Histórico de Revisões

Data	Versão	Descrição	Aprovação
17/11/2025	1.0	Programa de Governança em Proteção de Dados Pessoais	Diretoria Executiva-Diretor Presidente

INSTITUTO ADECON

PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 17 de novembro de 2025.

INTRODUÇÃO

O Programa de Governança de Proteção de Dados Pessoais do **Instituto ADECON** foi concebido para assegurar que todas as atividades desenvolvidas pela entidade — desde ações de desenvolvimento profissional e social até a celebração de parcerias e a prestação de serviços especializados — sejam conduzidas em plena conformidade com a Lei Geral de Proteção de Dados (LGPD) e com elevados padrões de transparência, ética e responsabilidade. Fundada em 29 de setembro de 1975 e transformada em Instituto em 2003, a **ADECON** reúne pessoas físicas, jurídicas e diversos profissionais de nível superior vinculados às empresas energéticas do Estado de São Paulo e à Fundação CESP, incluindo associados beneméritos, honoríficos, universitários, especiais e contribuintes. Sua trajetória institucional, alinhada à missão de promover excelência, pluralismo de ideias e confiabilidade, cria o ambiente propício para a adoção de práticas robustas de governança, essenciais para proteger informações sensíveis e garantir a integridade das operações.

O Programa estabelece diretrizes e mecanismos de controle que sustentam os objetivos centrais do **Instituto,** tais como promover o desenvolvimento e a valorização profissional dos associados, defender seus direitos e interesses, firmar parcerias com entidades públicas e privadas, atuar como órgão técnico e consultivo, fomentar atividades educativas e promover integração social e cultural. Para assegurar que essas finalidades sejam cumpridas com segurança e eficiência, a governança de dados disciplina o tratamento adequado, legítimo e proporcional das informações pessoais, reforçando a cultura institucional de proteção de dados, mitigação de riscos e conformidade contínua. Dessa forma, o **Instituto ADECON** fortalece a confiança de seus associados, parceiros e da sociedade, garantindo que todas as suas iniciativas sejam sustentadas por práticas responsáveis e alinhadas às melhores referências nacionais e internacionais de proteção de dados.

Conheça, a seguir, a metodologia estruturada para o desenvolvimento e a implementação do Programa de Governança de Proteção de Dados Pessoais do **Instituto ADECON**, concebida para orientar cada etapa do processo de conformidade, fortalecer a cultura organizacional e garantir a adoção contínua das melhores práticas de proteção de dados.

1- PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS PESSOAIS

1.1 – O que é

A Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Boas Práticas e da Governança, dispõe no Art. 50, § 2º sobre as características mínimas do **PROGRAMA LGPD**, conforme apresentado na Figura 1:

