Modelo de Relatório de Impacto à Proteção de Dados Pessoais

Programa de Privacidade e Segurança da Informação

PPSI 2.0

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Versão 1.0

Brasília, 31 de julho de 2026

MODELO DE RELATÓRIO 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
Ricardo Borges Almeida

EQUIPE DE REVISÃO
Marta Juvina de Medeiros

Histórico de versões

Versão	Data	Descrição	Autor
1.0	31/07/2026	Elaboração do Modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	Equipe Técnica de Elaboração

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?

Orientações

1. Este modelo, assim como todos os modelos disponibilizados pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, deve ser utilizado como uma referência pelos órgãos e entidades, devendo ser realizada uma análise e adaptação considerando as particularidades dos seus ambientes a fim de construir diretrizes que sejam adequadas à sua realidade e às boas práticas.
2. O presente documento apoia diretamente a implementação das medidas 23.3, 25.8 e 25.10 do *framework* do PPSI 2.0.
3. As informações [destacadas em amarelo] neste modelo devem ser substituídas conforme o caso concreto. As [dispostas em vermelho], por sua vez, devem ser removidas. Também devem ser removidas, antes da publicação do documento, a capa, esta página e a página final.
4. Sobre as versões integral (interna) e publicizável (externa) do RIPD:

a. este modelo foi estruturado como modelo matriz, a partir do qual o órgão ou entidade deverá elaborar o RIPD integral e, quando entender necessária, a respectiva versão publicizável ou extrato público;

b. a versão integral do RIPD destina-se ao uso interno do órgão, à governança institucional, à prestação de contas e ao eventual encaminhamento à Agência Nacional de Proteção de Dados (ANPD), quando solicitado ou determinado; a versão publicizável, por sua vez, demonstra à sociedade o compromisso do controlador com a privacidade dos titulares e deve evitar a exposição de informações que possam comprometer 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;

c. sugere-se considerar, em regra, como informações publicizáveis: informações gerais sobre o produto ou serviço, escopo do RIPD, finalidade geral do tratamento, tipos de dados pessoais, categorias gerais de titulares, hipóteses legais de tratamento, informações gerais sobre compartilhamentos e transferências internacionais, prazos ou critérios gerais de retenção, canais de atendimento aos titulares, medidas gerais de transparência e governança, histórico público de atualizações e aprovação do RIPD;

d. quanto ao conteúdo publicizável com cautela, recomenda-se: justificativas de necessidade do RIPD, divergências, critérios de alto risco, descrição dos tratamentos, compartilhamentos, transferências internacionais, eliminação de dados, análise dos princípios da LGPD, medidas de atendimento aos direitos dos titulares e informações sobre agentes de tratamento, desde que redigidos em nível de generalidade adequado e sem exposição de detalhes técnicos, operacionais, contratuais ou de segurança;

e. por sua vez, o conteúdo restrito ou não recomendado para publicização envolve 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, identificação e análise de riscos, probabilidade, impacto, nível de risco, matriz de riscos preenchida, medidas específicas de tratamento de riscos, controles técnicos e administrativos

detalhados, testes de segurança, monitoramento, indicadores internos, riscos residuais, justificativas de aceitação de riscos e autoridade responsável por aprovar exceções;

f. a existência de informação considerada não publicizável em determinada seção ou subseção deste modelo não impede, caso o órgão ou entidade entenda necessário, a publicização de informações gerais sobre o mesmo tema. Nesses casos, o órgão ou entidade deverá elaborar redação resumida, agregada ou descritiva, de modo a não revelar vulnerabilidades, fragilidades, controles internos ou informações protegidas;

g. recomenda-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.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS DO [NOME DO PRODUTO OU SERVIÇO OBJETO DESTE RIPD]

Seção 1
Contexto do produto ou serviço

[A Agência Nacional de Proteção de Dados (ANPD), em suas perguntas e respostas sobre o RIPD, orienta que um relatório deve corresponder a cada **projeto ou processo** do controlador que reúna um conjunto de operações de tratamento voltadas a **uma mesma finalidade**. No âmbito do Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, e com vistas a manter a uniformidade com os termos já dispostos na LGPD, as seguintes ressalvas devem ser observadas:

- este modelo adota o termo "**produto ou serviço**" como unidade de escopo do RIPD, sem prejuízo do conteúdo da orientação da ANPD acima citada. No escopo deste modelo, o produto ou serviço pode corresponder, conforme a estruturação do órgão ou entidade, a um programa, um processo negocial, um sistema ou outra unidade equivalente.
- é importante distinguir a **finalidade do produto ou serviço** (finalidade geral, tratada nesta seção) das **finalidades do tratamento de dados pessoais** (finalidades específicas, nos termos do art. 6º, I, da LGPD), que são identificadas e descritas individualmente na subseção 2.1.]

Assim, nesta seção devem ser registradas as informações que apresentem uma visão clara do produto ou serviço considerando a sua **finalidade geral**, mencionando brevemente os tratamentos de dados pessoais advindos da finalidade geral e esclarecendo a necessidade de elaboração deste relatório. Deve-se atentar para não antecipar conteúdos que serão abordados nas seções e subseções seguintes.]

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é a documentação do controlador que descreve os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas de mitigação adotadas para mitigação dos riscos, nos termos do art. 5º, XVII, da LGPD.

Este RIPD possui como escopo o [nome do produto ou serviço].

O documento está organizado nas seguintes seções: contexto do tratamento (seção 1); tratamento dos dados pessoais, compreendendo a descrição das operações e o fluxo, os agentes envolvidos, os compartilhamentos, as transferências internacionais, a eliminação e os sistemas de informação relacionados (seção 2); análise dos princípios da LGPD (seção 3); garantia do exercício dos direitos pelos titulares (seção 4); gestão de riscos (seção 5); histórico de atualizações (seção 6) e aprovação (seção 7).

1.1 Visão geral

[Apresentar breve contextualização do produto ou serviço objeto deste RIPD, situando o contexto em que o tratamento de dados pessoais ocorre. Incluir apenas informações básicas e estritamente necessárias à compreensão do escopo, sem antecipar conteúdos detalhados nas demais seções, como finalidades e hipóteses de tratamento, agentes envolvidos ou riscos.]

1.2 Necessidade do RIPD

A elaboração deste RIPD observa as orientações da Agência Nacional de Proteção de Dados (ANPD) e decorre de uma ou mais das razões a seguir:

☐ determinação ou solicitação da referida Agência (LGPD, art. 10, § 3º; art. 32 ou art. 38);

☐ decisão do próprio controlador;

☐ enquadramento do tratamento como de alto risco, conforme apresentado a seguir.

A página do sítio da ANPD que dispõe sobre perguntas e respostas acerca do RIPD[2] indica que, na ausência de regulamentação específica da ANPD sobre o RIPD, adota-se 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 – segundo o qual o tratamento de dados pessoais é considerado de alto risco quando presentes, cumulativamente, ao menos um dos critérios gerais e ao menos um dos critérios específicos assinalados na Tabela 1.

[Não sendo o tratamento enquadrado como de alto risco, indicar e argumentar sobre a razão que fundamenta a elaboração deste RIPD. A tabela abaixo poderá ser excluída, ou ainda assim, ser utilizada como referência para construção da argumentação.]

Tabela 1: critérios gerais e específicos sobre alto risco

Critérios gerais (assinalar ao menos um)	Presente?	Justificativa
Tratamento de dados pessoais em larga escala – número significativo de titulares, considerados o volume de dados pessoais, a duração, a frequência e a extensão geográfica do tratamento	☐ Sim ☐ Não	[Indicar o volume dos dados pessoais tratados, o número de titulares envolvidos, além da duração, da frequência e da extensão geográfica do tratamento.]
Tratamento de dados pessoais que possa afetar significativamente interesses e	☐ Sim	[Indicar como o tratamento dos dados pessoais pode impedir o

[2] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd

direitos fundamentais dos titulares – inclusive quando puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais	☐ Não	exercício de direitos ou a utilização de um serviço, ou ocasionar danos materiais ou morais aos titulares.]
Critérios específicos (assinalar ao menos um)	**Presente?**	**Justificativa**
Uso de tecnologias emergentes ou inovadoras	☐ Sim ☐ Não	[Identificar a tecnologia emergente ou inovadora empregada e seu papel no tratamento dos dados pessoais.]
Vigilância ou controle de zonas acessíveis ao público	☐ Sim ☐ Não	[Descrever a zona acessível ao público que é monitorada e os meios de vigilância ou controle utilizados.]
Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive as destinadas a definir perfil pessoal, profissional, de saúde, de consumo, de crédito ou aspectos da personalidade do titular	☐ Sim ☐ Não	[Descrever a decisão automatizada e o tipo de perfil definido.]
Utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos	☐ Sim ☐ Não	[Indicar os dados pessoais sensíveis ou os dados pessoais de crianças, de adolescentes ou de idosos envolvidos.]

