PETROS

PROGRAMA DE PRIVACIDADE

MENSAGEM DA DIRETORIA

A Petros está implementando uma série de medidas para fortalecer a governança da Fundação, e este Programa de Privacidade é mais um passo nesta direção, acompanhando o movimento de grandes empresas, que têm investido cada vez mais em iniciativas para prevenir, detectar e corrigir desvios no tratamento de dados pessoais.

O programa é abrangente e está consolidado em princípios e instrumentos que envolvem maturidade da organização, segurança, governança e controle de riscos, com o objetivo de proteger a Petros de práticas que possam colocar em risco a privacidade dos titulares, o patrimônio dos participantes e a imagem da entidade.

Ferramenta fundamental neste processo é a observância da privacidade desde a criação de novas regras de negócios e as contratações de novos sistemas, até a exclusão de dados durante o ciclo de vida dos processos de negócios. Outro importante mecanismo é a Política de Proteção de Dados Pessoais, que foi integralmente revisada para contemplar as diretrizes do programa, indicando os papéis e as responsabilidades que devem ser adotados por toda organização. Criamos também processos internos e contratamos sistemas específicos para adaptá-los às melhores práticas de proteção de dados.

A implementação de um Programa de Privacidade desse porte reforça nosso compromisso com a segurança das informações, a ética e a governança, e é parte relevante do amplo trabalho para manter a Petros como um exemplo de conduta ética e referência no setor de Previdência Complementar.

Boa leitura!

Diretoria Executiva

INTRODUÇÃO

O programa de privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que as áreas precisam prover para conquistar a confiança dos titulares de dados e, ao mesmo tempo, cumprir com exigências apresentadas na Política de Proteção de Dados Pessoais (PL-0060). Um Programa de 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.

E, neste caso, a gestão de segurança e risco e suas respectivas partes responsáveis estão cada vez mais descobrindo requisitos complexos e restritivos a serem cumpridos para ter uma governança de privacidade eficaz durante o ciclo de vida de processamento de dados pessoais. Os planos de governança de privacidade devem ser implementados de forma ampla e inclusiva para gerenciar riscos crescentes nas mais diversas áreas. Melhorar a confiança de todas as partes interessadas exige que os gerentes de de segurança e risco expandam a frequência e a amplitude da comunicação, a fim de garantir que o uso de dados pessoais tenha uma finalidade definida e que os riscos específicos tenham sido mapeados e controlados.

O Programa de Privacidade foi estruturado em duas partes, sendo:

- O Capítulo 1, destacando seu escopo; e
- O Capítulo 2 ,tratando sobre suas etapas e como elaborá-las.

Este documento será permanentemente atualizado e ampliado para se adequar às diretrizes da Administração Nacional de Dados Pessoais (ANPD), tivemos como base o Guia de Elaboração de Programa de Governança em Privacidade divulgado pelo Governo Federal.

1 – PROGRAMA DE PRIVACIDADE

1.1 COMPROMETIMENTO E PATROCÍNIO DA ALTA ADMINISTRAÇÃO – CONSELHEIROS, PRESIDENTE E DIRETORES

A alta administração da Petros reconhece a importância dos valores, políticas, normativos e diretrizes que constituem o presente Programa de Privacidade, bem como o seu necessário patrocínio para que este tema avance muito além de normas e procedimentos. O programa deve ser pauta recorrente em reuniões de seus colegiados, com repercussões práticas em todos os níveis hierárquicos da Fundação, de modo a construir um ambiente espontâneo, conduzido pela demonstração efetiva deste comprometimento e patrocínio, em que os colaboradores e terceiros prezem por privacidade e proteção de dados pessoais para o cumprimento das medidas da Lei Geral de Proteção de Dados Pessoais.

O comprometimento da alta administração da Petros com o programa estende-se à não tolerância em face de eventuais atos lesivos à integridade da Fundação, devendo ser adotadas providências cabíveis, em todos os níveis hierárquicos, procedendo com a devida apuração e responsabilização pelos fatos que porventura deram origem à materialização da irregularidade.

Desta forma, o Programa de Privacidade conta com o patrocínio da alta administração da Petros perante os públicos interno e externo, podendo ser evidenciado, entre outras ações, pela participação e apoio nas etapas

de implementação do mesmo, adoção de uma postura ética que sirva de exemplo a todos os colaboradores e terceiros, aprovação das políticas e normativos relacionados ao programa, e garantia de provimento de recursos financeiros, materiais e humanos necessários à sua gestão.

