GUIA PARA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Defensoria Pública BAHIA

Defensoria Pública
BAHIA
Instituição essencial à Justiça

GUIA PARA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Salvador-Ba

2024

Av. Ulisses Guimarães, nº 3386, Ed. MultiCab Empresarial, CAB, Salvador, Bahia CEP: 41745-007
Tel.: 3117-9002. E-mail: gabinete@defensoria.ba.def.br

INTRODUÇÃO

A elaboração de Relatório(s) de Impacto à Proteção dos Dados Pessoais (RIPD) configura etapa fundamental no processo de adequação da Defensoria Pública do Estado da Bahia à Lei Geral de Proteção de Dados (Lei nº 13.709/2018), **estando prevista no Eixo 4 (Falhas, Riscos e Tratamentos) do Plano de Ação do Núcleo de Proteção de Dados.**

Diretamente relacionado à Governança na Instituição, trata-se de documento essencial para a verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela Defensoria, servindo tanto como instrumento de análise quanto para fins de documentação e registro.

Tem por objetivo fundamental a identificação e a avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados, bem como das medidas a serem adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Encontra previsão no art. 5º, XVII da LGPD:

> *XVII - 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;*

Ademais, nos termos do parágrafo único do art. 38 da referida Lei, o Relatório de Impacto deverá conter:

> *Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de*

> *tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*
>
> *Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotado*s.

Acerca da necessidade de elaboração do RIPD, a melhor descrição encontra-se no Guia de Boas Práticas da LGPD, disponibilizado pelo Governo Federal[1]:

> Além dos casos específicos previstos pela LGPD(...), é indicada a elaboração ou atualização do Relatório de Impacto **sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais**, resultante de: uma tecnologia, serviço ou outra nova iniciativa **em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados**; rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º); tratamento de 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**" (LGPD, art. 5º, II); processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20); tratamento de

[1] GOVERNO FEDERAL. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 29/08/2024

dados pessoais de **crianças e adolescentes** (LGPD, art. 14); tratamento de dados que possa **resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento** (LGPD, art. 42); tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º); **tratamento no interesse legítimo do controlador** (LGPD, art. 10, § 3º); alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Nesse sentido, considerando que a Defensoria Pública do Estado da Bahia trata diariamente com dados pessoais e dados pessoais sensíveis, tanto dos assistidos quanto dos Defensores, Servidores e demais colaboradores, e como forma de dar mais um passo à total adequação da Instituição à Lei Geral de Proteção de Dados, faz-se necessária a elaboração de Relatório(s) de Impacto à Proteção aos Dados Pessoais, ao menos em relação aos processos mais críticos.

Por tais motivos, o presente documento, elaborado pelo Núcleo de Proteção de Dados da Defensoria Pública do Estado da Bahia, com base no Guia de Boas Práticas da LGPD, de autoria do Governo Federal, visa a explicar os principais aspetos desta ferramenta de proteção aos dados pessoais, para fins de conhecimento e progressiva familiarização da Instituição.

DA ELABORAÇÃO DO RELATÓRIO DE IMPACTO

O RIPD pode ser elaborado em diversas etapas no processo de adequação de uma Instituição à LGPD, seja antes de iniciar o tratamento de dados pessoais, na fase

inicial do programa ou projeto que tem o propósito de usar esses dados, seja durante a execução das atividades, sempre que o tratamento de dados o impuser. No caso da Defensoria Pública do Estado da Bahia, a elaboração do relatório de impacto se fez viável no momento em que foi concluída a primeira fase do mapeamento dos processos em trâmite na Instituição.

A identificação e descrição dos processos de tratamento[2] de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.

