MINISTÉRIO PÚBLICO DO TRABALHO
Procuradoria Geral do Trabalho
Encarregado pelo Tratamento de Dados Pessoais
Gabinete do Procurador-Geral do Trabalho

PROGRAMA DE

GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

DO MINISTÉRIO PÚBLICO DO TRABALHO

Versão 1.0
Abril/2023

Procurador-Geral do Trabalho

José de Lima Ramos Pereira

Vice-Procuradora-Geral do Trabalho

Maria Aparecida Gurgel

Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT

José Fernando Ruiz Maturana – Procurador do Trabalho

Encarregado Adjunto pelo Tratamento de Dados Pessoais no âmbito do MPT

Diego Jimenez Gomes – Procurador do Trabalho

Equipe de Elaboração do Encarregado de Dados Pessoais no âmbito do MPT

José Fernando Ruiz Maturana – Procurador do Trabalho - Encarregado pelo Tratamento de Dados Pessoais/PGT

Diego Jimenez Gomes – Procurador do Trabalho - Encarregado Adjunto pelo Tratamento de Dados Pessoais/PGT

Tatiana Simas Stanchi – Analista do MPU/Tecnologia da Informação e Comunicação – Ofício do Encarregado pelo Tratamento de Dados Pessoais/PGT

Carlos Eduardo Correa Roque – Analista do MPU/Tecnologia da Informação e Comunicação – Seção de Segurança Institucional da Informação/PGT

Versão 1.0
Abril/2023

Histórico de Versões

Data	Versão	Descrição	Autor
26/04/2023	1.0	Primeira versão do Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT	Equipe de Elaboração

SUMÁRIO

I. Apresentação

Considerando a relevância da proteção de dados pessoais no Brasil e no mundo, como garantia ao direito fundamental à privacidade, conforme o artigo 5º da Constituição da República, nos seus incisos X e especialmente o inciso LXXIX, incluído pela Emenda Constitucional N º 115 de 10 de fevereiro de 2022, que assegura *"nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"*;

Considerando a necessidade do correto tratamento de dados pessoais no contexto da proteção, também, dos direitos fundamentais de liberdade e do livre desenvolvimento da personalidade da pessoa natural;

Considerando a necessidade de se desenvolver uma cultura de proteção de dados pessoais, inclusive nos meios digitais, no âmbito do Ministério Público do Trabalho, que englobe todas as suas atividades, tanto na área administrativa como na área finalística, e no trato das informações da sociedade em geral e do cidadão em particular;

Considerando a necessidade de instituir políticas de proteção e privacidade de dados pessoais e um programa de governança em privacidade e proteção de dados pessoais no âmbito do Ministério Público do Trabalho, com o estabelecimento de diretrizes gerais e medidas técnicas e administrativas capazes de garantir as condições necessárias para o pleno exercício das atividades da Instituição e de seus integrantes, em conformidade com a Lei nº 13.709, de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD),

O presente documento apresenta um roteiro de atividades que devem ser realizadas para a implementação do **Programa de Governança em Privacidade e Proteção de dados Pessoais do Ministério Público do Trabalho**, que em consonância com o Art. 50, § 2º, inciso I da Lei 13.709, de 14 de agosto de 2018, deve contemplar:

a) ações que demonstrem o comprometimento do Ministério Público do Trabalho 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) aplicabilidade a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

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

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

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

f) a integração e o alinhamento com a estrutura geral de governança e o estabelecimento e aplicação de mecanismos de supervisão internos e externos;

g) a elaboração de planos de resposta a incidentes e remediação;

h) a previsão e criação de mecanismos para a sua atualização constante, com base em informações obtidas a partir de monitoramento contínuo e de avaliações periódicas;

i) a implementação de mecanismos para demonstração da efetividade do programa de governança em privacidade e proteção de dados pessoais quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento da Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais).

II. Glossário

É importante entender os principais conceitos tratados no Programa de Governança em Privacidade e Proteção de Dados do MPT, seus atores, papéis e responsabilidades definidos na LGPD:

1) ANPD – Autoridade Nacional de Proteção de Dados Pessoais: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais em todo o território nacional;

2) titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, protegida pelo princípio da autodeterminação informativa (art. 2º, III). A LGPD estabelece direitos dos titulares (art.18) os quais são, em regra, exercidos em face do controlador;

3) tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art.5 º, X);

4) agentes de tratamento: controlador e operador (art. 5º, IX). Importante ressaltar que a LGPD atribui aos agentes de tratamento a responsabilidade de reparação por danos decorrentes de atos ilícitos, conforme disposto nos artigos 42 a 45;

5) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI). A ANPD destaca que são decisões essenciais do controlador: a finalidade do tratamento de dados pessoais, bem como sua respectiva base legal, a natureza dos dados tratados e a duração do tratamento. Além disso, o controlador fornece instruções aos operadores contratados para a realização de um determinado tratamento de dados pessoais (art. 5º, VII; art. 39) e deve cumprir com obrigações específicas previstas na LGPD, tais como: a de elaborar relatório de impacto à proteção de dados pessoais (art. 38), a de comprovar que o consentimento obtido do titular atende às exigências legais (art. 8º, § 2º), a de possibilitar o exercício de direitos dos titulares (art. 18) e a de comunicar à ANPD a ocorrência de incidentes de segurança (art. 48).

6) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador deve realizar o tratamento segundo as instruções fornecidas pelo controlador (art. 39). O operador pode definir elementos não essenciais do tratamento, como medidas técnicas.

7) encarregado: pessoa indicada pelo controlador para realizar as seguintes atividades (art. 41, § 2º): aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (I); receber comunicações da autoridade nacional e adotar providências (II); orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (III); e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (IV). As pessoas jurídicas de direito público que tratam dados pessoais devem indicar um encarregado (art. 23, III).

É importante observar que, embora não esteja explícito na Lei, "não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento" (ANPD, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado). Por outro lado, o servidor público que infrinja a LGPD é passível de responsabilização administrativa pessoal e autônoma, conforme o art. 28 do Decreto Lei n° 4.657, de 4 de setembro de 1942 (Lei de Introdução às normas do Direito Brasileiro). Além disso, tratar dados pessoais indevidamente, ou usar dados pessoais para fins ilegítimos pode levar à responsabilização civil e criminal do servidor público que praticou o ato ilegal.

III. Etapas e Atividades

As etapas do Programa seguem o ciclo de melhoria contínua de seus processos, para garantir a privacidade e a proteção dos dados pessoais.

A Figura 1 apresenta as três etapas desse ciclo: 1 – Preparação e Planejamento; 2 – Implementação e Execução; 3 – Monitoramento e Governança. O monitoramento pode indicar a necessidade de implementar novas ações para melhoria do programa e para mitigar riscos de privacidade e de segurança da informação, dando início a um novo ciclo.

Figura 1 – Etapas do Programa de Governança em Privacidade e Proteção de Dados Pessoais

A metodologia ágil será utilizada para implementar as ações previstas em cada etapa. Em resumo, o método ágil funciona em ciclos de implementação menores e rápidos, visando entregas funcionais. Em cada ciclo, são selecionadas as ações prioritárias que serão implementadas e entregues, em curto ou médio prazo, com acompanhamento frequente, a fim de possibilitar trocas de conhecimento e concluir o projeto com agilidade e qualidade.

Os seguintes passos podem facilitar o entendimento da metodologia ágil:

Passo 1 - Ter uma visão total do projeto;

Passo 2 - Dividir as ações;

Passo 3 - Definir prioridades;

Passo 4 - Dividir em fases;

Passo 5 - Iniciar uma fase;

Passo 6 – Revisar a fase.

O Programa será continuamente atualizado e ampliado para incluir necessidades identificadas na fase de monitoramento, para garantir o alinhamento com os objetivos estratégicos do MPT e para manter a conformidade com a legislação vigente, com as regulamentações da Autoridade Nacional de Dados Pessoais (ANPD) e com as resoluções do Conselho Nacional do Ministério Público (CNMP) e com as determinações de órgãos de controle.

O Programa de Governança em Privacidade e Proteção de Dados Pessoais deve ser amplamente divulgado a todos os integrantes do MPT, assim como todas as políticas, normas e recomendações estabelecidas para o tratamento de dados pessoais.

O Anexo I apresenta um cronograma, com o detalhamento das atividades de cada fase, as áreas responsáveis, a prioridade, a situação e o prazo de entrega de cada atividade. O cronograma permite um acompanhamento global do programa

1. Preparação e Planejamento

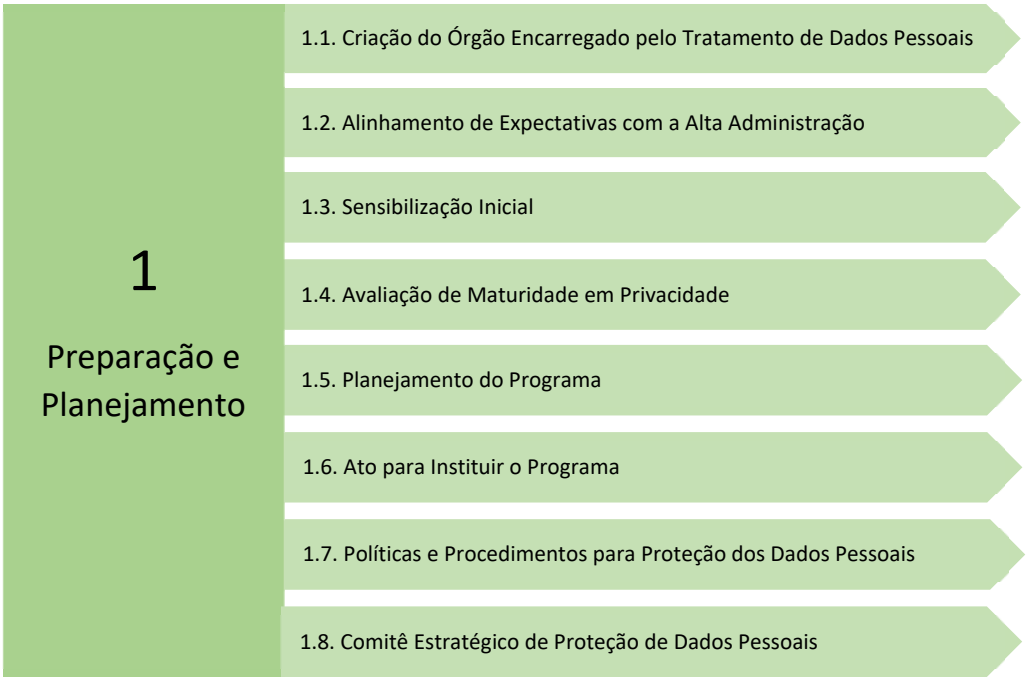

Figura 2 – Atividades da fase de Preparação e Planejamento

A Figura 2 apresenta as atividades da fase de preparação e planejamento, que se inicia com a criação da estrutura administrativa e a nomeação do Encarregado pelo tratamento de dados pessoais no âmbito da instituição. O Encarregado busca o alinhamento com as expectativas da Alta Administração e a colaboração de todos os integrantes do MPT. Nessa etapa é realizada uma avaliação da realidade organizacional, com o levantamento de informações que permitem mapear o grau de maturidade inicial do MPT em privacidade e proteção de dados pessoais.