1.2 O PROGRAMA

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º, as características mínimas de um Programa de Privacidade, conforme apresentado na Figura 1:

Figura 1 – Requisitos mínimos das boas práticas de governança

Tendo em vista as características do plano de governança de privacidade, o Programa de Privacidade proposto pela LGPD também precisa enfatizar seus principais participantes:

- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

● Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

● Encarregado: 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);

● 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.

Vale ressaltar que, ao contrário de um projeto, que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade. Pode-se, entretanto, criar projetos para se alcançar objetivos do programa. Na criação desses projetos, deve-se selecionar a metodologia mais adequada à realidade institucional. Após a escolha da metodologia, é necessário definir:

● Os objetivos, as metas e os indicadores;

● Os líderes responsáveis por cada frente de atuação do projeto (interação com o cidadão, operações de TI, segurança, jurídico, operadores, entre outros); e

● Os canais de comunicação com os líderes, cidadãos, com os operadores e com a Autoridade Nacional de Proteção de Dados - ANPD.

Por fim, recomenda-se ainda criar modelos padronizados para obtenção de respostas que subsidiarão relatórios para a alta administração.

1.3 – ESTRUTURAÇÃO

A estrutura do programa 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 em diferentes etapas, conforme ilustra a Figura 2, que serão descritas e detalhadas no próximo capítulo.

Figura 2. Etapas Programa de Privacidade

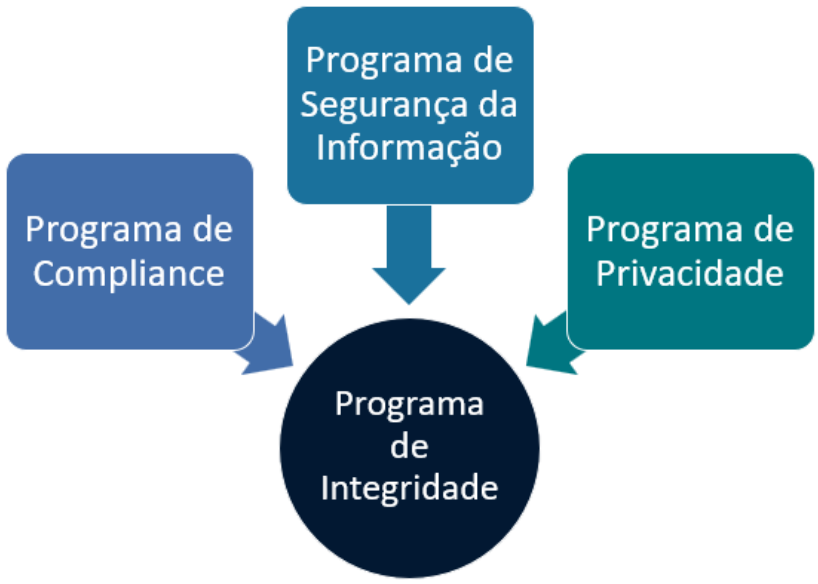
1.4 – SINERGIA

O Programa de Privacidade faz parte da estrutura de Governança Corporativa da Petros e está resguardado sob o Código de Condutas Éticas da Fundação, com relacionamento direto com os seguintes programas:

- Programa de Segurança da Informação; e
- Programa de Integridade.

Destacamos que as ações apresentadas no Programa de Integridade estão em linha com o Programa de Privacidade, como nos pontos destacados abaixo:

- Comprometimento e Patrocínio da Alta Administração – Conselheiros, Presidente e Diretores;
- Instância Interna Responsável pelo Programa de Privacidade – Setor de Compliance;
- Análise Periódica de Riscos;



2 – INSTRUMENTALIZAÇÃO DO PROGRAMA

2.1 – INICIAÇÃO E PLANEJAMENTO

A etapa de iniciação e planejamento busca 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

O início também deve incluir a criação de uma estrutura organizacional para compor o conhecimento de dados pessoais em toda a entidade ou órgão, além de supervisionar as três etapas de ação para criar e manter o Programa de Privacidade.

