

Abril de 2023

LGPD e os esclarecimentos sobre o RIPD

Confira respostas da ANPD para as principais dúvidas sobre o documento voltado à gestão de riscos no tratamento de dados pessoais

QUESTÕES

- 1 | Quando deve ser elaborado o RIPD?
- 2 | O que seria “alto risco” no RIPD?
- 3 | Quais são os requisitos mínimos do RIPD?
- 4 | Quais são os tópicos de um RIPD?
- 5 | Quais dados e informações incluir no RIPD?
- 6 | O RIPD deve ser público?
- 7 | O que fazer após elaborar o RIPD?
- 8 | Qual é o passo a passo para a elaboração do RIPD?



É RECOMENDADO QUE O RIPD SEJA ELABORADO:

Previamente a qualquer tratamento (**ação independente do controlador de dados em atenção ao princípio da responsabilização e prestação de contas**).

Em situações em que as operações de tratamento de dados pessoais possam representar alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais do titular de dados – critérios que devem ser avaliados pelo agente de tratamento.

Por motivação ou **determinação da ANPD**.

Situações específicas em que o RIPD pode ser exigido pela ANPD, segundo a LGPD: quando o tratamento tiver como base legal o interesse legítimo, ou seja, aquele em que o controlador é autorizado a tratar dados pessoais mesmo sem o consentimento do titular, ou quando envolver dados pessoais sensíveis.

Programa de governança em privacidade: a LGPD também prevê a possibilidade de sua criação para cumprimento dos princípios da segurança e da prevenção. O programa deve estabelecer garantias adequadas com base em um processo de avaliação sistemática de impactos e riscos à privacidade, procedimento que pode envolver a elaboração do RIPD.

O QUE SERIA “ALTO RISCO” NO RIPD?

A ANPD dispôs que, enquanto não for editado regulamento específico 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](#):

- Tratamento de dados pessoais **será considerado de alto risco se atender a pelo menos um dos critérios gerais e um dos critérios específicos** indicados na imagem ao lado – cenário no qual será recomendada a elaboração de um RIPD.

Esses **critérios não são exaustivos** e o controlador deve avaliar as circunstâncias do caso concreto para identificar se **há outros fatores que possam levar alto risco** aos princípios, liberdades ou direitos dos titulares.

Critérios de “alto risco”



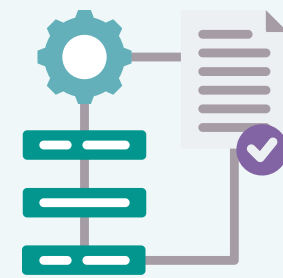
NA ELABORAÇÃO DO RIPD, É IMPORTANTE IDENTIFICAR:

- O maior número possível de fatores de risco e estimar a probabilidade de materialização; e
- O impacto dos danos que podem ser causados.

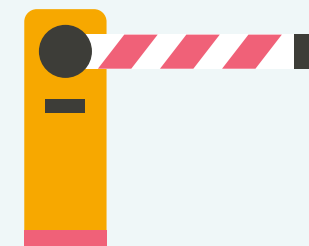
QUAIS SÃO OS REQUISITOS MÍNIMOS DO RIPD?



Descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma.



Metodologia usada para o tratamento e para a garantia da segurança das informações.



Análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

QUAIS SÃO OS TÓPICOS DE UM RIPD?

