PRIMEIRA PROPOSTA DE MODELO COM ORIENTAÇÕES PARA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

A Secretaria Municipal de Integridade, Transparência e Proteção de Dados (SMIT/RIO) propõe o presente modelo simplificado para confeccionar o relatório de impacto à proteção de dados pessoais (RIPD), o qual deverá ser adaptado e preenchido de acordo com o serviço prestado e com a atividade de tratamento de dados pessoais pelos órgãos ou pelas entidades municipais.

A finalidade é ajudar os órgãos e as entidades municipais na confecção deste importante e essencial documento do sistema de proteção de dados pessoais e previsto nos artigos 5º, XVII, e 38 da LGPD e no artigo 5º, XII da RESOLUÇÃO SEGOVI Nº 91, DE 1º DE AGOSTO DE 2022.

É relevante pontuar que quando for necessária a elaboração do RIPD, deverá ser avaliado se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

A ANPD tem o entendimento de que devem ser elaborados RIPDs específicos para cada tratamento que podem gerar altos riscos às liberdades civis e aos direitos fundamentais.

Desta forma, a maioria das seções do presente documento possui um texto exemplificativo para auxiliar na confecção do RIPD, não se constituindo textos obrigatórios ou definitivos, e, portanto, o responsável pela confecção do Relatório poderá editar, substituir ou excluir os textos de exemplo.

Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público a um sumário executivo do RIPD, por exemplo, pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD, uma vez que a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais. Nesse caso a versão pública do RIPD (sumário executivo) pode ser distinta da versão interna, no intuito de resguardar segredos comercial e industrial e outras informações protegidas por lei.

É relevante destacar que um RIPD corresponde a cada projeto/processo do controlador que contenha um conjunto de operações de tratamento voltadas para uma mesma finalidade. Em alguns casos, isso pode se traduzir em relatórios diferentes para cada operação de tratamento, especialmente se o controlador possui operações muito distintas. Ao elaborar relatórios separados para um conjunto de tratamentos que possuam a mesma finalidade, é possível visualizar melhor os tratamentos realizados e identificar com maior precisão os riscos associados a eles.

No entanto, se o controlador realiza múltiplas operações de tratamento

similares em termos de natureza, finalidade e riscos é razoável que seja elaborado apenas um RIPD que inclua todas essas operações de tratamento, como visto no quarto parágrafo acima.

É importante também observar que, em cenários em que há compartilhamento de dados pessoais entre diferentes controladores, cada controlador poderá ser responsável por um RIPD, ainda que utilizem uma plataforma compartilhada, uma vez que as finalidades do tratamento poderão ser distintas.

OBS: O que considerar como "alto risco" para fins de elaboração do RIPD: Enquanto não for editado regulamento específico pela ANPD sobre o RIPD, os controladores podem, no que couber, adotar como parâmetro o conceito de tratamento de alto risco definido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022. Nesse caso, o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral ("larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares") e de um critério específico ("uso de tecnologias emergentes ou inovadoras", "vigilância ou controle de zonas acessíveis ao público", "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" ou "utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos").

OBS2: O controlador tem o dever de encaminhar o RIPD apenas quando requisitado pela ANPD, sujeitando-se a medidas de fiscalização em caso de descumprimento.

Por fim, esta página introdutória e todo o conteúdo das "observações (OBS)", deverão ser excluídos na versão finalizada do documento. Já os textos sugestivos em itálico deverão ser avaliados e adaptados pelas áreas responsáveis pela elaboração dos documentos, se for o caso.

INTEGRIDADE
TRANSPARÊNCIA E
PROTEÇÃO DE DADOS

MODELO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Histórico de Revisões

Data	Versão	Descrição	Autor
Dez/2023	x	xxxxxx	xxxx

OBJETIVO: O Relatório de Impacto à Proteção de Dados Pessoais 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.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

1.1 – Nome do Controlador(es):
1.1.1 – Informações do(s) Encarregado(s) (nome, *e-mail* e telefone):

1.2 – Nome do Operador(es):
1.2.1 - Informações do(s) Encarregado(s) (nome, *e-mail* e telefone):

2 - NECESSIDADE DE ELABORAR O RELATÓRIO: Nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados abaixo expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pelo Órgão ou pela entidade.

