Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, maio de 2023

GUIA/MODELO DE ELABORAÇÃO 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 PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Julierme Rodrigues da Silva

Equipe Revisora

Loriza Andrade Vaz de Melo

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Equipe Técnica de Revisão - Versão 2.0

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Ivaldo Jeferson de Santana Castro

Julierme Rodrigues da Silva

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
07/12/2020	1.0	Primeira versão do Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD).	Equipe Técnica de Elaboração
05/05/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS **5**

INTRODUÇÃO **7**

ORIENTAÇÕES GERAIS PARA ELABORAÇÃO DO RIPD **8**

Responsável pela Elaboração do RIPD 8
Momento recomendado para Elaboração do RIPD 8
Definição de "alto risco" para fins de elaboração do RIPD 9
Publicação do RIPD 10
Encaminhamento do RIPD para a ANPD 10
Consulta a ANPD sobre mitigação dos riscos identificados 10
Ações pós elaboração do RIPD 11

ANEXO I **12**

Mudanças da Versão 2.0 12

ANEXO II **13**

Modelo RIPD 13

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia/Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), em atendimento ao previsto nos artigos 4º, § 3º, 10, § 3º, 32 e 38 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a autoridade nacional poderá solicitar ao controlador que elabore e/ou publique relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO) e do *National Institute of Standards and Technology* (NIST). Em complemento ao Guia do Framework de Privacidade e Segurança da Informação, este **Guia/Modelo** foi inspirado em publicações da *Information Commissioner's Office* (ICO) e da Autoridade Nacional de Proteção de Dados (ANPD). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO, NIST, ICO e da ANPD vice-versa;

b) não se manifesta em nome de autoridades de privacidade e segurança da informação;

c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, à ICO, à ANPD, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração **deste documento.**

Este Guia/Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) por órgãos e entidades da Administração Pública Federal (APF) direta, autárquica e fundacional.

O Controle 30 do Guia do Framework de Privacidade e Segurança da Informação (p. 69) estabelece que:

Controle 30: Avaliação de Impacto, Monitoramento e Auditoria – *Avaliar a necessidade de implementar, onde apropriado, uma avaliação de impacto à proteção de dados pessoais, quando novos tratamentos ou mudanças no tratamento existente de dados pessoais forem planejados e documentar medidas adotadas para a mitigação dos riscos identificados.*

O presente Guia/Modelo serve como um modelo prático a ser utilizado para auxiliar na adoção Controle 30 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 30 que estão contempladas por este modelo são: 30.1, 30.3, 30.4, 30.5 e 30.6.

O **art. 5, inciso XVII da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018, define o RIPD como:

> *"Art. 5º ...*
>
> *XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco."*

Importante ressaltar que adoção deste modelo não dispensa o órgão de considerar as diretrizes gerais estabelecidas pela ANPD.

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

ORIENTAÇÕES GERAIS PARA ELABORAÇÃO DO RIPD

Nesta seção são apresentadas orientações embasadas nas perguntas e respostas elaboradas pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD)[2], que objetivam orientar e esclarecer a sociedade sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Cumpre destacar que parte do indicado pelas perguntas e respostas da ANPD sobre elaboração do RIPD foi incorporada no modelo do Anexo II deste Guia.

Importante atentar para o destacado por essa seção antes da efetiva elaboração do RIPD.

Responsável pela Elaboração do RIPD

O controlador é o agente de tratamento responsável pela elaboração do RIPD, nos termos dos art. 5º, inciso XVII, e 38, da LGPD.

Momento recomendado para Elaboração do RIPD

Recomenda-se elaborar o RIPD antes de o controlador iniciar o tratamento dos dados pessoais para a finalidade desejada, justamente para que ele possa avaliar, de antemão, os possíveis riscos associados a esse tratamento.

Dessa forma, o controlador conseguirá, antes mesmo de usar os dados pessoais para aquela finalidade, identificar a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares e adotar as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados à hipótese.