Seção 2
Tratamento dos dados pessoais

[Detalhar nas subseções a seguir cada etapa do produto ou serviço que envolve o tratamento de dados pessoais, desde a coleta até o descarte. A principal fonte de informações desta seção deve ser o registro das operações de tratamento, do inglês *Record of Processing Activities* (ROPA).]

As operações de tratamento de dados pessoais descritas nesta seção correspondem às consignadas no registro das operações de tratamento do [órgão ou entidade] e abrangem o fluxo dos dados pessoais, as finalidades e hipóteses de tratamento, os agentes de tratamento envolvidos, os compartilhamentos, as transferências internacionais e os sistemas de informação que suportam essas operações.

2.1 Descrição do(s) tratamento(s)

[Preencher a tabela abaixo, utilizando uma linha para cada finalidade e substituindo o conteúdo destacado em amarelo. O quadro reproduz a estrutura da tabela de finalidades do Modelo de Aviso de Privacidade, disponibilizado no âmbito do PPSI. Na descrição do tratamento, considerar as operações do inciso X do art. 5º da LGPD (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração). Nos tipos de dados pessoais, agrupar por categoria (cadastrais, de contato, funcionais, financeiros, de localização etc.), conforme o inciso I do art. 5º da LGPD.]

A **Tabela 2** apresenta, para cada finalidade de tratamento específica, a respectiva descrição do tratamento, a categoria de titulares-alvo do [produto ou serviço], os tipos de dados pessoais tratados, bem como a hipótese de tratamento, [a previsão normativa (quando aplicável)] e a justificativa para a hipótese relacionada.

Tabela 2: descrição do tratamento para a finalidade [finalidade específica do tratamento]

Finalidade do tratamento	[Finalidade específica do tratamento]
Descrição do tratamento	[Descrição objetiva do tratamento dos dados pessoais realizado para atingir a finalidade específica – poderá ser detalhada em 2.2]
Categorias de titulares	[Categorias de titulares abrangidos, destacando a presença de crianças, adolescentes ou outras categorias de vulneráveis (por exemplo, idosos)]
Tipos de dados pessoais	[Tipos de dados pessoais, agrupados por categoria, com indicação destacada para dados pessoais sensíveis]
Hipótese de tratamento	[Hipótese aplicável (art. 7º ou art. 11 da LGPD)]
Previsão normativa (caso hipótese seja art. 7º, incisos II ou III, ou art. 11, inciso II, alíneas a) ou b))	[Indicação da previsão normativa caso a hipótese de tratamento seja art. 7º, incisos II ou III, ou art. 11, inciso II, alíneas a) ou b)]
Justificativa para escolha da hipótese de tratamento	[Argumentação para definição da hipótese de tratamento registrada acima]

2.2 Fluxo do tratamento dos dados pessoais

[Apresentar o fluxo do tratamento dos dados pessoais de forma clara, completa e de fácil compreensão, permitindo que qualquer pessoa entenda como os dados pessoais são tratados. Utilize recursos visuais, tais como fluxogramas, diagramas, tabelas ou imagens para ilustrar o fluxo dos dados pessoais e facilitar a compreensão das etapas do tratamento. Descrever, ainda, os meios pelos quais os dados pessoais são obtidos (forma de coleta) e a tramitação ou fluxo interno dos dados pessoais entre unidades do órgão ou entidade, quando houver.]

2.3 Agentes de tratamento e partes interessadas ou envolvidas

[Nesta subseção devem ser apresentados os agentes de tratamento envolvidos no tratamento de dados pessoais, bem como as responsabilidades de cada um. Também devem ser registradas outras partes interessadas envolvidas no tratamento, conforme "**Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**" da ANPD.]

Nesta subseção, são apresentados os agentes de tratamento e as demais partes interessadas ou envolvidas no tratamento de dados pessoais objeto deste RIPD.

2.3.1 Controlador(es)

[Identificar todos os controladores envolvidos no tratamento, indicando se atuam como controladores singulares ou conjuntos; registrar também os respectivos encarregados pelo tratamento de dados pessoais. Replicar o quadro abaixo para cada controlador.]

CONTROLADOR [órgão ou entidade]

CNPJ: [CNPJ do órgão ou entidade]

Endereço: [endereço completo do órgão ou entidade]

Contato: [dados de contato com a unidade responsável pelo produto ou serviço]

Enquadramento do agente de tratamento: [indicar se o órgão atua como controlador singular ou controlador conjunto]

Responsabilidade: [registrar as decisões referentes aos tratamentos dos dados pessoais no âmbito do produto ou serviço]

Encarregado: [identificação e dados de contato do encarregado pelo tratamento de dados pessoais]

Encarregado substituto: [identificação e dados de contato do encarregado pelo tratamento de dados pessoais substituto]

O encarregado foi consultado na elaboração deste RIPD?

☐ Sim: [conforme registro no Anexo X]

☐ Não: [justificar razões pelas quais o encarregado não foi consultado]

2.3.2 Operador(es)

[Descrever nesta subseção os operadores envolvidos no tratamento (o operador deve ser um ente distinto do controlador). Repetir o bloco abaixo para cada operador. Caso não haja operador, indicar nesta subseção que "não há operadores envolvidos"].

OPERADOR [Identificação do operador – razão social ou nome completo]

CNPJ / CPF: [número de CNPJ ou CPF]

Responsabilidade: Realizar o tratamento de dados pessoais em nome do [órgão ou entidade] no que se refere a [descrição das atividades que o operador executa].

Este operador foi consultado na elaboração deste RIPD?

☐ Sim: [informar aqui o registro da evidência com respectiva manifestação (ex.: conforme registro no Anexo X)].

Motivo da consulta: [registrar qual o envolvimento do operador no objeto deste RIPD, justificando a razão pela qual ele foi consultado]

☐ Não: [justificativa]

Divergências: [descrever a existência ou não de divergências, indicando pontualmente a(s) divergência(s) existente(s) juntamente aos respectivos encaminhamentos e justificativa da opção escolhida]

2.3.3 Outra(s) parte(s) interessada(s) ou envolvida(s) no tratamento

[Identificar nesta subseção outras partes interessadas ou envolvidas no tratamento, a exemplo das áreas jurídica, financeira, de tecnologia ou de outras áreas de negócio. Caso as partes sejam consultadas no processo de elaboração, recomenda-se que as consultas e respectivas manifestações sejam registradas em documentos próprios – por exemplo, notas técnicas sobre a consulta –, que podem ser anexados a este RIPD. Destaca-se que a aprovação do Relatório compete ao representante do controlador. Replicar o quadro para cada parte interessada consultada; caso não haja partes interessadas, registrar expressamente essa condição.]

PARTE INTERESSADA [Razão social ou nome completo da parte interessada]

CNPJ / CPF: [número de CNPJ ou CPF da parte interessada]

Contato: [dados de contato da parte interessada]

Esta parte foi consultada na elaboração deste RIPD?

☐ Sim: [informar aqui o registro da evidência com respectiva manifestação (ex.: conforme registro no Anexo X)].

Motivo da consulta: [registrar qual o envolvimento da parte no objeto deste RIPD, justificando a razão pela qual ela foi consultada]

☐ Não: [justificativa]

Divergências: [descrever a existência ou não de divergências, indicando pontualmente a(s) divergência(s) existente(s) juntamente aos respectivos encaminhamentos e justificativa da opção escolhida]

2.4 Compartilhamento de dados pessoais

[Considera-se compartilhamento, para os fins deste modelo de RIPD, a comunicação de dados pessoais a outro controlador. O envio de dados pessoais a operador que atue por conta e sob instruções do controlador não constitui compartilhamento e deve ser tratado na subseção "2.3 Agentes de tratamento". A tramitação ou o fluxo interno de dados pessoais entre unidades do próprio órgão ou entidade também não configura compartilhamento, devendo ser descrito na subseção "2.2 Fluxo do tratamento dos dados pessoais". As transferências internacionais de dados pessoais são objeto da subseção 2.5.

Selecionar a opção aplicável: A (sem compartilhamento) ou B (com compartilhamento) e remover a opção não utilizada, bem como as instruções desta subseção.]

[Opção A – sem compartilhamento:] No âmbito do [produto ou serviço], o [órgão ou entidade] não realiza nenhum compartilhamento de dados pessoais.

[Opção B – com compartilhamento:] No âmbito do [produto ou serviço], o [órgão ou entidade] realiza compartilhamento de dados pessoais com as seguintes instituições, previamente identificadas na lista de controladores em 2.3.1:

[Consolidar na tabela abaixo, em linhas individualizadas, todos os compartilhamentos de dados pessoais realizados.]

