FGV DCI
DIRETORIA DE
CONTROLES INTERNOS

GUIA DE PROTEÇÃO DE DADOS PESSOAIS

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

CC.04.004.2024

OUTUBRO DE 2024

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

VERSÃO 1.0 – OUTUBRO, 2024.

Diretoria de Controles Internos – DCI
Maria Alice da Justa Lemos
Diretora de Controles Internos

Analista responsável por este Guia:
Taís Povill Rocha

Jordan Vinícius de Oliveira
Encarregado de Proteção de Dados Pessoais

FICHA TÉCNICA

Equipe Extracontratual:

Laila Sá Ferreira
Taís Povill Rocha
Alessandra Rigueti Barcellos
Nadja Nayra da Cruz Ferreira Ribeiro

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.004.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

AVISO LEGAL

Este Guia foi elaborado pela Equipe do Encarregado de Proteção de Dados Pessoais da Fundação Getulio Vargas – FGV e tem como objetivo o compartilhamento de conhecimento envolvendo a conformidade de atividades de tratamento de dados pessoais para o tema escolhido.

O presente documento possui intuito meramente informativo, não sendo utilizado para fins de exploração comercial e apresenta a devida referência na página 2. Do mesmo modo, este documento não deve ser considerado como aconselhamento jurídico e não substitui a avaliação de uma equipe profissional de proteção de dados para cada caso.

SUMÁRIO

1. CONTEXTUALIZAÇÃO

O presente Guia é um dos frutos do projeto de adequação da Fundação Getulio Vargas – FGV em relação à Lei Geral de Proteção de Dados ("LGPD"), aprovada em agosto de 2018, e outras leis setoriais sobre o tema.

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural, pessoa jurídica de direito privado ou pessoa jurídica de direito público. Na condição de Instituição de Ensino Superior ("IES"), a FGV desenvolve, entre outras atividades, operações de caráter administrativo, acadêmico e educacional (como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, realização de pesquisas, desenvolvimento de projetos etc.). Nesse sentido, na condição de Instituição Educacional, a FGV deverá observar as obrigações normativas específicas das entidades públicas reguladoras, como, por exemplo, o Ministério da Educação ("MEC") e a Autoridade Nacional de Proteção de Dados (“ANPD”).

Assim, a FGV desenvolveu, em maio de 2019, um projeto para cumprir com os objetivos de sua conformidade regulatória perante as leis de proteção de dados, denominado **Projeto Presidência - Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais (“Projeto”)**. Esta iniciativa, entre outras atividades, buscou parametrizar ações de conformidade da FGV ao novo contexto regulatório de proteção de dados, bem como, a partir das lições aprendidas, fornecer subsídios e materiais de apoio ao setor educacional.

Após a conclusão do Projeto inicial, a FGV criou a **Equipe do Encarregado de Proteção de Dados Pessoais**, no âmbito de sua Diretoria de Controles Internos ("DCI"). Esta Equipe tem como finalidade principal manter a FGV em adequação às normas de proteção de dados aplicáveis às suas atividades, bem como funcionar na condição de interlocutora junto aos variados setores da Organização, à ANPD, aos titulares de dados pessoais e aos demais agentes de tratamento.

O objetivo geral deste Guia é fornecer algumas diretrizes para a definição dos Agentes de Tratamento, principalmente no âmbito das atividades realizadas por IES.

Como objetivos específicos, este Guia pretende:

(a) Apresentar os principais pontos sobre o Relatório de Impacto trazidos pela LGPD e outras normas aplicáveis;

(b) Ressaltar a importância do mapeamento adequado das atividades de tratamento de dados pessoais;

(c) Fornecer orientações para a elaboração do Relatório de Impacto.

2. ASPECTOS GERAIS

A Lei 13.709/2018 (Lei Geral de Proteção de Dados – "LGPD") trouxe consigo diversas inovações no cenário legislativo brasileiro, implicando novas obrigações a serem observadas pelos administrados no que diz respeito às atividades que ensejam o tratamento de dados pessoais[1]. Um dos temas mais debatidos após o advento da supramencionada lei é a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), definido no art. 5°, XVII da LGPD como: "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".

A partir desta definição legal, é possível destacar alguns pontos importantes. O primeiro aspecto a ser analisado é que a obrigação legal de produzir o RIPD recai sobre o Controlador, e não sobre o Operador. Existe uma lógica inquestionável sobre este aspecto: o Controlador é responsável pelas decisões referentes ao tratamento de dados pessoais, o que inclui a implementação de eventuais medidas de mitigação para reduzir riscos, não sendo razoável exigir do Operador que ele se responsabilize pela adoção de tais providências.

Neste sentido, reforça-se: quando as operações com dados pessoais envolverem mais de um agente de tratamento, há que se atentar para o papel de cada um para que se possa definir, com exatidão, de quem será a função de elaborar o RIPD. É possível que exista, por exemplo, uma relação de controladoria conjunta, na qual dois ou mais agentes de tratamento envolvidos em determinada atividade sejam Controladores. Neste caso, ambos terão a atribuição de produzir o documento estudado neste Guia, salvo se determinado em contrário por instrumento contratual.

[1] Nos termos do art. 5°, I da LGPD, **dado pessoal** é a informação relacionada a pessoa natural identificada ou identificável.

Para mais detalhes, consulte o **Guia Orientativo de Proteção de Dados Pessoais da FGV: agentes de tratamento**.