Além disso, nessa etapa implementam-se outras providências iniciais, como a elaboração das políticas gerais norteadoras, o planejamento da implementação e a instituição formal do Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGP) e a criação de um Comitê Estratégico de Proteção de Dados Pessoais, visando a adequação institucional à Lei Geral de Proteção de Dados Pessoais - LGPD. As atividades dessa etapa estão descritas a seguir.

1.1. Criação do Órgão Encarregado pelo Tratamento de Dados Pessoais

O Procurador Geral do Trabalho deve criar na estrutura administrativa um órgão para atuação do Encarregado pelo Tratamento de Dados pessoais no MPT, com uma equipe de apoio.

Esta atividade foi implementada com a PORTARIA PGT nº 258.2022, publicada no Boletim de Serviço 040/2022, em 25 de fevereiro de 2022, que criou o órgão Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT, vinculado ao Gabinete do Procurador-Geral do Trabalho.

1.1.1. Nomeação do Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT

O Procurador Geral do Trabalho deve nomear o Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT, atendendo ao disposto no inciso III do art. 23 da LGPD.

Esta atividade foi implementada com a PORTARIA PGT nº 408.2022, publicada no Boletim de Serviço 065/2022, em 05 de abril de 2022, que designou:

- O Procurador do Trabalho JOSÉ FERNANDO RUIZ MATURANA Encarregado pelo Tratamento de Dados Pessoais no âmbito do Ministério Público do Trabalho.

- O Procurador do Trabalho DIEGO JIMENEZ GOMES Encarregado Adjunto pelo Tratamento de Dados Pessoais no âmbito do Ministério Público do Trabalho.

A Portaria PGT 404.2022 também definiu as atribuições do Encarregado:

> *"Art. 3º Além das obrigações legais e das incumbências previstas no Art. 8º-A do Regimento Interno do MPT, inserido pela Portaria PGT nº 258/2022, caberá ao Encarregado pelo Tratamento de Dados Pessoais coordenar a elaboração do Plano de Ação para implementação da Lei Geral de Proteção de Dados Pessoais – LGPD e governança em privacidade (Lei nº 13.709, de 14 de agosto de 2018), o qual será submetido ao Procurador(a)-Geral do Trabalho, para aprovação, contemplando as seguintes etapas:*
>
> *a) avaliação da realidade organizacional;*
> *b) medidas de conformação; e*
> *c) implementação e monitoramento;"*

No MPT o encarregado deve ter autonomia e a garantia da independência funcional para executar suas atribuições, realizar a avaliação das operações de tratamento de dados pessoais e propor medidas técnicas e administrativas, capacitações e treinamentos, visando um contínuo aperfeiçoamento da segurança da informação e da proteção de dados pessoais.

1.2. Alinhamento de Expectativas com a Alta Administração

O apoio da Alta Administração é fator crítico de sucesso do trabalho realizado pelo Encarregado. No MPT, o Encarregado conta com o apoio do Procurador-Geral do Trabalho, com reuniões frequentes para alinhamento de expectativas, definição de metodologia, diretrizes e ações prioritárias. E dentro da disponibilidade estrutural, com o fornecimento de recursos necessários de pessoal, treinamentos, dentre outros, para viabilizar a execução do Programa.

O alinhamento com a Alta administração e a priorização de ações guiam o estabelecimento da cultura de proteção de dados na instituição.

1.3. Sensibilização Inicial

A sensibilização inicial consiste em ações informativas e de conscientização de todas as pessoas do MPT sobre a importância da privacidade e proteção de dados pessoais, bem como sobre os papéis e as responsabilidades de cada um na adequação da instituição à Lei Geral de Proteção de Dados Pessoais.

O Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT realizou a palestra: "O Que a LGPD tem a ver comigo? A LGPD no MPT", em 18/05/2022, abordando "as peculiaridades do tratamento de dados pessoais pelo Poder Público e a necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais, trazendo a visão do MPT e a proposta de atuação."

A sensibilização também incluiu atividades de capacitação, como a Oficina LGPD que ocorreu no período de 28 a 29/09/2022, com o aprofundamento dos conceitos, a apresentação do plano de implementação e das atividades que serão inicialmente priorizadas, apresentação dos documentos elaborados pela equipe do Encarregado e que servirão de base para a implementação, além de conceitos sobre o Registro de Operações de Tratamento de Dados Pessoais com demonstração prática de um estudo de caso, conceitos iniciais de Avaliação de Risco e Relatório de Impacto e as medidas de segurança que devem ser adotadas para proteção dos dados pessoais. A oficina cumpriu o objetivo educativo e de apresentar a necessidade de apoio de todas as unidades administrativas ao Encarregado, no atendimento às solicitações de informações em relação às operações de tratamento de dados pessoais, além do amplo acesso do Encarregado à estrutura organizacional, para investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas.

1.4. Avaliação de Maturidade em Privacidade

A avaliação de maturidade tem por finalidade o levantamento inicial de informações sobre o tratamento de dados pessoais no MPT e as medidas de proteção adotadas. O levantamento consiste em: um questionário disponibilizado a todos os integrantes ativos do MPT, consultas à Secretaria Executiva de Tecnologia da Informação e Comunicação do MPT, *Gap Analysis* do MPT em Privacidade e Proteção de Dados e *Gap Analysis* de segurança da informação. A partir desse levantamento será possível determinar o grau de maturidade em privacidade que servirá de subsídio para o planejamento do Programa.

1.4.1. Questionário de mapeamento preliminar

O questionário para mapeamento de informações sobre tratamento de dados pessoais no âmbito do MPT foi disponibilizado a todas as pessoas da organização que possuem e-mails, no período de 23 de agosto a 13 de setembro de 2022, com perguntas sobre as operações de tratamento de dados pessoais: se a pessoa trata dados pessoais, quais dados são tratados, quais as categorias de titulares dos dados pessoais tratados, como o tratamento é realizado, se há compartilhamento, se houve necessidade de coleta de consentimento e como foi realizada, se a pessoa conhece a finalidade e a duração do tratamento, se são tratados dados sensíveis ou de crianças e adolescentes, onde os dados são armazenados, se a pessoa adota medidas de segurança para proteção dos dados pessoais, dentre outras perguntas relevantes.

No total, 428 pessoas responderam ao questionário de mapeamento preliminar e as respostas foram compiladas e analisadas, chegando a um diagnóstico de que são necessárias ações planejadas para difundir a cultura de privacidade, proteção de dados pessoais e segurança da informação no âmbito do MPT, possibilitando reforçar as medidas comportamentais que constituem boas práticas de proteção dos dados pessoais.

1.4.2. Consulta à Secretaria Executiva de Tecnologia da Informação e Comunicação

O Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT autuou Processo Administrativo (PGEA 20.02.0001.0005075.2022.01) em 12 de maio de 2022, para consultar a Secretaria Executiva de Tecnologia da Informação e Comunicação do MPT (SETIC) sobre a existência de um Programa de Governança em Privacidade na versão atual da Política Nacional de Segurança da Informação do MPT, bem como se são elaborados relatórios de avaliação de risco à proteção de dados pessoais, vinculados aos bancos de dados do Ministério Público do Trabalho. O levantamento teve como finalidade municiar o Encarregado de Dados para o cumprimento do dever legal de informar a autoridade nacional sempre que

demandado e de orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

A consulta à SETIC relevou que o MPT está em fase inicial de implantação de Governança em Tecnologia da Informação, com a criação de uma assessoria específica para Governança e Inovação. Também foi constatado que existe uma Política Nacional de Segurança de Tecnologia da Informação publicada pelo Comitê Estratégico de Tecnologia da Informação, na Resolução CETI nº 21, de 22 de março de 2021, que não abrange um programa de governança em privacidade nem estipula a necessidade de criação de relatórios de avaliação de risco à proteção de dados pessoais.