Tabela 3: compartilhamentos de dados pessoais

Razão social	Finalidade do compartilhamento	Tipos de dados pessoais compartilhados	Hipótese de tratamento e previsão normativa	Previsão normativa
[razão social]	[finalidade]	[tipos de dados pessoais]	[identificação da base legal, conforme art. 7º ou 11 da LGPD]	[previsão normativa, quando aplicável]
[adicionar linhas				

conforme necessário]				

2.5 Transferência internacional de dados pessoais

[Considera-se transferência internacional a operação de tratamento por meio da qual o órgão ou entidade transmite, compartilha ou disponibiliza acesso a dados pessoais a agente de tratamento localizado em país estrangeiro ou organismo internacional, observados os arts. 33 a 36 da LGPD e a Resolução CD/ANPD nº 19, de 23 de agosto de 2024.

Selecionar a opção aplicável e remover a não utilizada, bem como as instruções desta subseção. Caso a opção B seja utilizada, consolidar no modelo de tabela abaixo, em linhas individualizadas, as transferências internacionais de dados pessoais realizadas. Não havendo transferência internacional, escolher a Opção A e registrar expressamente a condição.]

[Opção A – sem transferência internacional:] No âmbito do [produto ou serviço], o [órgão ou entidade] não realiza nenhuma transferência internacional de dados pessoais.

[Opção B – com transferência internacional:] No âmbito do [produto ou serviço], o [órgão ou entidade] realiza transferência internacional de dados pessoais – observando as hipóteses e garantias previstas nos art. 33 a art. 36 da LGPD e na Resolução CD/ANPD nº 19, de 23 de agosto de 2024 – para os seguintes países ou organismos internacionais:

Tabela 4: transferências internacionais de dados pessoais

Razão social	**Tipos de dados pessoais transferidos**	**País(es) ou organismo(s) internacional(is) de destino**	**Mecanismo de transferência internacional**
[razão social]	[tipos de dados pessoais]	[país(es) ou organismo(s) de destino]	[mecanismo aplicável, nos termos do art. 33 da LGPD]
[adicionar linhas conforme necessário]			

2.6 Eliminação de dados pessoais

[Preencher a tabela abaixo por finalidade ou tipo de dado pessoal, substituindo o conteúdo destacado em amarelo. Indicar, quando aplicável, os períodos específicos de retenção, datas-limite ou critérios objetivos para determinação do término do tratamento – por exemplo, "5 anos a partir da data da coleta" ou "até a publicação da decisão final no processo administrativo".]

Os dados pessoais tratados no âmbito das finalidades descritas na **subseção 2.1** serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação nas hipóteses previstas no art. 16 da LGPD.

Tabela 5: eliminação de dados pessoais

Finalidade ou tipo de dado pessoal	**Prazo ou critério objetivo de retenção**	**Hipótese de conservação após o término do tratamento (art. 16 da LGPD)**	**Método de descarte**
[finalidade ou tipo de dado pessoal]	[prazo específico, data-limite ou critério objetivo]	[hipótese aplicável do art. 16, se houver conservação]	[forma de eliminação segura]
[adicionar linhas conforme necessário]			

2.7 Sistemas de informação relacionados

[Relacionar os sistemas de informação que suportam as operações de tratamento objeto deste RIPD, indicando, para cada um, a organização hospedeira (própria, outro órgão ou fornecedor externo), a condição de sistema estruturante ou não estruturante, e a(s) funcionalidade(s) ou recurso(s) do sistema relacionado(s) ao tratamento de dados pessoais no âmbito do produto ou serviço.]

Tabela 6: sistemas de informação que suportam o [produto ou serviço]

Sistema de informação	**Organização hospedeira**	**Sistema estruturante?**	**Funcionalidades**
[nome do sistema, aplicação ou plataforma]	[próprio órgão / outro órgão / fornecedor externo - identificar]	☐ Sim ☐ Não	[indicar a(s) funcionalidade(s) relacionada(s) ao tratamento de dados pessoais suportada(s) por este sistema no âmbito do produto ou serviço]
[adicionar linhas conforme necessário]			

Seção 3
Análise dos princípios da LGPD

Esta seção demonstra que o tratamento dos dados pessoais descrito na **subseção 2.1** deste documento está sendo realizado em estrita observância dos princípios definidos no art. 6º da LGPD.

3.1 Princípio da finalidade

[Art. 6º, I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

a) Legítima: a finalidade deve estar amparada em hipótese de tratamento válida (art. 7º ou art. 11 da LGPD) e ser compatível com a legislação. A argumentação pode ser construída com base no campo hipótese de tratamento das tabelas de descrição do tratamento dispostas na subseção 2.1 deste documento, bem como na indicação de outra legislação relacionada ao escopo deste RIPD.

b) Específica: a finalidade deve ser definida de forma clara e precisa desde o momento da coleta, evitando descrições genéricas como "diversas finalidades" ou "aprimoramento dos serviços". Isso pode ser argumentado referenciando o campo finalidade do tratamento contido nas tabelas de descrição do tratamento da subseção 2.1 deste documento. Também pode ser considerada a inclusão de cláusulas que delimitem as finalidades em instrumentos de compartilhamento ou de transferência internacional e em contratos com operadores.

c) Explícita e informada ao titular: a finalidade deve ser comunicada de forma aberta e compreensível ao titular, não bastando que seja inferida a partir do contexto ou mencionada apenas em termos de uso genéricos. Uma das principais formas de atendimento deste requisito é pela disponibilização de avisos de privacidade, podendo ser anexado ao RIPD, bem como registrada a forma pela qual ele é apresentado aos titulares.

d) Sem tratamento posterior incompatível: os dados pessoais tratados para cada finalidade não podem ser reutilizados para finalidade incompatível com a original. Exemplo de medida relevante pode ser o registro no RIPD, bem como em aviso de privacidade, indicando que os tratamentos dos dados pessoais estão estritamente vinculados às finalidades informadas ao titular e que qualquer outra finalidade incompatível será objeto de nova análise de conformidade.]

A realização do tratamento para propósitos legítimos, específicos e sem possibilidade de tratamento posterior de forma incompatível com essas finalidades fica demonstrada na **subseção 2.1** deste documento, especialmente considerando as **finalidades** apresentadas, as respectivas **descrições**, bem como **hipóteses de tratamento** registradas. Adicionalmente, destaca-se que os propósitos são explícitos e informados ao titular em razão do aviso de privacidade disposto no [Anexo X], que é apresentado ao titular antes do tratamento de seus dados pessoais no [local Y].

3.2 Princípio da adequação

[Art. 6º, II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Recomenda-se garantir que a descrição do tratamento para cada finalidade disposta na subseção 2.1 seja suficientemente clara para compreender que o tratamento é compatível com a finalidade, além de descrever sobre como os titulares de dados pessoais serão informados sobre as finalidades do tratamento, a exemplo da apresentação do aviso de privacidade em um determinado local – *link* em um site, placa com *QR Code* em balcão de cadastro, entre outros.]

A compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, fica demonstrada pela **descrição do tratamento** associada a cada **finalidade** disposta na **subseção 2.1** deste documento, bem como pelo aviso de privacidade disposto no [Anexo X] – que é apresentado aos titulares antes do tratamento de seus dados pessoais no [local Y].

3.3 Princípio da necessidade

[Art. 6º, III - necessidade: limitação do 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.

a) Mínimo necessário: o tratamento deve limitar-se ao estritamente indispensável à realização da finalidade, evitando a coleta de dados pessoais apenas por eventual utilidade futura não determinada.

b) Pertinência: cada dado pessoal tratado deve guardar vínculo lógico e direto com a finalidade informada; dados sem essa relação não devem ser tratados.

c) Proporcionalidade e não excesso: o volume, o nível de detalhamento e a abrangência de titulares alcançados pelo tratamento não podem exceder o que a finalidade razoavelmente demanda – o que inclui não tratar dados de todo um grupo quando apenas um subconjunto de titulares é necessário, tampouco tratar dados pessoais além do exigido pela finalidade.

Uma possível forma de demonstrar o atendimento deste princípio é justificá-lo pela argumentação e informações dispostas nas tabelas de descrição do tratamento na subseção 2.1, revisando e inserindo informações complementares que esclareçam a conformidade ao disposto neste princípio. Exemplos de medida: justificativa fundamentada de que os dados pessoais tratados são estritamente necessários às finalidades informadas; revisão periódica dos campos tratados frente à finalidade declarada, com eliminação ou anonimização dos dados que se mostrarem excessivos; ou adoção de política de retenção proporcional, conforme registrado na subseção 2.6.]

A limitação do tratamento ao mínimo necessário para a realização de suas finalidades – com abrangência dos dados pessoais pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados pessoais – fica demonstrada nos campos **tipos de dados pessoais**, **descrição do tratamento** e **finalidade do tratamento** contidos nas tabelas de **descrição do tratamento** dispostas na **subseção 2.1** deste documento, bem como na subseção 2.6.

