Secretaria Executiva Subsecretaria de Planejamento e Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação

PROGRAMA DE

GOVERNANÇA EM PRIVACIDADE DO MCOM

MINISTÉRIO DAS COMUNICAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Sumário Executivo

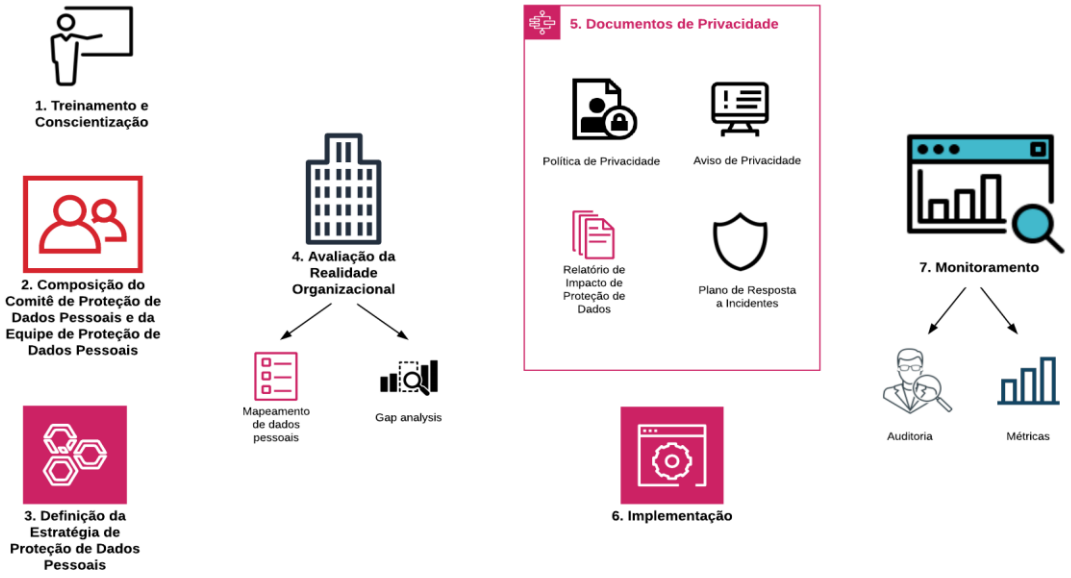
O presente documento apresenta, de forma sucinta, um roteiro de atividades que devem ser realizadas para a implementação de um **Programa de Governança em Privacidade**, em conformidade com o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n. 13.709, de 14 de agosto de 2018).

O roteiro é baseado em boas práticas da indústria e em modelos internacionais, mas leva em consideração a estrutura organizacional do Ministério das Comunicações (MCom), de forma a construir uma lista de atividades que se adeque à realidade deste Ministério. Para a realização de um Programa de Governança em Privacidade destacam-se, como essenciais, as seguintes atividades:

1. **Treinamento e Conscientização**
2. Composição do **Comitê de Proteção de Dados Pessoais** e da **Equipe de Proteção de Dados Pessoais**
3. Definição da **Estratégia de Proteção de Dados Pessoais**
4. Avaliação da **Realidade Organizacional** (*Business Case*)
5. **Elaboração dos Documentos de Privacidade**
6. **Implementação** do Programa de Governança em Privacidade
7. **Monitoramento** do Programa de Governança em Privacidade

O presente documento apresenta **proposta de Programa de Governança em Privacidade, que deverá ser validado e complementado pelo Comitê de Proteção de Dados do MCom.** A figura a seguir apresentada resume as sete atividades que contemplam o Programa de Governança em Privacidade e suas subatividades, que serão descritas ao longo deste documento.

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE



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 o art. 50, I, da LGPD, 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.

A seguir detalham-se as sete atividades consideradas essenciais para a realização de um Programa de Governança em Privacidade. É importante frisar que algumas dessas atividades ocorrerão em paralelo e se repetirão ao longo de várias etapas. Por exemplo, atividades de treinamento e de conscientização devem ocorrer em todas as fases do plano em que se detecte a necessidade de nivelamento organizacional sobre noções de privacidade e proteção de dados pessoais (ou conhecimentos mais especializados, a depender da área).