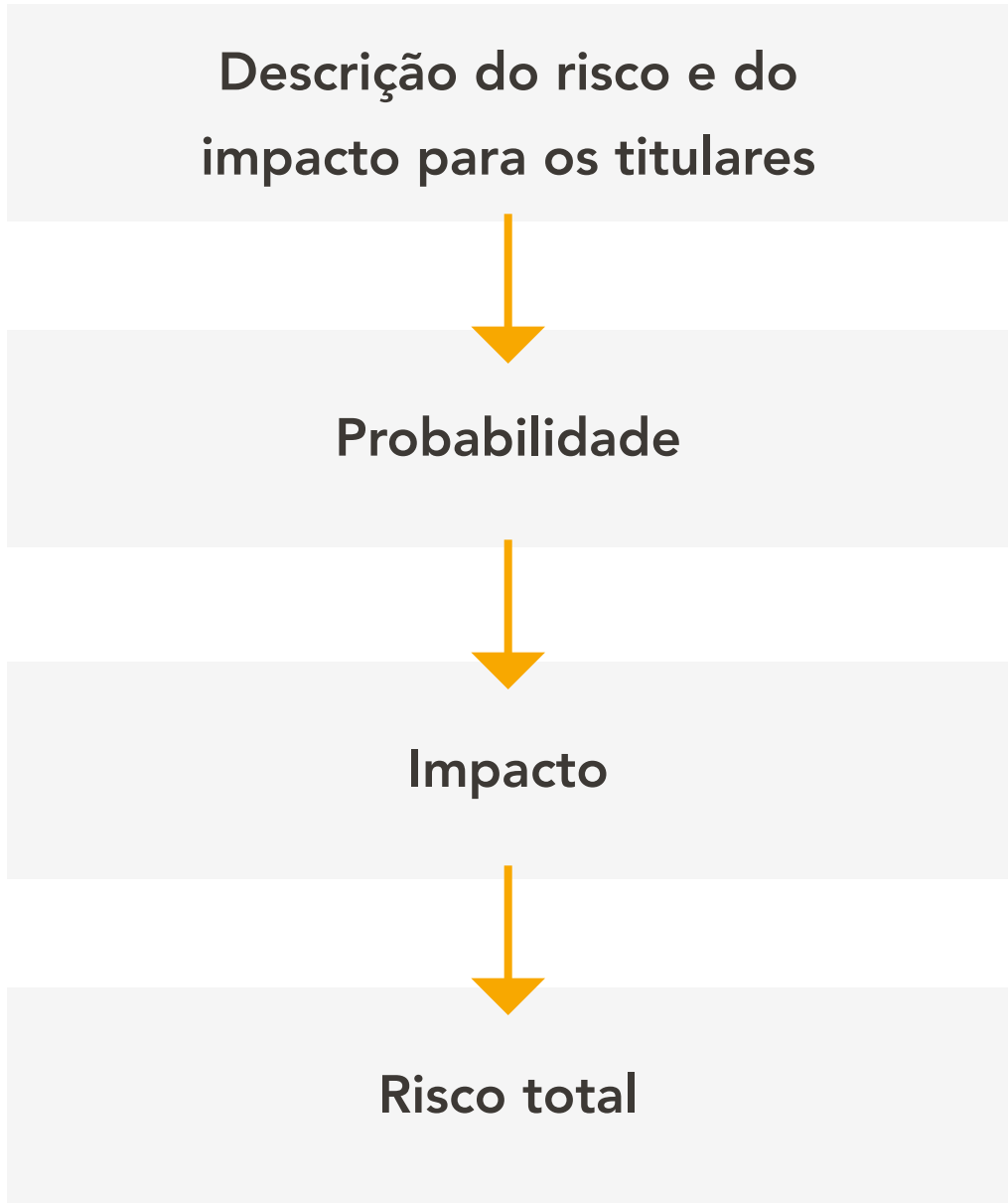
- Descrição dos tipos de dados pessoais tratados;
- Nome das operações de tratamento;
- Finalidades do tratamento (incluindo interesses legítimos);
- Base legal adotada;
- Avaliação da necessidade e da proporcionalidade das operações de tratamento;
- Análise de riscos para os direitos e liberdades dos titulares de dados; e
- Medidas a serem adotadas para minimizar esses riscos.

Em qualquer caso, a ANPD poderá solicitar informações adicionais sempre que necessário.