Em que pese a obrigação legal de elaborar o RIPD recaia sobre o Controlador, nada obsta que o Operador possa registrar as minúcias das operações de tratamento de dados pessoais sob sua gerência bem como as medidas adotadas em seu âmbito para garantir maior segurança a estas atividades. Caso opte por produzir tais registros, esta medida poderá ser considerada uma boa prática, nos termos do art. 50 da LGPD. Ainda, é possível que por arranjo contratual o Operador proponha ou contribua com a redação do RIPD junto ao Controlador, desde que este acordo não implique em isenção das obrigações legais exigíveis ao Controlador pela LGPD.

O segundo ponto de destaque da definição trazida pelo art. 5°, XVII da LGPD é que não são todas as operações de tratamento de dados pessoais que deverão constar no RIPD, e sim aquelas que efetivamente possam gerar riscos às liberdades civis e aos direitos fundamentais. Ainda, o art. 55-J, XIII da LGPD estabelece como uma das competências da ANPD editar regulamentos sobre Relatórios de Impacto à Proteção de Dados Pessoais "*para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais*". Nos próximos tópicos serão abordados, com mais detalhes, os parâmetros para definir o conceito de "alto risco".

Neste aspecto, a ANPD publicou[2] um documento de "perguntas e respostas" sobre a elaboração de Relatórios de Impacto, informando que, enquanto não for editado regulamento específico para a produção deste registro, é possível considerar a definição de "alto risco" do art. 4° da Resolução CD/ANPD n° 2 de 27 de janeiro de 2022, cuja redação segue destacada a seguir:

> Art. 4º. Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
>
> I - critérios gerais:
>
> a) tratamento de dados pessoais em larga escala; ou
>
> b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
>
> II - critérios específicos:

[2] BRASIL. Autoridade Nacional de Proteção de Dados. *Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais*. Governo Federal. Disponível em: <link>. Acesso em 07 dez. 2023.

a) uso de tecnologias emergentes ou inovadoras;

b) vigilância ou controle de zonas acessíveis ao público;

c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou

d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Ainda no que diz respeito à inserção de operações de tratamento de dados pessoais no RIPD, há que se mencionar o art. 10, §3° da LGPD, que estabelece o seguinte: "(...) 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". Quanto a este dispositivo, cabe o seguinte questionamento: todas as operações de tratamento de dados pessoais que utilizem o art. 7°, IX da LGPD como fundamento legal precisam, necessariamente, ser registradas no RIPD?

Sobre o ponto acima, a ANPD publicou um Estudo Preliminar[3] sobre o Interesse Legítimo, manifestando o seguinte: "(...) também deve constar do registro o Relatório de Impacto à Proteção de Dados (RIPD), **caso o tratamento envolva alto risco** (...)". De igual modo e, complementarmente, o ICO[4] entende que não há a necessidade de elaborar RIPD para as atividades de tratamento de dados baseadas no interesse legítimo caso elas não apresentem elevado risco aos direitos e liberdades fundamentais dos titulares. Neste caso, é possível criar apenas um registro mais simples, denominado "*Legitimate Interests Assessment (LIA)*". Já por outro lado, caso a operação apresente um risco significativo, é recomendado produzir um RIPD. Para mais informações sobre a elaboração do documento LIA, consulte o **Guia Orientativo de Proteção de Dados Pessoais da FGV: marketing**.

Por fim, cabe ressaltar que o RIPD deve ser idealmente elaborado na fase de concepção de uma rotina que enseje o tratamento de dados de risco relevante. Neste caso, o RIPD constituirá uma parte integrante da privacidade desde a concepção (*privacy by design*)[5]. Caso, contudo, isso não

[3] BRASIL. Autoridade Nacional de Proteção de Dados. *Consulta à Sociedade de Estudo Preliminar sobre Legítimo Interesse*, 16 ago. 2023. Participa + Brasil. Disponível em: <link>. Acesso em: 06 dez. 2023.
[4] REINO UNIDO. Information Comissioner's Office. *How do we apply legitimate interests in practice?* Disponível em: <link>. Acesso em: 06 dez. 2023.
[5] REINO UNIDO, Information Comissioner's Office (ICO). *Data protection by design and default.* Disponível em: <link>. Acesso em: 06 dez. 2023.

seja possível, deverão ser providenciados ajustes a partir de riscos identificados e seus respectivos mitigadores na atividade de tratamento que já se encontre em curso.

3. ETAPAS PRÉVIAS À ELABORAÇÃO DE UM RIPD

O Relatório de Impacto é o produto final de um longo processo de análise de riscos de diversas atividades de tratamento de dados pessoais. Logo, antes de produzir este tipo de documento, é necessário que sejam realizadas algumas etapas, a saber: o mapeamento das atividades, a análise e o cálculo de riscos previamente e após a proposição e aprovação de seus mitigadores.

3.1. MAPEAMENTO

O mapeamento de dados pessoais (ou *data mapping*) é o processo pelo qual são registradas as informações sobre as atividades de tratamento de dados pessoais de determinada Instituição. Para facilitar a compreensão, chamaremos estas atividades de "**rotinas**".

DEFINIÇÃO

ROTINAS

São as atividades que envolvem o tratamento de dados pessoais realizadas por uma instituição no exercício de suas operações.