3.4 Princípio do livre acesso

[Art. 6º, IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

a) Consulta facilitada: o titular deve dispor de meios simples e acessíveis para exercer seus direitos relacionados aos dados pessoais tratados, sem exigências desproporcionais ou procedimentos excessivamente complexos. Recomenda-se descrever os canais disponibilizados para atendimento aos titulares, tais como portal eletrônico, endereço eletrônico institucional, serviço de protocolo ou atendimento presencial.

b) Gratuidade: o exercício do direito de acesso deve ser assegurado gratuitamente, ressalvadas as hipóteses previstas na legislação. Recomenda-se registrar no RIPD que o atendimento às solicitações relacionadas aos direitos dos titulares não implica cobrança de qualquer valor.

c) Forma e duração do tratamento: o titular deve poder obter informações sobre como seus dados pessoais são tratados, incluindo as finalidades, hipóteses legais, tipos de dados pessoais tratados, compartilhamentos realizados, prazos de retenção e critérios utilizados para eliminação ou anonimização dos dados. Essas informações podem ser disponibilizadas por meio do aviso de privacidade e complementadas mediante solicitação do titular, sendo relevante o registro nesta subseção sobre como esses recursos poderão ser operacionalizados.

d) Integralidade dos dados pessoais: o titular deve poder solicitar acesso aos seus dados pessoais tratados pelo controlador. Recomenda-se indicar como esse acesso será operacionalizado pelo órgão, seja por meio de funcionalidade tecnológica específica ou de solicitação aos responsáveis pelo serviço (em complemento à solicitação via encarregado para atendimento do direito previsto no inciso II do art. 18 da LGPD).

Sugestões práticas para demonstrar o atendimento deste princípio incluem: a disponibilização de canal eletrônico de autoatendimento para consulta aos dados pessoais tratados; o registro dos demais canais disponibilizados para atendimento aos titulares; a referência ao aviso de privacidade; e a descrição dos procedimentos adotados para resposta às solicitações de acesso aos dados pessoais do titular, incluindo os responsáveis pelo atendimento e, quando aplicável, a atuação do encarregado pelo tratamento de dados pessoais – alinhando-se ao disposto na seção 4 quanto ao direito do art. 18, II.]

A garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos dados pessoais tratados, é assegurada por meio dos canais de

atendimento disponibilizados aos titulares, descritos no aviso de privacidade constante do [Anexo X], bem como pelos demais canais institucionais de atendimento do órgão dispostos a seguir:

- atendimento presencial: [informar o local e documentos necessários para o atendimento]
- [informar demais canais de atendimento além dos já dispostos no aviso de privacidade]

Por meio desses canais, os titulares podem obter informações sobre o tratamento de seus dados pessoais, incluindo as finalidades do tratamento, as hipóteses legais aplicáveis, os prazos de retenção, os compartilhamentos e transferências internacionais eventualmente realizadas e demais informações pertinentes, além de viabilizar o exercício dos demais direitos previstos na LGPD.

As solicitações são tratadas de forma gratuita e em conformidade com os procedimentos internos do órgão, observados os prazos e as limitações previstos na legislação aplicável.

3.5 Princípio da qualidade dos dados

[Art. 6º, V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

a) Exatidão: os dados pessoais tratados devem representar corretamente as informações relativas ao titular, reduzindo a ocorrência de registros incorretos, incompletos ou inconsistentes. Recomenda-se descrever as medidas adotadas para validação das informações no momento da coleta e durante sua utilização, especialmente quando essas informações possam subsidiar decisões que afetem o titular, considerando possíveis integrações com outros sistemas para coleta de dados pessoais (ex.: autenticação via gov.br).

b) Clareza: os registros de dados pessoais devem ser mantidos de forma compreensível, preservando seu significado e contexto. Quando aplicável, recomenda-se identificar a origem dos dados, distinguir fatos objetivos de registros opinativos ou estimativas e manter histórico das alterações relevantes, evitando interpretações equivocadas.

c) Relevância: a qualidade dos dados também depende de sua adequação à finalidade do tratamento. Recomenda-se demonstrar que os dados utilizados permanecem pertinentes para a finalidade declarada e que informações reconhecidamente incorretas, desnecessárias ou desatualizadas são corrigidas, eliminadas ou deixam de ser utilizadas, conforme o caso.

d) Atualização: devem ser adotados procedimentos para a revisão e atualização dos dados pessoais. Recomenda-se incluir mecanismos proativos de atualização – que não dependam de iniciativa do titular –, tais como: integração com bases de dados oficiais para verificação e sincronização periódica das informações (ex.: consulta a cadastros da Receita Federal, do gov.br ou de outros registros públicos); rotinas automatizadas de revalidação cadastral em periodicidade definida, com bloqueio ou sinalização dos registros vencidos até a confirmação pelo titular; notificações ou lembretes ativos ao titular para confirmação ou atualização dos

seus dados, sobretudo antes de eventos que dependam de a informação estar atual (ex.: renovação de benefício, vencimento de documento, celebração de novo contrato); e verificação automática de consistência entre sistemas integrados, com alerta para divergências que indiquem desatualização. Quando não for viável adotar mecanismo proativo, descrever o procedimento reativo disponibilizado ao titular e a periodicidade mínima recomendada para sua utilização.

e) Correção de inconsistências: recomenda-se descrever os procedimentos adotados para tratamento de dados pessoais incorretos ou contestados, incluindo mecanismos para análise das solicitações dos titulares, retificação das informações quando cabível e registro das alterações realizadas, observados os direitos previstos na LGPD.

Para atendimento deste princípio, sugere-se apresentar os mecanismos utilizados para validação das informações tratadas, os procedimentos de atualização cadastral, os controles destinados à identificação e correção de inconsistências, bem como os canais disponibilizados para que os titulares solicitem a retificação de seus dados pessoais. Também podem ser referenciadas políticas de gestão da informação, procedimentos de governança de dados ou controles operacionais que assegurem a manutenção da qualidade dos dados ao longo de seu ciclo de vida. Quando a correção não puder ser realizada diretamente pelo órgão ou entidade – por exemplo, quando o dado tiver origem em base cadastral de outro controlador –, o titular deve ser orientado sobre o meio adequado para realizar a atualização por conta própria ou informado do canal competente para o qual a solicitação deve ser encaminhada.]

A garantia da exatidão, clareza, relevância e atualização dos dados pessoais tratados é assegurada mediante procedimentos de validação das informações coletadas, incluindo:

- utilização de fontes confiáveis de informação: [especificar qual fonte];
- revisão dos registros sempre que necessário à finalidade do tratamento: [descrever o procedimento de revisão];
- adoção de mecanismos para identificação e correção de inconsistências: [apresentar estes mecanismos de forma detalhada].

Os dados pessoais são mantidos compatíveis com as finalidades descritas na **subseção 2.1** deste documento e permanecem atualizados sempre que essa atualização seja necessária para o adequado cumprimento dessas finalidades. Quando aplicável, registros históricos são preservados de forma a refletir corretamente o contexto temporal das informações, sem prejuízo de sua integridade.

Adicionalmente, os titulares podem solicitar a atualização, correção ou complementação de seus dados pessoais por meio dos canais institucionais, conforme os procedimentos internos descritos na **seção 4** acerca do direito previsto no inciso III do art. 18 da LGPD. As solicitações recebidas são analisadas e, quando procedentes, as informações são retificadas sem demora injustificada, preservando-se, quando necessário, os registros das alterações realizadas para fins de rastreabilidade e auditoria.

3.6 Princípio da transparência

[Art. 6º, VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

a) Clareza e precisão das informações: as informações disponibilizadas aos titulares devem descrever o tratamento de dados pessoais de forma objetiva, compreensível e compatível com o público a que se destinam, evitando linguagem excessivamente técnica, ambígua ou genérica. Recomenda-se referenciar o aviso de privacidade elaborado conforme o Guia para Elaboração de Avisos de Privacidade do PPSI, garantindo que ele contemple, de forma consistente e naquilo que lhe cabe, as informações registradas na seção 2 deste RIPD.

b) Facilidade de acesso: as informações sobre o tratamento devem permanecer facilmente acessíveis durante todo o ciclo de vida do tratamento, por meio de canais adequados ao contexto em que os dados pessoais são tratados, como páginas eletrônicas, sistemas, formulários, aplicativos, atendimento presencial ou outros meios institucionais. Recomenda-se indicar como os titulares terão acesso a essas informações.

c) Informações sobre o tratamento: recomenda-se demonstrar que os titulares são informados, de modo adequado, sobre aspectos relevantes do tratamento, tais como as finalidades, as hipóteses legais, os tipos de dados pessoais tratados, os compartilhamentos e as transferências internacionais realizados, os prazos de retenção, os direitos dos titulares, os canais de atendimento e a identificação dos agentes de tratamento, quando aplicável.

d) Transparência ao longo do tratamento: as informações disponibilizadas aos titulares devem permanecer compatíveis com a realidade do tratamento de dados pessoais. Sempre que ocorrerem alterações relevantes nas finalidades, na forma de tratamento, nos tipos de dados tratados ou em outros aspectos que possam impactar os titulares, recomenda-se revisar e atualizar os avisos de privacidade, documentos informativos e demais mecanismos de comunicação utilizados.

e) Limites da transparência: o dever de transparência deve ser observado sem prejuízo da proteção de informações cujo acesso seja restringido por disposição legal, por razões de segurança da informação ou pela necessidade de preservação de segredos comercial, industrial ou de outros interesses legalmente protegidos, em conformidade com a legislação aplicável.

A comprovação da observância deste princípio pode referenciar o aviso de privacidade aplicável ao tratamento, descrever os canais utilizados para disponibilização das informações aos titulares, indicar os mecanismos empregados para comunicação de alterações relevantes no tratamento de dados pessoais e demonstrar que as informações fornecidas permanecem consistentes com os tratamentos descritos no RIPD.]

A garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados pessoais e sobre os respectivos agentes de tratamento é assegurada por meio do aviso de privacidade constante do [Anexo X], bem como pelos demais canais institucionais de comunicação disponibilizados aos titulares.

As informações disponibilizadas aos titulares contemplam, entre outros aspectos, as finalidades do tratamento, as hipóteses legais aplicáveis, os tipos de dados pessoais tratados,

os eventuais compartilhamentos e transferências internacionais, os prazos de retenção, os direitos previstos na LGPD, os canais para exercício desses direitos e as informações de contato dos responsáveis pelo tratamento, quando aplicável.

Os mecanismos de transparência são revisados sempre que ocorrerem alterações relevantes nas atividades de tratamento, de modo a assegurar que as informações disponibilizadas aos titulares permaneçam compatíveis com os tratamentos efetivamente realizados e descritos neste RIPD.

A divulgação dessas informações observa os limites estabelecidos pela legislação aplicável, preservando informações cuja restrição de acesso seja necessária para proteção da segurança da informação, de segredos comercial e industrial ou de outros interesses legalmente protegidos.

3.7 Princípio da segurança

[Art. 6º, VII - segurança: utilização de medidas 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 difusão;

A segurança deve ser observada durante todo o ciclo de vida do tratamento de dados pessoais, mediante a adoção de medidas técnicas e administrativas compatíveis com o tratamento e com os riscos aos direitos e liberdades dos titulares. Essas medidas devem buscar prevenir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais. Para demonstrar a observância deste princípio, recomenda-se considerar, de forma integrada, as medidas descritas nas demais seções do RIPD. Diversas medidas relacionadas à segurança decorrem diretamente da observância dos princípios analisados nesta subseção, dos mecanismos adotados para garantir o exercício dos direitos pelos titulares, descritos na seção 4, e das medidas de tratamento de riscos apresentadas na seção 5, as quais detalham as medidas técnicas e administrativas aplicáveis às atividades de tratamento.]

A utilização de medidas técnicas e administrativas destinadas à proteção dos dados pessoais é evidenciada pelas medidas descritas neste RIPD. Em especial, destacam-se os mecanismos adotados para atendimento aos princípios da LGPD descritos nesta seção, as medidas implementadas para assegurar o exercício dos direitos pelos titulares apresentadas na **seção 4**, bem como as medidas técnicas e administrativas detalhadas na **seção 5**.

Em conjunto, essas medidas buscam proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

3.8 Princípio da prevenção

[Art. 6º, VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

A prevenção pressupõe a adoção de medidas antecipadas destinadas a reduzir a probabilidade de ocorrência de danos aos titulares decorrentes do tratamento de dados pessoais. Diferentemente de uma atuação reativa, baseada exclusivamente na resposta a incidentes, este princípio exige que riscos à privacidade e à proteção de dados pessoais sejam considerados desde a concepção e ao longo de todo o ciclo de vida das atividades de tratamento.

Nesse contexto, recomenda-se considerar a adoção dos princípios de segurança desde a concepção em conjunto com a privacidade desde a concepção (*privacy by design*) e por padrão (*privacy by default*), incorporando medidas de proteção de dados pessoais no planejamento, desenvolvimento, aquisição, implantação, operação, manutenção e descontinuação de processos, serviços, sistemas e demais atividades de tratamento.

Para demonstrar a observância deste princípio, recomenda-se considerar, de forma integrada, as medidas descritas nas demais seções do RIPD. A prevenção de danos aos titulares decorre da adequada observância dos princípios analisados nesta seção, dos mecanismos adotados para garantia do exercício dos direitos pelos titulares, descritos na seção 4, e das medidas de identificação, avaliação, tratamento e monitoramento de riscos apresentadas na seção 5.]

A prevenção da ocorrência de danos decorrentes do tratamento de dados pessoais é promovida mediante a consideração dos aspectos de privacidade e segurança desde a concepção e ao longo de todo o ciclo de vida das atividades de tratamento, buscando identificar e mitigar riscos antes que estes produzam impactos aos titulares dos dados pessoais.

A observância deste princípio é evidenciada pelas medidas descritas neste RIPD – o qual foi concebido antes de iniciarem as atividades de tratamento de dados pessoais – incluindo os mecanismos adotados para atendimento aos princípios da LGPD apresentados nesta seção, as medidas implementadas para garantia do exercício dos direitos pelos titulares descritas na **seção 4** e os processos de identificação, avaliação e tratamento de riscos detalhados na **seção 5**.

Em conjunto, essas medidas contribuem para reduzir a probabilidade de ocorrência de danos aos titulares e para assegurar que a proteção de dados pessoais seja considerada de forma preventiva nas atividades de tratamento realizadas.

3.9 Princípio da não discriminação

[Art. 6º, IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

O tratamento de dados pessoais não deve ser utilizado para produzir discriminações ilícitas ou abusivas contra os titulares. Para tanto, recomenda-se avaliar se as finalidades, os critérios utilizados nas atividades de tratamento, os processos decisórios, as regras de negócio, os modelos estatísticos ou algoritmos empregados podem resultar em tratamento discriminatório incompatível com a legislação ou com os direitos fundamentais dos titulares. Sempre que o tratamento envolver dados pessoais sensíveis, decisões que produzam efeitos

relevantes sobre os titulares, técnicas de perfilamento (*profiling*), inteligência artificial ou outras tecnologias com potencial de gerar vieses discriminatórios, recomenda-se avaliar a necessidade de adoção de medidas adicionais para prevenir ou mitigar riscos.

A observância deste princípio não impede tratamentos diferenciados quando estes decorrerem de obrigação legal, política pública, decisão judicial ou outra hipótese legítima prevista no ordenamento jurídico, desde que compatíveis com a finalidade do tratamento, proporcionais e fundamentados.

Para demonstrar a observância deste princípio, recomenda-se descrever as medidas adotadas para prevenir ou mitigar riscos de discriminação decorrentes do tratamento de dados pessoais, podendo ser referenciadas, quando aplicável, as medidas descritas nesta seção e as medidas de tratamento de riscos apresentadas na seção 5.]

A impossibilidade de utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos é assegurada mediante procedimentos – incluindo a elaboração deste RIPD – destinados a verificar se as finalidades do tratamento, os critérios utilizados para tomada de decisão e as regras de negócio aplicáveis são compatíveis com a legislação, os direitos fundamentais dos titulares e a finalidade que justifica o tratamento.

Dentre as medidas especificamente voltadas para este princípio, a análise sobre possíveis impactos das finalidades – dispostas na **seção 2** – que podem produzir efeitos relevantes sobre os titulares envolveu diferentes áreas da organização, [como as áreas de negócio, jurídica, de proteção de dados e de tecnologia da informação], de modo a avaliar a adequação dos critérios utilizados e reduzir o risco de adoção de práticas discriminatórias.

Outra medida que se destaca diz respeito aos agentes públicos envolvidos nas atividades de tratamento, que receberam orientação e capacitação sobre os princípios da igualdade, da não discriminação e da proteção de dados pessoais.

Essas medidas atuam diretamente sobre os critérios, as regras de negócio e os processos decisórios que orientam o tratamento dos dados pessoais, reduzindo o risco de utilização dos dados para fins discriminatórios ilícitos ou abusivos e contribuindo para que eventuais diferenciações observem critérios objetivos, proporcionais, compatíveis com a finalidade do tratamento e em conformidade com a legislação aplicável.

3.10 Princípio da responsabilização e prestação de contas

[Art. 6º, X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O princípio da responsabilização e prestação de contas pressupõe que o controlador seja capaz de demonstrar, de forma objetiva e verificável, que as atividades de tratamento estão em conformidade com a LGPD e que as medidas adotadas para proteção dos dados pessoais são efetivamente implementadas, monitoradas e periodicamente avaliadas quanto à sua

eficácia. O atendimento a este princípio não decorre apenas da existência isolada de documentos ou controles, mas da adoção de um conjunto consistente de medidas de governança que evidenciem a conformidade das atividades de tratamento ao longo de todo o seu ciclo de vida.

Nesse contexto, recomenda-se demonstrar que a organização mantém mecanismos destinados a documentar as atividades de conformidade, registrar as decisões relacionadas à proteção de dados pessoais, definir responsabilidades, monitorar a implementação das medidas previstas, revisar periodicamente os controles adotados e promover a melhoria contínua das práticas de governança em privacidade e proteção de dados pessoais.

O Programa de Governança em Privacidade (PGP) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) constituem importantes instrumentos para demonstrar a observância deste princípio – além das portarias de designação do encarregado pelo tratamento de dados pessoais e do gestor de segurança da informação, do ROPA e dos avisos de privacidade, da celebração de contratos com cláusulas protetivas de dados pessoais, de relatórios que apresentem indicadores acerca do programa de conscientização em privacidade e segurança da informação, entre outros.]

A organização mantém mecanismos de governança destinados a demonstrar a conformidade das atividades de tratamento com a LGPD. Esses mecanismos incluem o **registro das operações de tratamento (ROPA)**, a definição de responsabilidades na Política de Proteção de Dados Pessoais e em normas derivadas, a implementação e o monitoramento de medidas de privacidade, a avaliação periódica da eficácia dessas medidas e a promoção da melhoria contínua das práticas de proteção de dados pessoais. Essas ações são documentadas no planejamento do Programa de Governança em Privacidade (PGP) e em relatórios periódicos.

Em complemento, o presente **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** documenta a descrição dos tratamentos realizados no âmbito do [produto ou serviço], a análise de conformidade com os princípios da LGPD, os mecanismos adotados para garantir o exercício dos direitos pelos titulares, a avaliação dos riscos e as respectivas medidas de tratamento.

Em conjunto, essas evidências demonstram que as medidas de proteção de dados pessoais são efetivamente implementadas, monitoradas, revisadas e continuamente aperfeiçoadas, contribuindo para assegurar a observância da LGPD e a efetividade das práticas de governança adotadas.

Seção 4
Garantia do exercício dos direitos pelos titulares

Esta seção demonstra as medidas adotadas pela organização para assegurar o exercício dos direitos dos titulares de dados pessoais relacionados às atividades de tratamento abrangidas pelo escopo deste RIPD, em conformidade com a LGPD.

O atendimento aos direitos dos titulares depende da implementação de medidas organizacionais, administrativas e técnicas que permitam receber, registrar, analisar, processar, responder e documentar as solicitações apresentadas, observando os prazos legais e as características de cada direito.

4.1 Medidas gerais para garantia do exercício dos direitos pelos titulares

[Recomenda-se que a organização implemente medidas que permitam aos titulares o exercício de direitos de forma padronizada, tempestiva e rastreável, independentemente do direito específico requerido pelo titular. Essas medidas constituem a base para garantia dos direitos previstos na LGPD e demais normas aplicáveis.

Entre as medidas que podem demonstrar a observância desta seção destacam-se:

a) designação formal do encarregado pelo tratamento de dados pessoais;
b) disponibilização de canal para recebimento das solicitações dos titulares, seja sistema próprio, formulário eletrônico, endereço eletrônico institucional, atendimento presencial, plataforma Fala.BR ou outro mecanismo equivalente;
c) definição de procedimentos para confirmação da identidade do titular ou do seu representante legal;
d) definição de procedimentos internos para recebimento, registro, classificação, análise, encaminhamento, atendimento e resposta às solicitações;
e) manutenção de registros das solicitações recebidas, das análises realizadas, das providências adotadas e das respostas encaminhadas aos titulares;
f) estabelecimento de fluxos internos envolvendo, quando necessário, as áreas de negócio, de proteção de dados pessoais, jurídica, de tecnologia da informação, de segurança da informação e demais unidades responsáveis;
g) implementação de mecanismos que permitam localizar, recuperar, atualizar, corrigir, restringir, anonimizar, eliminar ou disponibilizar os dados pessoais tratados, conforme o direito exercido;
h) definição de prazos internos compatíveis com os prazos legais e regulamentares;
i) capacitação periódica dos agentes envolvidos no atendimento aos titulares;
j) revisão periódica dos procedimentos adotados, considerando alterações na legislação, regulamentação, processos de negócio, tecnologias empregadas e atividades de tratamento.]

A seguir, são apresentadas as medidas gerais aplicáveis aos direitos dos titulares implementadas pela organização:

a) a organização mantém processo institucional destinado ao atendimento dos direitos dos titulares de dados pessoais, contemplando procedimentos para recebimento, registro, análise, encaminhamento, atendimento e resposta às solicitações apresentadas;

b) o atendimento aos titulares é realizado por meio de canal específico disponibilizado em [...] para essa finalidade, sendo as solicitações encaminhadas às unidades responsáveis conforme a necessidade;
c) a organização possui procedimentos destinados à confirmação da identidade do solicitante quando necessária, ao registro das solicitações recebidas, ao acompanhamento de seu atendimento e à documentação das providências adotadas. [Descrever os procedimentos];
d) as áreas responsáveis atuam de forma coordenada para garantir o exercício dos direitos dos titulares, observando os prazos legais, a legislação aplicável e as características das atividades de tratamento descritas neste RIPD.

4.2 Medidas específicas para garantia do exercício dos direitos pelos titulares (por direito)

[Além das medidas gerais descritas na subseção 4.1, recomenda-se demonstrar, para cada direito aplicável às atividades de tratamento abrangidas pelo RIPD, as medidas específicas adotadas para assegurar seu exercício ou, quando pertinente, justificar sua inaplicabilidade.

As medidas descritas devem considerar as características das atividades de tratamento, as limitações previstas na legislação e os procedimentos internos estabelecidos pela organização para o atendimento aos titulares.

Quando determinado direito não for aplicável às atividades de tratamento analisadas, recomenda-se registrar expressamente essa circunstância e sua respectiva justificativa.]

As medidas específicas adotadas para assegurar o exercício dos direitos dos titulares aplicáveis às atividades de tratamento descritas neste RIPD encontram-se apresentadas na **Tabela 7**, que também registra a correlação com as medidas dispostas na **subseção 4.1**.

Tabela 7: descrição das medidas específicas para garantia dos direitos dos titulares

Direito	**Aplicabilidade (Sim/Não)**	**Medidas específicas ou justificativa de inaplicabilidade**
Acesso facilitado às informações sobre o tratamento de seus dados pessoais (art. 9º)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: aviso de privacidade com informações objetivas sobre o tratamento; disponibilização de canal eletrônico de autoatendimento; disponibilização de canal de contato com o encarregado.]
Confirmação da existência de tratamento (art. 18, I)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: canal de contato com o encarregado; processo de atendimento e resposta à solicitação do titular

		confirmando a existência de tratamento, em prazo determinado.]
Acesso aos dados pessoais (art. 18, II)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: disponibilização, mediante solicitação do titular, de extrato ou relatório com os dados pessoais tratados; menu no sistema para autoatendimento e acesso direto aos dados pessoais pelos titulares.]
Correção de dados pessoais incompletos, inexatos ou desatualizados (art. 18, III)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: funcionalidade de atualização cadastral pelo próprio titular ou canal de solicitação de correção.]
Anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: procedimento interno de revisão da solicitação e eventual exclusão ou anonimização de dados pessoais mediante solicitação, observados os prazos legais de retenção.]
Portabilidade dos dados pessoais a outro fornecedor de serviço ou produto (art. 18, V)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Ex.: exportação dos dados pessoais em formato estruturado e interoperável, quando tecnicamente viável.]
Eliminação dos dados pessoais tratados com base no consentimento (art. 18, VI)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Ex.: procedimento de eliminação dos dados pessoais após a revogação do consentimento, ressalvadas as hipóteses de conservação do art. 16 da LGPD.]
Informação sobre as entidades com as quais o controlador realizou uso compartilhado de dados pessoais (art. 18, VII)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Ex.: relação dos destinatários do compartilhamento disponibilizada

		mediante solicitação no canal de atendimento via encarregado.]
Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Ex.: esclarecimento, no momento da coleta ou no aviso de privacidade, sobre a possibilidade de recusa de consentimento e suas consequências.]
Revogação do consentimento (art. 18, IX)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: funcionalidade em sistema ou canal específico para revogação do consentimento, com efeitos a partir da manifestação do titular; procedimentos de restauração de *backup* com cuidados específicos para evitar sobreposição da situação do consentimento.]
Revisão de decisões tomadas unicamente com base em tratamento automatizado (art. 20)	[Sim/Não]	[Descrever as medidas que asseguram o direito ou justificar sua inaplicabilidade. Exs.: disponibilização de canal para solicitação de revisão, quando o tratamento envolver decisão unicamente automatizada, e procedimento de revisão incluindo unidades envolvidas.]

Seção 5
Gestão de riscos

[A identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos relacionados às atividades de tratamento de dados pessoais devem observar a metodologia institucional de gestão de riscos adotada pela organização. Na ausência de metodologia própria, pode-se utilizar como referência o Guia de Gestão de Riscos do Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

Ao identificar os riscos relacionados às atividades de tratamento descritas no RIPD, recomenda-se avaliar se as medidas já implementadas e descritas ao longo deste documento, especialmente nas seções 3 e 4, são suficientes para reduzir os riscos identificados a níveis aceitáveis ou se permanecem riscos relevantes aos titulares dos dados pessoais que demandem a implementação de medidas adicionais de tratamento de riscos.

Sempre que possível, as medidas já descritas neste RIPD deverão ser referenciadas nesta seção, evitando sua repetição. Por sua vez, as medidas adicionais necessárias para reduzir os riscos identificados deverão ser registradas na tabela proposta nesta seção.

As escalas de probabilidade, impacto e nível de risco apresentadas neste modelo possuem caráter exemplificativo e deverão ser adaptadas para manter aderência à metodologia institucional de gestão de riscos adotada pela organização, desde que sejam mantidos critérios consistentes durante toda a avaliação.]

Esta seção apresenta os riscos relacionados às atividades de tratamento de dados pessoais abrangidas pelo escopo deste RIPD, bem como as respectivas medidas de tratamento de riscos.

No decorrer deste documento, especialmente nas seções 3 e 4, foram registradas medidas destinadas à observância dos princípios da LGPD e à garantia dos direitos dos titulares de dados pessoais, respectivamente; essas medidas também contribuem para o tratamento dos riscos relacionados às atividades de tratamento de dados pessoais analisadas neste RIPD.

Por sua vez, nesta seção tais medidas poderão ser referenciadas sempre que contribuírem para o tratamento dos riscos identificados, ainda que seus detalhes já tenham sido apresentados anteriormente – podendo ser complementadas por outras medidas de tratamento de riscos, quando necessário.

5.1 Critérios básicos

Esta subseção estabelece os critérios de impacto, probabilidade, estimativa e aceitação de riscos utilizados na avaliação constante da **subseção 5.2**, tomando como referência as escalas e a matriz de risco estabelecidas pela organização, adaptadas para refletir os efeitos sobre os titulares de dados pessoais.

5.1.1 Critérios para determinar o nível de impacto dos riscos

[**Observação 1**: para fins deste modelo, os níveis de impacto devem ser interpretados considerando os potenciais efeitos sobre os direitos e as liberdades fundamentais dos titulares de dados pessoais, devendo a organização adaptar a descrição dos critérios apresentados em sua metodologia institucional para refletir esse contexto.

Observação 2: todas as tabelas propostas neste modelo como sugestão de resposta, inclusive as quantidades de níveis, representam apenas exemplos que devem ser adaptados à metodologia de gestão de riscos do órgão ou entidade, assim como à sua realidade institucional.

Recomenda-se que os critérios sejam especificados em razão dos danos e possíveis custos aos titulares de dados pessoais envolvidos em um evento de risco, considerando minimamente: classificação dos ativos de informação afetados; consequências da violação de dados pessoais, incluindo perda de disponibilidade, confidencialidade ou integridade; dano à reputação;

volume de dados pessoais possivelmente impactados e tipos de dados pessoais envolvidos. Recomenda-se, ainda, considerar os critérios de alto risco do art. 4º da Resolução CD/ANPD nº 2/2022 (ver subseção 1.2).]

A **Tabela 8** apresenta os [cinco níveis] de impacto adotados neste RIPD, com os respectivos critérios de enquadramento centrados nos efeitos sobre os titulares de dados pessoais.

Tabela 8: critérios para determinar o impacto

Impacto	Critérios
[MUITO BAIXO - 1]	[Acontecimentos que não produzam qualquer desconforto perceptível aos titulares de dados pessoais, sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais anonimizados ou agregados, sem possibilidade de reidentificação.]
[BAIXO - 2]	[Acontecimentos que não produzam desconforto significativo aos titulares de dados pessoais, sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais pseudonimizados (desde que a chave para reidentificação do titular também não tenha sido comprometida), dados pessoais de difícil identificação (ex.: endereços IP).]
[MÉDIO - 3]	[Acontecimentos que produzam desconforto aos titulares, sem prejuízos financeiros e sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais imediatamente identificáveis (ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (ex.: histórico de atividades, preferências).]
[ALTO - 4]	[Acontecimentos que produzam restrição relevante às liberdades civis e aos direitos fundamentais dos titulares, de difícil reversão, ou prejuízos financeiros significativos. Dados pessoais de crianças, adolescentes ou outras categorias de vulneráveis, dados pessoais sensíveis ou que possam gerar discriminação ao titular.]
[MUITO ALTO - 5]	[Acontecimentos que produzam restrição grave e possivelmente irreversível às liberdades civis e aos direitos fundamentais dos titulares, com potencial de dano à vida, à integridade física ou à dignidade da pessoa. Volume elevado de titulares afetados, dados pessoais sensíveis em grande volume ou de crianças, adolescentes ou outras categorias de vulneráveis, ou tratamento enquadrado como de alto risco nos termos da subseção 1.3.]

5.1.2 Critérios para determinar a probabilidade dos riscos

[Recomenda-se que sejam definidos critérios específicos e mensuráveis, e suas respectivas escalas, para determinar a probabilidade de um evento de risco. Para complementar os critérios, sugere-se a utilização de dados apresentados em relatórios que registram as estimativas sobre os principais riscos de desconformidade com a LGPD[3].]

Os [cinco níveis] de probabilidade adotados neste RIPD são apresentados na **Tabela 9**, com os respectivos critérios de enquadramento baseados na frequência esperada de ocorrência do evento de risco.

Tabela 9: critérios para determinar a probabilidade

Probabilidade	Critérios
[MUITO BAIXA - 1]	[Improvável. Acontecimentos que ocorrem, em média, menos de uma vez a cada dois anos.]
[BAIXA - 2]	[Pouco provável. Acontecimentos que ocorrem, em média, pelo menos uma vez a cada ano.]
[MÉDIA - 3]	[Provável. Acontecimentos que ocorrem, em média, pelo menos uma vez a cada semestre.]
[ALTA - 4]	[Muito provável. Acontecimentos que ocorrem, em média, pelo menos uma vez ao mês.]
[MUITO ALTA - 5]	[Praticamente certa. Acontecimentos que ocorrem, em média, mais de uma vez ao mês.]

5.1.3 Estratégia para estimativa dos riscos

[A estratégia para determinar o nível de risco deve ser definida com o objetivo de subsidiar a avaliação dos cenários de riscos.]

A matriz a seguir (Tabela 10) apresenta o nível de risco resultante da combinação entre os níveis de impacto e de probabilidade definidos nas subseções 5.1.1 e 5.1.2, calculado pela multiplicação entre ambos (Nível de Risco = Impacto × Probabilidade). Cada nível resultante é classificado em uma das [quatro] faixas a seguir, identificadas na matriz pelas cores correspondentes:

[3] Na ausência de indicadores nacionais relevantes, considere avaliar a eventual utilização de dados relacionados à GDPR, como o https://www.enforcementtracker.com.

- [**Pequeno** (níveis 1 a 3) - indicado em **verde**: risco aceitável, dentro do apetite a risco do órgão ou entidade;]
- [**Moderado** (níveis 4 a 6) - indicado em **amarelo**: risco aceitável, podendo ser reduzido caso o custo da medida seja proporcional ao benefício esperado;]
- [**Alto** (níveis 8 a 12) - indicado em **laranja**: risco inaceitável, exigindo a implementação de controles com custo-benefício adequado;]
- [**Crítico** (níveis 15 a 25) - indicado em **vermelho**: risco inaceitável, exigindo a implementação imediata de controles com custo-benefício adequado.]

Tabela 10: matriz para determinar o nível de risco

IMPACTO \ PROBABILIDADE	[1]	[2]	[3]	[4]	[5]
[5]	5	10	15	20	25
[4]	4	8	12	16	20
[3]	3	6	9	12	15
[2]	2	4	6	8	10
[1]	1	2	3	4	5

5.1.4 Critérios para aceitação dos riscos

[Os critérios para a aceitação do risco devem ser especificados considerando políticas, metas e objetivos do órgão. Recomenda-se a definição de uma escala de níveis de aceitação do risco tendo como referência os critérios de probabilidade e impacto e a estratégia para estimativa de riscos. Exemplo: considerando a estratégia para estimativa de risco anteriormente apresentada e a tabela a seguir, serão aceitos riscos categorizados como “PEQUENO”.

Nesse contexto, o órgão deve utilizar o apetite a risco definido em sua metodologia de gestão de riscos ou naquela que o adotou oficialmente, o que influenciará no tratamento dos riscos identificados. As escalas aqui citadas servem apenas como referência e exemplos de aplicação do processo. Para exemplificar, o Guia de Gestão de Riscos do MGI adota, como padrão institucional, apetite MODERADO – aceitando riscos de nível Pequeno ou Moderado, desde que não representem consequências críticas.]