2.1.1 – O ENCARREGADO

A indicação do encarregado deve acontecer no início do Programa de Privacidade. Conforme o Art. 5º inciso VIII da LGPD, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Entre as competências de um encarregado apresentadas no Art. 41 da LGPD, pode-se citar:

1. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

2. Receber comunicações da autoridade nacional e adotar providências;

3. Orientar os colaboradores e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Demais competências:

5. Apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinado pelo Art. 37 da LGPD;

6. Conduzir ou aconselhar a elaboração do relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em qual tal documento é necessário – Art. 10 § 3º da LGPD; e

7. Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo Art. 50 da LGDP.

Além das competências elencadas pela LGPD, é importante que sejam considerados requisitos de experiência, conhecimentos e formação para o desempenho da função de encarregado. Assim, com base em inspiração resultante de pesquisa realizada em publicações associadas à General Data Protection Regulation (GDPR), recomenda-se que também sejam considerados para designação do encarregado os requisitos listados abaixo:

- Experiência na análise e elaboração de resposta de pedidos de acesso à informação demandados pela Ouvidoria e Central de Relacionamento;

- Conhecimentos multidisciplinares, incluindo as áreas de: gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção de privacidade e governança de dados; e

- Conclusão e Certificação relacionados a Proteção de Dados reconhecidos no mercado.

É importante, ainda, que o encarregado tenha independência para determinar a aplicação de recursos e as ações necessárias, bem como o pronto apoio das unidades administrativas no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais. Também deve ter amplo acesso à estrutura organizacional, investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir nas lacunas encontradas.

É válido destacar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros.

Diante da nítida importância do encarregado para a implementação da LGPD e, consequentemente, para o Programa de Privacidade, a seguir é apresentada uma proposta de tópicos a serem abordados, analisados e tratados pelo encarregado. É recomendado que o trabalho a ser executado pelo encarregado também seja dividido em etapas e os seguintes passos são sugeridos ao longo da proposta:

- Alinhamento de expectativas entre o encarregado e a alta direção da entidade;

- Alcance de credibilidade e valor entre os dirigentes da entidade;

- Apresentação, para as demais áreas (gerentes, diretores e coordenadores), do papel exercido pelo encarregado como relevante e influenciador;

- Como o encarregado pode servir e agregar valor ao órgão, dado o disposto na LGPD;

- Confirmar e garantir aos colaboradores da Petros que, enquanto representante interno da ANPD, seu papel deve ser uma assistência de grande valor, não um obstáculo;

- Priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de compliance da entidade;

- Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações;

- Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais serviços que utilizam dados pessoais da entidade.

- Apresentação de minuta de política de proteção de dados pessoais aos dirigentes da entidade, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;

- Projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário para, no mínimo, os próximos 12 meses, bem como a associação e o relacionamento aos pontos de atenção listados;

- Neste início sugere-se concentrar em poucos assuntos, balanceando entre as áreas de maior risco e as mais simples da entidade, quanto à privacidade dos dados.

---

1 Article 29 Data Protection Working Party WP 243 revi.01 The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data

2 The DPO Handbook Guidance seção 2.5.3

2.1.2 - ALINHAMENTO DE EXPECTATIVAS COM A ALTA ADMINISTRAÇÃO

Ao longo da etapa de Iniciação e Planejamento também é importante 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.

2.1.3 – MATURIDADE DA ORGANIZAÇÃO

Outro ponto a se analisar é a maturidade da organização, 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 (elaborando, por exemplo, a política de proteção de dados pessoais, bem como a comunicação sobre o uso de cookies). O índice de maturidade da organização é acompanhado por modelo já construído desde a concepção do plano de adequação à LGPD. Além de retratar o nível de adequação à LGPD, o índice de maturidade é utilizado como um índice de performance e será apresentado na etapa de item 2.3.1, sobre o Monitoramento do **Programa de Privacidade.**

2.1.4 – MEDIDAS DE SEGURANÇA

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 na construção do Programa de Privacidade como um todo são as seguintes normas técnicas relacionadas à segurança da informação e à gestão de riscos:

- ABNT NBR ISO/IEC 27001:2022. Sistemas de gestão da segurança da informação;
- ABNT NBR ISO/IEC 27002:2022. Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27005:2022. Gestão de riscos de segurança da informação;
- ABNT NBR ISO/IEC 31000:2018. Gestão de riscos – Diretrizes;
- ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001.

2.1.5 – ESTRUTURA ORGANIZACIONAL PARA GOVERNANÇA E GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS

Recomenda-se como suporte para a estrutura do Programa de Privacidade, 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, que atue de forma independente, conforme descrito no item 2.1.1.