Contudo, caso não seja possível elaborar o RIPD antes do início do tratamento, recomenda-se elaborá-lo assim que se identificar um tratamento que possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados

De todo modo, o controlador deverá, ainda, elaborar o RIPD caso seja solicitado pela ANPD.

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

Definição de "alto risco" para fins de elaboração do RIPD

Os controladores podem, no que couber, enquanto não for editado regulamento específico sobre o RIPD, adotar como parâmetro o conceito de tratamento de alto risco definido no art. 4º do Regulamento[3] de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022.

De acordo com esse dispositivo, o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral ("larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares") e de um critério específico ("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" ou "utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos").

Considerando esses critérios, recomenda-se elaborar o RIPD, por exemplo, se o tratamento de dados pessoais abranger número significativo de titulares ("larga escala", critério geral) e dados pessoas sensíveis (critério específico). Outro exemplo que pode ser mencionado é a decisão tomada unicamente com base em tratamento automatizado de dados pessoais (critério específico), da qual possa resultar a negativa para o exercício de um direito ou para a utilização de um serviço ("afetar significativamente interesses e direitos", critério geral).

Ressalte-se que, para fins de elaboração do RIPD, esses critérios não devem ser considerados exaustivos, de modo que o controlador poderá verificar a existência de alto risco em situações diferentes das indicadas. Assim, em conformidade com o princípio da responsabilização e prestação de contas, cabe ao controlador avaliar as circunstâncias relevantes do caso concreto, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança apropriadas, considerando os possíveis impactos às liberdades e direitos fundamentais dos titulares e a probabilidade de sua ocorrência.

[3] https://in.gov.br/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Publicação do RIPD

Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD.

Para isso, o controlador pode disponibilizar o RIPD em meios de fácil acesso pelo titular, especialmente em seus sítios eletrônicos, com informações sobre suas atividades de tratamento de dados pessoais, de forma clara, adequada e ostensiva. Contudo, nesse caso a versão pública do RIPD pode ser distinta da versão interna, no intuito de resguardar segredos comercial e industrial e outras informações protegidas por lei.

Especificamente em relação a entidades e órgãos públicos, o RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011.

Encaminhamento do RIPD para a ANPD

A LGPD não determina, como regra geral, o encaminhamento do relatório à ANPD. Não obstante, no exercício efetivo das suas atribuições fiscalizatórias e nas hipóteses previstas na LGPD, a Autoridade poderá requerer ao controlador o encaminhamento do RIPD, além de cópia de documentos, físicos ou digitais, e de dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais.

Assim, o controlador tem o dever de encaminhar o RIPD apenas quando requisitado pela ANPD, sujeitando-se a medidas de fiscalização em caso de descumprimento.

Consulta a ANPD sobre mitigação dos riscos identificados

A ANPD não responde individualmente consultas jurídicas em tese ou que demandem a emissão de pronunciamento específico sobre uma condição hipotética ou concreta. Nesse sentido, não cabe manifestação da ANPD sobre as salvaguardas e medidas adequadas a serem adotadas para mitigar os riscos identificados em um determinado caso.

Não obstante, o controlador pode encaminhar suas dúvidas e questionamentos para a ANPD, por meio do endereço eletrônico ouvidoria@anpd.gov.br. As demandas recebidas são avaliadas e consolidadas, podendo ser consideradas no processo de elaboração de regulamentos ou para fins de futuras orientações sobre o tema.

Ações pós elaboração do RIPD

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

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

Por fim, **recomenda-se ao controlador a revisão contínua do RIPD**, em especial, quando houver fatos novos que possam ensejar mudanças nos riscos identificados, tais como alteração nas operações de tratamento, identificação de novos fatores de risco, agravamento dos fatores de risco anteriormente identificados, ou em caso de novas regulamentações ou orientações emitidas pela ANPD.

ANEXO I

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia/Modelo de Elaboração do RIPD.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1, elaborado e publicado pela SGD em novembro de 2022, e com as orientações e esclarecimentos sobre o RIPD elaborados pela ANPD.

