessível a todos os funcionários, abrangente, conciso, orientado para a prática, mensurável e testável. Seus principais componentes são:

a) Objetivo: porque a política existe e metas a serem alcançadas;

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

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

d) 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.

5.2. 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. Mas no Iperon será disponibilizado um c*ard* no web site institucional intitulado aviso de privacidade, num ambiente que conta também com outros documentos pertinentes ou seja uma notificação geral de quais dados estão sendo coletados e para quais finalidades e informando que maiores detalhes podem ser acionadas via contato com o Instituto no endereço e contato telefónico disponibilizados na área do especifica canais de comunicação Canais de comunicação (iperon.ro.gov.br).

5.3. Inventário de Dados

O Inventário de Dados Pessoais – IDP consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (LGPD. Art. 37). De uma forma geral, esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

a) Atores envolvidos (agentes de tratamento e o encarregado);

b) Finalidade (o que a instituição faz com o dado pessoal);

c) Hipótese (arts. 7º e 11 da LGPD);

d) Previsão legal;

e) Dados pessoais tratados pela instituição;

f) Categoria dos titulares dos dados pessoais;

g) Tempo de retenção dos dados pessoais;

h) Instituições com as quais os dados pessoais são compartilhados;

i) Transferência internacional de dados (art. 33 LGPD); e

j) Medidas de segurança atualmente adotadas.

O IDP representa um documento importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD. A princípio será estruturado em planilha eletrônica disponibilizado pelo governo digital https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx e preenchida por representantes dos setores técnicos do Iperon.

5.4. 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.

A estruturação do relatório poderá seguir os requisitos mínimos previstos no parágrafo único do art.38 da Lei 13.709/2019, como também *templates* disponível pelo governo digital que teve como condução a ISO 29134.

5.5. Plano de Resposta a Incidentes

Por mais cuidadosa que seja uma instituição, ela sempre estará sujeita a riscos inerentes a 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:

a) Instruções para garantir o sigilo de informações sensíveis quanto ao vazamento;

b) Definição de funções e responsabilidades de unidades organizacionais durante o vazamento;

c) Escalonamento de possíveis problemas e relato de atividades suspeitas;

d) Classificações de gravidade de incidentes; e

e) Orientações para comunicações externas (por exemplo, com reguladores, fornecedores de serviços, seguradoras, titulares, etc).

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:

i) Uso de criptografia para proteção de bases de dados e meios de comunicação;

ii) Minimização e pseudonimização de bases de dados;

iii) Controle de acesso baseado em funções;

iv) Mecanismo de respostas a requisições e reclamações dos titulares de dados;

v) Plano de respostas a incidentes e remediação de segurança e privacidade;

vi) Segurança física;

vii) Políticas de privacidade para aquisição de produtos/serviços;

viii) Políticas de gerenciamento da segurança da informação; e

ix) 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. MONITORAMENTO

Um Programa de Governança em Privacidade não é estático. Ele deve evoluir com o tempo, acompanhando mudanças regulatórias, alterações estruturais da instituição, novos projetos que envolvam atividades de tratamento de dados, e aquisição de novas tecnologias, dentre outros. O monitoramento deve ser conduzido pelo Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados. A partir desse monitoramento, o Comitê poderá identificar lacunas e pontos de melhoria para aperfeiçoamento do Programa de Governança em Privacidade. No que diz respeito às atividades de monitoramento, cabe destacar o papel do gerenciamento de risco, das auditorias e do uso de métricas. Como o gerenciamento de riscos já foi abordado ao se comentar sobre o RIPD, destacam-se aqui os dois últimos elementos:

7.1. Auditorias

Auditorias fornecem evidências sobre se o Programa de Governança em Privacidade cumpre o que foi projetado a realizar, e se os controles estabelecidos são gerenciados corretamente. Seu escopo deve incluir todas as unidades organizacionais que tratam dados pessoais e, eventualmente, terceiros integrados às atividades da instituição. Um procedimento de auditoria inclui fases de planejamento/preparação, execução e produção do relatório. Ela pode ser conduzida internamente ou terceiros independentes.

A auditoria interna é utilizada para realizar autoavaliações do Programa de Governança em Privacidade. Ela ajuda a verificar em que estado se encontra o programa e deficiências a serem corrigidas.

No caso do Iperon, a Auditoria Interna é comandada pela Audint é a unidade mais indicada para assessorar o Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados na condução deste tipo de auditoria.

A auditoria por terceiros independentes pode ser realizada por empresas de consultoria especializadas ou, ainda, por autoridades de supervisão, como a ANPD. A depender de quem realiza a auditoria, certificações podem ser emitidas (como no caso de algumas consultorias) ou sanções administrativas podem ser aplicadas (no caso da ANPD).

7.2. 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. Exemplos de métricas específicas para os mais variados fins do Programa incluem:

a) Número de treinamentos realizados / percentual de equipe treinada;

b) Percentual de treinamentos concluídos;

c) Porcentagem de conformidade de sistemas;

d) Número de requisições de titulares de dados;

e) Número de reclamações de titulares de dados;

f) Número de incidentes de segurança / vazamento de dados;

g) Tempo médio entre incidentes;

h) Tempo médio para recuperação; e

i) Porcentagem de existência de planos de resposta;

O Comitê Multidisciplinar de Segurança da Informação e Proteção de Dados, na figura do Encarregado, é responsável por reportar as métricas para o Controlador de Proteção de Dados, de modo que decisões estratégicas possam ser tomadas.

8. CONCLUSÃO

Este roteiro aborda as principais atividades referentes à estruturação de um Programa de Governança em Privacidade, fornecendo etapas importantes que precisam ser cumpridas para garantir que uma instituição atenda às principais obrigações da LGPD. Com isso, o Instituto de Previdência dos Servidores Públicos do Estado de Rondônia poderá garantir a implementação de um Programa de Governança em Privacidade, em observância à norma e o respeito aos titulares de dados.

Documento assinado eletronicamente por **Tiago Cordeiro Nogueira**, **Presidente**, em 03/04/2025, às 11:46, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0058789179** e o código CRC **8964C61B**.

Referência: Caso responda esta Resolução, indicar expressamente o Processo nº 0016.005013/2024-81 SEI nº 0058789179