Guia para Elaboração de Relatórios de Impacto à Proteção de Dados Pessoais

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Programa de Privacidade e Segurança da Informação

PPSI 2.0

Versão 1.0

Brasília, 31 de julho de 2026

GUIA PARA ELABORAÇÃO DE RELATÓRIOS DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL
Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE
Marta Juvina de Medeiros
Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO
Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE EDITORAÇÃO
Rejane Monique Brelaz Castro

EQUIPE TÉCNICA DE ELABORAÇÃO
Anderson Souza de Araújo
Marta Juvina de Medeiros
Ricardo Borges Almeida

EQUIPE DE REVISÃO
Marta Juvina de Medeiros

Histórico de versões

Versão	Data	Descrição	Autor
1.0	31/07/2026	Construção do Guia para Elaboração de Relatórios de Impacto à Proteção de Dados Pessoais	Equipe Técnica de Elaboração

Sumário

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

Medidas do *framework* do PPSI 2.0 apoiadas por este documento

Id	Medida
23.3	O órgão elabora o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais?
25.8	O órgão implementa medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?
25.10	O órgão adota medidas de responsabilização e prestação de contas, capazes de evidenciar o cumprimento das normas de proteção de dados pessoais?

1 Termos e definições

As definições relevantes ao entendimento do conteúdo exposto neste Guia são apresentadas a seguir. Demais termos utilizados neste Guia podem ser encontrados na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) [1], na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 [2], nas resoluções da Agência Nacional de Proteção de Dados (ANPD) ou no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021 [3].

Unidade responsável ou Unidade: unidade do órgão ou entidade gestora do produto ou serviço objeto do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

2 Introdução

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) [1] é uma legislação baseada em riscos, que trata o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em diversos dispositivos: no art. 5º, XVII, ao conceituá-lo; no art. 10, § 3º, ao prever que a Agência Nacional de Proteção de Dados (ANPD) pode solicitar o relatório quando o tratamento tiver como fundamento o legítimo interesse do controlador; no art. 32, ao facultar à ANPD solicitar a agentes do Poder Público a publicação de RIPDs; e no art. 38, ao facultar à ANPD determinar ao controlador a sua elaboração.

Embora preconize a necessidade de elaboração do RIPD nas situações em que as operações de tratamento de dados pessoais impliquem riscos às liberdades civis e aos direitos fundamentais dos titulares, a Lei não explicita objetivamente as situações em que essa elaboração é imprescindível, dispondo genericamente sobre tal obrigação.

O Programa de Privacidade e Segurança da Informação (PPSI 2.0), instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 [2], aborda a necessidade de elaboração do RIPD nos controles 23 e 25 de seu *framework* [4]. O controle 23, que trata da análise das operações de tratamento, estabelece, em sua medida 23.2, a necessidade de o órgão público elaborar o RIPD dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Segundo a Secretaria de Governo Digital (SGD) [4]:

> Para cada uma das operações de tratamento de dados pessoais registradas em decorrência do Controle 19, avaliar se podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares; em caso positivo, elaborar o RIPD contendo, no mínimo, o disposto na Lei nº 13.709/2018, art. 38, parágrafo único: a descrição dos tipos de dados pessoais coletados; a metodologia aplicada para a coleta e o armazenamento; as medidas adotadas para garantir a segurança das informações; e a análise do controlador quanto aos riscos à privacidade e às salvaguardas implementadas para mitigá-los [4, p. 85].

Já o controle 25, que trata dos princípios da LGPD, aborda, em sua medida 25.8, a necessidade de o órgão público implementar medidas que previnam a ocorrência de danos em razão do tratamento de dados pessoais – entre elas, a elaboração de RIPDs; na medida 25.10, aborda a necessidade de adoção de medidas de responsabilização e prestação de contas que evidenciem, de forma sistemática e auditável, o cumprimento das normas de proteção de dados pessoais, o que também inclui os RIPDs elaborados pelo órgão.

A ANPD, por sua vez, disponibiliza em seu sítio eletrônico um conjunto de perguntas e respostas que orienta e esclarece sobre o RIPD [5]. Conforme exigência do art. 38 da LGPD, a Agência deverá regulamentar o relatório; até que isso ocorra, o conteúdo das perguntas e respostas disponibilizado pela ANPD auxilia sobremaneira na compreensão da relevância e das regras gerais para sua elaboração.