A Política Nacional de Segurança de Tecnologia da Informação existente possui diretrizes para a segurança da informação nos meios de tecnologia da informação e algumas diretrizes específicas para a proteção de dados pessoais, tais como:

a) o alinhamento da proteção de dados pessoais nos meios de tecnologia da informação com uma "Política Nacional de Proteção de Dados Pessoais do MPT";

b) Registros de eventos (*logs*) dos ativos que suportam serviços e sistemas de informação do MPT devem ser coletados e armazenados, com temporalidade de retenção mínima que atenda, no caso de dados pessoais, à Lei 13.709/2018 e conforme regulamentação da Autoridade Nacional de Proteção de Dados Pessoais.

c) a exigência da realização de testes e de validações necessárias para identificar, avaliar e tratar possíveis vulnerabilidades de segurança, antes de colocar em produção um sistema ou serviço;

d) a proibição da utilização de dados reais para realização de testes em sistemas e serviços sem a devida descaracterização e, para o caso de dados pessoais, sem a devida anonimização;

e) a especificação das regras para proteção de dados pessoais na contratação de serviços de nuvem, bem como a exigência de que a operadora contratada para prestação de serviços em nuvem declare explicitamente seguir a Lei 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais – LGPD e emita relatórios mensais de conformidade para verificação da segurança da informação e proteção de dados pessoais;

f) a exigência de que a localização do armazenamento dos dados em nuvem contratada esteja em um país ou respectiva unidade federativa que possua uma lei capaz de prover o mesmo nível de proteção de dados pessoais que a Lei 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais -LGPD.

O resultado da consulta foi importante para constatar a necessidade de implementação deste Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT, bem como a necessidade de realizar avaliações de risco periódicas, tanto para a elaboração do Relatório de Impacto à Proteção de Dados

Pessoais, quanto para o aprimoramento contínuo de medidas, salvaguardas e mecanismos de mitigação de risco de segurança e de privacidade.

1.4.3. *Gap Analysis* de conformidade do MPT com a LGPD

O *Gap Analysis* (análise de lacunas) de conformidade com a LGPD, conforme ilustrado na Figura 3 é uma análise dos requisitos de obrigações de conformidade, baseada num modelo de maturidade, na qual se identifica a situação atual de uma organização e as lacunas existentes, que devem ser tratadas para alcançar um nível desejado de maturidade em privacidade e proteção de dados.

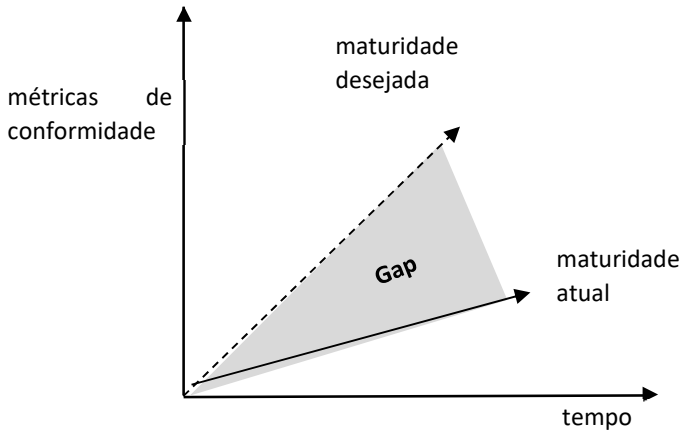

Figura 3 – Gap Analysis de conformidade com a LGPD

Conforme registrado no PGEA 20.02.0001.0008170/2022-88, no ano de 2020 o Tribunal de Contas da União (TCU) encaminhou questionário a todos os Órgãos federais, para realização de *Gap Analysis* de conformidade às disposições da LGPD, cujas respostas foram registradas no processo TC 039.606/2020-1. Em 2022, o TCU expediu ofício (Doc. 031763.2022) que notificou o MPT a respeito da decisão contida no Acórdão 1384/2022-TCU - Plenário, que apreciou o processo TC 039.606/2020-1 com recomendações no que tange à gestão, classificação e proteção de dados e informações baseadas na Lei n.º 13.709/2018.

As respostas do MPT e as recomendações do TCU serviram de subsídio ao Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT para identificar as lacunas existentes, priorizar ações imediatas de conformidade e determinar a elaboração do Programa de Governança em Privacidade e Proteção de Dados Pessoais.

Na auditoria inicial do TCU, em abril de 2021, o MPT foi classificado no nível inicial de maturidade em LGPD. Em março de 2023, a equipe do Encarregado repetiu o questionário e, em razão das atividades já implementadas, o MPT alcançou o nível intermediário de maturidade em LGPD.

1.4.4. *Gap Analysis* das medidas de segurança para proteção de dados pessoais

O *Gap Analysis* (análise de lacunas) de segurança da informação é um levantamento do estado atual de implementação das salvaguardas necessárias para proteção de dados pessoais nos sistemas do MPT e a identificação das lacunas existentes, que devem ser tratadas para atender a um conjunto de requisitos de segurança e proteção de dados pessoais definidos com base nas boas práticas recomendadas na LGPD e nas famílias de normas ABNT NBR ISO/IEC 27000 e 29100.

A equipe do Encarregado disponibilizou (através do PGEA 20.02.0001.0012076.2022-65) aos gestores dos sistemas corporativos do MPT uma planilha para o levantamento da situação de implementação dos controles de segurança recomendados para proteção de dados pessoais. Esse levantamento servirá de base para a priorização das medidas de segurança cuja implementação será sugerida, a partir de uma análise de riscos dos processos de tratamento de dados pessoais.

1.5. Planejamento do Programa

O diagnóstico da maturidade do MPT em privacidade revelou a necessidade de elaboração de um plano de implementação do Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT. É importante destacar a necessidade de que o plano de implementação tenha a flexibilidade necessária para que seja revisado e adaptado aos novos contextos, expectativas e necessidades que certamente irão se revelar ao longo da implementação.

1.6. Ato para Instituir o Programa

O Plano de implementação do Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT (PGP) deve ser submetido ao Procurador-Geral do Trabalho e, quando aprovado o plano, o Programa deverá ser instituído em ato formal, com a definição de papéis e responsabilidades.

Os principais atores do Programa são definidos a seguir.

1.6.1. Encarregado

O Encarregado tem a responsabilidade de planejar, orientar e acompanhar a execução das atividades previstas nas etapas de preparação, implementação e monitoramento do Programa de Governança em Privacidade e Proteção de Dados Pessoais.

1.6.2. Controlador

O controlador, através das chefias e servidores das unidades administrativas do MPT, tem a responsabilidade de preparar, implementar e monitorar o Programa de Governança em Privacidade e Proteção de Dados Pessoais. O Encarregado, quando julgar oportuno, poderá sugerir ao Controlador a criação de comitê, comissões ou grupos de trabalho, para atuação no Programa de Privacidade.

1.6.3. Chefias das unidades administrativas e gestores de sistemas

A participação colaborativa das chefias das unidades administrativas e dos gestores de sistemas do MPT é de extrema importância para o sucesso do Programa. Eles precisam fornecer tempestivamente as informações solicitadas pelo Encarregado sobre o tratamento de dados pessoais, e devem executar, no prazo estipulado, as atividades de implementação e de monitoramento do Programa, de acordo com as priorizações e as orientações do Encarregado.

1.6.4. Todas as pessoas integrantes do MPT

Todas as pessoas integrantes do MPT devem conhecer e realizar o tratamento de dados pessoais em conformidade com a Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e o Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT, suas políticas, normas e recomendações de boas práticas.

1.7. Políticas para Proteção dos Dados Pessoais

Uma política é um tipo de controle administrativo a ser aplicado em um programa de privacidade. E um controle é uma medida que mantém e/ou modifica um risco (ABNT NBR ISO/IEC 27002:2022, 3.1.8).

Conforme a ABNT NBR ISO/IEC 27001:2013, seção 5.2, complementada pela ABNT NBR ISO/IEC 27701:2019, seção 5.1, a Alta Direção deve *estabelecer política de segurança da informação e de privacidade que: seja apropriada ao propósito da organização; inclua os objetivos de segurança da informação e privacidade ou forneça a estrutura para estabelecer os objetivos de segurança da informação e privacidade; inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação e privacidade; e inclua o comprometimento com a melhoria contínua do programa de privacidade.*

Portanto, é de extrema importância que o Procurador-Geral do Trabalho estabeleça políticas para proteção de dados pessoais e para a segurança da informação. A elaboração dessas políticas deve considerar, além das recomendações supracitadas: a estratégia e os requisitos dos processos de negócio do MPT; a legislação, regulamentações e contratos; os riscos e ameaças atuais e projetados para a privacidade e a segurança da informação.

As políticas gerais não devem tentar abarcar todos os temas desses assuntos. O ideal é a existência de uma política específica por tema (*intenções e diretrizes sobre um assunto ou tema específico, como formalmente expressos pelo nível apropriado de gestão* – ABNT NBR ISO/IEC 27002:2022, 3.1.35). As políticas por tema devem ser alinhadas e complementares às políticas gerais.

Convém que a escolha das políticas por temas que serão estabelecidas considere: o contexto do tratamento de dados pessoais no MPT; os riscos identificados e a necessidade de estabelecer controles para determinadas áreas de segurança e privacidade; além das necessidades de áreas específicas da organização.

São exemplos de políticas por tema (que não se esgotam nesta listagem):

a) política de controle de acesso lógico, contemplando a política de usuários, senhas e métodos de autenticação, que foi estabelecida pela Resolução CETI nº 22, publicada em 13 de dezembro de 2022;

b) política de proteção de dados em teletrabalho;

c) política de proteção de dados em equipamentos móveis;

d) política de proteção de dados em mídias removíveis;

e) política para uso adequado da internet e do e-mail institucional, contemplada na Resolução CETI nº 21/2022, em 22 de março de 2021;

f) política de segurança e proteção de dados pessoais em serviços de nuvem;

g) política de segurança da informação na rede;

h) política para cópias de segurança (*backups)*;

i) política para testes de segurança em serviços e sistemas;

j) política de controle de acesso às áreas físicas;

k) política para transferência segura, descarte seguro ou anonimização de dados pessoais após o final do tratamento;

l) política para proteção de dados pessoais em imagens CFTV, dentre outras.

As fontes de referência para a elaboração dessas políticas são: a própria LGPD, os guias e recomendações da ANPD, os guias e boas práticas do Governo Federal e as boas práticas recomendadas na coleção de normas ABNT NBR ISSO/IEC.