Exemplo: uma Instituição Educacional realiza como atividades (i) processos seletivos; (ii) matrícula de novos alunos; (iii) correção de provas; e (iv) lançamento de notas. Cada uma destas atividades pode ser considerada uma rotina e, portanto, cada uma delas deve ser estudada separadamente, com todas as minúcias relativas a suas execuções. Portanto, cada uma dessas rotinas deverá ser mapeada de forma individualizada.

A partir do conceito acima destacado, cabe também ressaltar a definição de "dados pessoais" pelo art. 5°, V da LGPD como "a informação relacionada a pessoa natural identificada ou identificável". Ora, se o mapeamento consiste no estudo das atividades de tratamento de dados pessoais, **não** se verifica a necessidade de incluir neste procedimento:

- ✓ As operações que tratam dados exclusivos de pessoas jurídicas (*e.g.:* CNPJ, sede, e-mail institucional de área *etc.*). Aqui não se incluem os dados pessoais dos sócios, representantes da empresa e/ou afins;
- ✓ As operações que tratam dados completamente anônimos ou previamente anonimizados[6] (por outro controlador) à operação do agente de tratamento (*e.g.:* uma pesquisa de uma instituição X que utiliza apenas os dados censitários agregados divulgados publicamente pela instituição Y).

Deste modo, reforça-se que devem constar no mapeamento todas as atividades significativas de tratamento de dados pessoais para fins de registro, análise posterior e acompanhamento.

PONTO DE ATENÇÃO

TITULARES NÃO VINCULADOS À INSTITUIÇÃO

- As rotinas que dizem respeito a titulares não vinculados à Instituição por um instrumento contratual de forma estrita também podem necessitar de mapeamento e, caso impliquem riscos às liberdades civis e aos direitos fundamentais, também devem constar no RIPD. Exemplo: reconhecimento facial da gravação de imagens de transeuntes por câmeras de segurança.

3.1.1. REGISTRO DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

A partir das considerações iniciais deste capítulo, para começar o mapeamento das atividades de tratamento de dados, primeiro deve-se escolher o meio utilizado para registrá-las. É essencial que seja realizado um Registro de Operações de Tratamento de Dados Pessoais (*Record of Processing Activities* – "ROPA"). Este documento deve permitir[7], entre outras ações:

- ✓ O registro das atividades de tratamento de dados pessoais em formato que permita a atualização de informações de forma facilitada; e
- ✓ A revisão regular das atividades mapeadas, garantindo que elas permaneçam precisas e atualizadas.

[6] Nos termos do art. 5°, III da LGPD, **dado anonimizado** é aquele relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
[7] REINO UNIDO, Information Comissioner's Office (ICO). *Records of processing and lawful basis.* Disponível em: <link>. Acesso em: 07 dez. 2023.

É possível a utilização de recursos de planilhas em formato .xlsx, programas especialmente desenvolvidos para *data mapping*, tabelas em arquivos .docx *etc.* Não há um padrão formalmente estabelecido para a documentação dos mapeamentos. Após escolher o meio pelo qual ocorrerá o registro das informações, é recomendável que a Instituição faça uma segmentação em áreas específicas, como: Recursos Humanos, Marketing, Jurídico, Tesouraria, Tecnologia da Informação, entre outros.

Esta segmentação, que pode/deve seguir o organograma de áreas da instituição, se disponível, auxilia a compreensão das rotinas das suas áreas/departamentos/unidades. Tal contextualização tem vital importância no momento da análise de risco, para que se evite fazer recomendações incompatíveis e, ainda, que possam inviabilizar as atividades da área. As questões relacionadas às análises de risco serão melhor desenvolvidas no próximo item.

Para auxiliar os agentes de tratamento de pequeno porte, a ANPD divulgou[8] um modelo de registro simplificado de operações de dados pessoais, que contêm os campos considerados essenciais para o exercício de suas atividades fiscalizatórias.

Tendo-se em vista que o mapeamento é uma etapa anterior à análise de riscos, é importante que as informações coletadas neste momento possibilitem um estudo posterior mais aprofundado sobre cada rotina registrada.

Embora até a data de publicação deste Guia não se tenha, ainda, uma regulamentação sobre quais informações devem constar, obrigatoriamente, na fase de mapeamento das rotinas, além do modelo de registro unificado da própria ANPD é possível utilizar ainda algumas orientações no cenário internacional como referência. Neste cenário, temos o Regulamento (UE) 2018/1725[9] do Parlamento Europeu e do Conselho, publicado em 23 de outubro de 2018. Este dispositivo, em seu artigo 31, estabelece o seguinte (tradução livre):

> 1. Cada responsável pelo tratamento deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo devem constar todas as informações seguintes:

[8] BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP): Agentes de tratamento de pequeno porte (ATPP) terão modelo simplificado para registrar operações de tratamento de dados pessoais*: 14 jul. 2023. Governo Federal. Disponível em: <link>. Acesso em: 07 dez. 2023.
[9] UNIÃO EUROPEIA. European Data Protection Supervisor (EDPS). Records Register. Disponível em: <link>. Acesso em: 07 dez. 2023.