OBS: Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:

a) 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 (recomendação prevista pelo § 3º do art. 4º, referindo-se às exceções constantes do inciso III do art. 4º);

b) quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, por orientação da ANPD (arts. 31 e 32 combinados); e

c) a qualquer momento sob determinação da ANPD (art. 38).

<u>Exemplos</u> de redação para o item 2:

"2 - NECESSIDADE DE ELABORAR O RELATÓRIO:

2.1 - A elaboração deste Relatório de Impacto à Proteção de Dados Pessoais ocorre considerando a possibilidade de ocorrer no serviço/aplicativo/software/sistema xxxxxxx, impacto na privacidade dos dados pessoais, resultante de 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)."

Ou

"2 - NECESSIDADE DE ELABORAR O RELATÓRIO:

2.1 - O Programa de Localização de Desaparecidos realizará tratamentos de dados pessoais de pessoas desaparecidas e dos comunicantes do desaparecimento por meio do Sistema de Localização de Desaparecidos.

2.2 - Dentre o público alvo do Programa também poderão ser tratados dados pessoais de crianças e adolescentes desaparecidos."

OBS: Com o intuito de auxiliar o(s) responsável(is) pela elaboração do RIPD nos órgãos e nas entidades municipais, será adotado como <u>exemplo</u>, o RIPD elaborado em Estudo de Caso do Programa de Localização de Desaparecidos do <u>Departamento de Segurança Pública (DSP) do Ministério da Justiça e Segurança Pública</u>. O exemplo poderá servir como base prática ao RIPD a ser elaborado e deverá ser adaptado ao caso em concreto do tratamento de dados pessoais ocorrido no órgão ou entidade municipal.

3 - DESCRIÇÃO DO TRATAMENTO: A descrição dos processos de tratamento 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. 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.

3.1 – NATUREZA DO TRATAMENTO: A natureza representa como o dado pessoal será tratado. Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados do Órgão/entidade municipal. Importante descrever, por exemplo:

a) como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
b) fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
c) com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;
d) 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;
e) se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
f) medidas de segurança atualmente adotadas.

*"**3.1 – NATUREZA DO TRATAMENTO:***

*3.1.1 - Os dados pessoais são coletados mediante preenchimento de formulário eletrônico do Sistema Nacional pelo titular dos dados pessoais. Os dados são transferidos armazenados nas instalações físicas da Empresa de Processamento e Tecnologia Fictum. A empresa Fictum realiza processamento sobre os dados pessoais e disponibiliza para uso do DSP. O DSP disponibiliza os dados pessoais para utilização e consumo do comunicante. O DSP transfere dados de comunicantes e pessoas desaparecidas para a SDH desenvolver as ações de apoio psicológico para as famílias dos desaparecidos. Os dados pessoais podem ser eliminados a pedido do titular. Nesse caso, o DSP encaminha essa solicitação para a empresa Fictum executar a eliminação dos dados pessoais da base de dados do SND [***IDP**[1]**, item xx]. Esse fluxo de tratamento de dados é demonstrado pela figura abaixo.***