Além das políticas por tema, é importante que cada área da instituição estabeleça os procedimentos de como realizar as ações necessárias para que os objetivos definidos nas políticas sejam alcançados.

As políticas e procedimentos devem ser amplamente comunicados no âmbito do MPT, estando disponíveis para as partes interessadas como uma informação documentada e de fácil acesso.

1.7.1. Política Nacional de Proteção de Dados Pessoais

O Encarregado pelo Tratamento de Dados Pessoais no âmbito do MPT encaminhou ao Procurador-Geral uma minuta de Política de Proteção de Dados Pessoais no MPT, compatível com os requisitos da legislação brasileira e das boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção, com base em riscos identificados, para os dados pessoais tratados pela instituição, no intuito maior de proteger os direitos fundamentais de liberdade, de privacidade e de proteção dos dados pessoais e o livre desenvolvimento da personalidade da pessoa natural.

A Portaria PGT nº 204/2023, publicada no Boletim de Serviço nº 043/2023, em 03 de março de 2023, instituiu a Política de Proteção de Dados Pessoais no MPT. Esta Portaria está divulgada no Portal do MPT.

1.7.2. Políticas de Segurança da Informação

O diagnóstico de maturidade do MPT revelou que existe uma Política Nacional de Segurança de TI e uma norma de uso de recursos de TI, que definem diretrizes e estabelecem controles importantes relacionados à informação no sentido *lato*, e com diretrizes para alguns controles gerais de proteção de dados pessoais, mas que carecem de uma revisão pormenorizada quanto aos controles específicos de proteção de dados pessoais.

Além disso, a política existente se restringe à proteção lógica das informações nos meios digitais de TI, ou seja, são necessárias políticas para: a segurança da informação na documentação em meios físicos; a segurança física das áreas e das instalações; e a segurança da informação de pessoas, que visa adequar o aspecto comportamental.

Assim, é importante recomendar:

a) ao Comitê Estratégico de Tecnologia da Informação a revisão da Política de Segurança de Tecnologia da Informação, para inclusão de todos os controles necessários para garantir a proteção de dados pessoais;

b) ao Comitê Estratégico de Segurança Institucional, em conjunto com a Comissão Permanente de Gestão Documental (CPGD), a elaboração de uma Política de Segurança da Informação que contemple: a segurança da informação nas áreas e instalações; a segurança da informação na documentação em meios físicos e a segurança da informação de pessoas;

1.7.3. Norma de classificação da informação

O Encarregado deve recomendar ao controlador o encaminhamento da Portaria MPT nº 438, de 21 de julho de 2014, que dispõe sobre a classificação, o tratamento e a gestão da informação sigilosa e da informação pessoal contida na documentação, em qualquer suporte, do Ministério Público do Trabalho – MPT, à Comissão Permanente de Gestão Documental, para revisão, com a colaboração do Departamento de Documentação e Gestão da Informação, visando a conformidade com a LGPD. A norma deve incluir a classificação dos dados pessoais tratados no âmbito do MPT e definir os graus de sigilo adequados a cada classificação.

1.8. Comitê Estratégico de Proteção de Dados Pessoais

A Portaria nº 204/2023, que instituiu a Política de Proteção de Dados Pessoais do MPT, também criou o Comitê Estratégico de Proteção de Dados Pessoais (CEPDP), vinculado ao Comitê de Planejamento e Gestão Estratégica – CPGE, como instância consultiva, propositiva e deliberativa pertinente ao programa, às políticas, às diretrizes, ao planejamento e às ações de governança corporativa em privacidade e proteção de dados pessoais, órgão colegiado de natureza permanente, subordinado ao Procurador Geral do Trabalho. Na política estão especificadas as atribuições e a composição do CEPDP.

2. Implementação e Execução

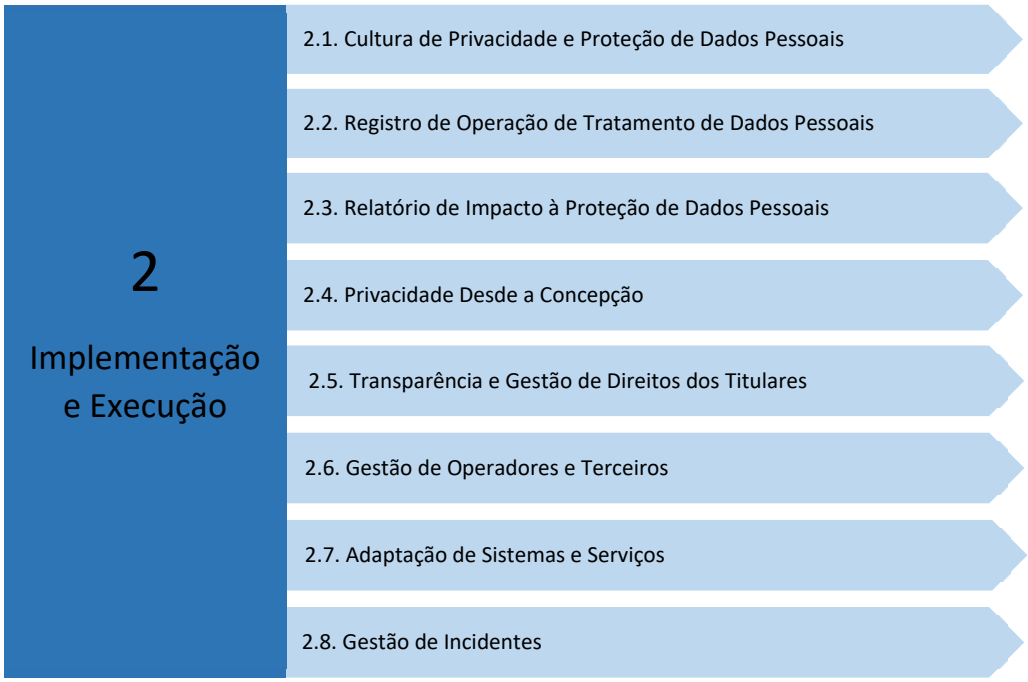

Figura 4 – Atividades da fase de Implementação e Execução

A implementação do Programa congrega diversas disciplinas, apresentadas na Figura 4, numa abordagem estruturada. Para cada disciplina, é definido um conjunto de ações a serem implementadas para que o MPT atenda aos requisitos de conformidade legal e às expectativas das partes interessadas, reduzindo o risco de violação de dados pessoais.

2.1. Cultura de Privacidade e Proteção de Dados Pessoais

A Alta Administração deve promover uma cultura de privacidade e proteção de dados pessoais no MPT, com o intuito de comunicar os objetivos, metas e indicadores utilizados no Programa, além de divulgar o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. A difusão de uma cultura de privacidade requer atividades de divulgação, conscientização e de capacitação.

2.1.1. Estratégia de divulgação do Programa de Governança em Privacidade e Proteção de Dados Pessoais

O CEPDP em conjunto com a Secretaria de Comunicação Social do MPT (SECOM) deve propor uma abordagem estratégica para comunicar e obter a adesão de toda instituição para o Programa. Essa estratégia deve considerar a necessidade de mudar a mentalidade e a perspectiva das pessoas integrantes do MPT no que se refere ao tratamento de dados pessoais. É preciso consolidar a ideia de que todos no MPT, em todos os níveis hierárquicos, cargos e funções, têm um papel a desempenhar na proteção dos dados pessoais que o MPT coleta, usa, compartilha e divulga. Todos devem entender essa responsabilidade e empregar práticas fundamentais necessárias para proteger os dados pessoais.

A partir dessa estratégia, o Encarregado deve acompanhar e orientar a SECOM na elaboração de um planejamento mais detalhado das ações de divulgação que serão implementadas, constando o objetivo da ação, os meios de comunicação adotados e o público-alvo.

2.1.2. Página do Programa de Governança em Privacidade e Proteção de Dados Pessoais

Uma ação importante é a criação na Intranet da página do Programa. Nessa página podem ser divulgados: políticas, procedimentos, resoluções do Comitê Estratégico de Proteção de Dados Pessoais, as ações

implementadas, os relatórios de governança do programa, conteúdos informativos e técnicos sobre temas relacionados à privacidade e proteção de dados pessoais.

Visando garantir o princípio da transparência, é recomendável que seja disponibilizado um extrato desse programa no portal do MPT.

2.1.3. Plano de Capacitação

O CEPDP, em conjunto com a Secretaria de Treinamento e Formação Continuada, ouvindo as áreas interessadas, deve propor um plano de capacitação em privacidade, proteção de dados pessoais e segurança da informação, abrangendo treinamentos gerais para todos os integrantes do MPT, assim como treinamentos específicos, conforme a necessidade de aprofundamento, para a preparação das equipes de implementação do Programa, em consonância com o cronograma das ações priorizadas.

Uma atenção especial deve ser dada à capacitação e difusão de uma cultura de privacidade desde a concepção (*privacy by design*) e por padrão (*privacy by default*). Todas as equipes envolvidas com projetos, sistemas, processos de negócio e serviços devem ser capacitadas nesses temas.

2.2. Registro de Operação de Tratamento de Dados Pessoais

De acordo com o art. 37 da LGPD, de maneira geral, compete à Instituição manter o registro de todo o tratamento de dados pessoais. O Registro Geral de Operação de Tratamento de Dados Pessoais (ROTDP) tem como objetivo mapear todos os processos que realizam operações de tratamento de dados pessoais no MPT, levantando informações que vão além de uma simples enumeração dos dados pessoais tratados, permitindo compreender a atividade de tratamento como um todo, ou seja, o contexto, a natureza, o escopo, a finalidade, o fluxo do tratamento durante todo o ciclo de vida do dado pessoal e o grau de adesão aos princípios e exigências da legislação.