2.1.6 – INVENTÁRIO DE DADOS PESSOAIS

Para obter um mapeamento dos dados pessoais utilizados pela entidade, recomenda- se a realização de um inventário de dados, especialmente dos dados pessoais. Conforme o Guia de Elaboração de Inventário de Dados Pessoais, o Inventário de Dados Pessoais representa documento primordial, pois registra o tratamento de dados pessoais realizados pela instituição, em alinhamento com o previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que a entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

Estruturado em formato de planilha eletrônica, é uma abordagem top/down, onde o serviço e os processos de negócio, e não os dados propriamente ditos, são analisados. Atualizado regularmente, o inventário permitirá atender tanto ao requisito de manter um registro das operações de tratamento de dados pessoais, quanto ao de auxiliar no controle do atendimento aos princípios, ambos estabelecidos pela LGPD.

2.1.7 – LEVANTAMENTO DE 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.

2.2 – CONSTRUÇÃO E EXECUÇÃO

O Programa de Privacidade deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes.

Assim, na etapa de construção de um programa de gerenciamento da privacidade, deve-se considerar os seguintes pontos de atenção:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Logo, neste capítulo, os marcos a serem alcançados na etapa de construção e execução, apresentados abaixo, serão descritos e detalhados.

2.2.1 – POLÍTICAS E PRÁTICAS PARA PROTEÇÃO DA PRIVACIDADE DO TITULAR

Na construção de um Programa de Privacidade devem ser especificadas políticas e práticas para proteger a privacidade do titular, 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. 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.

A finalidade do órgão ou entidade e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, realizado na fase de Iniciação e Planejamento, são informações úteis na construção das operações de tratamento. Elas auxiliam no detalhamento do ciclo de vida dos dados pessoais dentro da organização. Por exemplo, na definição da finalidade do tratamento, como, onde e por quanto tempo o dado é armazenado, entre outros.

2.2.2 – CULTURA DE SEGURANÇA E PROTEÇÃO DE DADOS E PRIVACIDADE DESDE A CONCEPÇÃO (PRIVACY BY DESIGN)

A promoção de uma cultura de segurança e proteção de dados deve ser tratada na etapa de construção e execução de um programa de privacidade, com o intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da Petros como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos titulares. As informações do programa de privacidade 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 diz 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. A privacy by design 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 TI ou das práticas de negócio: busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

- Privacidade incorporada ao projeto (design): a privacidade deve estar incorporada ao projeto, à arquitetura dos sistemas de TI e às práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação 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 projeto 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 visa 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)

É na etapa de Construção e Execução do programa de privacidade 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.

2.2.4 – MEDIDAS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E AVISO DE PRIVACIDADE

Ainda na etapa de construção e execução do Programa de Privacidade, 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 reter determinados dados tratados e se contratos precisam ser revistos. Desse modo, foram desenvolvidas a Política de Segurança da Informação (PL-0004), bem como a Política de Proteção de Dados Pessoais (PL-0060), sendo o Aviso de Privacidade o documento específico para o público externo.

O Aviso de Privacidade é um documento informativo pelo qual a Petros transparece ao titular a forma como a empresa realiza o tratamento dos dados pessoais e fornece privacidade ao titular, além de descrever a responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informar como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º da LGPD. Portanto, o documento é, ao mesmo tempo, um dever do controlador e um direito do titular. No Aviso de Privacidade, a empresa deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares seja garantida de forma eficiente e como os princípios listados 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).

Sugere-se que um Aviso de Privacidade contenha os seguintes tópicos:

- Controlador
- Operador
- Encarregado
- Quais dados são tratados
- Como os dados são coletados
- Qual o tratamento realizado e para qual finalidade
- Compartilhamento de dados
- Segurança dos dados
- Cookies
- Tratamento posterior dos dados para outras finalidades
- Tratamento irregular de dados
- Transferência internacional de dados

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de construção do Programa de Privacidade. Segurança desde a Concepção (security by design) e a importância da adoção de 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, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais essas informações precisão constar previamente publicadas no Aviso de Privacidade.

2.2.5 – ADEQUAÇÃO DE CLÁUSULAS CONTRATUAIS

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 a Petros revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o processo de seleção. 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 como é realizada a coleta e o tratamento de dados;
- A possibilidade de o titular acessar os seus dados coletados;
- A forma como é realizada a correção, o bloqueio ou a eliminação de dados mediante solicitação do titular;
- A 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 as entidades manterem o Programa de Privacidade a longo prazo. Assim sendo, esta última etapa do programa 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. Abaixo apresentamos os marcos da etapa de monitoramento, que serão apresentados a seguir.