A Resolução CD/ANPD nº 18, de 16 de julho de 2024 [6], também trata do tema ao estabelecer, em seu art. 16, inciso III, a atribuição do encarregado de prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação do RIPD.

Este Guia tem como objetivo apresentar orientações às unidades dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) para avaliar a necessidade de elaboração do RIPD de um produto ou serviço que envolva tratamento de dados pessoais, bem como para conduzir sua elaboração. O modelo de RIPD do PPSI 2.0, disponibilizado em conjunto com este Guia, operacionaliza essas orientações em um documento estruturado para preenchimento pelo órgão ou entidade.

Este Guia está organizado em cinco seções. A seção 1 apresenta os termos e definições relevantes. Esta seção 2 traz a introdução e contextualiza o Guia no âmbito do PPSI 2.0. A seção 3 apresenta considerações iniciais sobre quando e por quem o RIPD deve ser elaborado, sua relação com a gestão de riscos corporativa e a sua possível publicização. A seção 4 detalha o conteúdo do RIPD, orientando o preenchimento do modelo do PPSI 2.0. A seção 5, por fim, traz as considerações finais.

3 Considerações iniciais

Esta seção reúne considerações que devem ser avaliadas pela unidade responsável previamente à elaboração do RIPD, incluindo em quais situações ele deve ser produzido, quem é responsável por sua elaboração, sua relação com a gestão de riscos corporativa do órgão e as diretrizes para sua publicização.

3.1 Em quais situações o RIPD deve ser elaborado

A elaboração do RIPD deve ser realizada nas situações em que as operações de tratamento envolvam risco às liberdades civis e aos direitos fundamentais dos titulares. O RIPD deve ser elaborado no início do planejamento das operações de tratamento, de modo que as medidas técnicas e administrativas de privacidade e segurança da informação necessárias possam ser implementadas em tempo hábil.

Apesar de a LGPD prever a possibilidade de a ANPD solicitar a agentes de tratamento do Poder Público a publicação de RIPD (art. 32) e de determinar ao controlador a sua elaboração (art. 38), a Lei não evidencia objetivamente as situações em que essa elaboração torna-se obrigatória. Na ausência de regulamentação específica da ANPD sobre o tema, o FAQ da Agência sobre o RIPD [5] indica que se adota, como parâmetro para a caracterização do alto risco, o critério do art. 4º da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022 [7] – resolução expressamente referenciada pelo FAQ da ANPD para esse fim: será considerado de alto risco o tratamento que atender cumulativamente a pelo menos um critério geral e um critério específico, entre os seguintes:

Critérios gerais:

- tratamento de dados pessoais em larga escala; ou
- tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares.

Critérios específicos:

- 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, inclusive as destinadas a definir perfil pessoal, profissional, de saúde, de consumo ou de crédito, ou aspectos da personalidade do titular; ou
- utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos [7, art. 4º].

Como boa prática de governança baseada em recomendações internacionais do *Article 29 Data Protection Working Party* [8], recomenda-se considerar a elaboração do RIPD também quando a operação de tratamento apresentar isoladamente dois ou mais desses fatores de risco, ainda que não estejam presentes, cumulativamente, um critério geral e um critério específico.

Constatada a obrigatoriedade ou manifestada a conveniência da elaboração, cabe à unidade responsável registrar essa análise na subseção 1.2 do modelo de RIPD do PPSI 2.0, indicando qual critério geral e qual critério específico estão presentes, com a respectiva justificativa. A Figura 1 sintetiza os critérios utilizados para identificar tratamentos de alto risco.

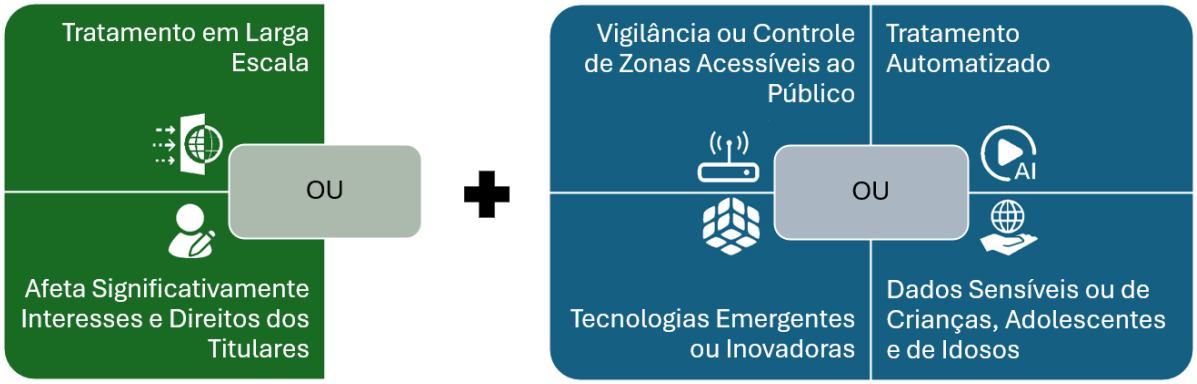

Figura 1: critérios para identificar tratamentos de dados pessoais que geram alto risco.