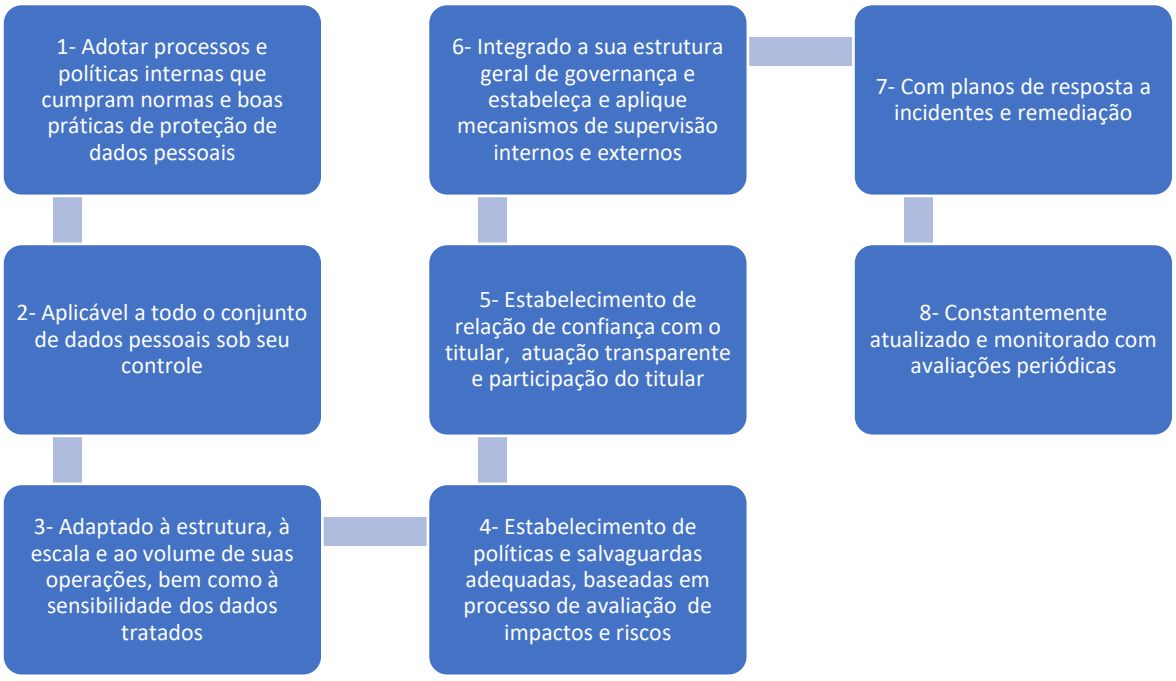


Figura 1. Características Mínimas de um Programa Governança de Proteção de Dados Pessoais

1.2. Atores do Programa

Diante da obrigatoriedade legal e regulatória estabelecida pela LGPD é necessário destacar seus principais atores:

1.2.1. No papel central, por sua importância, tem-se o **titular**, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso III do art. 2º da Lei Geral de Proteção de Dados);

1.2.2. A seguir, o **controlador**, pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da Lei Geral de Proteção de Dados). O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador;

1.2.3. O **operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da Lei Geral de Proteção de Dados). Ambos, controlador e operador, recebem a nomeação de "agentes de tratamento" (inciso IX do art. 5º da Lei Geral de Proteção de Dados);

1.2.4. O **encarregado** de dados é a 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).

1.2.5. Finalmente, a **Autoridade Nacional de Proteção de Dados - ANPD** tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados Pessoais.

1.3. Nomeação da equipe. Neste contexto, o I**NSTITUTO ADECON** estabelece as seguintes diretrizes e equipe para o desenvolvimento do **"Programa":**

1.3.1. **Encarregada de Dados** : **MAYRA MOTTA SOCIEDADE INDIVIDUAL DE ADVOCACIA,** inscrita no CNPJ sob o n. 25.011.890/0001-68, estabelecida no Estado de São Paulo, na cidade de São Paulo ,sito à Alameda Santos, n. 455, conjunto 801, Ed. Paulista Plaza The Office, CEP 01418-000, neste ato representada por sua sócia proprietária **MAYRA MOTTA**, brasileira, advogada, inscrita na OAB/SP sob nº 135.123, e-mail: dpo@institutoadecon.org.br

1.3.2**. Comitê LGPD :** (i) **Rui Carlos Ortega,** Cargo: Diretor Vice-Presidente, RG: 4.391.847-5, CPF: 308.741.498-00, Estado Civil: Casado, Profissão: Administrador, Endereço: Rua Castro Alves, 20 - Apto. 142 - Embaré - Santos/SP; (ii) **José Carmo de Felice**, Cargo: Diretor de Comunicação, RG: 5.718.768, CPF: 873.912.798-20, Estado

Civil: Casado, Profissão: Administrador, Endereço: Rua Passo da Pátria, 855, Ap. 82 - Bela Aliança, Capital/SP; (iii) **Roberto Magno Lamboglia Gomes**, Cargo: Diretor Administrativo e Jurídico, RG: 6.568.371, CPF: 634.781.888-49, Estado Civil: Casado, Profissão: Administrador, Endereço: Avenida Alfredo Zumkeller, 71, Ap. 42 - Mandaqui, Capital/SP.