> a) O nome e os contatos do responsável pelo tratamento, do Encarregado de Proteção de Dados e, se for caso, do subcontratante e do responsável conjunto pelo tratamento;
> b) As finalidades do tratamento dos dados;
> c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
> d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em Estados-Membros ou em países terceiros, ou pertencentes a organizações internacionais;
> e) Se for aplicável, as transferências de dados pessoais para um país terceiro ou para uma organização internacional, incluindo a identificação desse país terceiro ou dessa organização internacional, e a documentação que comprove a existência das garantias adequadas;
> f) Se possível, os prazos previstos para a exclusão das diferentes categorias de dados;
> g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 33° (...).

3.2. ANÁLISE DE RISCOS

Antes de adentrar no estudo analítico do risco, é importante entender a sua conceituação. A ABNT NBR ISO 3100:2018[10] define o risco como o "efeito da incerteza nos objetivos". O termo em questão também pode ser encontrado na Instrução Normativa n° 1 de maio de 2016 da Controladoria Geral da União (CGU), conforme segue abaixo:

> Art. 2°. Para fins desta Instrução Normativa, considera-se: (...)
> XIII – **risco**: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;
> XIV – **risco inerente**: risco a que uma organização está exposta em considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
> XV – **risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (...).

Verifica-se, a partir disto, que o risco deverá ser analisado quanto à **probabilidade** de ocorrência de um evento adverso e quanto ao **impacto** eventualmente causado, se o fato danoso vier a ocorrer. Ainda, um mesmo risco deverá ser analisado duas vezes, em diferentes ocasiões: a primeira sendo

[10] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 31000:2018**: Gestão de risco – Diretrizes, 2018, p.1. Disponível em: <link>. Acesso em: 17 jan. 2024.

antes da adoção de qualquer medida de mitigação (risco inerente) e, a segunda, após a adoção destas medidas (risco residual).

Inicialmente, para a análise do risco inerente, recomenda-se que seja criada uma espécie de *checklist* para avaliar se a rotina estudada tem potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Quanto a este ponto, enquanto ainda não há uma regulamentação específica no Brasil sobre a elaboração de Relatórios de Impacto, a própria ANPD[11] já se manifestou no sentido de que é possível, por ora, utilizar o conceito de "alto risco" definido no art. 4° da Resolução nº 2/2022 desta própria Autoridade.

No que tange à criação das *checklists* supramencionadas, algumas autoridades de dados pessoais em âmbito internacional disponibilizam exemplos quanto ao que pode implicar que uma rotina será ou não incluída em um Relatório de Impacto. Aqui, destaca-se o ICO, que apresenta em seu site uma lista[12] de verificação de triagem do DPIA (*Data Protection Impact Analysis*)[13], a qual se subdivide em dois pontos, conforme demonstrado a seguir.

LISTA DE VERIFICAÇÃO DE TRIAGEM DO ICO

(I) SERÁ CONSIDERADA A POSSIBILIDADE DE INCLUIR A ROTINA NO RELATÓRIO DE IMPACTO SE ELA INCLUIR:

- Formas de avaliação ou pontuação;
- Tomada de decisão automatizada com efeitos significativos;
- Monitoramento sistemático;
- Tratamento de dados sensíveis ou de natureza íntima;
- Tratamento de dados pessoais em larga escala;
- Tratamento de dados relativos a titulares vulneráveis;
- Soluções tecnológicas ou organizacionais inovadoras;
- Tratamento que pode impedir que os titulares dos dados exerçam um direito ou usem um serviço ou contrato.

[11] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais, 06 abr. 2023. Disponível em: <link>. Acesso em: 26 dez. 2023.
[12] REINO UNIDO. Information Comissioner's Office (ICO). *Data protection impact assessments*. Disponível em: <link>. Acesso em: 04 jan. 2024.
[13] O ICO estabelece estes critérios para a realização de um DPIA (*Data Protection Impact Analysys*), procedimento exigido pela lei de proteção de dados aplicável ao Reino Unido. Por analogia e, para fins exemplificativos, utilizou-se as orientações desta Autoridade para os fins de elaboração do Relatório de Impacto à Proteção de Dados exigido pela LGPD.

(II) A ROTINA SEMPRE SERÁ INCLUÍDA NO RELATÓRIO DE IMPACTO SE ELA ABRANGER:

- Utilização de perfis sistemáticos e extensivos ou tomada de decisão automatizada para tomar decisões significativas sobre pessoa;
- Tratamento de dados sensíveis ou dados de infrações penais em larga escala;
- Monitoramento sistematicamente de local acessível ao público em larga escala;
- Utilização de tecnologias inovadoras combinadas com qualquer dos critérios das orientações europeias;
- Realização de perfilamento em larga escala;
- Tratamento de dados biométricos ou genéticos em combinação com qualquer um dos critérios das orientações europeias;
- Combinação ou comparação de dados de várias fontes;
- Tratamento de dados pessoais sem prover um aviso de privacidade em combinação com qualquer um dos critérios das diretrizes europeias;
- Rastreio da localização ou do comportamento online ou offline dos titulares, em combinação com qualquer um dos critérios das diretrizes europeias;
- Tratamento de dados pessoais de crianças para definição de perfis ou tomada de decisões automatizadas ou para fins de marketing ou para oferecer serviços on-line diretamente a elas;
- Tratamento de dados pessoais que possam resultar em risco de danos físicos em caso de violação de segurança.