A identificação prévia, no setor público, de riscos às liberdades civis e aos direitos fundamentais é uma ação indispensável, dado o caráter frequentemente obrigatório do tratamento de dados pessoais para a prestação de serviços estatais. Ao mapear essas vulnerabilidades sob a ótica dos direitos humanos e das garantias constitucionais, a administração pública cumpre seu dever de evitar práticas discriminatórias ilícitas e abusos de poder antes que qualquer dano se materialize.

Ademais, a Lei nº 15.211, de 17 de setembro de 2025 (ECA Digital) [10], estabelece obrigações adicionais para o tratamento de dados de crianças e adolescentes em ambientes digitais. Quando o produto ou serviço envolver tal público, devem ser considerados, além dos critérios da LGPD e da Resolução CD/ANPD nº 2/2022, as disposições do ECA Digital e as orientações da ANPD sobre o tema.

3.2 Quem é responsável pela elaboração do RIPD?

A elaboração do RIPD deve ser conduzida pela unidade responsável pelo produto ou serviço em que ocorre o tratamento de dados pessoais objeto do relatório, com o apoio técnico das áreas de tecnologia da informação, jurídica e de segurança da informação, conforme as especificidades do tratamento analisado.

Tal elaboração não deve ocorrer de forma isolada nas unidades de tecnologia ou nas assessorias jurídicas: ela precisa caminhar em conjunto com a gestão de riscos corporativa do órgão ou entidade, como ferramenta de governança. Por esse motivo, a análise sobre a necessidade de sua elaboração deve ocorrer logo no início do planejamento de qualquer novo produto ou serviço que utilize dados pessoais, garantindo que a organização implemente, em tempo hábil, as salvaguardas necessárias antes do início da operação.

Essa combinação de perfis não decorre de exigência normativa específica, mas de uma lógica de complementaridade de conhecimentos que tende a qualificar o RIPD, cabendo à unidade responsável avaliar, caso a caso, quais perspectivas são efetivamente necessárias. A unidade

responsável pelo produto ou serviço, por conhecer o contexto operacional do tratamento – motivações, público atendido e fluxo real das informações –, costuma estar em melhor posição para descrever com precisão as operações de tratamento de dados pessoais e as finalidades que as justificam.

A área de tecnologia da informação tende a deter o conhecimento técnico necessário para descrever a arquitetura de sistemas, as medidas técnicas já implementadas e a viabilidade de novas ações. A assessoria jurídica pode contribuir com a análise da hipótese legal aplicável e da conformidade do tratamento com a LGPD e demais normativos, enquanto a área de segurança da informação tende a aportar a avaliação técnica dos riscos e das medidas de proteção sob a ótica da confidencialidade, integridade e disponibilidade dos dados. Nem sempre essas perspectivas estarão disponíveis como unidades formalmente segregadas – em órgãos de menor porte, é comum que um mesmo servidor acumule mais de uma dessas funções –, mas recomenda-se que, na medida do possível, elas sejam efetivamente incorporadas à elaboração do RIPD.

O encarregado, por sua vez, deve ser consultado na elaboração e na análise das conclusões do RIPD. É desejável sua participação ativa no processo (FAQ ANPD, Pergunta 12), tendo em vista o conhecimento especializado em proteção de dados pessoais e o papel de interlocução entre o controlador, os titulares e a ANPD que lhe são próprios (LGPD, art. 5º, VIII, e art. 41); também lhe incumbe prestar assistência e orientação à unidade responsável na definição e implementação do RIPD, nos termos do inciso III do art. 16 da Resolução CD/ANPD nº 18/2024 [6], competindo ao representante do controlador a aprovação final do relatório.