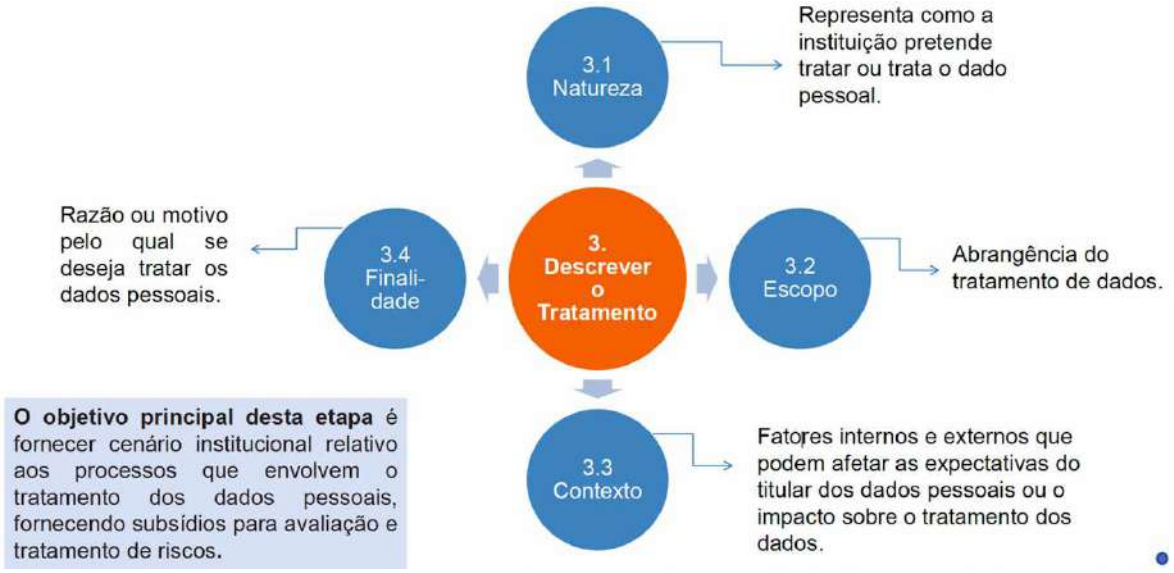

Figura 1 - Descrição do Tratamento (.gov. br)

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos. Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

Entende-se ser mais adequado à realidade da Defensoria Pública especificar cada um dos achados, de modo a que a Instituição, através de seus setores e

[2] À luz do art. 5º, X, da LGPD, "tratamento" constitui 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.

coordenações, promovam mudanças que assegurem confluência com os ditames previstos na LGPD.

Considerando que o RIDP trata-se de um *documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, que preveem medidas, salvaguardas e mecanismos de mitigação de risco,* torna-se prudente existirem duas frentes.

A primeira frente envolve os achados dos Encarregados de Proteção de Dados Pessoais na análise dos processos, momento em que se torna imprescindível uma prévia reunião com os setores competentes para instruir de forma adequada o RIPD e, como uma segunda frente, há a obrigação de todos os Coordenadores, na sua dinâmica operativa, identificarem processos que podem gerar riscos às liberdades civis e aos direitos fundamentais envolvendo dados pessoais e, que devem, imediatamente, prever medidas, salvaguardas e mecanismos de mitigação destes, comunicando ao NPD para elaboração de RIPD.

Passa-se a analisar os elementos do RIPD, tendo como base o Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD), do Governo Federal:

a. Da Natureza do tratamento

A natureza do tratamento representa como a instituição pretende tratar ou trata o dado pessoal, sendo importante descrever, por exemplo, como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados; a fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.); se há o compartilhamento de dados pessoais com outros órgãos, entidades ou empresas os dados pessoais serão compartilhados; quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam.

Importante informar ainda se a Instituição adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais, a fim de possibilitar a identificação de possíveis riscos resultantes de tal uso, bem como a informação se há medidas de segurança atualmente adotadas.

Destaca-se que, o Guia disponibilizado pelo Governo Federal aduz a **importância de, nessa fase, consultar um diagrama ou outra documentação análoga que demonstre os fluxos de dados da instituição.**

b. Do escopo do tratamento.

O escopo representa a **abrangência do tratamento** de dados. Nesse sentido, merece importante destaque as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis; o volume de tais dados; a extensão e frequência em que os dados são tratados; o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados. Descreve ainda o número de titulares de dados afetados pelo tratamento e a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em baixa ou alta escala.

c. Do Contexto do tratamento

Para descrição do contexto do tratamento, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados. O levantamento das seguintes informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;

- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;

- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

- destacar se o tipo de tratamento realizado sobre os dados é

condizente com a expectativa dos titulares dos dados pessoais.

• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;

• destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

d. Da finalidade do tratamento

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É de suma importância estabelecer claramente a finalidade, pois é ela que j**ustifica o tratamento** e fornece os elementos para informar o titular dos dados. Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os artigos 7º e 11º da LGPD, como: cumprimento de obrigação legal ou regulatória pelo controlador; execução de políticas públicas; alguma espécie de estudo realizado por órgão de pesquisa; execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do próprio titular; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física do titular ou de terceiro, bem como para tutela da saúde.

Destaca-se ainda, o tratamento feito com a finalidade de atender aos interesses legítimos do controlador ou de terceiro; de proteção do crédito e de garantia da prevenção à fraude e à segurança do titular, dentre outros. Desse modo, ao detalhar a finalidade do tratamento dos dados pessoais, é importante ainda indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, bem como os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

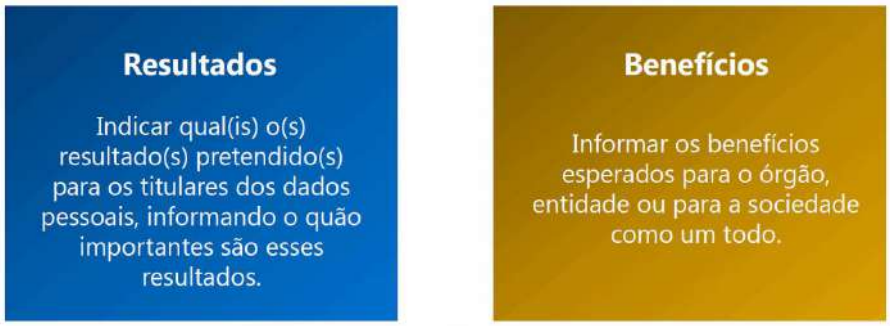

Figura 2 Resultados e Benefícios (.gov.br)

e. Da Identificação das partes interessadas consultadas

Nesta etapa da elaboração do Relatório de Impacto, importa identificar as partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento. Assim, é importante a identificação de quais partes foram consultadas, bem como o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise.

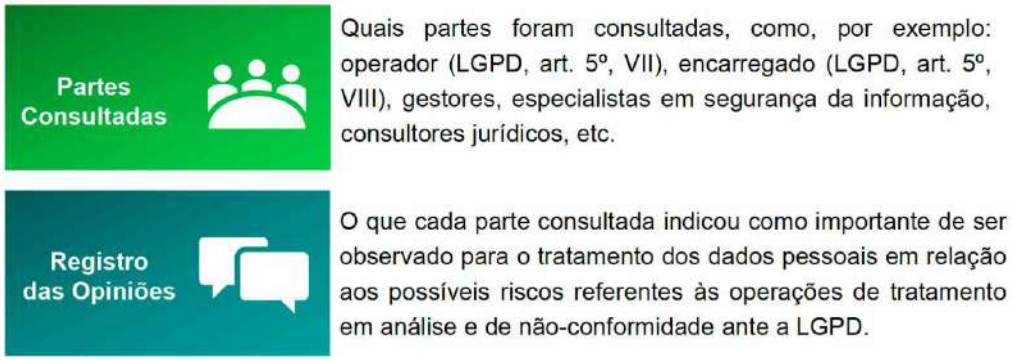

Figura 3 Partes Consultadas (.gov.br)

Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da

informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

f. Da descrição da necessidade e proporcionalidade

Nessa fase de elaboração do RIPD, importa descrever como a instituição avalia a necessidade e proporcionalidade dos dados. Visa 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 (LGPD, art. 6º, III).

Nesse sentido, cabe destacar, além da fundamentação legal para o tratamento dos dados pessoais, a forma com que será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados) e minimização dos dados; quais medidas são adotadas a fim de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição controladora (LGPD, art. 5º, VI).

Ademais, caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), hipótese residual de tratamento, faz-se necessário demonstrar sua indispensabilidade e que esse processamento de fato auxilia no propósito almejado. Deve-se demonstrar ainda, como estão implementadas as medidas que assegurem o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.

g. Da identificação e avaliação dos riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco“. Antes de defini-las, contudo, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, importa definir-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Para tanto, conforme consta no Guia de Boas Práticas para Adequação à LGPD do

Governo Federal[3], parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste Relatório foram inspirados no referido documento.

A tabela abaixo demonstra **valores estipulados para classificação dos ricos de acordo com o grau (baixo, moderado ou alto) de probabilidade de sua ocorrência e de impacto gerado, caso ocorra**:

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Tabela 1 Parâmetros Escalares (.gov.br)

A figura a seguir apresenta a **Matriz Probabilidade x Impacto, resultante do produto entre os valores atribuídos,** sendo instrumento de apoio para a definição dos critérios de classificação do nível de risco.

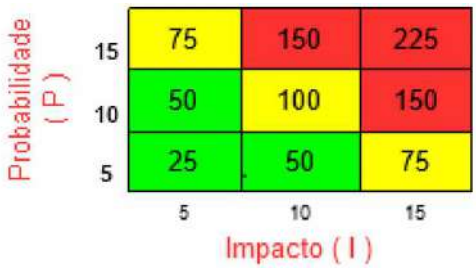

Figura 4 Matriz Probabilidade x Impacto

[3] GOVERNO FEDERAL. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 29/08/2024

O **produto da probabilidade pelo impacto de cada risco** deve se enquadrar em uma região da matriz apresentada pela Figura 4. O risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Desse modo, é importante destacar que o **gerenciamento de riscos** relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016[4].

De acordo com a referida Norma, a avaliação de risco consiste em um processo permanente de identificação e análise dos riscos relevantes que impactam o alcance dos objetivos da organização e determina a resposta apropriada ao risco.