Outro exemplo é o das atividades de monitoramento, que permanecerão após a implementação do Programa de Governança em Privacidade, para garantir seu aprimoramento contínuo. Ao final, apresenta-se uma lista de sugestões bibliográficas para maior aprofundamento de tópicos citados neste material.

1. Treinamento e Conscientização

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

Com relação ao MCom, enquanto conhecimentos gerais sobre a política de privacidade devem ser comunicados a todas as equipes, algumas funções podem necessitar de capacitações específicas e mais especializadas, a saber:

- A **Gestão de Pessoas** deve ser informada sobre procedimentos administrativos para tratar dados pessoais do corpo funcional durante todo o ciclo de vida dos dados;
- A **Tecnologia da Informação** deve ser capacitada para a implementação de medidas técnicas de segurança que protejam os dados pessoais tratados no âmbito da instituição;
- A **Ouvidoria** deve ser preparada para receber solicitações e reclamações de titulares de dados, com respeito a seus direitos e eventuais vazamentos de dados.
- A **Comunicação Socia**l 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, *e-learning*, reuniões de equipe, boletins informativos, e-mails, pôsteres, folhetos, slogan e informações no portal eletrônico.

Treinamentos podem ser conduzidos por representantes internos ou externos à instituição, de acordo com as diretrizes definidas pelo Comitê de Proteção de Dados Pessoais (ver seção 2). Contudo, treinamentos podem ser necessários antes mesmo da composição deste Comitê, ou na sua fase inicial de constituição, para orientá-lo em como deverá realizar suas atribuições. Neste caso, deve-se selecionar funcionários especializados em Privacidade e Proteção de Dados para instruir a alta administração sobre o tema.

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

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

2. Composição do Comitê de Proteção de Dados Pessoais e da Equipe de Proteção de Dado Pessoais

Para elaborar um Programa de Governança em Privacidade, dois grupos essenciais devem ser compostos: (i) o **Comitê de Proteção de Dados Pessoais**; e (ii) a **Equipe de Proteção de Dados Pessoais**.

A seguir apresenta-se uma explicação de quais são as funções de cada grupo. Considerando que o MCom possui uma estrutura limitada esta proposta não pretende prever novos cargos para a composição desses grupos, mas sugere áreas que poderiam indicar representantes.

O **Comitê de Proteção de Dados Pessoais** reúne os principais interessados que lideram e que são responsáveis por atividades de tratamento de dados pessoais relevantes da instituição. Para sua composição, deve-se considerar representantes sênior de 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 (ver seção 5).

No contexto do MCom, entende-se, em primeira análise, que áreas estratégicas para possuírem representantes no Comitê são o Gabinete da Secretaria Executiva, a Coordenação-Geral (CG) de Planejamento e Gestão Estratégica, a CG de Orçamento e Finanças, a CG de

Gestão de Pessoas, a CG de Tecnologia da Informação, a Ouvidoria e as Secretarias finalísticas (órgãos específicos singulares).

Por sua vez, a **Equipe de Proteção de Dados Pessoais** estrutura e coloca em prática o Programa de Governança em Privacidade a partir das diretrizes definidas pelo Comitê. Idealmente, as seguintes funções compõem a Equipe:

i. Encarregado;
ii. Analistas de proteção de dados pessoais;
iii. Atendentes de solicitações e reclamações de titulares de dados pessoais;
iv. Técnicos de segurança da informação e de resposta a incidentes de segurança que acarretem a divulgação indevida de dados pessoais;

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

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

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

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) receber comunicações da autoridade nacional e adotar providências;
c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

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:

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

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

No contexto do MCom, conquanto não seja possível dispor de cargos suficientes para a composição de uma Equipe robusta, é essencial que o Encarregado possa contar diretamente com ao menos um representante da Ouvidoria para questões relacionadas a solicitações e reclamações de titulares de dados pessoais, e um representante da Coordenação-Geral de Tecnologia de Informação que responda a ele sobre questões relacionadas à segurança da informação, auxilie na implementação de medidas técnicas de segurança e contenção de dados em cenários de vazamento (*data breaches*).