2.3.1 – INDICADORES DE PERFORMANCE

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Programa de Privacidade, assim como o status de outras iniciativas de privacidade. Utilizaremos os seguintes indicadores:

- Percentual de implantação do programa de privacidade;
- Grau de maturidade da Petros;
- Percentual de respostas conforme SLAs definidos (máximo 15 dias);
- Tempo médio de atendimento aos direitos dos titulares de dados;
- Número de requisições de titulares de dados;
- Número de reclamações de titulares de dados;
- Índice de conscientização de privacidade;
- Total de violação de dados;
- Tempo médio de resposta a violações; e
- Tempo médio entre violações.

2.3.2 – GESTÃO DE INCIDENTES

É importante incluir nesta etapa do Programa de Privacidade um processo de gestão de incidentes, que registre os incidentes de segurança da informação e de privacidade ocorridos e 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 entidade está exposta, considerando os critérios de aceitabilidade de riscos definidos pelo Petros.

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

2.3.3 – ANÁLISE E REPORTE DE RESULTADOS

A análise e o reporte de resultados são indicados para demonstrar o valor do Programa de Privacidade para a alta administração. Mostrar a evolução das ações e os resultados obtidos, bem como o papel da privacidade para o titular, reforçam e fortalecem a cultura de privacidade dos dados.

2.3.4 – AGENTE DE PRIVACIDADE

Agente de Privacidade é o ponto focal da área de negócio da Petros e o Encarregado, este indicado pelo Gerente Setorial ou manifestação própria, deve permitir que cada agente de privacidade cumpra suas funções, introduzindo um programa de treinamento personalizado. O treinamento inclui tópicos como processamento de dados e períodos de retenção de dados, mas também deve cobrir uma visão geral das políticas internas, bem como dos sistemas corporativos de privacidade e das responsabilidades e deveres associados ao Agente. Uma parte importante do currículo de treinamento trata da revisão inicial dos processos das equipes, com foco no tratamento de dados pessoais e na manutenção da documentação regulatória, como o Relatório de Impacto de Dados Pessoais e o Inventário de Dados Pessoais.

3 GLOSSÁRIO

Alta Administração: conjunto de dirigentes que integram o nível estratégico da Fundação com poderes constituídos pelo Estatuto Social para estabelecer as políticas, os objetivos e a direção geral da Petros.

Análise de Riscos: processo de compreender a natureza do risco e determinar a sua magnitude, expressa por meio da combinação de impacto e probabilidade, fornecendo base para as decisões sobre o tratamento do risco.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Auditoria: processo de avaliação independente da saúde financeira de uma empresa (ou instituição financeira), realizada por profissionais sem nenhum vínculo permanente com a empresa (ou instituição financeira). O objetivo desse procedimento é dar maior credibilidade às informações divulgadas, bem como maior segurança para os usuários destas informações.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Colaboradores: são os empregados da Fundação, os empregados cedidos pela patrocinadora, estagiários, membros do Conselho Deliberativo, do Conselho Fiscal e da Diretoria Executiva;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Dado pessoal: Informação ou dado relacionado à pessoa natural identificada ou identificável.

Segurança da Informação: é a proteção da informação de vários tipos de ameaças para garantir a continuidade e minimizar o risco ao negócio, além de maximizar o retorno sobre os investimentos e as oportunidades de negócio. É obtida a partir da implementação de um conjunto de controles adequados, que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

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

Violação de dados pessoais: situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.

4 REFERÊNCIAS

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS Nª 13.709/18, Governo Federal em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html

ASSOCIAÇÃO BRASILEIRA DE NORMASTÉCNICAS. NBRISO/IEC29100 DE 03/2020

Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade

ASSOCIAÇÃO BRASILEIRA DE NORMASTÉCNICAS. NBRISO/IEC27701 DE 11/2019 Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

GUIA DE BOAS PRÁTICAS LEIGERAL DE PROTEÇÃO DE DADOS (LGPD), Governo Federal em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

GUIAS OPERACIONAIS PARA ADEQUAÇÃO À LGPD, Governo Federal em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

GUIA DE ELABORAÇÃO DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE, Governo Federal em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf

PETROS