PROCESSO DE ELABORAÇÃO DO RIPD

JUNHO DE 2022

Equipe Técnica do Grupo ADX

Adriano Lima Head de Projetos	**Adgenison Nascimento** Head de Negócios
Hendrick Arcanjo Consultor de Tecnologia	**Gessica Alcântara** Gestora de Projetos
Saulo Santos Advogado	

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	22/06/2022	Grupo ADX	Elaboração do documento

SUMÁRIO

ÍNDICE DE FIGURAS

1 – OBJETIVO

O objetivo deste documento é definir a metodologia para elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), no âmbito do SENAC AL, 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

- **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 também 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;
- **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);
- **RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS** - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- **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 – RIPD

O relatório de impacto à proteção de dados pessoais (RIPD) é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Ele também apresenta as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme o artigo 5º, inciso XVII da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). A análise de impacto de todos os processos críticos foi realizada na auditoria de segurança e a partir de agora será preciso definir um modelo para esse documento, bem como quais processos precisam ter esse modelo preenchido para futuras solicitações da ANPD.

Os benefícios da elaboração do RIPD para os titulares dos são:

- Garantia de que as organizações que usam suas informações seguiram as melhores práticas relacionadas a segurança e proteção de dados.
- Um projeto que tenha sido submetido a um RIPD deve ter menos privacidade intrusiva e, portanto, menos propensão a afetar os indivíduos de maneira negativa;
- Melhora nos níveis de transparência e na facilidade de compreensão sobre como e por que as informações estão sendo usadas.

Os benefícios da elaboração do RIPD para a empresa são:

- Melhora a forma como elas usam informações que impactam a privacidade individual;
- Ajuda a entender melhor os clientes e suas preocupações com privacidade;
- Reduz a probabilidade de não cumprirem suas obrigações legais;
- Reduz custos na resolução de problemas de privacidade(by design);
- Melhoria a segurança geral de processos e sistemas.

A obrigação da elaboração do RIPD é do controlador. Inclusive podendo ser terceirizada. O DPO deve dar apoio a todo o processo e registrar o seu parecer em relação a autorização do tratamento de dados analisado.

A **Figura 1** mostra os principais papéis na elaboração de um RIPD.

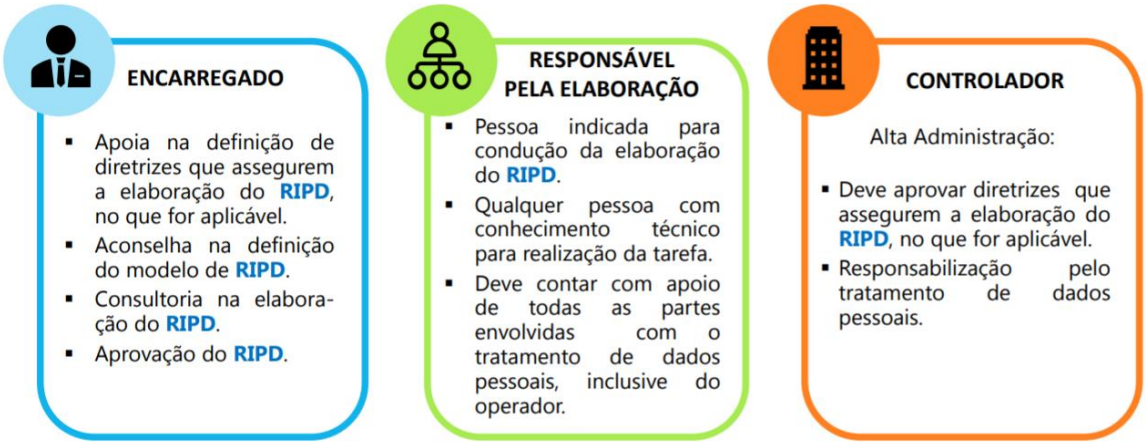

Figura 1 - Papéis envolvidos na elaboração do RIPD.

5 – ETAPAS PARA ELABORAÇÃO DO RIPD

O processo de elaboração do RIPD deve ser sistematizado dentro da empresa e deve ser conhecido por todos. O mesmo deve ser instanciado toda vez que um novo tratamento de dados pessoais for necessário. As etapas para elaboração do RIPD podem ser vistas na **Figura 2**.