Recomenda-se, ainda, o registro de opiniões divergentes identificadas durante a elaboração do RIPD, incluindo as justificativas para a opção adotada, como boa prática de transparência, responsabilização e prestação de contas (FAQ ANPD, Pergunta 13).

3.3 Gestão de riscos

O FAQ da ANPD sobre o RIPD esclarece que a definição dos critérios e da metodologia de gestão de riscos utilizados na elaboração do relatório é de responsabilidade do próprio controlador, devendo as diretrizes gerais deste processo estar alinhadas à política de segurança do órgão ou entidade e considerar, entre outros aspectos, os objetivos estratégicos, os processos, a estrutura organizacional e os requisitos da LGPD e demais normativos aplicáveis. Ou seja: não há uma metodologia de gestão de riscos obrigatória para fins de elaboração do RIPD, cabendo à unidade responsável adotar a metodologia institucional já em uso pelo órgão ou entidade.

Na ausência de metodologia própria consolidada, uma referência possível é o modelo metodológico do Poder Executivo federal, detalhado no Guia de Gestão de Riscos [9] do Ministério da Gestão e da Inovação em Serviços Públicos (MGI). A título de exemplo, o Guia trata o apetite a risco como o nível de exposição que o órgão aceita para atingir seus objetivos; no setor público, adota-se geralmente um apetite geral moderado – a instituição aceita riscos baixos, mas exige tratamento obrigatório para riscos altos ou críticos –, associado a uma diretriz de tolerância zero para problemas que afetem a integridade, a conformidade legal ou os direitos fundamentais. Qualquer tratamento de dados pessoais que ameace essas garantias ultrapassaria, nesse modelo, o limite de aceitabilidade do órgão, exigindo resposta imediata –

o que reforça, mas não substitui, a análise específica de alto risco apresentada na subseção 3.1.

Cabe ressaltar, contudo, que a gestão de riscos realizada no âmbito do RIPD tem um objeto distinto do objeto da gestão de riscos corporativa. Enquanto esta última tende a mensurar o impacto de um risco sobre os objetivos estratégicos, a reputação ou a continuidade operacional do próprio órgão, a gestão de riscos do RIPD deve ter como referência primária o impacto sobre as liberdades civis e os direitos fundamentais do titular dos dados pessoais (LGPD, art. 5º, XVII) – ainda que, secundariamente, essas mesmas situações também possam gerar consequências institucionais, como sanções ou danos reputacionais. Por isso, ao adaptar uma metodologia de gestão de riscos corporativa – própria ou de referência, como o Guia de Gestão de Riscos do MGI – para fins de elaboração do RIPD, recomenda-se recalibrar os critérios de impacto e de probabilidade para refletir os efeitos do tratamento sobre o titular, e não apenas sobre o órgão. É possível, por exemplo, que um risco seja classificado como de baixo impacto sob a ótica estritamente institucional e, ainda assim, representar um risco relevante às liberdades e aos direitos fundamentais do titular – cenário em que, no RIPD, deve prevalecer a perspectiva do titular.

3.4 Publicização do RIPD

Embora a publicização do RIPD não constitua uma obrigação irrestrita para todas as organizações, sua disponibilização ao público funciona como um importante mecanismo de transparência ativa na administração pública. Essa prática evidencia o compromisso do órgão com a segurança da informação e com a privacidade dos titulares, atendendo diretamente aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas estabelecidos, respectivamente, nos incisos IV, VI e X do art. 6º da LGPD.

Para promover a publicização do RIPD, o órgão ou entidade pode disponibilizar o relatório de forma clara, adequada e ostensiva em seus canais oficiais de comunicação, com destaque para o sítio eletrônico institucional. No entanto, para salvaguardar segredos industriais ou comerciais de parceiros públicos e privados – bem como a segurança da sociedade e do Estado, a segurança institucional e a confidencialidade de informações protegidas por lei –, o controlador pode publicar uma versão com supressão de informações consideradas críticas ou restritas, mantendo a integridade da versão interna original.

Sugere-se que fluxos detalhados de tratamento, arquitetura tecnológica, sistemas de informação relacionados, integrações entre sistemas, identificação detalhada de operadores e fornecedores quando houver risco ou sigilo aplicável, evidências internas, controles técnicos e administrativos detalhados, testes de segurança, monitoramento e indicadores internos compõem o conteúdo restrito ou não recomendado para publicização.