A Autoridade Europeia de Proteção de Dados (*European Data Protection Supervisor* – EDPS) também publicou um documento[14] que pode auxiliar a elaboração destas. A referida listagem segue destacada abaixo, com tradução livre para o português brasileiro:

CRITÉRIOS PARA PROCESSAMENTO "SUSCETÍVEL DE RESULTAR EM ALTO RISCO"
1. Avaliação sistemática e extensa de aspectos pessoais ou pontuação, incluindo *profiling.*
2. Tomada de decisão automatizada com efeitos legais ou similares significativos: tratamento que visa a tomada de decisões sobre os titulares dos dados.
3. Monitorização sistemática: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, especialmente em locais acessíveis ao público. Isto pode abranger a câmeras de vigilância, mas também outros tipos de monitorização, por exemplo, uso da Internet pelos funcionários.

[14] UNIÃO EUROPEIA. European Data Protection Supervisor (EDPS). *Data Protection Impact Assessment List*, p. 5-6. Publicado em: 17 jul. 2019. Disponível em: <link>. Acesso em: 30 jan. 2024.

4. Dados sensíveis ou dados de natureza altamente pessoal: dados que revelem origem étnica ou racial, opiniões políticas, religiosas ou crenças filosóficas, filiação sindical, dados genéticos, dados biométricos para identificar de forma inequívoca uma pessoa singular, dados relativos à saúde ou à vida sexual ou à orientação sexual, condenações criminais ou crimes e medidas de segurança relacionadas ou dados de natureza altamente pessoal.
5. Dados processados em grande escala, seja com base no número de pessoas envolvidas e/ou na quantidade de dados processados sobre cada deles e/ou permanência e/ou cobertura geográfica.
6. Conjuntos de dados combinados em diferentes operações de processamento de dados realizadas para diferentes fins e/ou por diferentes controladores de dados de uma forma que exceda as expectativas razoáveis do titular dos dados.
7. Dados relativos a titulares de dados vulneráveis: situações em que existe um desequilíbrio na relação entre a posição dos dados sujeito e o controlador podem ser identificados.
8. Uso inovador ou aplicação de soluções tecnológicas ou organizacionais que possam envolver novas formas de coleta de dados e uso. Na verdade, as consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas.
9. Impedimento dos titulares quanto ao exercício de direitos, utilização de serviço ou celebração de contrato.

Conforme não há, até a data de publicação deste Guia, a exigência normativa de critérios taxativos a serem observados nesta etapa, cada Instituição poderá criar suas próprias “listas de triagem”, de acordo com o que for aplicável ou não às suas atividades.

Após a criação das *checklists*, deve-se vislumbrar os infortúnios que podem acontecer e, para isso, é mister que se conheça as particularidades do setor e de suas atividades, entre outros aspectos. Neste momento, é importante que já se tenha estabelecido a metodologia a ser utilizada para realizar a análise de riscos. Segundo a norma ISO/IEC 31010:2019, alguns critérios relevantes[15] são:

- ✓ Como será feita a análise se um determinado risco é ou não aceitável;
- ✓ Como a relevância dos riscos será estabelecida;
- ✓ Como o risco será analisado nas rotinas onde cada uma delas pode haver múltiplos critérios de risco, com consequências negativas, positivas ou ambas;
- ✓ Como a relação entre os riscos será considerada.

[15] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *IEC 31010:2019*, p. 14. Geneva, junho de 2019. Tradução livre. Disponível em: <link>. Acesso em: 15 dez. 2023.

De modo geral, a análise de risco busca possibilitar a identificação de múltiplos fatores[16] que podem se apresentar em uma única rotina, a saber:

Probabilidade de eventos e consequências
Natureza e magnitude das consequências
Complexidade e conectividade
Fatores temporais e volatilidade
Eficácia dos controles existentes
Sensibilidade e níveis de confiança

Seja qual for o critério de análise adotado, é importante entender que o conceito[17] de risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades. Sendo assim, é sempre importante definir os critérios que serão considerados para análise da probabilidade (P) e do impacto (I) em uma rotina.

3.2.1. ANÁLISE DE PROBABILIDADE

A análise da probabilidade de ocorrência de eventos adversos consiste, basicamente, em estudar as chances de que uma certa situação indesejada possa ocorrer e, consequentemente, causar danos (em maior ou menor grau) aos titulares. Assim, neste momento, a pergunta a ser feita quando do estudo da rotina é “quais as chances de ocorrer algum dano ou risco relevante aos titulares?”. Para esta reflexão, seguem abaixo algumas questões[18] que podem ser consideradas para avaliar a probabilidade de ocorrência de eventos adversos:

RECURSOS TÉCNICOS E DE REDE (*HARDWARE* E *SOFTWARE*)	Conexões de rede podem apresentar vulnerabilidades contra fontes externas (*e.g.* ataques de *hackers*) e contra fontes internas (*e.g.* sistemas de TI da própria organização que pode apresentar falhas de segurança). Alguns recursos de *hardware* e *software* também podem apresentar ameaças pela falta de manutenção e configuração adequadas, entre outras questões.

[16] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 31000:2018:* Gestão de riscos — Diretrizes, p.13. 2ª edição. Rio de Janeiro: ABNT, 2018.
[17] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. op. cit, p. 1.
[18] UNIÃO EUROPEIA. European Union Agency for Cybersecurity (ENISA). *Guidelines for SMEs on the security of personal data processing*, p.24 a 25. 27 jan. 2017. Disponível em: <link>. Acesso em: 26 dez. 2023.

PROCEDIMENTOS-PADRÃO RELACIONADOS ÀS OPERAÇÕES DE TRATAMENTO DE DADOS	Em alguns casos, as vulnerabilidades podem surgir da falta de procedimentos apropriados, sendo necessárias regras e práticas específicas dentro da organização para o tratamento de dados pessoais. Tais ameaças incluem acesso aos dados por pessoas não autorizadas, modificação/destruição não autorizada de dados, eliminação acidental ou perda de dados *etc*.
PESSOAS ENVOLVIDAS NA OPERAÇÃO DE TRATAMENTO DE DADOS PESSOAIS	As falhas de segurança podem surgir por parte das pessoas que operacionalizam as atividades de tratamento de dados pessoais, isto é, os funcionários de uma Instituição diretamente envolvidos na ação. Ameaças relevantes neste sentido incluem ataques internos maliciosos, erro humano, divulgação não autorizada de dados por contratados/contratantes *etc*.
SETOR DE NEGÓCIOS E ESCALA DO TRATAMENTO DE DADOS	A área de negócios de uma Instituição e, ainda, a quantidade de dados tratados podem afetar significativamente o tipo e nível de falhas de segurança. Por exemplo, se o tipo de dado pessoal é considerado um ativo valioso, e/ou se o tratamento diz respeito a uma população inteira de um país, *hackers* mal-intencionados podem ter mais interesse em acessar estes dados.

Estes são alguns exemplos do que deve ser considerado em uma análise de probabilidade de ocorrência de eventos adversos. Após a efetiva compreensão dos fatores que podem interferir nas chances de ocorrência de dano, é interessante colocá-los em uma perspectiva escalonada para entender se esta probabilidade é alta ou menor. Para facilitar o entendimento, consta abaixo um quadro exemplificativo que permite compreender as variações neste tipo de análise:

PROBABILIDADE	**DESCRIÇÃO**
RARO	A possibilidade de ocorrência de evento adversos é excepcional, quase impossível.
IMPROVÁVEL	Pode ser que ocorra algum evento adverso em circunstâncias não normais.
POSSÍVEL	Existem chances consideráveis de ocorrer algum evento adverso.
QUASE CERTO	Caso não seja adotada nenhuma medida de mitigação, certamente ocorrerá algum evento adverso.

O quadro acima é meramente exemplificativo, podendo ser adotadas outras métricas para este tipo de estudo. O importante é atribuir escalas para compreender a dimensão da probabilidade de

ocorrência de danos, uma vez que este entendimento permitirá a avaliação de risco total de uma rotina a partir, também, do estudo de uma análise quanto ao impacto.

Assim, o interesse que um determinado banco de dados pode gerar a terceiros, os controles jurídicos, administrativos e de segurança existentes e os modos de tratamento pelos agentes envolvidos são indicadores que podem igualmente interferir no nível de probabilidade de dano.

Por exemplo, cita-se que a probabilidade de eventos adversos em proteção de dados pessoais com um banco de dados sobre funcionários tratado por poucas pessoas em um servidor seguro e com criptografia é menor do que a de um outro banco de dados de alunos tratado por muitas pessoas em seus computadores pessoais e que trocam arquivos por anexos de e-mail sem proteção.

3.2.2. ANÁLISE DE IMPACTO

A avaliação de impacto de uma rotina deve considerar fatores como a natureza e variedade dos dados pessoais tratados, os titulares envolvidos, a criticidade da operação, entre outros fatores. Aqui se deve vislumbrar os possíveis efeitos que o titular poderia sofrer caso ocorresse algum evento danoso. Para este tipo de avaliação, alguns pontos podem ser considerados:

TIPO DE DADO PESSOAL	Essa informação poderá aumentar ou diminuir o nível de impacto com base na criticidade da categoria de dado pessoal tratado. Por exemplo, rotinas que envolvam a utilização de dados médicos ou opinião política podem causar danos mais graves aos titulares do que rotinas que envolvam o tratamento de dados mais comuns, como nome, *e-mail etc*.
CRITICIDADE DA OPERAÇÃO DE TRATAMENTO DE DADOS	Seguindo a mesma lógica do ponto acima, é importante avaliar a criticidade global da operação de tratamento. Deverá ser dada especial atenção às operações de tratamento que se baseiem ou possam conduzir ao rastreio, monitorização ou vigilância sistemáticos de indivíduos.
VOLUME DE DADOS PESSOAIS	Quanto maior for a quantidade de dados pessoais sobre um mesmo titular utilizada em uma rotina, maiores as chances de ocorrência de eventos adversos.
CARACTERÍSTICAS ESPECIAIS DO AGENTE DE TRATAMENTO	Este parâmetro se refere à área de atuação e às atividades de negócio de uma Instituição, que podem, por sua própria natureza, revelar informações adicionais para um certo conjunto de dados. Por exemplo, a quebra de confidencialidade de uma lista de clientes pode ser maior se essa lista pertencer a uma farmácia do que a uma papelaria.

CARACTERÍSTICAS ESPECIAIS DOS TITULARES DOS DADOS	O impacto também poderá aumentar caso os titulares dos dados pertençam a um grupo social com necessidades específicas (*e.g.*: crianças, figuras públicas *etc*.). Por exemplo, o processamento de uma lista de números de telefone se torna mais crítico se pertencer a membros conhecidos do Parlamento nacional.

PONTO DE ATENÇÃO

O IMPACTO E A PERSPECTIVA DO TITULAR

- A análise quanto ao impacto no âmbito de um RIPD à Proteção de Dados Pessoais deverá ser sempre realizada do ponto de vista do titular. Ou seja, aqui não se leva em consideração o impacto sofrido pela Instituição, e sim o dano eventualmente causado ao titular de dados pessoais.

Da mesma forma que é necessário atribuir uma escala quanto à probabilidade de ocorrência de eventos adversos (conforme explicado no item 4.2.1), também é importante a criação de uma escala de avaliação quanto à intensidade do impacto eventualmente causado se o dano venha a ocorrer. Neste sentido, o quadro[19] abaixo demonstra uma possível forma de medir o prejuízo causado ao titular em decorrência de um fato lesivo.

IMPACTO	DESCRIÇÃO
BAIXO	Os titulares podem encontrar alguns pequenos inconvenientes, que eles vão superar sem qualquer problema (*e.g.: tempo gasto reinserindo informações, aborrecimentos, irritações etc.*).
MÉDIO	Os titulares podem encontrar inconvenientes significativos, que eles serão capazes de superar apesar de algumas dificuldades (*e.g.: custos extras, negação de acesso a serviços empresariais, medo, falta de compreensão, estresse, pequeno mal-estar físico etc.*).
ALTO	Os titulares podem encontrar consequências significativas, que eles devem ser capazes de superar, embora com sérias dificuldades (*e.g.: desvio de fundos, lista proibida por parte de instituições financeiras, danos materiais, perda de emprego, intimação, agravamento de saúde etc.*).
MUITO ALTO	Os titulares podem encontrar consequências significativas ou mesmo irreversíveis, que podem não conseguir superar (*e.g.: incapacidade para o trabalho, doenças psicológicas ou físicas de longo prazo, ameaças concretas à integridade física ou psicológica, etc.*).

[19] UNIÃO EUROPEIA. European Union Agency for Cybersecurity (ENISA). *Guidelines for SMEs on the security of personal data processing*, p.20. 27 jan. 2017. Disponível em: <link>. Acesso em: 26 dez. 2023.

Após a avaliação da probabilidade de ocorrência de eventos adversos (P) e do impacto eventualmente causado ao titular diante de um fato danoso (I), proceder-se-á com o cálculo de riscos, etapa essencial para a compreensão do risco real de uma rotina.

3.3. CÁLCULO DOS RISCOS

Após a análise da probabilidade (P) e do impacto (I), é interessante fazer uma escala de risco, uma vez que a atribuição de valores aos critérios estudados traz maior objetividade ao estudo da rotina. Segundo a ISO/IEC 31010:2019, existem vários métodos[20] que podem ser utilizados em matéria de análise de riscos em sentido amplo, como, por exemplo, o teorema de Bayes, a análise de impacto no negócio (BIA), o método de causa e efeito (CCA), árvore de eventos (ETA), árvore de falhas (FTA), o método da confiabilidade humana (HRA), a análise de Markov, a simulação de Monte Carlo, a análise de impacto na privacidade (PIA) e a análise de impacto na proteção de dados pessoais (DPIA).

Os dois últimos tipos de estudo de riscos (PIA e DPIA) ajudam as organizações na identificação, avaliação e gerenciamento dos riscos de associados ao tratamento de dados pessoais. Estes processos de análise são mais simples que os demais já mencionados, sendo de fácil compreensão e aplicação. Deve-se observar, contudo, que essas formas de avaliação podem apresentar algumas desvantagens[21], como a imprecisão do grau de severidade do risco atribuído na análise preliminar. Uma metodologia adequada para o cálculo do risco possibilita entender melhor sua dimensão e, por conseguinte, o seu grau de aceitabilidade e a razoabilidade das medidas de mitigação a serem tomadas.

O risco total de uma rotina pode ter como classificação geral os valores: baixo, médio e alto, dependendo da metodologia adotada pela Instituição. Para que seja possível atribuir tais valores ao risco total de uma determinada rotina, é necessário que se tenha em mente a avaliação da probabilidade de ocorrência de dano (P) e do impacto (I). Tendo essas informações em vista, recomenda-se a utilização de uma matriz P x I para facilitação do cálculo do risco, conforme destacado abaixo:

[20] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *IEC 31010:2019*, p. 66 - 85. Geneva, junho de 2019. Tradução livre. Disponível em: <link>. Acesso em: 15 dez. 2023.
[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *IEC 31010:2019*, p. 85. Geneva, junho de 2019. Tradução livre. Disponível em: <link>. Acesso em: 15 dez. 2023.

IMPACTO \ PROBABILIDADE	1 Remoto	2 Improvável	3 Acreditável	4 Provável	5 Quase certo
1 Insignificante	1	2	3	4	5
2 Baixo	2	4	6	8	10
3 Moderado	3	6	9	12	15
4 Maior	4	8	12	16	20
5 Catastrófico	5	10	15	20	25

A matriz acima possibilita que se atribua um valor de 1 (um) a 5 (cinco) para a probabilidade de ocorrência de eventos adversos e um valor também de 1 (um) a 5 (cinco) pata o impacto eventualmente causado ao titular na eventualidade de ocorrer um dano. Assim, é possível entender que o valor do risco equivale ao produto da multiplicação do valor da probabilidade pelo valor do impacto.