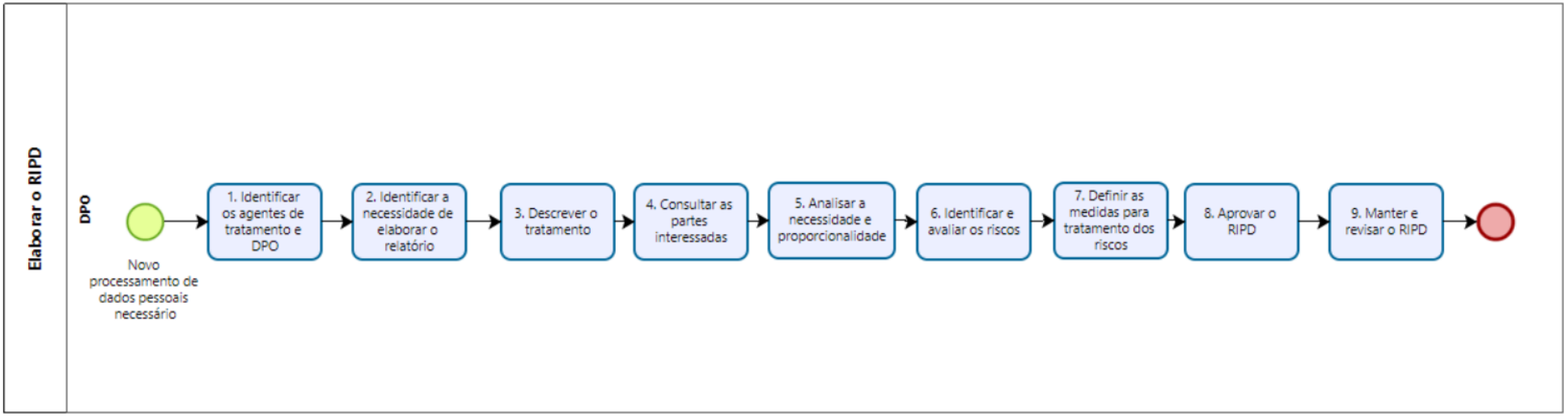

Figura 2 - Processo de elaboração do RIPD.

Etapa 1: Identificar os agentes de tratamento e DPO : consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art. 5º da LGPD).

Etapa 2: . Identificar a necessidade de elaborar o Relatório: consiste em justificar a verdadeira necessidade de elaboração do documento, descrevendo se ele será único para um tratamento de dados pessoais ou se teremos vários tratamentos agrupados. Os casos previstos pela ANPD para solicitação do RIPD são:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
- A qualquer momento sob determinação da ANPD (art. 38).

Etapa 3: Descrever o tratamento: consiste na descrição detalhada do tratamento de dados pessoais dentro do contexto da organização. Devem ser registrados a natureza do tratamento (como), o escopo (abrangência), o contexto (fatores internos e externos) e a finalidade (bases legais).

Etapa 4: Consultar as partes interessadas: consiste na consulta às partes interessadas relevantes, internas e externas, a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Etapa 5: Analisar a necessidade e proporcionalidade: consiste em demonstrar que as operações realizadas sobre os dados pessoais limitam o 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.

Etapa 6: Identificar e avaliar riscos: consiste em descrever medidas, salvaguardas e mecanismos de mitigação de risco.

Etapa 7: Definir medidas para tratar os riscos: consiste em adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Etapa 8: Aprovar o relatório: consiste em formalizar o RIPD por meio da obtenção das assinaturas das partes indicadas como responsáveis pela aprovação do Relatório.

Etapa 9: Manter e revisar o RIPD: consiste em revisar frequentemente o documento para adaptação a mudanças no ambiente corporativo ou na própria LGPD.

8 CONCLUSÃO

Além do requisito legal para minimização dos riscos ao tratamento de dados pessoais, o RIPD também prepara a empresa para um patamar mais alto em segurança e proteção de dados. Essa prática gera um diferencial de mercado que potencializa a marca e aumenta o valor gerado para os seus clientes.

É importe a consciência de todos no seguimento do processo para sempre que possível realizar a análise da necessidade de desenvolvimento desse documento. O DPO deve ser envolvido em todas as decisões estratégicas envolvendo novos, projetos, processos, sistemas, campanhas e demais ações que manipulem dados pessoais.

9 REFERÊNCIAS

- Lei nº 13.709 – Lei Geral de Proteção de Dados;
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;
- Norma ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Técnicas de Segurança;
- Norma ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação;
- Norma ABNT NBR ISO 27701:2019 – Técnicas de Segurança – Extensão da ABNT ISSO/IEC 27001;
- Norma ABNT NBR ISO 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- Norma ABNT NBR ISO 29134:2017 – Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade – Diretrizes;
- Norma ABNT NBR ISO 29151:2017 – Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais
- Guias Operacionais da LGPD do Governo Brasileiro;