O ROTDP é uma demonstração do compromisso do MPT em se adequar às exigências da LGPD. Além disso, o mapeamento serve de subsídio para a elaboração do aviso de privacidade, para realização de avaliação de risco de privacidade e para a elaboração do relatório de impacto.

O ROTDP deve ser parte de um processo de ponta a ponta, desde a definição dos requisitos de dados até a manutenção pós-produção. Assim, sempre que um processo sofrer alteração, o ROTDP deve ser revisado.

Cabe ao Encarregado propor um modelo de formulário com as informações que devem constar no ROTDP. Essas informações devem ser coletadas e registradas de forma estruturada, em planilhas ou, preferencialmente, numa base de dados que permita gerenciá-las de forma facilitada e que possibilite a extração de relatórios gerenciais, resultantes da compilação de todos os tratamentos realizados no MPT, para apoiar as tomadas de decisões.

A execução do ROTDP é descentralizada, nas unidades administrativas do MPT, conforme o planejamento e a orientação do Encarregado, além das assessorias técnicas: da Comissão Permanente de Gestão Documental para análise e compilação dos dados coletados; da SSI e da SETIC para análise de assuntos pertinentes à segurança da informação e dos meios tecnológicos.

Considerando a amplitude da atuação do MPT, o Encarregado deve traçar um cronograma de execução do ROTDP, iniciando por áreas que coletam e compartilham dados pessoais com outras áreas, como o Departamento de Gestão de Pessoal, e áreas que tratam dados sensíveis e demandam atenção imediata, como a área médica.

O ROTDP relativo aos dados pessoais do plano de saúde, que estão sob custódia do MPT e são tratados no sistema MPT COSMOS Plan-Assiste, já foi realizado. Com a unificação do Plan-Assiste de todos os ramos do MPU, a contar de 05/01/2023, toda a estrutura do Plan-Assiste da Procuradoria Geral do Trabalho foi transferida para a Procuradoria Geral da República. Assim, o MPT permanece como controlador apenas dos dados legados, enquanto houver necessidade de guarda, com a responsabilidade de adotar as medidas de proteção necessárias e a destinação adequada desses dados, conforme prazos e destinação final estabelecidos na Tabela de Temporalidade e Destinação de Documentos - Atividade Meio do MPT.

2.3. Relatório de Impacto à Proteção de Dados Pessoais

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPDP) está descrito no art. 5º, XVII, da LGPD, como *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*.

O Encarregado deve definir um modelo de relatório de impacto, considerando o disposto no parágrafo único do art. 38 da LGPD: *o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.*

Adicionalmente, o Encarregado deve estabelecer critérios objetivos para avaliar se um determinado processo de tratamento de dados pessoais requer a elaboração do relatório de impacto, levando em consideração as boas práticas e as recomendações da ANPD.

Na alínea d) do inciso I do art. 50, a LGPD determina que o programa de governança em privacidade e proteção de dados pessoais deve estabelecer *políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade*. Assim, a elaboração do relatório de impacto pressupõe a avaliação de impactos e riscos à privacidade.

2.3.1. Avaliação de impactos e riscos à privacidade

Em consonância com a LGPD, o Programa de Governança em Privacidade e Proteção de Dados Pessoais do MPT considera que as medidas de proteção de dados pessoais têm como objetivo a garantia dos direitos dos titulares de dados pessoais à liberdade, à privacidade, à proteção de dados pessoais, à autodeterminação informativa e ao livre desenvolvimento.

Assim, a metodologia de avaliação de impactos e riscos à privacidade deve considerar a probabilidade de concretização de um risco e as consequências para os titulares de dados pessoais.

As práticas de segurança da informação são fundamentais para a proteção de dados pessoais e o art. 37 da LGPD define que é obrigação dos agentes de tratamento garantir a segurança da informação, mesmo após o seu término.

A segurança da informação tem como objetivo a aplicação de medidas e salvaguardas durante todo o ciclo de vida dos dados, para garantir confidencialidade, integridade, disponibilidade e autenticidade, além de definir papeis e responsabilidades. Falhas na segurança podem levar a um vazamento de dados pessoais, a acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação.

Portanto, o escopo da avaliação de impactos e riscos à privacidade deve considerar os riscos à segurança da informação, que também são riscos aos dados pessoais. Porém, diferente de uma avaliação tradicional de riscos à segurança, que considera os impactos aos ativos de informação, a metodologia adotada neste Programa deve manter o foco principal nos impactos de privacidade para os titulares dos dados pessoais, devendo também avaliar os impactos para o MPT.

Vale ressaltar que não basta garantir a segurança da informação para assegurar a privacidade. Existem riscos à privacidade que não são decorrentes de lacunas na segurança da informação, mas de falhas no processo de tratamento de dados pessoais. Por isso, é importante entender o processo de tratamento de ponta a ponta, mediante o ROTDP, e ampliar o escopo da avaliação para considerar todos os riscos à privacidade decorrentes do processo de tratamento.

Assim, o Programa do MPT adota uma metodologia de avaliação de impactos e riscos à privacidade baseada nas normas ABNT NBR ISSO/IEC 31000:2018 (gestão de riscos – diretrizes), 27005:2019 (gestão de riscos de segurança da informação) e 29134:2020 (avaliação de impacto de privacidade). A metodologia engloba e valoriza a segurança da informação, mas não se resume ao tratamento de riscos

à segurança. O escopo é ampliado para avaliação de impactos e riscos à privacidade, com a adoção de medidas para garantir a concretização plena dos direitos fundamentais dos titulares de dados.

A ABNT NBR ISSO/IEC 29134:2020 define uma avaliação de impacto de privacidade como *um instrumento para avaliar os potenciais impactos de privacidade de um processo, sistema de informação, programa, módulo de software, ou outra iniciativa que trate dados pessoais e, em consulta às partes interessadas, tomar ações necessárias para tratar risco à privacidade.*

E na sua seção 3.7 define que uma análise de impacto de privacidade é *um processo geral de identificação, análise, avaliação, consultoria, comunicação e planejamento do tratamento de potenciais impactos à privacidade com relação ao tratamento de dados pessoais, contida numa estrutura mais ampla de gestão de riscos da organização.*

Isso posto, o Encarregado tem a responsabilidade de propor uma metodologia para avaliação de riscos à privacidade, detalhando as ameaças à privacidade e vulnerabilidades que provém da segurança da informação e aquelas inerentes ao processo de tratamento de dados pessoais, considerando os possíveis impactos aos titulares e ao MPT.

A execução da avaliação de impactos e riscos à privacidade deve ser descentralizada nas unidades administrativas, sob a orientação do Encarregado.

2.4. Privacidade Desde a Concepção

A privacidade desde a concepção está prevista no art. 46 da LGPD:

> *Art. 46 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.*
>
> *(...)*
>
> *§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.*

Privacidade desde a concepção (*privacy by design*) é uma metodologia criada nos anos 90 por Ann Cavoukian, comissária de informação e privacidade de Ontário – Canadá, que é adotada para garantir a privacidade do titular e a proteção dos dados pessoais tratados desde a concepção de qualquer sistema, serviço ou processo de negócio. Assim, desde a fase inicial de um projeto, os requisitos de segurança da

informação e de proteção de dados pessoais devem ser considerados e incorporados à arquitetura e ao design de processos/sistemas/serviços.

A privacidade desde a concepção vai além da conformidade com leis e regulamentos. Ela é uma cultura e deve se tornar a forma padrão de funcionamento da instituição no que se refere ao tratamento de dados pessoais. Para isso, a privacidade desde a concepção deve ser uma diretriz estabelecida nas políticas de proteção de dados pessoais e de segurança da informação do MPT. Adicionalmente, a capacitação em privacidade desde a concepção deve ser priorizada, conforme descrito no item 2.1.3.

2.4.1. Princípios da privacidade desde a concepção

Os objetivos da privacidade desde a concepção podem ser alcançados observando-se os sete princípios fundamentais:

2.4.1.1. Proativo não reativo; preventivo não corretivo

A abordagem da metodologia é caracterizada pela adoção de medidas proativas e não reativas: antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. O objetivo é aplicar controles para minimizar riscos, evitando tanto a ocorrência de incidentes, quanto os impactos e danos para o titular dos dados e para a organização.

2.4.1.2. Privacidade como configuração padrão (*privacy by default*)

A privacidade e a proteção de dados pessoais estão incorporadas aos processos/sistemas/serviços por padrão, assegurando o grau máximo de privacidade ao titular e garantindo que os dados pessoais sejam protegidos automaticamente, sem a necessidade de intervenção ou solicitação do titular.

2.4.1.3. Privacidade embarcada no design

A privacidade deve estar incorporada no design e na arquitetura dos sistemas e processos de negócio, e não adicionada como complemento. Assim, a privacidade é um componente essencial na funcionalidade entregue, ou seja, torna-se parte dos sistemas/processos/serviços, sem diminuir sua funcionalidade.

2.4.1.4. Funcionalidade integral

A metodologia acomoda todos os interesses e objetivos legítimos numa soma positiva de “ganha-ganha”, considerando que os objetivos de privacidade, de segurança e das funcionalidades do processo/sistema/serviço não se contrapõem nem concorrem. Ao incorporar a privacidade em uma

determinada tecnologia, processo ou sistema, isso deve ser feito de forma que a funcionalidade total não seja prejudicada e, na medida do possível, que todos os requisitos sejam otimizados.

2.4.1.5. Segurança de ponta a ponta: proteção durante todo o ciclo de vida da informação

As medidas para garantir segurança e privacidade devem ser aplicadas em todas as operações de tratamento de dados pessoais, durante todo o ciclo de vida da informação, desde a coleta até o descarte definitivo.