3. Definição da Estratégia de Proteção de Dados Pessoais

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

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

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

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

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

b) Envolver unidades interessadas, que lidam diretamente com dados pessoais internos e ou externos à instituição;
c) Estruturar mecanismos de comunicação e colaboração entre as partes interessadas;

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

i. Gabinete;
ii. Secretaria-Executiva, tanto a Subsecretaria de Orçamento e Administração, quanto a Subsecretaria de Planejamento e Tecnologia da Informação; e
iii. Consultoria Jurídica;
iv. Assessoria Especial de Controle Interno, em particular a Ouvidoria.
v. Secretarias finalísticas

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

No caso do Ministério das Comunicações, 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 de grupos centrais – o Comitê e a Equipe, respectivamente**.

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. Neste caso, recomenda-se a adoção de um modelo híbrido. Para mais detalhes sobre RIPDs, verificar a seção 5.

4. Avaliação da Realidade Organizacional

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

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

Em seguida, devem ser identificadas lacunas que serão preenchidas para garantir a correta adequação à LGPD. Desse modo, a avaliação da realidade organizacional pode ser separada em duas etapas: (i) mapeamento de dados pessoais e (ii) *gap analysis*.

4.1. Mapeamento de dados pessoais

O **mapeamento de dados pessoais ou "inventário de dados"** é uma lista que contempla como é realizado o tratamento de dados pessoais dentro da instituição. Ele permite identificar áreas-chave, papéis e responsabilidades para o Programa de Governança em Privacidade.

O inventário deve ser organizado em torno do ciclo de vida dos dados - coleta, uso, transferências, retenção e destruição. Idealmente, deve contemplar todas as atividades de tratamento previstos na LGPD (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração). Algumas perguntas que o inventário de dados deve responder são:

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

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

4.2. Gap analysis

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

No contexto brasileiro, a principal norma aplicável é a LGPD, porém, a depender das atividades da instituição, devem-se também considerar a aplicação de normas setoriais e de

leis estrangeiras, como o regulamento europeu – RGPD, ou as leis de privacidade dos EUA – GLBA (lavagem de dinheiro), HIPAA (dados de saúde), CCPA (dados de consumidores da Califórnia), etc. Neste documento, será dado foco apenas aos requisitos da LGPD.

Essa análise permite identificar quais lacunas existem para a correta adequação às legislações aplicáveis. Operações de tratamento devem ser identificadas e avaliadas ao longo de toda a instituição, e uma boa prática é a realização de sessões *assess-and-coach*, onde, ao mesmo tempo em que riscos e deficiências são identificados, recomendações são oferecidas sobre como saná-los. De forma similar ao inventário de dados, planilhas que identificam práticas vigentes também são bastante importantes. Algumas das perguntas que esse segundo mapeamento pode contemplar são:

- Qual a base legal para o tratamento dos dados pessoais (art. 7º da LGPD)?
- Existem dados pessoais sensíveis sendo tratados (art. 11º)? Se sim, quais as bases legais e quais as medidas de segurança para sua proteção adicional?
- Existem dados pessoais de crianças e adolescentes sendo tratados (art. 14º)? Há necessidade de consentimento parental? Quais as medidas para confirmar a obtenção desse consentimento?
- Quais os procedimentos para eliminação de dados pessoais? Quais as exceções legais aplicáveis para armazenamento de dados além do período pré-estabelecido (art. 16)?
- Quais os procedimentos que permitam aos titulares de dados serem informados e exercerem seus direitos (art. 18)?
- As regras para tratamento de dados pessoais pelo poder público são cumpridas (arts. 23 a 27)?
- Há operações de transferência internacional de dados pessoais? Se sim, para onde são enviados, quais as entidades envolvidas, qual o procedimento? Qual a base legal para a transferência internacional (art. 33)?
- Existe registro das operações de tratamento de dados pessoais? Como esse registro é atualizado (art. 37)?
- Foi realizada uma análise de riscos preliminar das operações de tratamento? Há necessidade de elaboração de um Relatório de Impacto de Proteção de Dados (art. 38)? Este relatório foi elaborado?
- Existe encarregado de proteção de dados pessoais? Quais suas competências (art. 41)?
- Quais medidas de segurança, técnicas e administrativas são adotadas para proteger os dados pessoais de acessos não autorizados e outras situações acidentais ou ilícitas - destruição, perda, alteração, comunicação, tratamento inadequado ou ilícito (art. 46)?

