<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pelo órgão ou entidade que exerça o papel de controlador (art. 5º, inc. VI, LGPD);

• Como estão implementadas as medidas que asseguram o direito do titular de dados pessoais de obter do controlador (agente de tratamento) o previsto pelo art. 18 da LGPD;

• Como o órgão ou entidade pretende fornecer informações de proteção de dados pessoais para os titulares;

• Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

<O art. 5º, inc. XVII, da LGPD, preconiza que o Relatório de Impacto à Proteção de Dados Pessoais deve descrever *"medidas, salvaguardas e mecanismos de mitigação de risco"*.>

<Antes de definir essas medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular de dados pessoais.>

<Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco e o possível impacto na eventualidade da ocorrência do risco, a fim de avaliar o nível potencial de risco para cada evento.>

<Parâmetros escalares podem ser utilizados para representar os níveis de **probabilidade** e **impacto** que, após a multiplicação, resultarão em 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.>

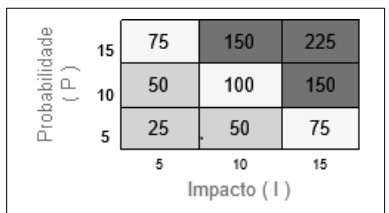

Figura 1: Matriz Probabilidade x Impacto

<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:

- verde, é entendido como baixo;

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

- amarelo, representa risco moderado; e

- vermelho, indica risco alto.>

<As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação, a análise e a gestão de riscos realizados no RIPDP.>

	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
	<Risco 1>			
	<Risco 2>			
	<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).

<A título de informação, é destacada a seguir uma lista não exaustiva de **riscos à privacidade e proteção de dados pessoais e à segurança da informação**. A probabilidade, o impacto e o nível dos riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada órgão ou entidade. Os doze primeiros riscos foram obtidos da norma ISO/IEC 29134:2017, seção 6.4.4.>

	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
1	Acesso não autorizado.	10	15	150
2	Modificação não autorizada.	10	15	150
3	Perda.	5	15	75
4	Roubo.	5	15	75
5	Remoção não autorizada.	5	15	75
6	Coleção excessiva.	10	10	100
7	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
8	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
9	Falha em considerar os direitos do titular dos dados pessoais (*v.g.*, perda do direito de acesso).	5	15	75

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
13	Falha/erro de processamento (*v.g.*, 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
14	Reidentificação de dados pseudonimizados.	5	15	75

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

7 – MEDIDAS 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.>

<A coluna "*Medida(s)*" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.>

<**O órgão ou entidade nem sempre precisa eliminar todos os riscos.** Nesse sentido, pode-se decidir que alguns **riscos são aceitáveis** – até um risco de nível alto – devido aos benefícios do tratamento de dados pessoais e as **dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a Autoridade Nacional de Proteção de Dados (ANPD) antes de prosseguir com as operações de tratamento dos dados pessoais**.>

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
<Risco 1>	<Medida 1; Medida 2; Medida N>					
<Risco 2>	<Medida 1; Medida 2; Medida N>					
<Risco N>	<Medida 1; Medida 2; Medida N>					

Legenda: P – Probabilidade; I – Impacto.

Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[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 | Aceitar.

[2] **Risco residual** é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelos agentes de tratamento. Preencher a coluna com: Sim | Não.

Prodesp GOVERNO DO ESTADO DE SÃO PAULO documento assinado digitalmente

A Companhia de Processamento de Dados do Estado de Sao Paulo - Prodesp garante a autenticidade deste documento quando visualizado diretamente no portal www.imprensaoficial.com.br

sexta-feira, 22 de julho de 2022 às 05:01:06