



TRÊS RIOS
—PREFEITURA—

**Comissão Gestora e de
Regulamentação, Monitoramento e
Acompanhamento para
Implantação da Lei Federal n.º
13.709, de 14 de agosto de 2018 –
Lei Geral de Proteção de Dados
Pessoais (LGPD)**

**RELATÓRIO DE
IMPACTO A PROTEÇÃO
DE DADOS PESSOAIS
(RIPD)**

Setembro / 2022

Processo n.º: 6109/2022

Protocolo n.º:

Folha n.º:

Rubrica

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD

Histórico de Alterações			
Versão	Data	Autor	Notas da Revisão
V1.0	05/09/2022	Eduardo dos Santos Oliveira	Versão Inicial do Relatório de Impacto a Proteção de Dados Pessoais.

SUMÁRIO

1. Introdução	3
1.1. Finalidade do Documento	3
1.2. Embasamento Legal	3
1.3. Conteúdo Mínimo do RIPD	3
1.4. Metodologia Aplicada	4
1.4.1. Processo de Elaboração	4
1.4.1.1. Identificar os Agentes de Tratamento e o Encarregado	4
1.4.1.2. Identificar a necessidade de elaborar o Relatório	5
1.4.1.3. Descrever o tratamento	6
1.4.1.3.1. Natureza do tratamento	7
1.4.1.3.2. Escopo do tratamento	7
1.4.1.3.3. Contexto do tratamento	8
1.4.1.3.4. Finalidade do tratamento	8
1.4.1.4. Identificar as partes interessadas consultadas	10
1.4.1.5. Descrever necessidade e proporcionalidade	10
1.4.1.6. Identificar e avaliar os riscos	11
1.4.1.7. Identificar e avaliar os riscos	14
1.4.1.8. Aprovar o Relatório	15
1.4.1.9. Manter Revisão	15
2. Modelo do Relatório	15

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

1. Introdução

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental, a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

1.1. Finalidade do Documento

O Relatório de Impacto à Proteção dos Dados Pessoais (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.

1.2. Embasamento Legal

Segundo o inciso XVII, do art. 5º da LGPD, o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é documentação que deve ser mantida pelo Controlador dos dados pessoais.

Art. 5º Para os fins desta Lei, considera-se:

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;

1.3. Conteúdo Mínimo do RIPD

O conteúdo mínimo do Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é indicado pelo parágrafo único do art. 38, grifado abaixo.

Art. 38º. 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 adotados.

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 3 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

1.4. Metodologia Aplicada

O processo de elaboração do RIPD seguiu a metodologia apresentada pelo Guia de Boas Práticas para Implementação na Administração Pública Federal, publicado pelo Comitê Central de Governança de Dados, em agosto de 2020, bem como pelas boas práticas apresentadas na publicação LGPD – Lei Geral de Proteção de Dados Pessoais – Manual de Implementação, Thomson Reuters, 2021, 2.ª Edição.

1.4.1. Processo de Elaboração

O RIPD deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa ou projeto que tem o propósito de usar esses dados.

A elaboração contempla as etapas destacadas a seguir:

- Identificar os Agentes de Tratamento e o Encarregado;
- Identificar a necessidade de elaborar o Relatório;
- Descrever o tratamento;
- Identificar partes interessadas consultadas;
- Descrever necessidade e proporcionalidade;
- Identificar e avaliar os riscos;
- Identificar medidas para tratar os riscos;
- Aprovar o Relatório; e
- Manter Revisão.

1.4.1.1. Identificar os Agentes de Tratamento e o Encarregado

A etapa consiste em identificar quem são os agentes de tratamento, ou seja, o controlador e operador, bem como o encarregado no RIPD, em conformidade com o art. 5º da LGPD.