- Quais os procedimentos para responder a incidentes de segurança/vazamento de dados pessoais (art. 48)?

No contexto do MCom, é importante que a **Consultoria Jurídica** participe do procedimento de *gap analysis* para garantir que obrigações legais da LGPD e outras leis aplicáveis sejam cumpridas.

5. Elaboração de 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 LGPD. Neste roteiro, os seguintes documentos são destacados: (i) **política de privacidade**, de uso interno; (ii) **aviso de privacidade**, para usuários externos; (iii) **relatório de impacto de proteção de dados - RIPD**; (iv) **plano de resposta a incidentes**.

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

Contudo, RIPDs devem refletir realidades específicas das unidades organizacionais que estejam conduzindo um processo ou projeto de tratamento de dados que justifique a elaboração deste documento. Deste modo, um RIPD deverá ser produzido pela área técnica competente e revisado pela Equipe de Proteção de Dados Pessoais.

Uma vez elaborados, os documentos de privacidade deverão ser submetidos para avaliação do Comitê de Proteção de Dados Pessoais.

5.1. Política de privacidade

A política de privacidade é um **documento interno** dirigido a funcionários e eventuais terceiros que forneçam produtos e serviços para a instituição (contratados). No caso do MCom, isso significa tanto a equipe de servidores públicos, 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 às necessidades organizacionais e as legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados, incluindo como o aviso de privacidade será formado, se necessário, e o que ele conterá.

A política de privacidade deve ser considerada por toda a instituição – do mais alto nível de governança institucional até às equipes operacionais. Deve ser compreensível,

acessível a todos os funcionários, abrangente, conciso, orientado para a prática, mensurável e testável.

Seus principais componentes são:

i. **Objetivo:** porque a política existe e metas a serem alcançadas;
ii. **Escopo:** que recursos (pessoas, processos e tecnologias) a política protege;
iii. **Responsabilidades:** quais papéis são responsáveis por quais atividades relacionadas à proteção de dados, incluindo líderes, gerentes, demais funcionários e terceiros;
iv. **Conformidade:** estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos complementares (ex. política de controle de acesso) e regime de sanções disciplinares por desrespeito à política de privacidade.

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.

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

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

5.3. Relatório de Impacto de Proteção de Dados

O Relatório de Impacto de Proteção de Dados - RIPD, é uma análise dos riscos à proteção de dados associados ao tratamento de dados pessoais em relação a um

determinado projeto, produto ou serviço. O RIPD também deve sugerir ou fornecer ações corretivas ou mitigações necessárias para evitar ou mitigar esses riscos.

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

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

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

i. **Análise preliminar:** conduzir uma análise preliminar de riscos, para determinar se o RIPD é necessário. Se for concluído por existência de atividades de alto-risco, a elaboração do RIPD deve ser conduzida;
ii. **Preparação do RIPD:** coleta de informações sobre as operações de tratamento. O inventário de dados pessoais e o *gap analysis* são dois procedimentos importantes nessa etapa preparatória.
iii. **Elaboração do RIPD:** identificar o escopo do tratamento, determinar os requisitos de proteção de dados relevantes (princípios, bases legais, direitos dos titulares, transferências internacionais, etc.), acessar o risco (identificação, análise e avaliação do risco) e elaborar o plano tratamento do risco (medidas técnicas e administrativas *security by design* e *privacy by design*).
iv. **Monitoramento do RIPD:** preparar e publicar o relatório, implementar o plano de tratamento de risco, revisar o relatório.