Merece ressalva semelhante o conteúdo do RIPD relativo aos riscos identificados e às respectivas medidas técnicas e administrativas adotadas para mitigá-los. Ainda que esse conteúdo não configure segredo comercial ou industrial de terceiros, sua publicização detalhada pode, em si, ampliar a superfície de exposição da organização, na medida em que descreve vulnerabilidades e o estado dos controles de segurança implementados – informação que, se conhecida por agentes mal-intencionados, poderia ser explorada para comprometer a proteção dos dados pessoais tratados.

No âmbito específico do PPSI 2.0, essa preocupação encontra fundamento ainda mais direto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 [2], que conceitua como informações críticas sobre privacidade e segurança da informação quaisquer dados sobre infraestrutura, configurações e características técnicas dos ativos de informação, políticas, normas e procedimentos operacionais e arquiteturas de negócio que possam expor vulnerabilidades e comprometer a privacidade dos titulares ou a confidencialidade, a integridade, a disponibilidade ou a autenticidade das informações (art. 2º, III) – definição que, no contexto do RIPD, tende a abranger justamente a descrição de riscos e das respectivas medidas técnicas e administrativas de mitigação. A mesma Portaria determina que as informações críticas geradas na execução de etapas, atividades ou procedimentos nela previstos são consideradas imprescindíveis à segurança da sociedade e do Estado, somente podendo ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos respectivos ativos de informação (art. 5º).

Essa disciplina normativa reforça a recomendação anterior: ao preparar a versão do RIPD destinada à publicização, a unidade responsável deve avaliar se o conteúdo relativo a riscos e medidas enquadra-se como informação crítica nos termos do PPSI 2.0 e, em caso positivo, restringir seu detalhamento na versão disponibilizada ao público, preservando o conteúdo integral apenas na versão interna do documento.

Recomenda-se, portanto, que a unidade responsável avalie, para cada risco e medida registrados no RIPD, se o nível de detalhamento adequado à versão publicizável compromete a eficácia dos controles de segurança, restringindo-se, quando necessário, o teor dessas informações na versão publicizada – sem prejuízo de sua manutenção integral na versão interna do documento.

Por fim, sugere-se que eventual publicização do RIPD seja precedida de revisão pelo encarregado pelo tratamento de dados pessoais, pelas áreas responsáveis pela segurança da informação e, quando necessário, pela unidade jurídica ou pela autoridade competente em transparência e acesso à informação – indicando, quando aplicável, que determinadas informações foram omitidas ou apresentadas de forma resumida para preservar a segurança da sociedade e do Estado, a segurança institucional, a confidencialidade de informações protegidas por lei ou a efetividade das medidas de segurança adotadas.

4 Conteúdo do RIPD

Esta seção apresenta as orientações que fundamentam o conteúdo do RIPD, na mesma sequência em que o modelo de RIPD do PPSI 2.0 as operacionaliza: contexto e tratamento dos dados pessoais (subseção 4.1); análise dos princípios da LGPD (subseção 4.2); garantia dos direitos dos titulares (subseção 4.3); gestão de riscos (subseção 4.4); versoinamento e atualização do RIPD (subseção 4.5) e aprovação (subseção 4.6). Como o modelo já operacionaliza essas orientações, seção a seção, por meio de instruções específicas de preenchimento destacadas entre colchetes, o conteúdo a seguir não as repete: apresenta o raciocínio que deve orientar a leitura e o preenchimento de cada bloco, complementando – sem substituir – as orientações incorporadas ao modelo.

4.1 Contexto e tratamento de dados pessoais

O modelo de RIPD do PPSI 2.0 operacionaliza as orientações sobre o contexto e o tratamento de dados pessoais em duas de suas seções: a seção 1 (Contexto do produto ou serviço) e a seção 2 (Tratamento dos dados pessoais). A primeira reúne a visão geral do produto ou serviço e a justificativa da necessidade de elaboração do relatório; a segunda, mais extensa, reúne a descrição das operações de tratamento e o respectivo fluxo, os agentes de tratamento e as demais partes interessadas, o compartilhamento e a transferência internacional de dados pessoais, a eliminação dos dados e os sistemas de informação relacionados.

A visão geral do produto ou serviço deve situar o leitor em seu propósito sem antecipar conteúdos próprios das seções seguintes, como finalidades específicas do tratamento, agentes envolvidos ou riscos identificados – esses elementos têm lugar reservado nas subseções correspondentes. Já a justificativa da necessidade deve remeter à análise realizada conforme a subseção 3.1 deste Guia, indicando expressamente a razão ou as razões que fundamentam a elaboração: determinação ou solicitação da ANPD; decisão do próprio controlador; enquadramento do tratamento como de alto risco.