2.4.1.6. Visibilidade e transparência

A metodologia considera que visibilidade e transparência são essenciais para estabelecer responsabilidade e promover a confiança do titular de dados pessoais, assegurando a todos os interessados que, seja qual for a tecnologia envolvida e o processo de negócio, as operações de tratamento de dados pessoais estão, de fato, sendo realizadas de acordo com os requisitos de segurança e objetivos de proteção declarados, sujeitos à verificação independente. Assim, os titulares devem ser informados sobre a finalidade e demais características do tratamento, e sobre as políticas e práticas de proteção adotadas.

2.4.1.7. Respeito à privacidade do usuário

Os interesses e necessidades dos titulares devem ser priorizados por todos da organização, oferecendo medidas como fortes padrões de proteção de dados, aviso de privacidade apropriado e interface amigável para o titular exercer o direito de gerir seus próprios dados.

2.4.2. Implementação da privacidade desde a concepção

Além de diretrizes para adotar privacidade desde a concepção nas políticas, são necessárias ações concretas de implementação. O Encarregado deve trabalhar em conjunto com as áreas de gerenciamento de processos, segurança institucional, gestão de documentos e de tecnologia da informação para a construção de um *framework* orientativo e o detalhamento das medidas e ações a serem adotadas, pois o conceito perpassa três grandes áreas: as práticas responsáveis de tratamento de dados pessoais nos processos de negócio, os sistemas de tecnologia da informação, o projeto físico e a infraestrutura de redes.

O *framework* de implementação de privacidade desde a concepção deve considerar as recomendações das normas ABNT NBR ISSO/IEC 27701:2019 e ABNT NBR ISSO/IEC 29151:2020, sobre os controles que

devem ser implementados para proteção de dados pessoais, além da avaliação de riscos à privacidade. Vale destacar alguns exemplos:

a) Indicação de limitação de coleta;

b) Limitação de uso, retenção e divulgação;

c) Definição de precisão e qualidade dos dados;

d) Minimização de dados pessoais tratados;

e) Definição de métodos para anonimização, retorno, transferência e/ou descarte seguro dos dados ao final do tratamento;

f) Atenção ao descarte seguro de arquivos temporários;

g) Definição clara de prazo de retenção;

h) Existência de política e procedimentos para descarte seguro de dados;

i) Controles para a transmissão segura de dados pessoais;

j) Registro de transferência e de divulgação de dados pessoais para terceiros.

2.5. Transparência e Gestão de Direitos dos Titulares

2.5.2. Canal para o exercício de direitos do titular de dados pessoais

O controlador deve disponibilizar um canal acessível para o exercício de direitos dos titulares de dados pessoais, que estão previstos no art. 18 da LGPD, em conformidade com o princípio do livre acesso (LGPD, art. 6º, IV), que garante aos titulares de dados pessoais *consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais*. No MPT, esse canal é um formulário disponibilizado na página da Ouvidoria e na Página sobre LGPD.

Todos os integrantes do MPT devem ser informados sobre o canal para exercício de direitos do titular e preparados para orientar o titular a usá-lo. Todos os contatos realizados por titulares devem ser encaminhados para esse canal. O link do canal deve constar em todos os avisos de privacidade divulgados nas páginas, sistemas e serviços do MPT disponibilizados na internet e na intranet.

Todo requerimento de titular deve ser respondido, independentemente da pertinência. Além disso, em razão da necessidade de cumprimento de obrigação legal ou regulatória do MPT, alguns direitos do titular previstos na LGPD poderão não ser concretizados. Caso o MPT não possa atender a um requerimento,

uma resposta deve ser enviada, informando o motivo de forma clara e objetiva. Deve-se tomar cuidado especial para que as respostas a um requerimento não contenham dados de outros titulares, por exemplo, uma atenção específica deve ser dada às imagens de CFTV, que podem conter imagens de outros titulares.

O Encarregado deve definir um processo para responder às solicitações dos titulares. O processo deve mapear o fluxo de informações e as providências a serem adotadas desde a chegada de um requerimento até o envio da resposta, definindo papéis e responsabilidades. O processo deve conter mecanismos de rastreamento para assegurar que todas as solicitações recebidas sejam analisadas e adequadamente respondidas em tempo hábil, conforme prazo regulamentado pela ANPD (15 dias após o recebimento) ou prazos estabelecidos nas legislações específicas, aplicadas ao Poder Público (LGPD, art. 23, § 3º). O processo também deve prever que o Encarregado poderá solicitar informações a todas as áreas que tratam dados pessoais e que as chefias têm a responsabilidade de responder dentro do prazo estipulado pelo Encarregado, possibilitando o envio tempestivo da resposta.

O Encarregado deve recomendar que gestores de processos/sistemas/serviços se responsabilizem pela implementação dos procedimentos para a resposta a todos os tipos de requerimentos dos titulares que se aplicarem à operação de tratamento realizada.

Em cumprimento ao disposto na LGPD (art. 18, § 6º), o MPT deve fornecer aos operadores ou terceiros com os quais compartilha o uso de dados pessoais qualquer alteração, correção, anonimização ou remoção de dados pessoais decorrentes do exercício de direitos do titular, para que repitam procedimento idêntico. Por outro lado, os operadores e terceiros devem colaborar com o MPT, fornecendo as informações necessárias para facilitar o exercício de direito do titular.

2.5.2.1. Autenticação do Titular

O canal para exercício de direito dos titulares deve ter um procedimento de autenticação do titular, que observe a proporcionalidade entre o requerimento, os dados tratados e os dados solicitados para a autenticação.

A coleta de dados para a autenticação deve se limitar ao mínimo de informações necessárias para assegurar a identificação correta do titular. Além disso, os dados coletados devem ser protegidos e convém que somente sejam retidos pelo tempo necessário ao cumprimento da finalidade.

2.5.2 – Aviso de Privacidade

O princípio da transparência da LGPD (art. 6º, VI) garante ao titular de dados pessoais "*informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento*", independentemente de requisição do titular.

Já a norma ABNT NBR ISSO/IEC 29100:2020 define aviso como *informações sobre o tratamento de dados pessoais apresentadas aos titulares por meio de diferentes canais, de forma concisa, transparente, inteligível e facilmente acessível, utilizando linguagem clara e simples*.

Por isso, o MPT deve divulgar avisos de privacidade para os titulares de dados pessoais em suas páginas principais da internet e da intranet, nas páginas dos sistemas e serviços do MPT e em locais onde sejam facilmente reconhecidos pelos titulares quando a coleta de dados pessoais não é realizada on-line, como é o caso das recepções das sedes, que coletam dados pessoais para o controle do acesso físico de pessoas.

O aviso deve ser exibido antes da coleta (e do consentimento, se aplicável), da utilização de dado coletado para finalidade diversa e da realização da coleta de novos dados.

A linguagem utilizada no aviso de privacidade deve ser de fácil compreensão para uma pessoa sem formação jurídica ou técnica. Além disso devem ser utilizadas técnicas para acessibilidade, para garantir a conformidade do aviso com o Estatuto da Pessoa com Deficiência (Lei 13.146/2015, Art. 63).

O art. 9º da LGPD delimita as informações que devem ser disponibilizadas aos titulares:

a) forma, duração e finalidade específica do tratamento;

b) se os dados são utilizados para a tomada automatizada de decisão;

c) se algum tratamento é realizado antes do uso (por exemplo, anonimização, combinação com outros dados, derivação, inferência);

d) identificação e endereço do controlador;

e) informações sobre o uso compartilhado de dados e a finalidade específica;

f) responsabilidades dos agentes que realizarão o tratamento;

g) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD;

h) a identidade e as informações de contato do encarregado (art. 41, §1º);

i) dados coletados (agrupados) e formas de coleta;

j) o *link* do canal para requerimentos do titular de dados pessoais ao encarregado.

Além disso, a LGPD prevê no art. 23 que o Poder Público deve disponibilizar "*informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades*". Assim, aos itens acima deve-se acrescentar:

k) bases legais para o tratamento de dados pessoais;

l) procedimentos e práticas utilizados (como as medidas para a segurança, uso de cookies);

m) informações sobre a ocorrência de tratamento posterior dos dados e a finalidade;

n) informações sobre a ocorrência de transferência internacional de dados.

Os Avisos de Privacidade também devem considerar as recomendações da norma ABNT NBR ISSO/IEC 29184:2021. Além do conteúdo a ser exibido, a norma apresenta uma série de sugestões para implementação dos avisos: em multicamadas, com um resumo na primeira tela e links para o conteúdo completo; em painéis; avisos *just-in-time*; ícones; notificação em *pop-ups*; legíveis por máquinas em formato XML ou JSON, dentre outras possibilidades.

2.6. Gestão de Operadores e Terceiros

Conforme recomenda o controle A.7.2.6, do Anexo A da norma ABNT NBR ISSO/IEC 27701:2019, constitui uma boa prática que o MPT firme contrato, convênio, ou outro instrumento formal com todos os operadores e os terceiros que fazem o uso compartilhado dos dados pessoais, para definir o objeto, a duração, as bases legais e a finalidade do tratamento dos dados, os tipos de dados pessoais tratados, os direitos, as obrigações e responsabilidades relacionadas ao cumprimento da LGPD. As cláusulas contratuais impõem limites à atuação do operador e do terceiro, fixam parâmetros objetivos para a alocação de responsabilidades entre as partes e reduzem os riscos e as incertezas decorrentes da operação. Adicione-se a essa recomendação a orientação da ANPD no Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público: *recomenda-se que o compartilhamento seja estabelecido em ato formal, a exemplo de contratos, convênios ou instrumentos congêneres firmados entre as partes*.

2.6.1. Levantamento de Contratos relacionados a Dados Pessoais

O Encarregado deve orientar às unidades administrativas responsáveis pela gestão de contratos, convênios e licitações a realização do levantamento de todos os instrumentos formais relacionados ao tratamento de dados pessoais. O mapeamento dos processos que tratam dados pessoais no ROTDP – Registro de Operação de Tratamento de Dados Pessoais viabiliza a realização de uma correlação com os contratos, convênios, editais e termos de referência em licitações que os suportam. Esse mapeamento contribui para possíveis e necessárias adequações de cláusulas, tanto nos instrumentos contratuais existentes, quanto nos futuros.

2.6.2. Adaptação de cláusulas contratuais

O Encarregado deve recomendar e as unidades administrativas devem implementar a adequação das cláusulas dos instrumentos contratuais, convênios e documentos utilizados em licitações, aos termos da LGPD. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados em seu art. 6º. O contrato deve apresentar informações claras e objetivas, para:

a) determinar qual parte é o controlador e qual é o operador, ou se são controladores conjuntos;
b) definir quem pode realizar a coleta de dados pessoais e como deve ser feita;
c) descrever o tratamento a ser realizado: finalidade, duração, bases legais, categorias de titulares, categorias de dados pessoais e a forma como o tratamento dos dados pessoais deve ser realizado;
d) proibir explicitamente o tratamento dos dados para finalidade diferente da especificada;
e) exigir que o tratamento de dados pessoais seja realizado no Brasil;
f) assegurar que os dados pessoais sejam exatos e atualizados, estabelecendo a obrigação de informar imediatamente o MPT se o operador/terceiro tomar conhecimento de que os dados pessoais tratados são inexatos ou estão desatualizados;
g) exigir que o tratamento mantenha o grau de sigilo com o qual a informação foi classificada na origem;
h) detalhar quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento;
i) estabelecer que o operador só deve conceder acesso dos dados pessoais, objeto de tratamento, aos seus prepostos na medida estritamente necessária para a execução, a gestão e o acompanhamento do contrato e que deve comprovar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas às obrigações legais de confidencialidade adequadas;
j) proibir o operador de divulgar dados pessoais objeto do contrato, salvo em caso de solicitação legalmente obrigatória que deverá ser informada ao MPT;
k) proibir o tratamento posterior e definir os procedimentos que devem ser adotados para garantir a segurança na operação de retorno, transferência, descarte ou anonimização de dados pessoais ao final da vigência do contrato;
l) restringir o direito e a capacidade do operador de terceirizar a execução do contrato;
m) exigir que o operador adote e informe as medidas técnicas e administrativas para proteção e segurança dos dados tratados;
n) estabelecer que o MPT poderá solicitar ao operador a elaboração do relatório de impacto, caso um tipo ou volume de tratamento constitua um potencial risco para os direitos e as liberdades dos titulares de dados pessoais, definindo que é o MPT quem delibera se o nível de risco está adequado;

o) definir as regras para instauração, planejamento e execução de possíveis auditorias para que o MPT possa verificar se os operadores estão adotando políticas e procedimentos adequados de proteção de dados;
p) estabelecer disposições sobre como as partes responderão no caso de violação dos dados pessoais: a definição de que as comunicações para a ANPD e outros órgãos fiscalizadores, para os titulares e para o público em geral devem ser realizadas exclusivamente pelo MPT; o dever do operador de comunicar imediatamente o incidente ao MPT, possibilitando o cumprimento do prazo de dois dias úteis estabelecido pela ANPD para a comunicação de um incidente a partir de sua ocorrência; como o operador deve colaborar com o MPT para a avaliação de impactos à privacidade decorrentes do incidente e para fornecer informações e subsidiar a comunicação do incidente; o compromisso de sigilo do operador sobre a ocorrência do incidente;
q) definir como as partes irão colaborar para assegurar o exercício de direitos do titular, estabelecendo que o operador deverá notificar imediatamente o MPT sobre qualquer requerimento de titular, prestando assistência ao MPT no cumprimento de suas obrigações e que as respostas aos requerimentos de titulares serão enviadas exclusivamente pelo MPT;
r) estabelecer que o MPT deverá informar sobre qualquer alteração, correção, anonimização ou remoção de dados pessoais decorrentes do exercício de direitos do titular e que o operador ou terceiro deverá adotar procedimento idêntico.

Os instrumentos licitatórios devem selecionar apenas participantes que utilizam medidas de segurança técnicas e administrativas apropriadas para a proteção dos dados pessoais, de acordo com uma avaliação de impactos e riscos da operação de tratamento, sempre que necessário. As medidas adotadas devem estar alinhadas ao conceito de privacidade desde a concepção e privacidade por padrão, e com as medidas relacionadas no Anexo B da norma ABNT NBR ISSO/IEC 27701:2019. A contratação de serviços envolvendo computação em nuvem deve considerar as recomendações da norma ABNT NBR ISSO/IEC 27018:2021, que estabelece o código de prática para proteção de dados em nuvens públicas que atuam como operadores de dados pessoais.

2.7. Adaptação de Sistemas e Serviços

O Comitê Estratégico de Proteção de Dados Pessoais deve estabelecer em suas políticas que os sistemas e serviços do MPT devem ser construídos usando a metodologia de privacidade desde a concepção e que os sistemas e serviços legados devem ser adaptados para incorporar ao seu design e arquitetura os controles de privacidade e para assegurar ao titular de dados pessoais a proteção de seus dados por padrão. Essa adaptação deve ser planejada pelos gestores de sistemas, com a orientação do Encarregado, estabelecendo um cronograma que seja factível e que não tarde nas principais providências para a conformidade com a LGPD.

O Encarregado, em conjunto com a Secretaria de Tecnologia da Informação, deve propor uma política de desenvolvimento seguro, a ser publicada em resolução do Comitê Estratégico de Proteção de Dados Pessoais, estabelecendo um conjunto mínimo de controles a serem implementados nos sistemas e nos serviços do MPT, considerando as recomendações apresentadas no item 2.4. Essa política deverá atribuir aos gestores de sistemas/serviços a responsabilidade de elaborar e executar um plano de adaptação dos sistemas legados, que deve ser aprovado pelo Comitê Estratégico de Proteção de Dados Pessoais e acompanhado pelo Encarregado.

2.8. Gestão de Incidentes

Os incidentes de segurança da informação podem implicar na violação de dados pessoais. A segurança da informação visa garantir confidencialidade, integridade e disponibilidade da informação. Qualquer violação a um desses aspectos pode significar uma violação aos dados pessoais.

O MPT deve definir um processo de gestão de incidentes, que registre os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações como: a descrição do incidente; as informações e os sistemas envolvidos; as medidas administrativas e técnicas utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

Os incidentes podem ocorrer por uma variedade de causas: ataques de códigos maliciosos ou *hackers*, perda ou roubo de dispositivos, vulnerabilidades inerentes ou decorrentes de configurações inadequadas em *hardwares* e *softwares*, divulgação indevida (intencional ou não) de dados, dentre outras. Vale ressaltar que uma das maiores causas de violação de dados pessoais é em decorrência de vulnerabilidades do comportamento humano, que se concretiza em erros e negligência de pessoas da organização, seja por falta de treinamento, ou em decorrência de uma atitude pouco cautelosa. Por isso, é muito importante que todos no MPT estejam conscientes da responsabilidade de adotar práticas para a proteção de dados pessoais.

2.8.1. Plano de resposta a incidentes de privacidade

Um plano de resposta a incidentes de privacidade deve estabelecer controles e procedimentos específicos para detecção, análise, coleta/preservação de evidências, tratamento e resposta a incidentes de segurança da informação e privacidade, adotando novas medidas de proteção para reduzir o nível de risco.

Um plano de resposta a incidentes de privacidade deve implementar os controles de gestão de incidentes de segurança da informação recomendados na norma ABNT NBR ISSO/IEC 27001: 2018 (Anexo A, Tabela A.1, Controles A.16).

2.8.1.1. Responsabilidades e procedimentos

O plano de resposta a incidentes deve estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação que impliquem em violação de dados pessoais.

O Plano deve definir como as diversas áreas do MPT irão agir de forma colaborativa com o Encarregado no caso de uma violação de dados pessoais. O Encarregado tem um papel de articulação das diversas áreas para responder à violação de dados pessoais. O plano deve prever a possibilidade de o Encarregado convocar o Gabinete de Gerenciamento de Risco do MPT, o Comitê Estratégico de Proteção de Dados Pessoais, a Alta Administração, a Secretaria de Comunicação Social e a Diretoria de Gestão de Pessoas.

O plano também deve contemplar a gestão do tempo, pois o prazo para comunicação de incidentes de violação de dados pessoais à ANPD, a fim de garantir o cumprimento dos prazos estabelecidos pela ANPD.

O Encarregado deve solicitar as informações necessárias para a análise do incidente e convocar o CEGPDP e o Gabinete de Gerenciamento de Risco do MPT, caso julgue necessário, para avaliar a necessidade de realizar a comunicação para a ANPD e os titulares afetados e definir as providências necessárias.

2.8.1.2. Notificação de eventos de segurança da informação e privacidade

Todos os integrantes do MPT devem estar cientes da responsabilidade de notificar imediatamente os eventos de segurança da informação e privacidade no sistema Atena, dirigido à Equipe de Resposta a Incidentes de Segurança da Informação. Os atendentes que receberem o chamado devem comunicar imediatamente o Encarregado.

2.8.1.3. Notificação de fragilidades de segurança da informação e privacidade

Os usuários dos sistemas de informação do MPT devem ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observadas ou suspeitas, em um canal para relatar problemas disponibilizado nos próprios sistemas.

2.8.1.4. Avaliação e decisão dos eventos de segurança da informação e privacidade

Os eventos de segurança da informação devem ser analisados e deve ser decidido se eles são classificados como incidentes de segurança da informação. A análise tradicional de um incidente de segurança da

informação deve ser ampliada para verificar a natureza dos dados pessoais afetados, os titulares de dados pessoais envolvidos e a avaliação dos possíveis impactos e danos para os titulares e para o MPT.