[1] **IDP = Inventário de Dados Pessoais.**

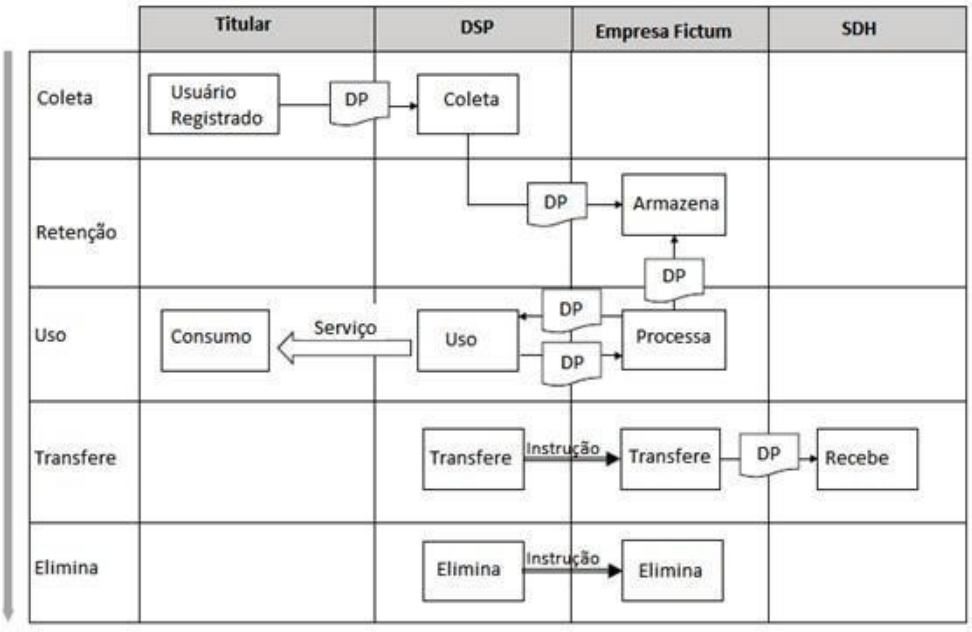

Figura 1: Fluxo tratamento dados pessoais (adaptado ISO 29134:2017)

Legenda figura fluxo de dados:

DP *- Dados Pessoais da pessoa desaparecida e do comunicante do desaparecimento.*
DSP *- Departamento de Segurança Pública representa o controlador dos dados pessoais.*
Empresa Fictum *- empresa que representa o operador dos dados pessoais.*
SDH *- Secretaria de Desenvolvimento Humano*
Titular *- Comunicante do desaparecimento titular dos dados pessoais.*

*3.1.2 A fonte de dados é o comunicante do desaparecimento mediante o preenchimento de formulário eletrônico do Sistema Nacional de Desaparecidos – SND [*IDP, item xx].*

*3.1.3 São compartilhados com a Secretaria de Desenvolvimento Humano os dados de nome , email, telefone, CPF e endereço residencial do comunicante com o objetivo dessa Secretaria fornecer apoio psicológico para as famílias das pessoas desaparecidas [*IDP, item xx].*

*3.1.4 O operador de dados pessoais é a Empresa de Tecnologia e Processamento Fictum [*IDP, item xx], a qual é responsável pela implementação do SND que automatiza todas as operações de tratamento de dados pessoais (Coleta, Retenção, Processamento, Compartilhamento e Eliminação) [*IDP, item 3.1].*

*3.1.5 As medidas de segurança atualmente adotadas são: Controle de Acesso Lógico, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física e do Ambiente [*IDP, itens de xx a xx].*

3.2 – ESCOPO DO TRATAMENTO: O escopo representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:

a) As informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
b) o volume dos dados pessoais a serem coletados e tratados;
c) a extensão e frequência em que os dados são tratados;
d) o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
e) o número de titulares de dados afetados pelo tratamento; e
f) a abrangência da área geográfica do tratamento.

OBS: O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em larga escala.

Exemplo de redação para o item 3.2:

*"**3.2 – ESCOPO DO TRATAMENTO***

3.2.1 Os dados pessoais tratados pelo PLD abrangem:

a) Informações de identificação pessoal: Nome, endereço residencial e telefone da vítima; e
*b) Endereço, Cidade e UF do desaparecimento; e Nome, e-mail, telefone e endereço residencial do comunicante; [*IDP, item xx];*
*c) Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG da vítima; e CPF do comunicante; [*IDP, item xx];*
*d) Dados de identificação eletrônica: Endereço IP do dispositivo eletrônico do comunicante; [*IDP, item xx];*
*e) Detalhes pessoais: Data de nascimento e sexo da vítima; [*IDP, item xx]*
*f) Descrição Física: Cor dos olhos, altura , sinais particulares (ex. tatuagem) e cabelo da vítima; [*IDP, item xx];*
*g) Familiares ou membros da família (Composição Familiar): Nome de pai e mãe da vítima; [*IDP, item xx];*
*h) Vídeo e imagem: Foto da vítima; [*IDP, item xx];*
*i) Registro boletim de ocorrência: Número do boletim de ocorrência, data do fato, Delegacia de registro e Data do registro da ocorrência; [*IDP, item xx];*
*j) Desaparecimento (Boletim de Ocorrência): Circunstâncias do desaparecimento; e [*IDP, item xx]*
*k) Dado sensível que revela origem racial ou ética: Cor da pele da vítima. [*IDP, xx].*