A descrição das operações de tratamento, por sua vez, é o detalhamento operacional que sustenta toda a análise realizada nas demais seções do RIPD: é a partir da descrição precisa de cada operação – finalidade, dados pessoais envolvidos, hipótese legal aplicável – que se torna possível avaliar, mais adiante, se cada princípio da LGPD está sendo observado. Por isso, recomenda-se que essa descrição seja preenchida com o mesmo rigor e nomenclatura utilizados no registro das operações de tratamento elaborado em decorrência do Controle 19 do *framework* do PPSI 2.0, evitando divergências entre os dois documentos. Quanto aos agentes de tratamento, é importante distinguir com precisão o papel de cada parte: um mesmo terceiro pode figurar como operador em uma atividade de tratamento e como controlador em outra – inclusive em regime de controladoria conjunta –, a depender de quem detém as decisões sobre finalidade e meios do tratamento (LGPD, art. 5º, VI e VII); essa distinção determina as responsabilidades legais aplicáveis a cada agente.

4.2 Análise dos princípios da LGPD

A seção 3 do modelo (Análise dos princípios da LGPD) exige que o controlador avalie o tratamento descrito na seção 2 à luz de cada um dos dez princípios elencados no art. 6º da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Essa seção existe porque a LGPD é uma legislação baseada em princípios, e não apenas em regras. Isso significa que a conformidade do tratamento não se esgota na existência de uma hipótese legal válida nem na limitação do volume de dados pessoais tratados ao mínimo necessário. Uma base legal adequada e um tratamento parcimonioso quanto ao volume de dados pessoais são condições necessárias, mas não suficientes: os princípios do art. 6º atuam como vetores interpretativos que devem orientar continuamente o desenho, a execução e a revisão do tratamento, mesmo quando a hipótese legal já está identificada e os dados pessoais tratados já estão limitados ao indispensável. É perfeitamente possível, por exemplo, que um tratamento tenha hipótese legal válida e dados pessoais estritamente necessários à finalidade e, ainda assim, viole o princípio da transparência (por não informar adequadamente o titular), o da segurança (por não adotar medidas técnicas compatíveis com o risco) ou o da não discriminação (por gerar efeitos discriminatórios ilícitos ou abusivos). Por isso, a análise principiológica não é redundante em relação às demais seções do RIPD: ela é o mecanismo pelo qual o controlador verifica se a conformidade formal se traduz em conformidade material com os valores que a LGPD pretende proteger.

O modelo de RIPD do PPSI 2.0 operacionaliza estas orientações em cada uma das subseções de sua seção 3 (3.1 a 3.10), trazendo, entre colchetes, a definição legal do respectivo princípio, os elementos que o compõem e sugestões de como demonstrá-lo. Ao conduzir essa análise, recomenda-se que a unidade responsável observe três aspectos metodológicos:

- evitar a mera repetição do texto legal do princípio como se fosse, em si, a demonstração de conformidade: a redação de cada subseção deve indicar como, concretamente, o tratamento descrito na seção 2 atende (ou não) ao princípio, e não apenas transcrever o inciso correspondente do art. 6º;
- tratar cada princípio de forma independente, ainda que dialoguem entre si: a análise da necessidade (art. 6º, III), por exemplo, não substitui a da finalidade (art. 6º, I), pois um tratamento pode ser proporcional ao seu propósito declarado e, ainda assim, ter finalidade insuficientemente específica ou não comunicada ao titular; e
- registrar honestamente eventuais lacunas identificadas durante a análise, indicando o encaminhamento adotado para saná-las: a análise principiológica é mais valiosa quando funciona como instrumento de identificação de não conformidades do que quando se limita a validar formalmente um tratamento já implementado.

O resultado dessa análise, incluindo os pontos fortes e as lacunas, deve alimentar diretamente o processo de gestão de riscos (seção 5 do modelo): um princípio não observado, ou observado apenas parcialmente, tende a configurar risco a ser identificado, avaliado, tratado e monitorado na subseção correspondente.

4.3 Garantia dos direitos dos titulares

A seção 4 do modelo de RIPD (Garantia dos direitos dos titulares) exige que o controlador demonstre, para o tratamento descrito na seção 2, como cada um dos direitos assegurados ao titular pela LGPD pode efetivamente ser exercido.