5.4. Plano de resposta a incidentes

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

O PRI deve fornecer instruções que auxiliem a identificar se um determinado incidente de segurança é também um vazamento de dados, ou seja, se o incidente detectado acarreta risco ou dano relevante aos titulares de dados. Caso positivo, as regras da LGPD se aplicarão,

o que inclui **obrigações de comunicação à autoridade nacional e aos titulares de dados sobre o incidente (art. 48).**

Algumas das informações que um PRI deve conter são: (i) instruções para garantir o sigilo de informações sensíveis quanto ao vazamento; (ii) definição de funções e responsabilidades de unidades organizacionais durante o vazamento; (iii) escalonamento de possíveis problemas e relato de atividades suspeitas; (iv) classificações de gravidade de incidentes; (v) orientações para comunicações externas (por exemplo, com reguladores, fornecedores de serviços, seguradoras, titulares, etc.).

6. 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 a **Equipe de Proteção de Dados Pessoais, liderada pelo 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: (i) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (ii) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente, e; (iii) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos. Alguns exemplos de medidas técnicas e organizacionais *privacy by design* incluem:

- uso de **criptografia** para proteção de bases de dados e meios de comunicação;
- **minimização e pseudonimização** de bases de dados;
- **controle de acesso** baseado em funções;

- mecanismo de **respostas a requisições e reclamações** dos titulares de dados;
- plano de **respostas a incidentes** e remediação de segurança e privacidade;
- segurança física;
- **políticas de privacidade** para aquisição de produtos/serviços;
- **políticas de gerenciamento** da segurança da informação;
- **política de retenção e eliminação** de dados pessoais.

Duas práticas importantes a serem implementadas são os mecanismos de respostas a requisições e reclamações dos titulares de dados e a incidentes de segurança e privacidade. Estes mecanismos têm como objetivo respeitar os direitos dos titulares de dados previstos na LGPD e preparar-se para cenários indesejados de vazamento de dados, identificando que áreas deverão ser envolvidas para conter o dano, informar as partes interessadas relevantes (ex. ANPD e titulares de dados) e lidar com responsabilizações judiciais.

No MCom, coordenações como Planejamento e Gestão Estratégica, Tecnologia da Informação, Consultoria Jurídica e Ouvidoria exercem importantes papeis para a correta implementação do Programa de Governança em Privacidade.

7. Monitoramento do Programa de Governança em Privacidade

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 pela **Equipe de Proteção de Dados Pessoais** e reportado periodicamente ao **Comitê de Proteção de Dados Pessoais.** A partir dessas informações trazidas, 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, em operadores de dados ou por terceiros independentes.

A auditoria interna é utilizada para realizar auto avaliações 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 MCom, a Assessoria Especial de Controle Interno é a unidade mais indicada para assessorar a Equipe de Proteção de Dados Pessoais na condução deste tipo de auditoria.

A auditoria em operadores de dados ocorre nas hipóteses em que a instituição, enquanto controladora de dados, quer se certificar de que entidades contratadas como operadoras de dados cumprem suas obrigações frente a legislações de proteção de dados, no caso a LGPD.

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

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

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

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

8. Conclusão

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

Espera-se, com isso, que o Ministério das Comunicações possa garantir a implementação de um Programa de Governança em Privacidade, garantindo a observância à norma e o respeito aos titulares de dados.

ANEXO I - Glossário de Termos

Autoridade Nacional de Proteção de Dados - ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Criada pela Lei nº 13.853 de 2019 e estruturada pelo Decreto nº 10.474 de 2020.

Controlador de dados: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador define a finalidade e os meios pelo qual os dados pessoais serão tratados e é o principal responsável pelas operações de tratamento de dados.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Seu escopo é amplo e pode se referir tanto a dados que identificam diretamente o indivíduo (ex. nome, CPF, email, etc.), como também atributos do indivíduo que, quando correlacionados permitem a sua identificação (ex. gênero, idade, altura, formação acadêmica, endereço físico, endereço IP, etc.).