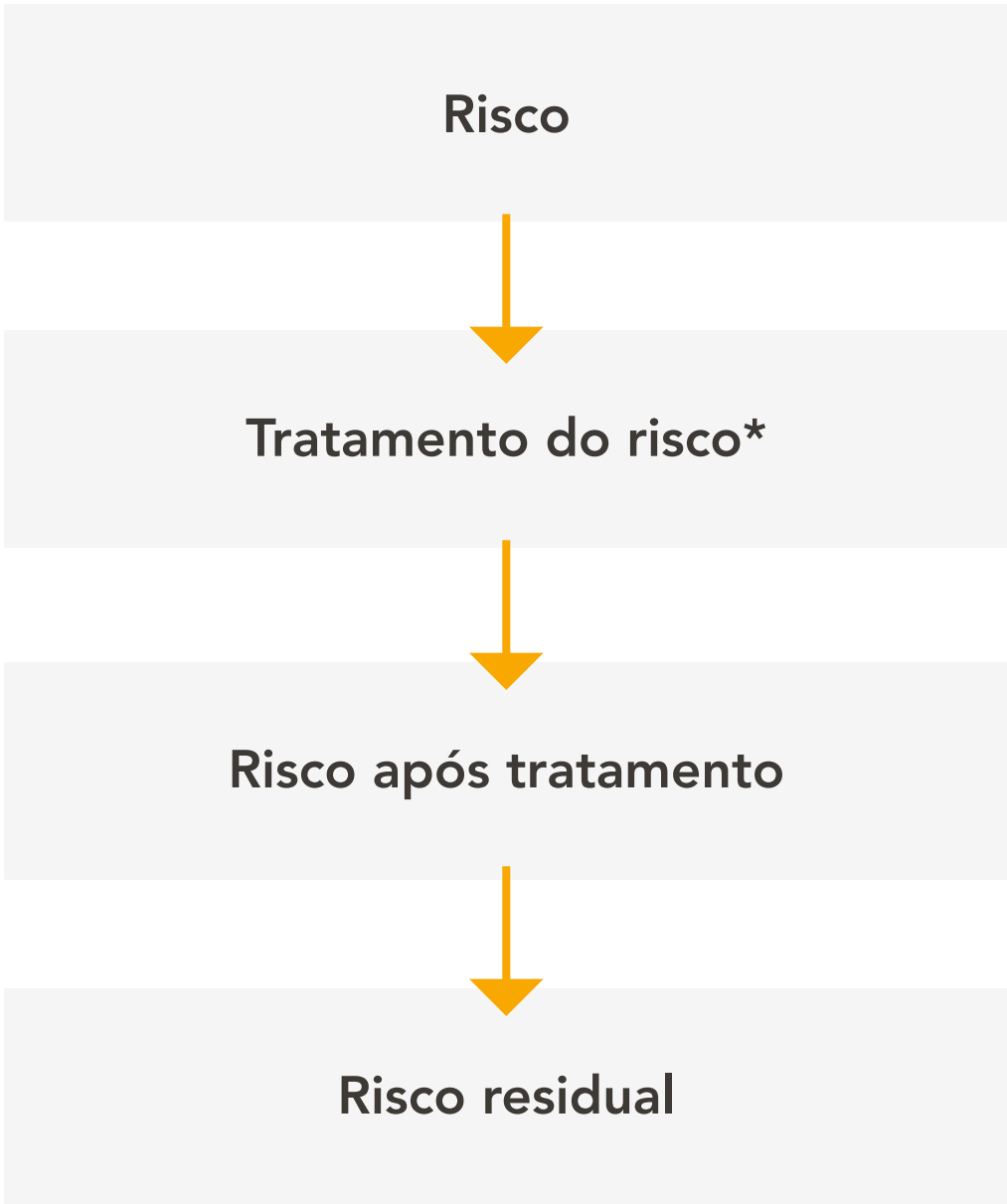


- A. Identificação dos agentes de tratamento e do encarregado.
- B. Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos.
- C. Justificativa da necessidade de elaboração do relatório.
- D. Projeto/processo que justifica a elaboração do RIPD.
- E. Sistemas de informação relacionados ao que justifica a elaboração do RIPD.
- F. Tratamento de dados, incluindo:
 - Descrição do tratamento (desde a coleta até a eliminação).
- Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa).
- Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa).
- Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços).
- Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver.
- Volume de dados pessoais tratados e número de titulares envolvidos no tratamento.
- Fonte de coleta.
- Finalidade do tratamento (justifique a finalidade de tratamento para cada dado).
- Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver).
- Política de armazenamento (descrever os prazos de retenção e métodos de descarte).
- G. Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento.
- H. Análise de princípios da LGPD.
- I. Riscos identificados ao titular.

J. Resultado apurado com base na metodologia utilizada pelo agente de tratamento:



K. Medidas, salvaguardas e mecanismos de mitigação de risco:



* Descrever as medidas adotadas para mitigação do risco.

Embora não seja obrigatório, a ANPD recomenda às entidades privadas tornar o RIPD público como uma medida que **demonstra a preocupação do controlador com a segurança dos dados pessoais e seu compromisso com a privacidade dos titulares**, atendendo aos princípios da transparência e responsabilização previstos na LGPD.



O controlador pode disponibilizar o RIPD em meios de fácil acesso ao titular, como em seus sites, desde que resguardados segredos comerciais e informações protegidas por lei.

ENTIDADES PÚBLICAS

No caso de entidades públicas, o RIPD deverá ser publicado por determinação da ANPD ou pelo próprio controlador, em conformidade com a Lei n.º 12.527/2011.

Após elaborar o RIPD, o controlador verificará a **viabilidade de prosseguir ou não com os processos de tratamento de dados pessoais** que levaram à elaboração do relatório ou à necessidade de modificação na forma do tratamento.

O agente de tratamento observará as recomendações provenientes do RIPD, especialmente no que se refere à **implementação de medidas, salvaguardas e mecanismos de mitigação de riscos adotados**.

Por fim, é importante que o controlador faça a **revisão contínua do RIPD**, em especial, quando houver fatos novos que possam gerar mudanças nos riscos identificados, tais como:

- Alteração nas operações de tratamento.
- Identificação de novos fatores de risco.
- Agravamento dos fatores de risco anteriormente identificados.
- Em caso de novas regulamentações ou orientações emitidas pela ANPD.



QUAL É O PASSO A PASSO PARA A ELABORAÇÃO DO RIPD?

RIPD
Relatório de Impacto à
proteção de dados pessoais