Assim como ocorre com os princípios, essa seção existe porque a garantia dos direitos dos titulares não decorre automaticamente da conformidade obtida nas seções anteriores do RIPD. Um tratamento pode ter finalidade legítima, base legal válida e estar alinhado a todos os princípios do art. 6º e, ainda assim, não oferecer ao titular um canal efetivo para exercer, por exemplo, o direito de acesso ou de correção de seus dados pessoais.

A LGPD trata a garantia dos direitos dos titulares como uma obrigação autônoma do controlador, e não como uma decorrência natural da regularidade do tratamento. Por isso, a seção 4 do modelo requer uma demonstração operacional – como o titular exerce cada direito, em quanto tempo, por qual canal – e não uma reafirmação de que os direitos existem.

O modelo operacionaliza estas orientações, entre colchetes, tanto nas medidas gerais quanto nas medidas específicas por direito do titular. Ao conduzir essa análise, recomenda-se que a unidade responsável verifique, para cada direito:

- se o direito é aplicável considerando o produto ou serviço objeto do RIPD;
- se existe um canal de atendimento identificado e efetivamente operacional – não bastando a previsão do direito em normativo interno sem um meio concreto para o seu exercício;
- se o prazo de atendimento observa os parâmetros legais e regulatórios aplicáveis, e se esse prazo é de conhecimento da unidade responsável pelo atendimento; e
- se há direitos cujo exercício, para o tratamento em análise, encontra alguma limitação legítima, hipótese em que a limitação e sua fundamentação devem ser expressamente registradas, e não simplesmente omitidas.

Tal qual ocorre na análise dos princípios, eventuais lacunas identificadas na garantia de um direito específico devem ser encaminhadas ao processo de gestão de riscos (seção 5 do modelo), na medida em que a impossibilidade de exercício de um direito pelo titular configura, em si, um risco a ser tratado acerca da liberdade e dos direitos fundamentais dos titulares.

4.4 Gestão de riscos

A seção 5 do modelo (Gestão de riscos) reúne os critérios básicos de avaliação (impacto, probabilidade, estimativa e aceitação de riscos), a identificação, análise e avaliação dos riscos propriamente ditos, o tratamento dos riscos identificados e o registro dos riscos residuais que permanecem acima do nível de aceitação.

Esta é a seção do RIPD para a qual convergem os resultados das análises anteriores: riscos podem ser identificados tanto a partir de lacunas apontadas na análise dos princípios (subseção 4.2 deste Guia) e na garantia dos direitos dos titulares (subseção 4.3), quanto a partir de vulnerabilidades próprias do desenho técnico e organizacional do tratamento descrito na subseção 4.1.

Recomenda-se que os critérios de impacto, probabilidade e aceitação adotados nesta seção estejam alinhados à metodologia de gestão de riscos do órgão ou entidade e à sua declaração de apetite a risco, conforme já discutido na subseção 3.3 deste Guia, de modo que o RIPD não constitua uma matriz de riscos paralela e desconectada da governança de riscos institucional.

4.5 Versionamento e atualização do RIPD

O RIPD não é um documento estático: deve ser revisado sempre que houver alteração relevante no tratamento de dados pessoais que descreve, entre elas: inclusão de nova finalidade ou de novos tipos de dados pessoais tratados; alteração da hipótese legal aplicável; inclusão de novo agente de tratamento, compartilhamento ou transferência internacional de dados pessoais; novas orientações ou regulamentações da ANPD; ou mudança relevante no cenário de riscos identificado, decorrente, por exemplo, de incidente de segurança.

A comunicação de incidente de segurança à ANPD (Resolução CD/ANPD nº 15, de 24 de abril de 2024) constitui, igualmente, gatilho obrigatório de revisão do RIPD, devendo ser avaliado se o incidente alterou o cenário de riscos originalmente identificado.

Recomenda-se, como boa prática, a revisão periódica do RIPD – independentemente da ocorrência dos gatilhos apontados nesta seção –, com periodicidade mínima anual, ou conforme definido pela unidade responsável em alinhamento com a metodologia de gestão de riscos institucional do órgão ou entidade.

4.6 Aprovação

A seção 7 do modelo (Aprovação) formaliza a validação do RIPD pelo representante do controlador. Reforça-se que a aprovação compete exclusivamente ao controlador.