Dado (pessoal) sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Devido à sua natureza mais sensível possui maiores restrições para seu tratamento, de acordo com o estipulado na LGPD.

Encarregado de dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O encarregado é normalmente um indivíduo, mas também pode se referir à equipe que exerce suas atribuições. Também pode ser interno ou externo à instituição controladora/operadora de dados.

***Gap analysis**:* atividade em que se avalia a realidade organizacional de uma instituição para entender qual a situação do atual gerenciamento de privacidade e proteção de dados frente às legislações aplicáveis, identificando lacunas legais. Para maiores informações, verificar a seção 4.2.

Incidente de segurança (da informação): qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação - Confidencialidade, Integridade e Disponibilidade. Ver também vazamento de dados, abaixo.

Programa de Governança em Privacidade: programa que guia uma instituição para a conformidade com leis e regulamentos de privacidade e proteção de dados, apoiando objetivos e metas de negócios mais amplos da organização.

Operador de dados: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador poderá definir os meios para o tratamento de dados, desde que designado pelo controlador. Um operador é sempre pessoa externa ao controlador (i.e., um funcionário de uma instituição controladora não é operador de dados).

Privacy by design: abordagem à engenharia de sistemas que leva em conta a privacidade durante todo o processo de construção do software (ou serviço). Envolve a implementação de medidas técnicas (ex. uso de criptografia e mecanismos lógicos de controle de acesso) e organizacionais (ex. políticas de privacidade).

Relatório de Impacto de Proteção de Dados – RIPD: 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. Para maiores informações, verificar a seção 5.3.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Para se configurar a transferência, o dado (ainda que sua cópia) deve ser armazenado em território estrangeiro – o tráfego de dados de efeito transitório não configura transferência.

Tratamento de dados: 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;

Vazamento de dados (*data breach*): incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados. Ver também, incidente de segurança, acima.

ANEXO II - Bibliografia Sugerida

- Carvalho *et al*. *Relatório de Impacto à Proteção de Dados Pessoais: Aspectos práticos relevantes à luz da LGPD*. Disponível em: https://bit.ly/2YF2CbP
- CCGD. *Guia de Boas Práticas para Implementação Lei Geral de Proteção de Dados na Administração Pública Federal*. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd.
- CIPL – Centre for Information Policy Leadership; CEDIS – Centro de Direito, Internet e Sociedade do IDP. Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD). Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-idp_white_paper_on_top_priorities_for_public_and_private_organizations_to_effectively_implement_the_lgpd__1_september_2020_.pdf
- CNIL. *Privacy Impact Assessment*. Disponível em: https://www.cnil.fr/en/privacy-impact-assessment-pia
- Densmore, R. *Privacy Program Management.* Disponível em: https://iapp.org/resources/article/privacy-program-management/
- ICO. *Auditing data protection: a guide to ICO data protection audits.* Disponível em: https://ico.org.uk/media/1533/auditing_data_protection.pdf
- ICO. *Data Protection Impact Assessment*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- ICO. *DPIA Template*. Disponível em: https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx
- ISO. *ISO/IEC 29134:2017 - Information technology — Security techniques — Guidelines for privacy impact assessment.* Disponível em: https://www.iso.org/standard/62289.html
- ITS. *Lei Geral de Proteção de Dados Pessoais (LGPD) e Setor Público*. Disponível em: https://itsrio.org/pt/publicacoes/lei-geral-de-protecao-de-dados-pessoais-lgpd-e-setor-publico/
- Maia, F. *LGPD: Aplicação Prática das Bases Legais.* Disponível em: https://bit.ly/2EDV0PC
- NIST. *Privacy Framework.* Disponível em: https://www.nist.gov/privacy-framework/privacy-framework.
- Yun, R. *Programa de Adequação à Proteção de Dados Pessoais – Guia Prático*. Disponível em: https://bit.ly/3jiaU16

MINISTÉRIO DAS COMUNICAÇÕES

gov.br/mcom

mincomunicacoes

MINISTÉRIO DAS COMUNICAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL