PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

MARÇO DE 2026

Equipe Técnica do Grupo ADX

Adriano Lima Head de Operações	**Gessica Alcântara** Head de Projetos
Laís Gomes Head de Processos	**Hendrick Arcanjo** Head de Tecnologia
Saulo Santos Advogado	

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	27/02/2026	Grupo ADX	Elaboração do documento

SUMÁRIO

ÍNDICE DE FIGURAS

1 – Introdução

A Lei Geral de Proteção de Dados (LGPD) – Lei 13.709, foi sancionada em agosto de 2018, e trata dos direitos à privacidade e uso de dados pelas organizações brasileiras, sejam públicas ou privadas. Na prática, a lei define regras para coleta e a utilização dos diferentes tipos de dados dos usuários, seja em meios físicos ou digitais. O objetivo é impedir o uso indevido das informações coletadas prejudicando a privacidade da pessoa natural.

O gerenciamento da privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que as empresas precisam prover para conquistar a confiança dos clientes, parceiros e colaboradores e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade. Um Programa de Governança em Privacidade captura e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

2 – Objetivo

O objetivo deste documento é criar o programa de governança em privacidade, no âmbito da Ytech, para atender às exigências legais previstas na Lei Geral de Proteção de Dados (LGPD), no tocante a gestão de segurança da informação e privacidade.

3 – Conceitos Importantes

- **AUDITORIA** - Auditoria é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa, cujo objetivo é averiguar se elas estão de acordo com as planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e adequadas à consecução dos objetivos.
- **ANÁLISE DE RISCOS** - uso sistemático de informações para identificar fontes e estimar o risco;
- **ATIVOS DE INFORMAÇÃO** - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso;

- **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)** - órgão da APF responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 14 de agosto de 2018;
- de um sistema;
- **AVALIAÇÃO DE RISCOS** - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- **CONTROLES DE SEGURANÇA** - medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;
- **DADO PESSOAL** - informação relacionada a pessoa natural identificada ou identificável;
- **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;
- **ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)** - pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
- **GOVERNANÇA -** A raiz da palavra governança vem de um vocábulo grego que significa direção. o significado fundamental da governança é dirigir a economia e a sociedade visando objetivos coletivos. O processo de governança envolve descobrir meios de identificar metas e depois identificar os meios para alcançar essas metas.
- **PRIVACIDADE -** Qualidade do que é privado, do que diz respeito a alguém em particular: não se deve invadir a privacidade de ninguém
- **POLÍTICA DE GESTÃO DE RISCOS** - declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de risco;
- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** - documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);
- **TRATAMENTO DA INFORMAÇÃO** - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
- **VAZAMENTO DE DADOS** - transmissão não-autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

4 – Importância do programa de Governança em Privacidade (PGP)

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:

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

5 – Atores do PGP

Diante das características de um Programa de Governança em Privacidade – PGP apresentadas pela LGPD é necessário também destacar seus principais atores:

- **Titular dos dados pessoais** - qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso III do art. 2º da Lei Geral de Proteção de Dados);

- **Controlador** - pessoa natural ou jurídica, de direito público ou privado, a quem competem 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;

- **Operador** - 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);

- **Encarregado de proteção de dados** - corresponde a uma pessoa natural inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer - DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VII do art. 5º da Lei Geral de Proteção de Dados);

- **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.

6 – Estrutura do PGP

A estrutura do PGP apresentada 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 foi estruturado nas seguintes etapas, conforme **Figura 1**.

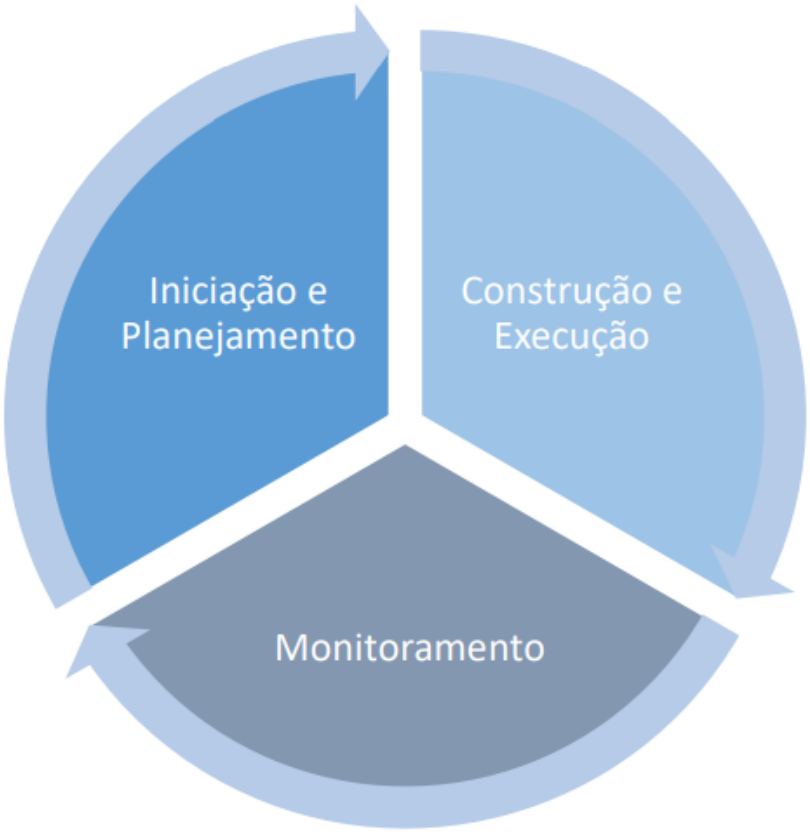

Figura 1 - Estrutura do PGP.

6.1 – Iniciação e planejamento

A etapa de Iniciação e Planejamento funciona como um grande diagnóstico e busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Essa etapa é constituída pelos processos apresentados na **Figura 2**, que serão detalhados a seguir.

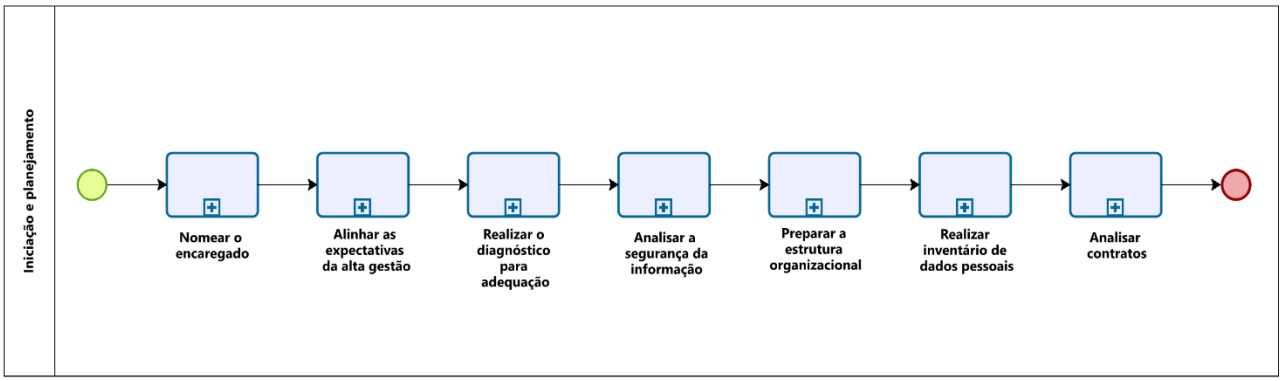

Figura 2 - Etapa de iniciação e planejamento.

6.1.1 – Nomear o encarregado de proteção de dados (DPO)

A nomeação do encarregado deve acontecer logo no início da estruturação do programa, pois além de ter que conhecer em detalhes todas as atividades, ele normalmente atua como o gerente do projeto de adequação à LGPD. O Encarregado é uma figura de natureza obrigatória, 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 de privacidade, 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.

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.

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

Para apoio ao trabalho do encarregado, a empresa deve criar um Comitê de Privacidade com representantes das áreas que mais tratam dados pessoais, como por exemplo: RH, marketing, TI, jurídico etc.

6.1.2 – Alinhar as expectativas com a alta gestão

Ao longo da etapa de Iniciação e Planejamento é importante ainda alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas. É importante destacar que o alinhamento com a Alta administração e a priorização de ações urgentes guiam o estabelecimento da cultura de proteção de dados na instituição. O sucesso do programa de conformidade depende do engajamento da alta gestão.

6.1.3 – Realizar o diagnóstico para adequação

O diagnóstico para adequação é uma fotografia da situação da empresa em um determinado momento. Este diagnóstico deve ser realizado pela equipe interna ou por uma consultoria especializada 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) identificação dos riscos associados ao tratamento dos dados.

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. 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:

- Quais dados pessoais são tratados?
- 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?
- Onde os dados são 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)?
- Quais sistemas e itens de infraestrutura de TI dão suporte aos dados pessoais dentro da organização?
- Quais bases legais autorizam o tratamento de cada dado pessoal existente na empresa?

A função da identificação dos riscos associados ao tratamento dos dados é entender qual a situação do atual gerenciamento de privacidade e proteção de dados pessoais frente às legislações aplicáveis, identificando as lacunas legais. Essa análise permite identificar quais lacunas existem

para a correta adequação às legislações aplicáveis. Algumas questões importantes para esse segundo momento são:

- 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)?

6.1.4 – Analisar a segurança da informação

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas. Nesse cenário, uma das ferramentas que podem auxiliar é o diagnóstico em relação às normas ISO 27001 e ISO 27701. Essas normas são referências de melhores práticas internacionais e ajudam de forma prática na definição de controles que aumentam a confidencialidade, integridade e disponibilidade das informações tratadas pela empresa.

6.1.5 – Preparar a estrutura organizacional

Recomenda-se ainda, como suporte para a estrutura do PGP, assim como para a realização das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da instituição. Essa estrutura deve contemplar entre outras coisas, equipe de apoio às atividades do encarregado e ferramenta para apoio à manutenção do programa de privacidade.

6.1.6 – Realizar o inventário de dados pessoais

o Inventário de Dados Pessoais representa um documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que a empresa faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

Para facilitar o gerenciamento dos dados e tratamento dos riscos, é extremamente importante identificar os dados pessoais e sensíveis através de fluxogramas visuais, deixando claro a origem, destino e local de armazenamento das informações. Outro ponto de extrema importância e o registro das operações de tratamento que delegam dados para operadores externos.

6.1.7 – Analisar os contratos relacionados a dados pessoais

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros. Os contratos que foram elaborados pela empresa precisam ser ajustados com cláusulas para adequação à LGPD e os contratos que foram elaborados pelos prestadores de serviço precisam ser identificados para realização da notificação aos operadores externos quanto a necessidade de também ajustarem as suas cláusulas contratuais.

6.2 – Construção e execução

Além do texto apresentado na LGPD, pode-se inferir da ABNT ISO/TR 18638:2019 que, um PGP deve ser projetado para proteger os direitos dos titulares em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes.

Os processos da etapa de Construção e Execução, apresentados na **Figura 3**, serão descritos e detalhados.

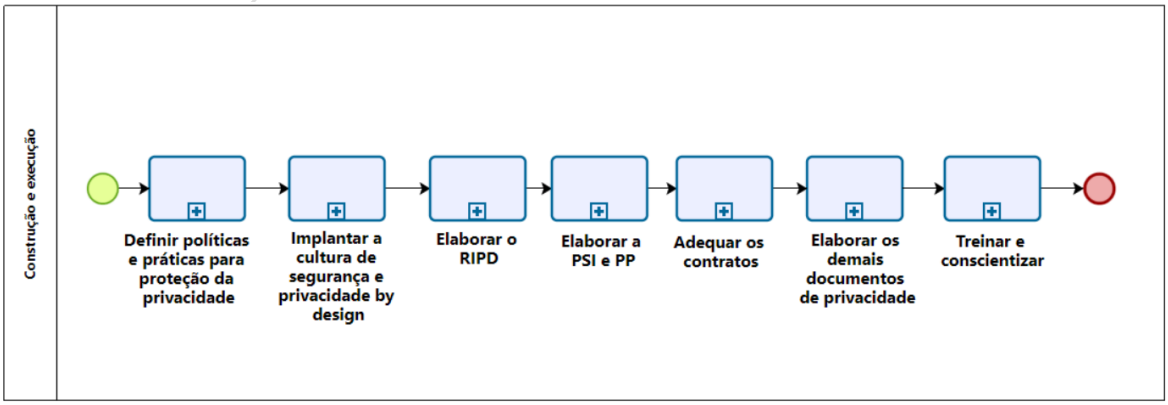

Figura 3 - Atividades da fase de Construção e Execução.

6.2.1 – Definir políticas e práticas para proteção da privacidade

Na construção de um PGP devem ser especificadas políticas e práticas para proteger a privacidade do titular, garantindo que todos os usos dos dados pessoais são 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, papéis específicos dos colaboradores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos cidadãos 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, são úteis na construção das operações de tratamento. Tais informações auxiliam 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.

6.2.2 – Implantar a cultura de segurança e privacidade by design

A promoção de uma cultura de segurança e proteção de dados deve ser tratada na etapa de construção e execução de um PGP com o intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da empresa como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos titulares. As informações do PGP devem 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 projeto, sistema, serviço, produto ou processo.

6.2.3 – Elaborar o relatório de impacto à proteção de dados

É ainda na etapa de Construção e Execução do PGP que o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição 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.

6.2.4 – Elaborar a política de segurança da informação e política de privacidade

Ainda na etapa de Construção e Execução do PGP, tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. 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. Desse modo, torna-se fundamental o desenvolvimento de uma política de segurança da instituição, bem como de uma política de privacidade de dados. Também é necessário a elaboração de uma Política de Privacidade. A Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. A Política de Privacidade, que faz parte do Termo de Uso, 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, o serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios abaixo são atendidos.

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de Construção do Programa de Governança em Privacidade. Segurança desde a Concepção (security by design) e a importância de se tomar medidas preventivas precisam ser consideradas, bem como a gestão dos riscos, a gestão de incidentes e a violação dos dados. Por fim, mas não menos importante, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, do ponto de vista do controlador, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

6.2.5 – Adequação dos contratos

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento, é importante rever os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que empresa revisite as cláusulas contratuais firmadas, mesmo após concluída a contratação. Pode 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;
- 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.

6.2.6 – Elaborar os demais 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 à LGPD. Neste roteiro, os seguintes documentos são destacados:

- Carta de nomeação do DPO;
- Ata de reunião nomeando o DPO e comitê de privacidade;
- Ficha de descrição de cargo do DPO;
- Organograma com a função do DPO ligado a alta administração;
- Plano de treinamentos sobre segurança e privacidade para os colaboradores;
- Modelo de LIA (Legitimate Interestes Assessment) ou teste de viabilidade da utilização da base legal do Legítimo Interesse;
- Registro de operação de tratamento de dados pessoais;
- Plano de gestão de riscos associados à LGPD;
- Planos de ações para adequação à LGPD;
- Plano de gestão de incidentes de segurança e privacidade;
- Modelo de notificação de violação de dados pessoais para um controlador;
- Modelo de notificação de violação de dados pessoais para a ANPD;
- Modelo de notificação de violação de dados para os titulares;
- Política de gerenciamento de fornecedores;
- Política de privacidade interna;
- Política de privacidade externa;
- Política de proteção de dados pessoais;
- Termos de uso;
- Política de classificação de dados pessoais;
- Modelos gerais de consentimento;
- Política para exercício de direitos dos titulares;
- Cláusulas em contratos com operadores;

- Cláusulas em contratos de trabalho;
- Política de auditoria no sistema de gestão da proteção de dados;
- Termo de confidencialidade para fornecedores;
- Termo de confidencialidade para colaboradores;
- Termo de consentimento de uso de imagem e voz para colaboradores, clientes, parceiros ou fornecedores.

6.2.7 – Treinar e conscientizar

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.

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. 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 com apoio da equipe de proteção de dados pessoais para desenvolver a cultura da privacidade dentro da instituição.

6.3 – Monitoramento

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para as empresas manterem o PGP a longo prazo. Assim sendo, esta última etapa do PGP aborda aspectos, detalhados nas próximas seções, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados. A **Figura 4** apresenta os marcos da Etapa de Monitoramento, que serão apresentados a seguir.

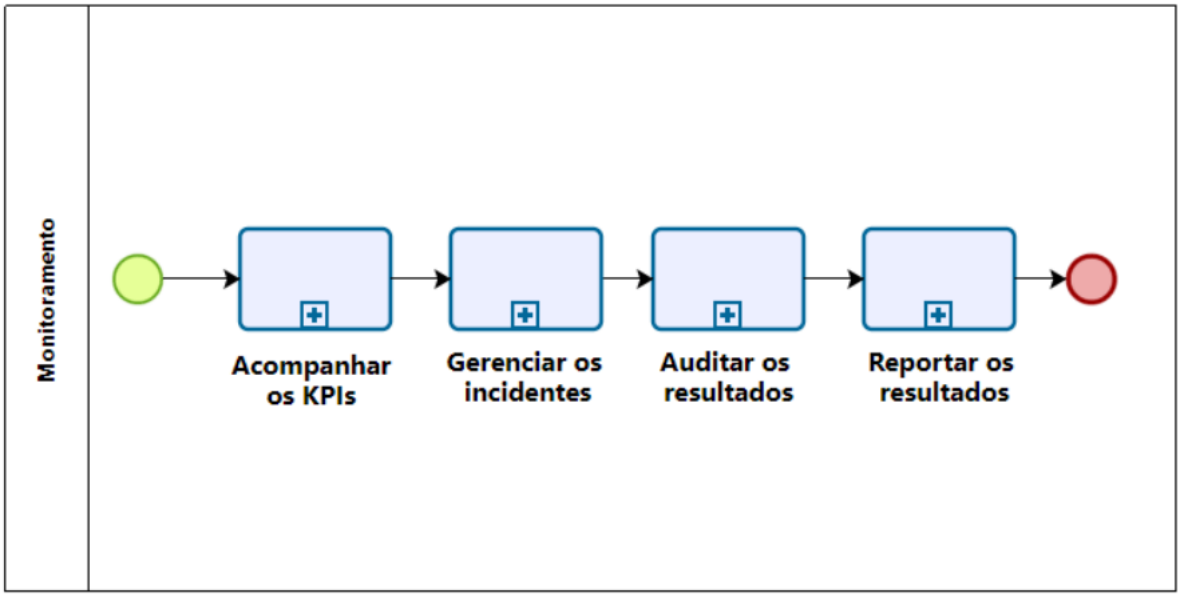

Figura 4 - Marcos da etapa de monitoramento

6.3.1 – Acompanhar os indicadores de performance (KPI)

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Programa de Governança em Privacidade 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;
- Número de requisições de titulares 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 / número de serviços com dados pessoais da empresa * 100;
- Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado / quantidade de serviços da empresa* 100;
- Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado / quantidade de serviços da empresa * 100;
- Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;
- Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço / quantidade total de controles de segurança e privacidade identificados para o serviço * 100.

6.3.2 – Gerenciar os incidentes

É importante incluir nesta etapa do PGP 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.

É 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 alta gestão. É recomendado ainda que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

6.3.3 – Auditar os resultados

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 Definição dos objetivos, planejamento da auditoria, condução, apresentação dos resultados e execução das ações corretivas.Ela pode ser conduzida internamente, em operadores de dados ou por terceiros independentes. Os detalhes podem ser vistos na **Figura 5**.

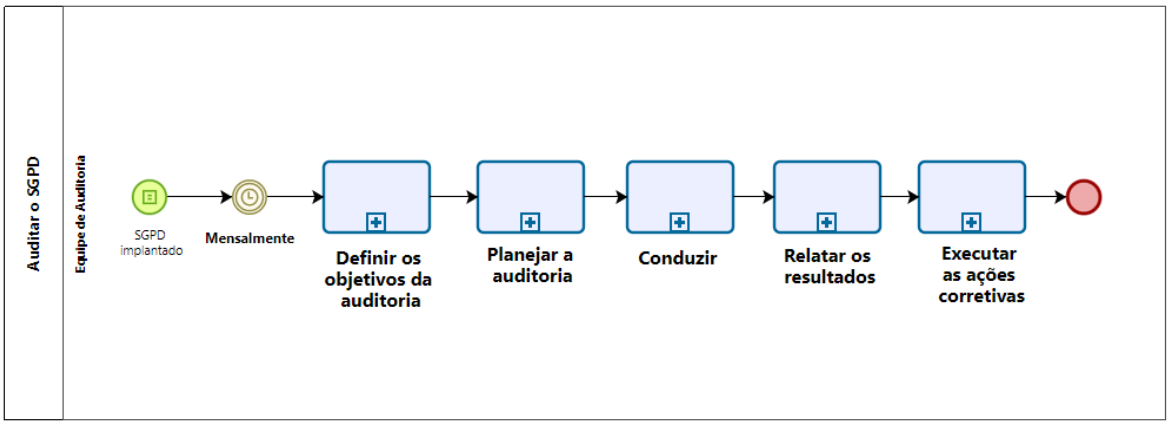

Figura 5 - Fases de uma auditoria.

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.

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).

6.3.4 – Reportar resultados

A análise e o reporte de resultados também é indicado na etapa de monitoramento para demonstrar o valor do PGP para a alta administração. Mostrar a evolução das ações e resultados

obtidos, bem como o papel da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados.

8 – Conclusão

O Programa de Governança em Privacidade de Dados é essencial, para garantir que a empresa esteja em conformidade com a LGPD.

A governança em privacidade é um programa que, além de promover o compliance e atuar na prevenção a sanções administrativas e judiciais, também (e principalmente) gera impactos positivos na operação da empresa e a valoriza. Como a governança de dados tem como um de seus pilares o compliance em matéria de privacidade e proteção de dados pessoais, acaba apresentando uma intersecção com a governança em privacidade. Ambas estão debaixo do guarda-chuva da governança corporativa, um sistema que dirige a organização por meio de boas práticas que contribuem para sua gestão e longevidade, bem como para o bem comum.

8 – Referências

- Lei nº 13.709 – Lei Geral de Proteção de Dados;
- Programa de governança em privacidade do MCOM;
- Guias Operacionais da LGPD do Governo Brasileiro;
- Carvalho et al. Relatório de Impacto à Proteção de Dados Pessoais: Aspectos práticos relevantes à luz da LGPD.
- CCGD. Guia de Boas Práticas para Implementação Lei Geral de Proteção de Dados na Administração Pública Federal.
- ICO. Auditing data protection: a guide to ICO data protection audits.
- ICO. Data Protection Impact Assessment.
- ITS. Lei Geral de Proteção de Dados Pessoais (LGPD) e Setor Público.
- Maia, F. LGPD: Aplicação Prática das Bases Legais.
- NIST. Privacy Framework.
- Yun, R. Programa de Adequação à Proteção de Dados Pessoais – Guia Prático.