As partes interessadas eventualmente consultadas ao longo da elaboração do relatório, conforme registrado na subseção 2.3.3 do modelo, não assinam o RIPD, ainda que suas manifestações devam ser consideradas e, quando divergentes, expressamente endereçadas. Quando pertinente, as partes interessadas poderão, no máximo, apor assinatura exclusivamente em suas próprias manifestações, pareceres ou registros de posicionamento, sem que isso implique aprovação, validação ou corresponsabilidade pelo conteúdo final do RIPD. Compete ao controlador analisar criticamente tais manifestações, solicitar os esclarecimentos que entender necessários e promover as diligências cabíveis até que disponha de elementos suficientes para fundamentar as decisões e os encaminhamentos registrados no relatório.

5 Considerações finais

O RIPD não se limita a demonstrar conformidade com a LGPD: é a documentação pela qual o controlador apresenta, de forma auditável, que ponderou riscos, obrigações e direitos dos titulares antes de iniciar, ou ao revisar, uma operação de tratamento de dados pessoais.

O RIPD constitui, ademais, uma das possíveis evidências primárias de conformidade em processos de fiscalização da ANPD, devendo ser elaborado com rigor técnico e guardado em formato que permita sua apresentação quando requisitado (FAQ ANPD, Pergunta 10).

As orientações reunidas neste Guia visam apoiar os órgãos e entidades do SISP na elaboração de relatórios que sejam, simultaneamente, juridicamente fundamentados e operacionalmente úteis à gestão de riscos do órgão ou entidade. Como destacado na subseção 4.2, essa fundamentação jurídica não se resume à identificação de uma hipótese legal válida ou à limitação do volume de dados pessoais tratados: a observância dos princípios do art. 6º da LGPD e a garantia efetiva dos direitos dos titulares são elementos autônomos de conformidade, que devem ser demonstrados de forma independente em cada RIPD.

A elaboração do RIPD, contudo, não é um ato isolado. Ela pressupõe que o órgão ou entidade tenha previamente mapeado as operações de tratamento de dados pessoais realizadas no âmbito do produto ou serviço analisado – identificando finalidades, bases legais, tipos de dados pessoais, agentes de tratamento envolvidos e prazos de retenção, conforme o registro elaborado em decorrência do Controle 19 do *framework* do PPSI 2.0. Sem esse mapeamento prévio, o RIPD corre o risco de ser um documento genérico, desconectado da realidade do tratamento – e, portanto, incapaz de cumprir sua função de instrumento de governança e de gestão de riscos.

Por fim, cabe situar o RIPD no contexto mais amplo do dever de prestação de contas do Poder Público. Dado o caráter frequentemente compulsório do tratamento de dados pessoais para a prestação de serviços estatais, mitigar proativamente os riscos às liberdades civis e aos direitos fundamentais dos titulares é um dever ético que protege o titular e preserva a legitimidade das instituições públicas.

Referências bibliográficas

1. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 mai. 2026.

2. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.** Estabelece as diretrizes para a governança de tecnologia da informação e comunicação. Diário Oficial da União: seção 1, Brasília, DF, 29 out. 2025. Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 22 mai. 2026.

3. BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprova o Glossário de Segurança da Informação. Brasília, DF: GSI/PR, 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 23 mai. 2026.

4. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia do *Framework* de Privacidade e Segurança da Informação (PPSI 2.0)**. Versão 1.2. Brasília: MGI, 30 jan. 2026. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/. Acesso em: 24 jul. 2026.

5. BRASIL. Autoridade Nacional de Proteção de Dados. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**: **perguntas e respostas**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 24 jul. 2026.

6. BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 18, de 16 de julho de 2024.** Aprova o Regulamento sobre a atuação do Encarregado pelo tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 17 jul. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 24 jul. 2026.

7. BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 24 jul. 2026.

8. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**: WP 248 rev.01. [S. l.]: Grupo de Trabalho do Artigo 29.º, 4 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 24 jul. 2026.

9. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Gestão de Riscos**. 1. ed. Brasília: MGI, 2025. Disponível em: https://www.gov.br/gestao/pt-br/acesso-a-informacao/estrategia-e-governanca/estrutura-de-governanca/citarc/guia_gr_mgi.pdf. Acesso em: 24 jul. 2026.

10. BRASIL. Lei nº 15.211, de 17 de setembro de 2025. **Institui medidas para a proteção de crianças e adolescentes em ambientes digitais (ECA Digital).** Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 24 jul. 2026.

gov.br

Dúvida?

Entre em contato conosco

Sítio do PPSI:
PPSI 2.0 — Governo Digital