*3.2.2 A quantidade de dados pessoais tratados são de 29 dados pessoais e 1 dado pessoal sensível (cor da pele) [*IDP, xx]. A frequência de tratamento dos dados pessoais é 24x7 (24 horas por dia nos 7 dias da semana) para*

*comunicação dos desaparecimentos e as demais fases e operações de tratamento são realizadas no horário comercial em dias úteis [*IDP, xx].*

*3.2.3 Os dados pessoais obtidos serão mantidos armazenados durante a existência do Programa de Localização dos Desaparecidos [*IDP, itens das seções 7 e 8]. Esse período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção.*

3.2.4 O número de titulares afetados pelo tratamento é de 950.000 entre comunicantes e vítimas desaparecidas, atingindo volume de 1GB de dados pessoais.

*3.2.5 A abrangência do tratamento de dados pessoais é nacional [*IDP, xx] para manutenção do cadastro nacional de desaparecidos e atuação das equipes do Programa de Localização dos Desaparecidos - PLD distribuídas por todos os estados do país.*

3.3 – CONTEXTO DO TRATAMENTO: Nesta seção, 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 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:

a) natureza do relacionamento da organização com os indivíduos;
b) nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
c) destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
d) destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pelo Órgão/entidade municipal ao titular de dados;
e) destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
f) destaque de avanços relevantes do Órgão/entidade municipal em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

<u>Exemplo</u> de redação para o item 3.3:

"3.3 – CONTEXTO DO TRATAMENTO

3.3.1 A natureza do relacionamento dos indivíduos com o DSP no âmbito do PLD é centrada na pessoa do comunicante do desaparecimento, o qual é responsável por informar dados da pessoa desaparecida, do boletim de ocorrência e dele próprio.

3.3.2 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos ao SND são avisados ao titular. Embora o campo CPF e nome do comunicante seja restrito para alteração e o campo e-mail exija um procedimento especial de atualização, os demais dados pessoais podem ser acessados e atualizados permanentemente pelo titular dos dados em questão. O titular pode requisitar informações sobre seus dados pessoais a qualquer momento.

3.3.3 Poderão ser tratados dados pessoais de crianças e adolescentes desaparecidos.

3.3.4 O tratamento de dados é realizado de acordo com a expectativa do titular de dados, conforme aviso de privacidade de ciência do titular dos dados ao se cadastrar no SND. Existem casos em que os titulares de dados (comunicantes) tornam públicos os dados da comunicação de desaparecimento (exceto CPF, RG e Endereço IP) na esperança de que isso acelere a localização da pessoa desaparecida.

3.3.5 O DSP detém razoável experiência em tratamento de dados pessoais e tem estabelecido ações para implementação (conformidade) do previsto pela LGPD.

3.3.6 O DSP utiliza recursos de segurança robustos e pretende investir em novas aplicações para 2020."

3.4 – FINALIDADE DO TRATAMENTO: A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados. Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com a LGPD.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos. Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

a) Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.

b) Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Exemplo de redação para o item 3.4:

"3.4 – FINALIDADE DO TRATAMENTO:

*3.4.1 Promover ações de identificação e busca de pessoas desaparecidas, bem como facilitar o apoio psicológico às famílias dos desaparecidos [*IDP, item .xx].*

*3.4.2 Os resultados pretendidos para os titulares de dados pessoais são: apoio psicológico para as famílias das pessoas desaparecidas; e promoção do respeito pela dignidade das famílias e das pessoas desaparecidas [*IDP, item .xx].*

*3.4.3 Os benefícios esperados para o órgão, entidade ou para a sociedade como um todo são: dados consolidados, centralizados e atualizados relativos ao número de pessoas desaparecidas no País; e informações qualificadas para o estabelecimento de ações coordenadas por equipe de localização de desaparecidos com abrangência nacional a fim de reduzir o número de pessoas desaparecidas [*IDP, item .6.5].*

4 – PARTES INTERESSADAS CONSULTADAS: 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. Nessa seção, é importante identificar:

a) quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e
b) 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. 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).

OBS: 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.

<u>Exemplo</u> de redação para o item 4:

"4 – PARTES INTERESSADAS CONSULTADAS:

4.1 Analistas de segurança da informação do DSP e da Empresa de Tecnologia e Processamento Fictum, os quais indicaram as oportunidades de melhoria para aperfeiçoamento da proteção dos dados pessoais tratados.

4.2 Consultor jurídico DSP, responsável por emitir parecer sobre a conformidade do tratamento de dados do PLD em relação aos aspectos legais da LGPD.

4.3 Coordenadores, servidores e Diretores do DSP e da Secretaria de Desenvolvimento Humano a fim de obter informações técnicas e administrativas sobre o processo de trabalho executado no âmbito do PLD.

4.4 Encarregado do tratamento de dados pessoais, que desempenhou o papel de conduzir o levantamento e apreciar as informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas.

4.5 Famílias das pessoas desaparecidas (comunicantes do desaparecimento), não foram consultadas mediante pesquisa, elas expressaram sua opinião em passeatas e manifestações públicas, solicitando das autoridades uma ação articulada para localização das pessoas desaparecidas.

4.6 Com exceção dos comunicantes de desaparecimento, todas as demais partes consultadas participaram do processo de análise de riscos relativos ao tratamento dos dados pessoais."

5 – NECESSIDADE E PROPORCIONALIDADE: Descrever como o Órgão/entidade municipal avalia a necessidade e proporcionalidade dos dados. É necessário 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, destacar:

a) A fundamentação legal para o tratamento dos dados pessoais.

b) Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que: b.1) esse tratamento de dados pessoais é indispensável; b.2) não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e b.3) esse processamento de fato auxilia no propósito almejado.

c) Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.

d) Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e

respeite os critérios estabelecidos pelo Órgão/entidade municipal que exerce o papel de controlador (LGPD, art. 5º, VI).

e) Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.

f) Como o Órgão/entidade municipal pretende fornecer informações de privacidade para os titulares dos dados pessoais.

g) Quais são as salvaguardas para as transferências internacionais de dados.

<u>Exemplo</u> de redação para o item 5:

"5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

*5.1.1 A hipótese legal para tratamento de dados pessoais é o art. 7º, III da LGPD: "pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (...)" [*IDP, item 6.1].*

*5.1.2 A necessidade de tratamento é respaldada pela previsão legal constante do Decreto 8.956/2018, que institui o PLD [*IDP, item 6.3].*

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.1.1 A escolha dos dados coletados para implementação do PLD foi resultado de intensos estudos realizados pelo DSP com a preocupação de coletar o mínimo de dados necessários para execução da política pública relacionada com esse Programa. As informações sobre pessoas desaparecidas utilizadas no PLD são providas pelo comunicante (fonte de informação). Ao acessar o SND pela primeira vez, ele manifesta sua concordância a Política de Privacidade do PLD, a qual em seu conteúdo destaca a responsabilidade do comunicante em informar dados precisos e atualizar qualquer mudança nos dados informados, como por exemplo, mudança de endereço, telefone ou e-mail de contato.

5.1.2 Está previsto para o próximo ano a integração do SND com bases de outros órgãos e entidades com o objetivo de assegurar a qualidade e atualização dos dados pessoais.

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 Em períodos planejados, o DSP conduz inspeção sobre os processos de tratamento de dados executados pela Empresa de Tecnologia e Processamento Fictum a fim de avaliar se esses processos estão em conformidade com as

diretrizes definidas pelo controlador.

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 O Sistema de Informação ao Cidadão (e-SIC.XP) e a Ouvidoria (Fala.XP) são disponibilizados para que os titulares dos dados pessoais possam demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações. A Política de Privacidade pode ser encontrada no link https://www.dsp.gov.xp/publicacoes/politica-privacidade. Caso o usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, é possível reportá-la também pela Ouvidoria (Fala.XP).

5.4.2 Quando solicitado pelo titular do dado pessoal, o DSP fornecerá informações de privacidade (confirmação de existência ou o acesso a dados pessoais) por meio de e-mail ou sob forma impressa, de acordo com a solicitação do referido titular.

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

*5.5.1 O PLD não realiza qualquer tipo de transferência internacional de dados [*IDP, item 13.1].”*

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE 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 definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-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.

Como exemplo, 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 documento são apresentados na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de

apoio para a definição dos critérios de classificação do nível de risco:

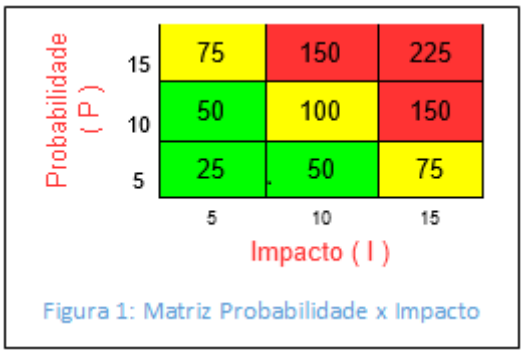

Figura 1: Matriz Probabilidade x Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

a) verde, é entendido como baixo;
b) amarelo, representa risco moderado; e
c) vermelho, indica risco alto.

OBS: As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD:

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

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).

A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a

proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada Órgão/entidade municipal. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017, seção 6.4.4.

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

<u>Exemplo</u> de redação para o item 6 (RIPD elaborado em Estudo de Caso do Programa de Localização de Desaparecidos do <u>Departamento de Segurança Pública (DSP) do Ministério da Justiça e Segurança Pública</u>):

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)

R 01	Acesso não autorizado.	10	15	150
R 02	Coleção excessiva.	10	15	150
R 03	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R 04	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	10	15	150
R 05	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	10	15	150
R 06	Informação insuficiente sobre a finalidade do tratamento.	15	15	225
R 07	Modificação não autorizada.	10	15	150
R 08	Perda.	15	15	225
R 09	Reidentificação de dados pseudonimizados.	15	15	225
R 10	Remoção não autorizada.	10	15	150
R 11	Retenção prolongada de dados pessoais sem necessidade.	15	15	225
R 12	Roubo.	10	15	150
R 13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R 14	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	10	15	150

7 – MEDIDAS E SALVAGUARDAS PARA TRATAR OS RISCOS: 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.). Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.

OBS: A coluna "Medida(s) e Salvaguarda(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório. O/a Órgão/entidade municipal

nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação.

A seguir são apresentados exemplos de medidas e salvaguardas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior.

Risco	Medida(s) e Salvaguarda(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	1. CONTROLE DE ACESSO LÓGICO 2. DESENVOLVIMENTO SEGURO 3. SEGURANÇA EM REDES	Reduzir	5	10	50	Sim
R04 Roubo.	1. CONTROLE DE ACESSO LÓGICO 2.CONTROLES CRIPTOGRÁFICOS 3. PROTEÇÃO FÍSICA E DO AMBIENTE	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

<u>Exemplo</u> de redação para o item 7:

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	Responsabilização: Compliance com a Privacidade; Gestão de Mudanças:	Reduzir	5	10	50	Sim

Legenda:

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 tratar o risco.
3 Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO: Esta seção visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. 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. O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pelo Órgão ou pela entidade municipal.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	**ENCARREGADO**
_____ xxxxxxxxxx **Matrícula/xxxx:** xxxxxxx Rio de Janeiro, ___ de _____ de 20____	_____ xxxxxxxxxx **Matrícula/xxxx:** xxxxxxx Rio de Janeiro, ___ de _____ de 20____

AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
_____ xxxxxxxxxx **Matrícula/xxxx:** xxxxxxx Rio de Janeiro, ___ de _____ de 20____	_____ xxxxxxxxxx **Matrícula/xxxx:** xxxxxxx Rio de Janeiro, ___ de _____ de 20____