1.3.3. **Controlador**: Ao **INSTITUTO ADECON** competem as decisões referentes ao tratamento de dados pessoais, ressalvadas as hipóteses previstas em contrato com um cliente corporativo, cuja responsabilidade poderá ser acordada como OPERADORA, definidas de acordo com as obrigações e o poder de decisão estabelecido entre as Partes.

1.4 – Framework

1.4.1. A estrutura do **PROGRAMA LGPD** apresentado neste documento é inspirada no ciclo PDCA (Plan, Do, Check e Act), bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. O **PROGRAMA LGPD** será estruturado nas seguintes etapas, conforme Figura 2, e serão descritas e detalhadas no próximo capítulo:

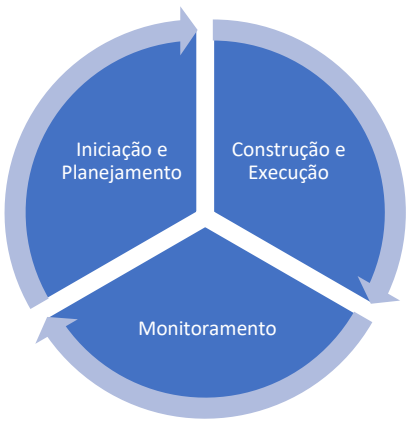


Figura 2. Etapas Programa de Governança em Proteção de Dados Pessoais

2- ETAPAS DO PROGRAMA LGPD

2.1 – Iniciação e Planejamento

A etapa de Iniciação e Planejamento buscará compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Essa etapa é constituída pelos marcos apresentados na Figura 3, que serão detalhados a seguir.