Foram realizadas as seguintes inclusões: seção sobre aviso preliminar e agradecimentos; referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais; seção de Introdução; seção de Orientações Gerais e anexo sobre atualização do Guia/Modelo de Elaboração do RIPD. Além disso, foram realizadas modificações, inclusões e exclusões de textos para melhor coesão textual.

ANEXO II

Modelo RIPD

Esta seção contém o Modelo para preenchimento do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Tal documento é resultado de pesquisa de modelos propostos por autoridades de proteção de dados europeias e consulta à norma ABNT ISO/IEC 29134:2017. A estrutura foi inspirada no modelo utilizado pela Inglaterra (ICO) devido à abordagem completa, simples e direta para registro da avaliação de impacto à proteção de dados pessoais.

Abaixo algumas orientações para utilização do documento:

- O modelo do RIPD se encontra disponível a partir da próxima página deste Guia;
- Os trechos marcados em azul no modelo a seguir são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

<Local>, <dia> de <mês> de <ano>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
XX/XX/20XX	1.0	Conclusão da primeira versão do relatório	XXXXXXXXXXX
XX/XX/20XX	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	XXXXXXXXXXX

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
<Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI)>.	
Operador	
<Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII)>.	
Encarregado	
<Nome da pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (LGPD, art. 5º, VIII).>	
E-mail Encarregado	**Telefone Encarregado**
<xxxx.xxxx.gov.br>	< (99)9999-9999>

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

< Como regra geral, é recomendado elaborar o RIPD em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme art. 5º, inciso XVII, e art. 55-J, inciso XIII, da LGPD, o que deverá ser avaliado pelo agente de tratamento.>

< A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como:

· nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);

· quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º);

· para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e

· para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).>

<Portanto, haverá situações em que o controlador elaborará o RIPD para atender à determinação da ANPD ou, em atenção ao princípio da responsabilização e prestação de contas (art. 6º, X), ao verificar que o tratamento a ser realizado pode implicar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.>

<Além disso, a LGPD prevê a possibilidade de que os controladores, para cumprimento dos princípios da segurança e da prevenção (art. 6º, VII e VIII), implementem programa de governança em privacidade que, entre outros itens, estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, § 2º, I, d), procedimento que pode envolver a elaboração de RIPD.> (aqui)

<Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.>

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

É importante também observar que, em cenários em que há compartilhamento de dados pessoais entre diferentes controladores, cada controlador poderá ser responsável por um RIPD, ainda que utilizem uma plataforma compartilhada, uma vez que as finalidades do tratamento poderão ser distintas. >

<Além dos casos específicos previstos pela LGPD no início desta seção 2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

• rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);

• tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II);

• processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);

• tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

• tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);

• tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);

• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);

• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.; e

• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

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

3 – DESCRIÇÃO DO TRATAMENTO

<A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.>

<A LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".>

<O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.>

<Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.>

3.1 – NATUREZA DO TRATAMENTO

<A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal.>

<Importante descrever, por exemplo:

• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

• fonte de dados (ex.: titular de dados, planilha eletrônica, arquivo xml, formulário em papel etc.) utilizada para coleta dos dados pessoais;

• com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;

• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e

• medidas de segurança atualmente adotadas.>

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

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

3.2 – ESCOPO DO TRATAMENTO

<O **escopo** representa a abrangência do tratamento de dados.>

< Nesse sentido, considerar destacar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis;
- categorias dos titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços, motoristas, servidores públicos, eleitores, contribuintes, motoristas, estudantes, etc.);
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.>

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

3.3 – CONTEXTO DO TRATAMENTO

<Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.>

<O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.>

3.4 – FINALIDADE DO TRATAMENTO

<A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.>

<Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados

pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7 º e 11 da LGPD), no que for aplicável:

• cumprimento de obrigação legal ou regulatória pelo controlador;

• execução de políticas públicas;

• alguma espécie de estudo realizado por órgão de pesquisa;

• execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• exercício regular de direitos em processo judicial, administrativo ou arbitral;

• proteção da vida ou da incolumidade física do titular ou de terceiros;

• tutela da saúde;

• atender aos interesses legítimos do controlador ou de terceiros;

• proteção do crédito; e

• garantia da prevenção à fraude e à segurança do titular.>

<Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.

• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.>

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

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> **I - apoio e promoção de atividades do controlador; e**
> **II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.**
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseados em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

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

4 – PARTES INTERESSADAS CONSULTADAS

<Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais,

técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.>

<Nessa seção, é importante identificar:

• quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.; e

• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Esse registro de opiniões (convergentes ou divergentes), incluindo as justificativas para a opção adotada, pode ser considerado uma boa prática em termos de transparência, responsabilização e prestação de contas >

< Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.>

5 – NECESSIDADE E PROPORCIONALIDADE

<Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III). >

< Nesse sentido, destacar:

• A fundamentação legal para o tratamento dos dados pessoais.

• Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:

- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.

• Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.

• Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).

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

• Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.

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

< O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

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

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

<Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.>

<Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:>

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

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

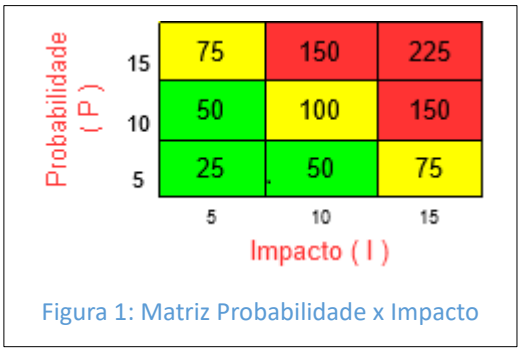

Figura 1: Matriz Probabilidade x Impacto

<O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- verde, é entendido como baixo;

- amarelo, representa risco moderado; e

- vermelho, indica risco alto.>

<As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

<A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade relacionados com a proteção de dados pessoais. **O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição**. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4. **É recomendado que a identificação de riscos compreenda qualquer tipo de risco que possa comprometer a privacidade dos titulares dos dados pessoais**.>

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50

R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudoanonimizados.	5	15	75

7 – MEDIDAS PARA TRATAR OS RISCOS

<Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46.).>

<Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.

<A coluna "Controle/Medida" pode ser preenchida com controle e medida específicos adotados para tratamento do risco identificado na seção 6 deste Relatório.

<**O Guia do Framework de Privacidade e Segurança da Informação elenca controles e medidas que representam referências fundamentais para ações de tratamento dos riscos,** disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>

<A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto-, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação.

Risco	Controle/Medida	Efeito sobre o Risco[1]	Risco Residual[2]			Controle/ Medida[3] Aprovado (a)
			P	I	Nível (P x I)	
<Risco 1>	<Controle 1: Medida 1.1, Medida 1.2; Controle 2: Medida 2.1; Controle N: Medida N>					
<Risco 2>	<Controle 1: Medida 1.1, Medida 1.2; Controle 2: Medida 2.1; Controle N: Medida N>					
<Risco N>	<Controle 1: Medida 1.1, Medida 1.2; Controle 2: Medida 2.1; Controle N: Medida N>					

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

seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação do(s) controle(s) descrito(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

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

[3] Controle/medida aprovado(a) pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

<A seguir são apresentados exemplos de controles para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior>.

Risco	Controle/Medida	Efeito sobre o Risco	Risco Residual			Controle/ Medida(s) Aprovado s(as)
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; Uso de MFA. SEGURANÇA DE APLICAÇÕES: Desenvolvimento Seguro.	Reduzir	5	10	50	Sim
R04 Roubo.	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; Uso de MFA. PROTEÇÃO DE DADOS: Descarte seguro de dados; Uso de criptografia em mídia removível.	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	MINIMIZAÇÃO DE DADOS: Coleta somente dos dados necessários para a finalidade; Revisão periódica dos dados pessoais coletados para alinhamento com a finalidade.	Reduzir	5	10	50	Sim

8 – APROVAÇÃO

<Esta seção **visa formalizar a aprovação do RIPD** por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

<**O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais** realizados pela instituição. Detalhes sobre a necessidade de revisão do RIPD podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas LGDP, disponível em**: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	**ENCARREGADO**
_____ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do encarregado> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>