A **Tabela 11** apresenta as faixas de riscos adotadas neste RIPD, correlacionando cada nível de risco calculado na **subseção 5.1.3** à respectiva classificação.

Tabela 11: níveis de risco

Nível de risco	Faixa
CRÍTICO	[15 a 25]
ALTO	[8 a 12]
MODERADO	[4 a 6]
PEQUENO	[1 a 3]

Para os fins deste RIPD, foi adotado o **apetite a risco** [nível de risco], razão pela qual são considerados **aceitáveis** os riscos enquadrados nas faixas [faixas].

5.2 Identificação, análise e avaliação de riscos

[Nesta subseção devem ser identificados, analisados e avaliados os riscos que possam comprometer a privacidade dos titulares de dados pessoais, considerando as medidas de conformidade com os princípios da LGPD e de garantia dos direitos dos titulares já descritas nas seções 3 e 4 deste RIPD. O nível de risco representado nesta subseção corresponde, portanto, à exposição que já reflete aquelas medidas, mas ainda não considera eventuais medidas adicionais e específicas de tratamento de riscos, que serão apresentadas na subseção 5.3.]

Esta subseção apresenta os riscos identificados nas atividades de tratamento de dados pessoais abrangidas pelo escopo deste RIPD, com base nos critérios estabelecidos na **subseção 5.1** e considerando as medidas já descritas nas seções 3 e 4 deste RIPD.

Tabela 12: riscos identificados

ID	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de risco (P x I)[3]
R01	[Ainda que estejam implementadas as medidas técnicas e administrativas de segurança da informação descritas na subseção	3	5	Crítico

ID	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de risco (P x I)[3]
	3.7 (Princípio da segurança), a integração do [produto ou serviço] com sistema operado por terceiro (ex.: plataforma de autenticação, gateway de pagamento, serviço de nuvem) pode gerar risco de acesso não autorizado a dados pessoais em caso de riscos não identificados nos controles do operador ou de falha de configuração na integração, o que poderá levar à exposição indevida de dados pessoais dos titulares, comprometendo a confidencialidade do tratamento e podendo configurar incidente de segurança nos termos do art. 48 da LGPD.]			
R02	[Ainda que estejam formalmente estabelecidos, na seção 4, os canais e procedimentos para atendimento às solicitações dos titulares relativas ao exercício de seus direitos (ex.: acesso, correção, eliminação), pode ocorrer atraso ou inconsistência na resposta em razão de falha operacional, dependência de múltiplas áreas para o atendimento da solicitação, ou ausência de rastreabilidade adequada do andamento do pedido, o que poderá levar ao descumprimento do prazo legal de resposta (art. 19 da LGPD) ou a respostas incompletas ou incorretas, comprometendo o exercício efetivo dos direitos pelo titular.]	3	3	Alto
	[adicionar linhas conforme necessário]			

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).

5.3 Tratamento dos 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).

A coluna “Medidas de tratamento” deve ser preenchida com a identificação das medidas específicas e adicionais adotadas para o tratamento dos riscos apresentados em 5.2. Para identificação das medidas e respectivos controles, sem prejuízo de outras fontes ou especificação própria, recomenda-se utilizar como referência o “Guia do *Framework* de Privacidade e Segurança da Informação (PPSI 2.0)”, o qual elenca os controles e medidas que

representam referências fundamentais para ações de tratamento dos riscos, disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0.

Destaca-se que, em situações específicas, a mitigação de todos os riscos que estejam de acordo com os critérios de aceitação pode ser inviável. Nesse sentido, pode-se decidir que alguns riscos em desacordo com o apetite de risco podem ser aceitos como **exceção**, em razão dos benefícios apresentados ou das dificuldades de mitigação (como por exemplo valores ou limitações contratuais), o que deverá ser registrado na subseção seguinte.]

A **Tabela 13** apresenta os controles e respectivas medidas, bem como suas justificativas para tratar os riscos identificados na subseção 5.2.

Tabela 13: medidas de tratamento de risco e nível do risco residual

ID do risco	Medida de tratamento	Descreva como cada medida aplicada gera o efeito sobre o risco	Tipo de resposta	Risco residual		
				P	I	Nível
R01	[Inclusão de cláusulas contratuais específicas de segurança da informação e proteção de dados pessoais nos contratos com os operadores envolvidos na integração, incluindo: obrigação de notificação de incidentes em prazo determinado; exigência de comprovação de certificações ou relatórios de auditoria de segurança dos fornecedores antes da integração; necessidade de realização de testes de segurança na integração antes de sua entrada em produção e em periodicidade definida.]	[As cláusulas contratuais e a exigência de certificações reduzem a probabilidade de vulnerabilidade não identificada no operador, ao condicionar a integração a um padrão mínimo de segurança verificável; a obrigação contratual de notificação de incidentes reduz o impacto ao permitir resposta tempestiva. Os testes de segurança prévios à entrada em produção reduzem a probabilidade de falha de configuração não detectada.]	Mitigar	2	3	Moderado
	[Monitoramento contínuo dos acessos e do tráfego de dados pessoais entre os sistemas integrados, com geração de alertas para comportamento anômalo.]	[O monitoramento contínuo reduz o impacto ao possibilitar a detecção e a contenção rápida de eventual acesso não autorizado.]				
R02	[Implementação de ferramenta de gestão de solicitações de titulares, com prazos automatizados e alertas de vencimento.]	[A ferramenta de gestão permite o monitoramento centralizado de todas as solicitações e alerta automaticamente a equipe responsável antes do vencimento do prazo legal, reduzindo a probabilidade de atraso.]	Mitigar	1	3	Baixo
	[Definição de fluxo interno com papéis e responsabilidades claras entre as áreas envolvidas no atendimento, observando prazo interno (SLA) inferior ao prazo legal, de modo a garantir margem de segurança.]	[O fluxo interno com SLA inferior ao prazo legal absorve eventuais atrasos pontuais de uma área específica sem comprometer o prazo final.]				
	[Auditoria periódica das solicitações já respondidas, verificando tempestividade e completude da resposta.]	[A auditoria periódica permite identificar e corrigir falhas recorrentes de completude nas respostas,				

		reduzindo o impacto de eventuais respostas incorretas ou incompletas.]				
	[adicionar linhas conforme necessário]					

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da subseção 5.2.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Aceitar, Evitar, Mitigar e Compartilhar/Transferir.

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

5.4 Riscos residuais acima do nível de aceitação

[Registrar, nesta subseção, os riscos identificados na subseção 5.2 cujo nível residual, após a aplicação das medidas descritas na subseção 5.3, permaneçam acima do nível de aceitação definido pelo órgão ou entidade. Para cada risco, apresentar a justificativa da aceitação como exceção – como exemplos: os benefícios do tratamento que superam o risco residual ou as limitações técnicas, orçamentárias ou contratuais que impedem sua mitigação adicional – e identificar a autoridade responsável pela aprovação dessa exceção. Não havendo riscos nessa condição, registrar expressamente essa informação.]

Esta subseção apresenta os riscos identificados na subseção 5.2 cujos níveis residuais, após a aplicação das medidas de tratamento descritas na subseção 5.3, permaneceram acima do nível de aceitação. Nesses casos, a aceitação do risco configura uma exceção e foi motivada expressamente e aprovada formalmente, observados os benefícios do tratamento ou as limitações existentes à sua mitigação adicional, conforme detalhado na Tabela 14.

Tabela 14: riscos residuais acima do nível de aceitação (com respectivas justificativas)

ID do risco	Nível residual	Justificativa da aceitação como exceção	Responsável pela aprovação da exceção
[R0X]	[Alto/Crítico/Moderado]	[descrever os benefícios do tratamento ou limitações técnicas, orçamentárias ou contratuais que motivam a aceitação]	[nome e cargo da autoridade responsável]
[adicionar linhas conforme necessário]			

Seção 6
Histórico de atualizações

[Esta seção não se confunde com o histórico de versões constante da folha de versões deste documento, que, por sua vez, registra a elaboração e a revisão do modelo de referência mantido pela DEPSI/SGD/MGI.]

Este RIPD é um documento que será revisado sempre que sobrevierem fatos novos, alterações relevantes no [produto ou serviço] ou no tratamento de dados pessoais nele descrito, novos fatores de risco ou novas orientações ou regulamentações da Agência Nacional de Proteção de Dados. A tabela a seguir registra as atualizações substanciais de conteúdo deste RIPD.

Data	Versão	Atualizações realizadas	Responsável
[dd/mm/aaaa]	[X.Y]	[descrição sucinta das alterações realizadas nesta versão do RIPD]	[nome ou unidade responsável pela atualização]
[adicionar linhas conforme necessário]			

Seção 7
Aprovação

Representante do Controlador

_____

[Nome do agente público]
[Cargo]

[Cidade, data]

Dúvida?

Entre em contato conosco

Acesse o sítio do PPSI 2.0:
PPSI 2.0 — Governo Digital