2.8.1.5. Resposta aos incidentes de segurança da informação e privacidade

A resposta aos incidentes de segurança da informação e privacidade deve ocorrer de acordo com procedimentos documentados. Devem ser adotadas medidas para conter o incidente, diminuir os impactos e restabelecer sistemas e serviços.

2.8.1.6. Aprendendo com os incidentes de segurança da informação e privacidade

Os conhecimentos obtidos na análise e resolução dos incidentes de segurança da informação e privacidade devem ser adotados para implementar medidas capazes de reduzir a probabilidade de ocorrência ou os impactos de um incidente futuro.

2.8.1.7. Coleta e preservação de evidências

O Plano deve prever a especificação de procedimentos para a identificação, coleta, aquisição e preservação das informações que possam servir como evidências.

2.8.2. Plano de comunicação de violações de dados pessoais

Nem todas as violações de dados pessoais requerem notificações. O art. 48 da LGPD estabelece que *o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*. E no seu parágrafo primeiro detalha as informações que devem constar necessariamente numa comunicação:

> *I – a descrição da natureza dos dados pessoais afetados;*
>
> *II – as informações sobre os titulares envolvidos;*
>
> *III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;*
>
> *IV – os riscos relacionados ao incidente;*
>
> *V – os motivos da demora, no caso de a comunicação não ter sido imediata; e*
>
> *VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo*.

O Encarregado, se necessário com a colaboração do Gabinete de Gerenciamento de Risco do MPT, tem a responsabilidade de avaliar as necessidades e as formas de comunicação de um incidente que implique

em violação de dados pessoais. Em geral é recomendado que a comunicação seja realizada à ANPD e diretamente aos titulares afetados pela violação de dados pessoais, quando possível. É importante avaliar a pertinência de um aviso público ou de notificação da imprensa, pois depois de atender aos requisitos de notificação, as organizações podem ser expostas ao escrutínio, o que pode assumir a forma de consultas regulatórias ou ações judiciais, incluindo ações coletivas. Porém, em alguns casos, quando é impossível identificar os titulares envolvidos, ou quando o fato se torna de conhecimento geral, pode ser necessário um esclarecimento público oficial.

3. Monitoramento e Governança

A instituição do Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGP) do MPT e a definição em âmbito institucional de viabilizadores de governança de privacidade, tais como políticas, processos e estruturas organizacionais, são importantes para que a instituição tenha condições mínimas de governar a proteção de dados pessoais na organização. No entanto, nem sempre os mecanismos estabelecidos são efetivos. É fundamental que o Comitê Estratégico de Proteção de Dados Pessoais tenha governança sobre o programa, com o acompanhamento das atividades de monitoramento e de avaliação periódica e, se necessário, indique a direção para a correção de lacunas e melhorias.

A governança do programa está baseada nas normas ABNT NBR ISSO/IEC 27014:2013, ABNT NBR ISSO/IEC 38500, ABNT NBR ISSO/IEC 38505-1:2020 e ABNT NBR ISSO/IEC 38505-2:2022, com as atividades principais apresentadas na Figura 5 e descritas a seguir.

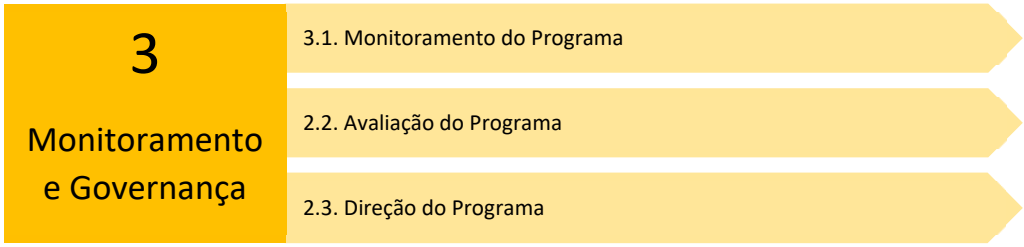

Figura 5 – Atividades da fase de Monitoramento e Governança

3.1. Monitoramento do Programa

O Comitê Estratégico de Proteção de Dados Pessoais deve monitorar o Programa por sistemas de medição apropriados, para verificar se as ações estão sendo implementadas de acordo com o plano traçado e aferir o nível de conformidade do MPT com as exigências legais e regulatórias para privacidade e proteção de dados pessoais.

A análise e o reporte de resultados são indicados na etapa de monitoramento para demonstrar o valor do Programa não somente para a Alta Administração, como também para todos os integrantes do MPT. Mostrar a evolução das ações e resultados obtidos, bem como o a importância da privacidade para o cidadão reforça e fortalece a cultura de privacidade e proteção de dados pessoais na instituição.

3.1.1. Definição de indicadores e métricas de desempenho

É responsabilidade do Comitê Estratégico de Proteção de Dados Pessoais definir os Indicadores de desempenho (*Key Performance Indicator – KPI*) e as métricas para o acompanhamento do Programa. A análise regular dos principais indicadores de desempenho permite verificar lacunas no Programa, assim como o status de outras iniciativas de privacidade.

3.1.2. Divulgação dos Resultados

A divulgação dos resultados para a Alta Administração deve ser realizada em relatórios de acompanhamento, cujos parâmetros e periodicidade serão definidos pelo Comitê Estratégico de Proteção de Dados Pessoais.

Adicionalmente, convém que os resultados sejam divulgados na página do Programa, para todos os integrantes do MPT.

3.2. Avaliação do Programa

O Comitê Estratégico de Proteção de Dados Pessoais deve avaliar os indicadores de desempenho, considerando o contexto organizacional do tratamento de dados pessoais, as tecnologias utilizadas e as obrigações legais e regulatórias.

Para realizar o processo de avaliação, o Comitê deverá:

a) assegurar que as iniciativas do MPT levem em consideração a privacidade e a proteção de dados pessoais;
b) responder aos resultados de desempenho do Programa, priorizar e iniciar ações necessárias.

3.3. Direção do Programa

A direção é o processo de governança pelo qual o Comitê Estratégico de Proteção de Dados Pessoais fornece o direcionamento dos objetivos do Programa que precisam ser implementados. Esse direcionamento pode incluir alterações nos níveis de recursos, alocação de recursos, priorização de atividades, revisões e aprovações de políticas, aceitação de riscos e planos de gestão de riscos.

Para realizar o processo de direção o Comitê deve:

a) determinar os níveis de risco de privacidade aceitáveis;
b) realizar atualizações no Programa, conforme resultados do processo de avaliação;
c) adequar o Programa às mudanças no contexto externo, como alterações nas leis e regulamentos para proteção de dados pessoais;
d) adequar o Programa em decorrência de mudanças no contexto interno, como alterações na natureza dos tratamentos de dados realizados no MPT ou adoção de novas tecnologias.

IV. Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISSO/IEC 27001:2013. Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação — Requisitos. Segunda edição: 08/11/2013 (válida a partir de: 08/12/2013).

- - - - -. ABNT NBR ISSO/IEC 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Terceira edição: 05/10/2022.

- - - - -. ABNT NBR ISSO/IEC 27005:2019. Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Terceira edição: 24/10/2019.

- - - - -. ABNT NBR ISSO/IEC 27014:2013. Tecnologia da informação – Técnicas de segurança – Governança da Segurança da Informação. Primeira edição: 25/06/2013.

- - - - -. ABNT NBR ISSO/IEC 27018:2021. Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP. Segunda edição: 12/03/2021.

- - - - -. ABNT NBR ISSO/IEC 27701:2019 Técnicas de segurança — Extensão da ABNT NBR ISSO/IEC 27001 e ABNT NBR ISSO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Primeira edição: 25.11.2019 (versão corrigida: 11/02/2020).

- - - - -. ABNT NBR ISSO/IEC 29100:2020. Tecnologia da Informação – Técnicas de segurança – Estrutura de Privacidade. Primeira edição: 27/03/2020.

- - - - -. ABNT NBR ISSO/IEC 29134:2020. Tecnologia da Informação – Técnicas de segurança – Avaliação de impacto de privacidade – Diretrizes. Primeira edição: 26/11/2020.

- - - - -. ABNT NBR ISSO/IEC 29151:2020. Tecnologia da Informação – Técnicas de segurança – Código de prática para proteção de dados pessoais. Primeira edição: 26/11/2020.

- - - - -. ABNT NBR ISSO/IEC 29184:2021. Tecnologia da Informação – Avisos de privacidade on-line e consentimento. Primeira edição: 25/06/2021.

- - - - -. ABNT NBR ISSO/IEC 31000:2018. Gestão de riscos – Diretrizes. Segunda edição: 28/03/2018.

- - - - -. ABNT NBR ISSO/IEC 38500:2018. Tecnologia da informação – Governança da TI para a organização. Segunda edição: 28/11/2018.

- - - - -. ABNT NBR ISSO/IEC 38505-1:2020. Tecnologia da Informação — Governança da TI – Governança de dados. Parte 1: Aplicação da ABNT NBR ISSO/IEC 38500 à governança de dados. Primeira edição: 22/01/2020.

- - - - -. ABNT NBR ISSO/IEC 38505-2:2022. Tecnologia da informação – Governança de TI – Governança de dados. Parte 2: Implicações da ABNT NBR ISSO/IEC 38505-1 para gerenciamento de dados. Primeira edição: 12/07/2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD: Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Versão 2.0. Brasília, abril, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em 25/08/2022.

- - - - -. ANPD: Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público. Versão 1.0. Brasília, janeiro, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf. Acesso em 24/10/2022.

- - - - -. ANPD: Guia Orientativo Cookies e proteção de dados pessoais. Versão 1.0. Brasília, outubro, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 24/10/2022.

Brasil. Ministério da Economia. Secretaria de Governo Digital. Guia de Elaboração de Programa de Governança em Privacidade. Versão 1.0. Brasília, outubro, 2020. Disponível em:https://www.gov.br/governodigital/pt-br/44overnanç-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso Em: 24/10/2022.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso Em: 24/10/2022.