O processo de identificação e avaliação de riscos envolve **elencar os eventos de risco, a probabilidade, o impacto e o nível de risco**. Para tanto, serão utilizados riscos de privacidade obtidos da norma ISO/IEC 29134:2017, seção 6.4.4, indicados pelo Governo Federal, sem prejuízo de eventuais outros riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais, conforme demonstrado na tabela abaixo:

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	NÍVEL DE RISCO (PxI)
R01	Acesso não autorizado			
R02	Modificação não autorizada			
R03	Perda			
R04	Roubo			

[4] Art. 2o Para fins desta Instrução Normativa, considera-se: (...) VII - gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização; (...) XIII - risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade; XIV - risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto; XV - risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco.

R05	Remoção não autorizada			
R06	Coleção excessiva			
R07	Informação insuficiente sobre a finalidade do tratamento			
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).			
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).			
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.			
R11	Retenção prolongada de dados pessoais sem necessidade.			
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.			
	Outros riscos identificados			

Tabela 2 - Riscos referentes ao tratamento de dados pessoais

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

h. Da identificação de medidas para tratar os riscos

Sabe-se que os agentes de tratamento devem 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).

A coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa “Identificar e avaliar riscos”.

Ademais, é importante ressaltar que a instituição nem sempre precisa eliminar todos os riscos, o que, por si só, não é factível. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto –, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação. No entanto, é necessário avaliar a real necessidade de se prosseguir com as operações de tratamento dos dados pessoais caso haja um risco residual de nível alto.

A seguir, são apresentados **exemplos de medidas** para lidar com os riscos identificados, bem como o risco residual, ou seja, o risco ainda existente após a adoção de medidas necessárias:

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S)[3] APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico. 2. Desenvolvimento seguro. 3. Segurança em Redes.	Reduzir	5	10	50	Sim

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: **Reduzir, Evitar, Compartilhar e Aceitar.**

2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

3. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela.

Neste momento, e a critério do responsável pela elaboração do RIPD, a coluna “Medida(s)” também pode ser preenchida de forma mais detalhada, indicando os principais aspectos da medida segurança ou controles de segurança adotados para tratar o risco de forma a propiciar mais visibilidade em relação ao tratamento do risco.

i. Da aprovação do Relatório

Esta etapa visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas dos responsáveis pela elaboração do RIPD, no caso, o encarregado de proteção de dados, os Coordenadores e chefes de setores, bem como a ciência das autoridades que representam o controlador.

O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

j. Da Revisão

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição. De uma forma geral, essa mudança pode ser motivada por alteração:

• significativa na finalidade do tratamento de dados pessoais;

• que impacte no processo de como esses dados são tratados;

• expressiva na quantidade de dados pessoais coletados; e

• no contexto do tratamento de dados resultantes de identificação de falha de segurança, uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

Cumpre destacar que as orientações referentes à identificação da necessidade de elaborar ou atualizar o RIPD constantes do item 2.5.2.2 deste documento também contribuem para a identificação de casos em que o Relatório de Impacto deve ser atualizado. A instituição deve manter revisão do RIPD a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

CONCLUSÃO

Ante o exposto, torna-se evidente que a elaboração de Relatório(s) de Impacto à Proteção de Dados Pessoais, acerca dos principais processos existentes na Defensoria Pública do Estado da Bahia, mostra-se fundamental para a completa adequação da Instituição às exigências das normas de proteção de dados pessoais, em especial a LGPD (Lei nº 13.709/18).

Não obstante, a elaboração do referido Relatório de Impacto trata-se de etapa prevista **no Eixo 4 (Falhas, Riscos e Tratamentos) do Plano de Ação do Núcleo de Proteção de Dados,** já aprovado por esta Instituição, e de documentação passível de requisição pela Autoridade Nacional de Proteção de Dados em eventual auditoria, sendo de suma importância à completa adequação da DPE/Ba à proteção de dados pessoais, na medida em que identifica riscos potenciais de inconformidade com a LGPD e propõe medidas para mitigação desses riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

INTERNETIONAL STANDART. ISO/IEC 29.134/2017.Information technology — Security techniques — Guidelines for privacy impact assessment. Disponóvel em: https://cdn.standards.iteh.ai/samples/62289/77bca86ed686490fb28b502d8f4131f1/ISO-IEC-29134-2017.pdf. Acesso em: 13/09/2004.

GOVERNO FEDERAL. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 29/08/2024

INSTRUÇÃO NORMATIVA CONJUNTA Nº 1,DE 10 DE MAIO DE 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Disponível em: file:///C:/Users/bruna.juca/Downloads/instrucao-normativa-conjunta-no-1-de-10-de-maio-de.pdf. Acesso em: 13/09/2024.