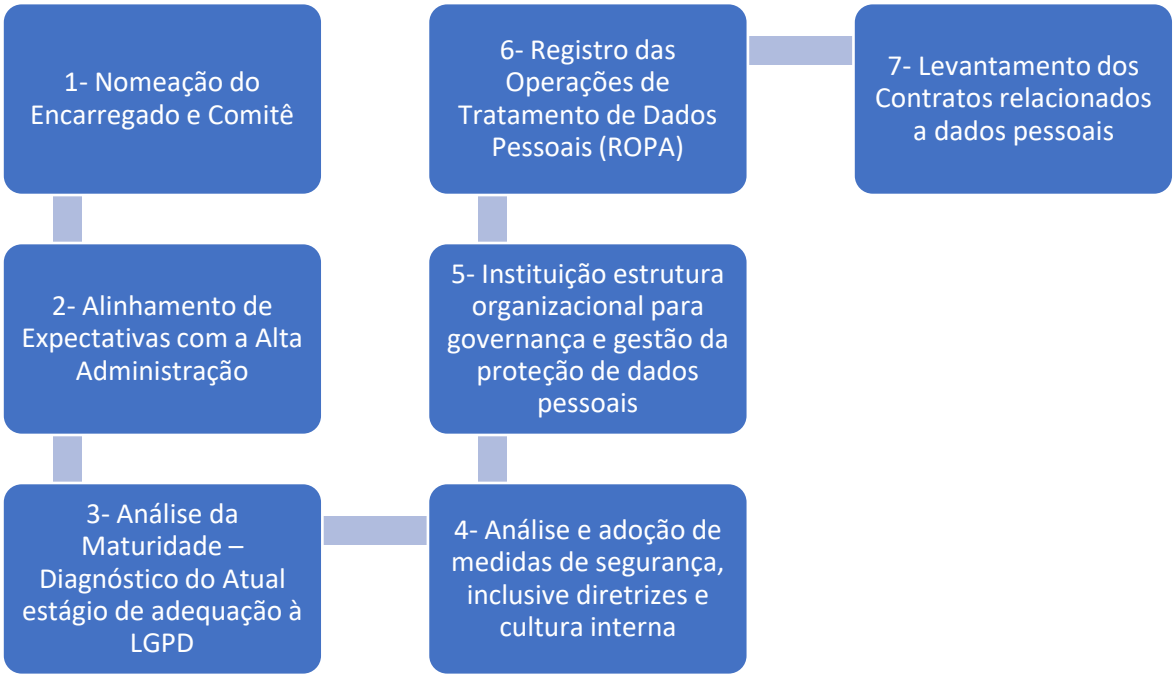


Figura 3. Marcos Etapa Iniciação e Planejamento

2.1.1 – O Encarregado. Conforme o Art. 5º inciso VIII da LGPD, o encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

2.1.2 - Alinhamento de Expectativas com a Alta Direção. Ao longo da etapa de Iniciação e Planejamento foram alinhadas as expectativas com a alta direção (Diretoria Executiva), priorizando as ações mais urgentes, os projetos e as estruturas da empresa envolvidas.

2.1.3 – Maturidade da Organização. Outro ponto analisado é a maturidade da **Entidade,**

observando fatores como a rastreabilidade de dados, estruturando-os e descrevendo as informações tratadas em cada sistema, a comunicação com o titular e a transparência.

2.1.4 – Medidas de Segurança. *As* medidas de segurança serão analisadas, revisadas e aprimoradas. Como itens de conformidade serão implementadas e/ou revisadas as seguintes medidas de melhorias técnicas e administrativas:

- Políticas de Segurança de Informação – O papel da política de segurança da informação em orientar a implementação e a gestão das boas práticas nas áreas e atividades da Entidade.
- Organização da Segurança da Informação – Controles sobre como as responsabilidades são definidas e gerenciadas;
- Gestão de Ativos da Informação – Controles relacionados ao inventário de ativos, uso aceitável, classificação de informação e manuseio de mídias;
- Controle de Acesso – Controles para a política de controle de acesso, gestão de acesso a sistemas e aplicações e responsabilidades dos usuários;
- Criptografia- Controles relacionados à gestão de chaves criptográficas;
- Segurança Física e do Ambiente – Controles definindo áreas seguras, controles de entrada, proteção contra ameaças, segurança de equipamentos, descarte seguro, política de mesa limpa e tela limpa;
- Segurança nas Operações – Controles relacionados à gestão da produção de TI: gestão de mudanças, gestão de capacidade, software malicioso, backups, registro de eventos, monitoramento, instalação, vulnerabilidades;
- Segurança nas Comunicações – Controles relacionados à segurança em rede, segregação, serviços de rede, transferência de informação, mensageria;
- Aquisição, desenvolvimento e manutenção de sistemas- Controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte;
- Relacionamento na cadeia de suprimento – Controles sobre o que incluir em acordos e como monitorar os fornecedores em TI;
- Gestão em incidentes de segurança da informação – Controles para reportar eventos e fraquezas, definindo responsabilidades, procedimentos de resposta e coleta de evidências;

- Aspectos da segurança da informação na gestão da continuidade do negócio- Controles requisitando o planejamento da continuidade do negócio, procedimentos, verificação e revisão e redundância da TI.;
- Conformidade – Controles requisitando a identificação de leis e regulamentações aplicáveis, proteção da propriedade intelectual, proteção, proteção de dados pessoais e revisões da segurança da informação.

2.1.5 – Estrutura Organizacional

2.1.5.a. O **INSTITUTO ADECON** atende a estrutura de governança estabelecida pela Resolução CD/ANPD nº 18/2024 , baseada na atuação formal e transparente do encarregado pelo tratamento de dados pessoais, detalhando definição, atribuições e relações com outros agentes de tratamento.