Art. 5º Para os fins desta Lei, considera-se:

- **VI - Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **VII - Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- **VIII - 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); (Redação dada pela Lei nº 13.853, de 2019)

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD

A conclusão desta etapa envolve registrar e publicar o e-mail e o telefone de contato do encarregado, uma vez que este é o canal de comunicação entre o controlador, os titulares dos dados e ANPD.

1.4.1.2. Identificar a necessidade de elaborar o Relatório

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

- 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 (art. 31º e 32º combinados); e
- A qualquer tempo, sob determinação da ANPD (art. 38º).

Quando for necessária a elaboração do RIPD, a instituição deve avaliar 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 elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPD segregados por ser mais adequado à sua realidade.

Além dos casos específicos previstos pela LGPD no início desta seção, relativas à elaboração do RIPD, 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);

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

- 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 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.

Em síntese, nessa etapa deve (m) ser explicitado (s) qual (is) dos itens elencados acima expressa (m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

1.4.1.3. Descrever o 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.

Lembrando que a LGPD (art. 5º, X) considera tratamento “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”.

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.

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 6 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

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.

1.4.1.3.1. Natureza do tratamento

A natureza representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, por exemplo:

- Como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- Fonte de dados (Exemplo: titular de dados, planilha eletrônica, arquivo .xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
- Com quais 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;
- 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
- Medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

1.4.1.3.2. Escopo do tratamento

O escopo representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:

- As informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
- O volume dos dados pessoais a serem coletados e tratados;
- 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;
- O número de titulares de dados afetados pelo tratamento; e
- A abrangência da área geográfica do tratamento.

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

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

1.4.1.3.3. Contexto do tratamento

Nesta etapa, 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:

- 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. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- 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.

1.4.1.3.4. 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 etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Execução de políticas públicas;
- Alguma espécie de estudo realizado por órgão de pesquisa;

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD

- Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiro;
- Tutela da saúde;
- Atender aos interesses legítimos do controlador ou de terceiro;
- Proteção do crédito; e
- Garantia da prevenção à fraude e à segurança do titular.

Cumprir 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:

- Indicar qual (is) o (s) resultado (s) pretendido (s) para os titulares dos dados pessoais, informando o quão importante são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

Art. 10.º. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- I. Apoio e promoção de atividades do controlador; e
- II. Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Cumprе ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

1.4.1.4. Identificar as 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 etapa, é importante identificar:

- 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
- 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).

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.

1.4.1.5. Descrever necessidade e proporcionalidade

Descrever como a instituição 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).

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
 - Esse tratamento de dados pessoais é indispensável;
 - Não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
 - Esse processamento de fato auxilia no propósito almejado.
- Como 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 (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
- Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Quais são as salvaguardas para as transferências internacionais de dados.

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

1.4.1.6. Identificar e avaliar os 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:

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 11 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Tabela 1.4.1.6-1: parâmetros escalares

A figura a seguir apresenta a Matriz Probabilidade X Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Figura 1.4.1.6-1 Matriz Probabilidade x Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.4.1.6-2.

Risco enquadrado na região:

- Verde, é entendido como baixo;
- 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 e avaliação de riscos realizada no RIPD.

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**.

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

Tendo em vista a seção 6 do modelo de RIPD constante do Anexo I, a identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco.

A título de informação, é destacada a seguir uma tabela com 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 risco indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros itens representam riscos de privacidade obtidos da norma **ISO/IEC 29134:2017** seção 6.4.4.

Lembrando que deve ser identificado qualquer risco que afete o tratamento de dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade).

ID	Risco referente ao tratamento de dados pessoais	[P] ¹	[I] ²	Nível de Risco [P X I] ³
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 fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Tabela 1.4.1.6-2: Risco referente ao tratamento de dados pessoais

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

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).

1.4.1.7. Identificar e avaliar 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 de cada risco identificado na etapa “Identificar e avaliar riscos”.

A instituição 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 processamento dos dados pessoais e dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

A seguir, são apresentados exemplos de medidas para lidar com os riscos a fim de demonstrar o preenchimento da tabela constante da seção 7 do RIPD, que consta no Anexo I.

ID	Risco	Medidas	Efeito sobre o Risco ¹	Risco Residual ²			Medidas Aprovadas ³
				P	I	P X I	
R01	Acesso não autorizado.	1. Controle de acesso Lógico.	Reduzir	5	10	50	Sim
		2. Desenvolvimento seguro.					
		3. Segurança em Redes.					

Tabela 1.4.1.7 Exemplos de medidas para lidar com os riscos

¹Efeito 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.

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

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

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 14 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

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. Esse procedimento propicia mais visibilidade em relação ao tratamento do risco.

1.4.1.8. Aprovar o Relatório

Esta etapa 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.

1.4.1.9. Manter 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.

Cumpra-se 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 PMTR 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.

2. Modelo do Relatório

O Modelo (template) do RIPD será apresentado a seguir.

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 15 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD



TRÊS RIOS
 —PREFEITURA—

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Três Rios/RJ, dd de mmmm de aaaa

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 16 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

Histórico de Alterações			
Versão	Data	Autor	Notas da Revisão
V1.0	05/09/2022	Eduardo dos Santos Oliveira	Versão Inicial do Relatório de Impacto a Proteção de Dados Pessoais.

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	Processo n.º: 6109/2022
		Protocolo n.º:
		Folha n.º:
		Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD		
Cód. do Projeto:	001/2022	Nome: Implantação da Lei Federal n.º 13.709 – LGPD

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

1) Finalidade do Documento

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.

2) Identificação dos Agentes de Tratamento

Controlador: Prefeitura do Município de Três Rios

Operador: Secretaria de Tecnologia da Informação e Proteção de Dados

Encarregado de Dados: Elisa Helena Maria Gomes

E-mail do Encarregado: lgpd@tresrios.rj.gov.br

Telefone do Encarregado: (24) 2251-7400

3) Necessidade de Elaborar o Relatório

4) Descrição do Tratamento

4.1) Natureza do Tratamento

4.2) Escopo do Tratamento

4.3) Contexto do Tratamento

4.4) Finalidade do Tratamento

5) Partes Interessadas Consultadas

6) Necessidade e Proporcionalidade

7) Identificação e Avaliação dos Riscos

ID	Risco referente ao tratamento de dados pessoais	[P] ¹	[I] ²	Nível de Risco [P X I] ³
R01				
R02				
R03				

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).

Etapa 2 – Gerenciamento do Projeto	Fase de Monitoramento e Controle
Relatório de Impacto a Proteção de Dados	Página 18 de 19

 TRÊS RIOS PREFEITURA	Comissão Gestora e de Regulamentação, Monitoramento e Acompanhamento para Implantação da Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)		Processo n.º: 6109/2022
			Protocolo n.º:
			Folha n.º:
			Rubrica
Relatório de Impacto à Proteção de Dados Pessoais – RIPD			
Cód. do Projeto:	001/2022	Nome:	Implantação da Lei Federal n.º 13.709 – LGPD

8) Medidas para Tratar os Riscos

ID	Risco	Medidas	Efeito sobre o Risco ¹	Risco Residual ²			Medidas Aprovadas ³
				P	I	P X I	

Legenda: P – Probabilidade; I – Impacto.

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

9) Aprovação

Responsável pela Elaboração do RIPD	Encarregado de Dados
Nome do Responsável Cargo do Responsável Matrícula: XXX.XXXX Três Rios/RJ, dd de mmmm de 202X	Nome do Responsável Cargo do Responsável Matrícula: XXX.XXXX Três Rios/RJ, dd de mmmm de 202X
Representante do Controlador	Representante do Operador
Nome do Responsável Cargo do Responsável Matrícula: XXX.XXXX Três Rios/RJ, dd de mmmm de 202X	Nome do Responsável Cargo do Responsável Matrícula: XXX.XXXX Três Rios/RJ, dd de mmmm de 202X