2.1.5.b. A encarregada nomeada exerce funções como canal entre controlador, titulares e ANPD, orientação interna, recebimento e encaminhamento de demandas, gestão de incidentes, apoio à elaboração de políticas internas e de programa , atuando sem conflito de interesses, assegurada sua autonomia e ausência de prejuízo à eficácia das atribuições.

2.1.6 – Registro das Operações de Tratamento de Dados -ROPA

Mapeamento dos dados pessoais utilizados pela **Entidade** e a realização de um inventário de dados, especialmente dos dados pessoais, consistente em fazer um balanço alinhado ao artigo 37 da LGPD, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles. O mapeamento será estruturado em formato disponibilizado pela própria ANPD (Registro de Operações de Tratamento de Dados).

2.1.7 – Levantamento de Contratos relacionados a Dados Pessoais

O levantamento das atividades que tratam dados pessoais viabilizará a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribuirá para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

2.2 – Construção e Execução

Assim, na etapa de construção do programa de gerenciamento da privacidade, deve-se considerar os pontos de atenção na Figura 4;

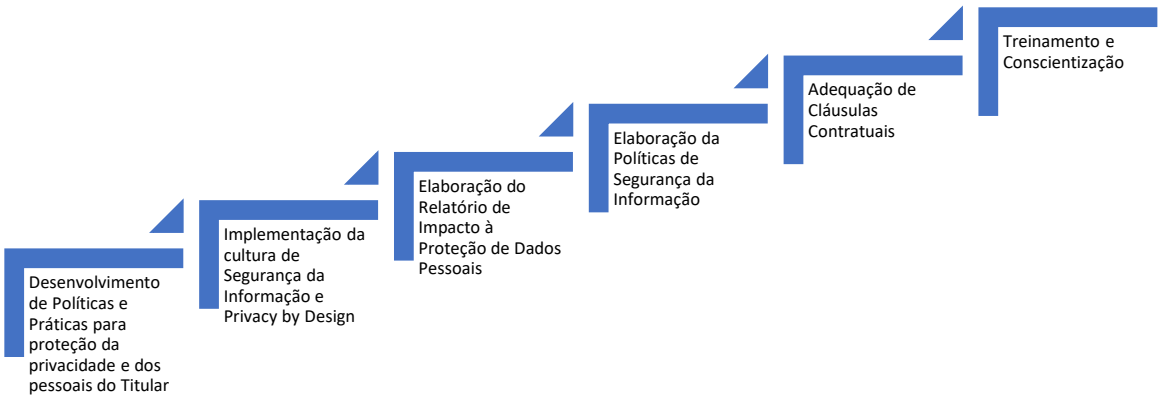


Figura 4. Marcos Etapa Construção e Execução

2.2.1 – Políticas e práticas para proteção da privacidade do titular de dados pessoais

Na construção e execução do **"PROGRAMA LGPD"** serão especificadas políticas e práticas para proteger a privacidade do titular de dados, garantindo que todos os usos dos dados pessoais sejam conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada.

Além das políticas e práticas, no **INSTITUTO ADECON,** papéis específicos dos colaboradores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais deverão ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos titulares em relação aos seus direitos quanto à privacidade da informação.

Informações como a finalidade e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, realizado na fase de Iniciação e Planejamento, serão úteis na construção das operações de tratamento. Tais informações auxiliarão na determinação dos detalhes do ciclo de vida dos dados pessoais, por exemplo, a finalidade do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

2.2.2 – Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design):

As informações do **"PROGRAMA LGPD**" deverão ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis. Capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção (privacy by design) seja instituída.

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do dado pessoal em sistemas, serviços, produtos ou processos.

Tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009), listados a seguir:

- Proativo, e não reativo; preventivo, e não corretivo: A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram.
- Privacidade deve ser o padrão dos sistemas de Tecnologia da Informação (T.I.) ou práticas de negócio: Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de T.I. ou prática de negócios.
- Privacidade incorporada ao projeto (design): A privacidade deve estar incorporada à arquitetura dos sistemas de T.I. e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em imple-

mentação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

- Funcionalidade total: A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do produto ou do serviço sejam atendidas.
- Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados: Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.
- Visibilidade e Transparência: A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança.
- Respeito pela privacidade do usuário: Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

2.2.3 – Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Ainda na etapa de Construção e Execução, o Relatório de Impacto à Proteção de Dados Pessoais - RIPD poderá ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela **Entidade** e serve tanto para a análise quanto para a documentação do tratamento

dos dados pessoais.

O RIPD visa descrever os 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.

2.2.4 – Medidas e Política de Segurança da Informação e Política de Privacidade

Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos.

Também é necessário a elaboração de uma Política de Privacidade, documento este informativo , pelo qual a **Entidade** transparece ao titular a forma como realiza o tratamento dos dados pessoais e a privacidade. A Política de Privacidade origina- se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º LGPD. Portanto, o documento é, ao mesmo tempo, um dever do controlador e um direito do titular. Assim, a **Entidade** deve informar ao titular do dado como ela fornece a privacidade necessária para que a confidencialidade seja garantida de forma eficiente e como os princípios abaixo são atendidos.

● Finalidade: Obrigatoriedade de tratamento somente para fins legítimos, específicos, explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I);

● Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II);

● Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, III);

● Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV).

● Qualidade dos dados: Critérios de qualidade dos dados, para garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V).

● Transparência: Critérios de transparência, para garantir, aos titulares, o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI).

● Segurança: Critérios de segurança, para que se utilize medidas 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 difusão (art. 6º, VII);

● Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII);

● Não discriminação: Critérios de não discriminação, para garantir que não se realize o tratamento de dados para fins discriminatórios ilícitos ou abusivos (art. 6º, IX).

● Responsabilização e prestação de contas: para que, para cada tratamento de dados se possa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X).

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de Construção do Programa de Governança em Privacidade.

É importante tomar medidas preventivas bem como a gestão de riscos, de incidentes, a violação dos dados e os direitos dos titulares precisam ser gerenciados.

2.2.5 – Adequação Cláusulas Contratuais

Para adaptar os contratos que impliquem no tratamento de dados pessoais, mapeados pelo Registro das Operações de Tratamento (ROPA) é importante rever os documentos vigentes e os dados já coletados. Poderá ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados em seu art. 6º. Como um dos princípios listados é a

transparência, torna-se essencial que o contrato apresente informações claras e objetivas, abordando, se pertinente:

- Delimitações claras e objetivas das responsabilidades do controlador e operador;
- A forma que é realizada a coleta e o tratamento de dados;
- A existência da possibilidade de o titular acessar os seus dados coletados;
- A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
- A existência da possibilidade de revogação do consentimento dado pelo titular;
- O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
- As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

2.3 – Monitoramento

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para a empresa a longo prazo. Assim sendo, esta última etapa do **Programa** abordará aspectos, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados. A Figura 5 apresenta os marcos da Etapa de Monitoramento, que serão apresentados a seguir.

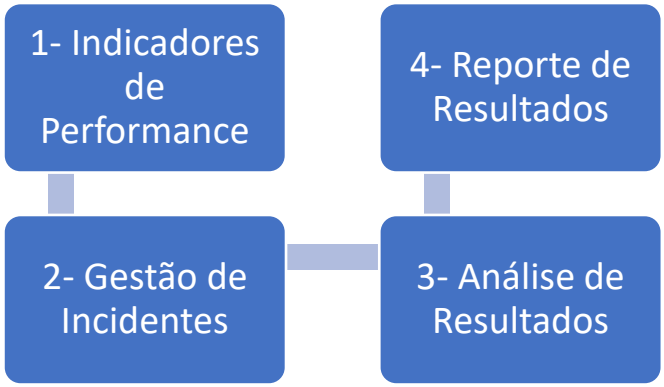


Figura 5. Marcos Etapa Monitoramento

2.3.1 – Indicadores de Performance

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho , assim como o status de outras iniciativas de privacidade. Recomenda-se o uso dos seguintes indicadores:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados
- Índice de serviços com contratos adequados;
- Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado
- Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos;
- Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço;

2.3.2 – Gestão de Incidentes

Será importante incluir 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 dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

Será válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou a empresa estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela empresa.

2.3.3 – Análise e Reporte de Resultados

A análise e o reporte de resultados também será indicada na etapa de monitoramento para demonstrar o valor do **PROGRAMA LGPD** para a alta direção. Mostrar a evolução das ações e resultados obtidos, bem como o papel da privacidade para o titular reforçam e fortalecem a cultura de privacidade dos dados: Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do Programa de Governança de Proteção de Dados, divulgação dos resultados entre as diversas áreas da **Entidade**- estabelecimento de uma estrutura de divulgação de resultados para a alta direção da **Entidade**, colaboradores e Associados.

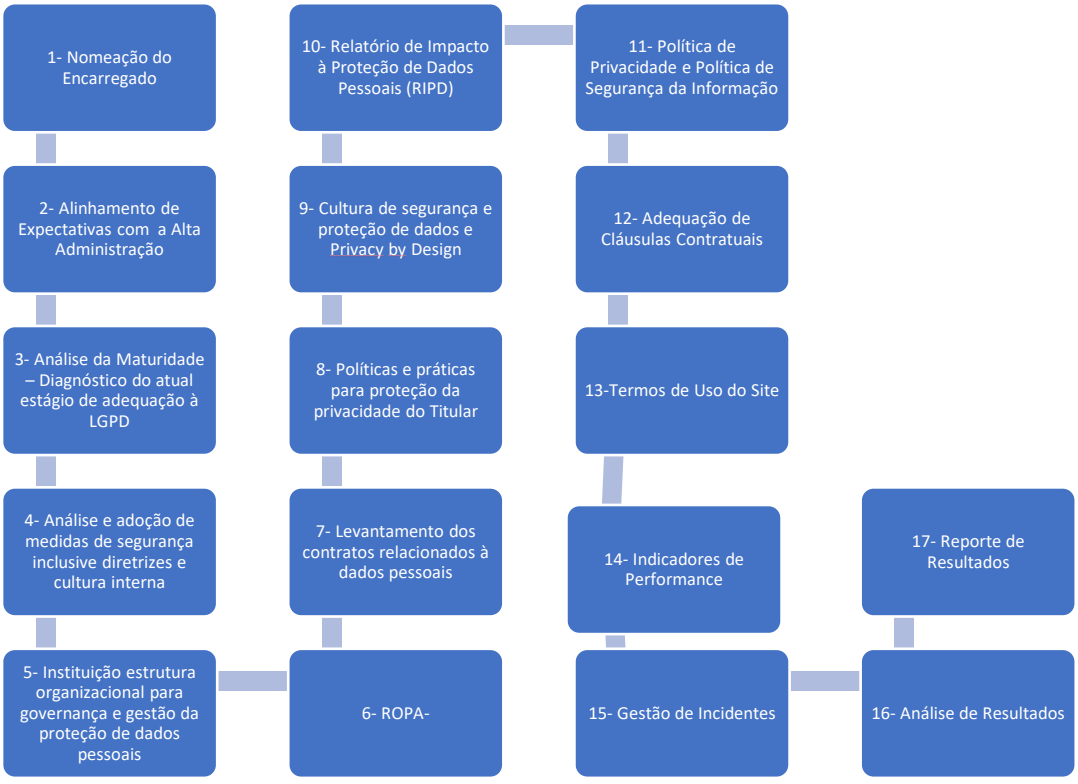


Figura 6. Passos das Etapas do **PROGRAMA LGPD**

APROVAÇÃO

Mario Molina Ribeiro
Presidente-Diretoria Executiva