Assim, temos: $Risco\ (R) = P\ x\ I$, onde P equivale à probabilidade e I equivale ao impacto.

É importante pontuar que o valor do risco sempre incidirá sobre a rotina analisada. Deste modo, caso uma única rotina apresente dois ou mais tipos de risco, é possível fazer um cálculo de média quanto aos riscos individuais, conforme o exemplo abaixo:

$Risco\ 1\ (R_1) = P_1\ x\ I_1$

$Risco\ 2\ (R_2) = P_2\ x\ I_2$

$Risco\ 3\ (R_3) = P_3\ x\ I_3$

Deste modo, temos: $Risco\ agregado\ da\ rotina\ (R) = \frac{(R_1+R_2+R_3)}{3}$

A utilização de cálculo permite obter uma classificação mais objetiva quanto ao grau do risco associado à rotina analisada. Após a realização do cálculo de riscos, passa-se à próxima etapa: a elaboração do RIPD.

4. ELABORAÇÃO DO RELATÓRIO DE IMPACTO

Após estabelecer quais rotinas serão incluídas no RIPD, conforme mencionado no item 3.2 e, ainda, tendo em vista a definição de Relatório de Impacto à Proteção de Dados Pessoais no Capítulo 3 deste Guia, existem alguns pontos centrais que devem ser levantados quando da elaboração do documento, como: o que ele deverá conter, como poderá ser editado *etc.* Estas e mais outras questões serão detalhadas nos próximos itens.

De um modo geral, o RIPD deve apresentar os métodos escolhidos pelo Controlador para analisar os riscos, pontuá-los, classificá-los e, finalmente, indicar as medidas de mitigação tomadas pela Instituição. A elaboração deste tipo de registro tem algumas exigências legais e regulamentares que devem ser observadas para que o documento esteja adequado às normas aplicáveis e para que ele atenda ao propósito ao qual se destina.

4.1. ESTRUTURAÇÃO DO RIPD

A LGPD traz, em seu art. 38, Parágrafo Único, a seguinte determinação:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A partir desta redação, é possível constatar alguns pontos importantes sobre o RIPD:

- ✓ Os segredos comercial e industrial não precisam/devem constar neste tipo de documento;
- ✓ O RIPD deve apresentar as seguintes informações obrigatórias: descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança dos dados, a análise do Controlador em relação às medidas de mitigação adotadas.

Conforme já mencionado, até a data de publicação deste Guia ainda não houve uma regulamentação específica por parte da ANPD sobre a forma de elaboração e estruturação de um

RIPD. Entretanto, ainda na legislação brasileira há alguns pontos que podem ser trazidos à luz para facilitar este processo, como a Resolução Conama n° 001/1986, a qual traz, em seu âmago, as figuras do Estudo de Impacto Ambiental (EIA) e o Relatório de Impacto Ambiental (RIMA). Estes documentos podem ser utilizados como uma referência para começar a elaborar um Relatório de Impacto à Proteção de Dados Pessoais. Em relação à regulamentação do RIPD, a ANPD, na Portaria n° 35 de novembro de 2022, divulgou que o tema possui previsão inicial de regulação até o final do ano de 2024. Ainda, para fins de referência, é possível consultar os Relatórios de Impacto já publicados por alguns Órgãos, como o Tribunal de Contas da União (TCU)[22] e o Banco Central do Brasil (Bacen)[23].

Reforça-se que a ANPD já se manifestou[24] no sentido da não obrigatoriedade de publicação do RIPD pelas instituições privadas. No que tange às instituições públicas, por outro lado e, caso a ANPD assim determine, elas poderão ser obrigadas a publicar seus respectivos Relatórios de Impacto, conforme é possível extrair da leitura do art. 32 da LGPD.

Quanto ao seu conteúdo e, ainda, por ser um documento legal que sintetiza a identificação de altos riscos e suas mitigações, o Relatório de Impacto à Proteção de Dados Pessoais precisa apresentar algumas informações para que a ANPD possa compreender o método de análise de riscos utilizado pela Instituição, a adequação e pertinência das medidas de mitigação adotadas, entre outros aspectos relevantes. Neste diapasão, a ANPD já se pronunciou[25] quanto aos dados e informações que devem ser incluídos no RIPD, a saber:

> Identificação dos agentes de tratamento e do encarregado.
>
> Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos.
>
> Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros).

[22] TRIBUNAL DE CONTAS DA UNIÃO (TCU). *Relatório de Impacto à Proteção de Dados Pessoais no Âmbito das contratações do TCU*. Governo Federal, 15 dez. 2021. Disponível em: <link>. Acesso em: 26 jan. 2024.
[23] BANCO CENTRAL DO BRASIL (Bacen). *Relatório de Impacto à Proteção de Dados Pessoais*. Governo Federal, out. 2022. Disponível em: <link>. Acesso em: 26 jan. 2024.
[24] BRASIL. Autoridade Nacional de Proteção de Dados. *Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais*. Governo Federal. Disponível em: <link>. Acesso em 18 jan. 2024.
[25] BRASIL. Autoridade Nacional de Proteção de Dados. *Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais*. Governo Federal. Disponível em: <link>. Acesso em 18 jan. 2024.

Projeto/Processo que justifica a elaboração do RIPD.
Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD.
Tratamento de dados: a) Descrição do tratamento (desde a coleta até a eliminação); b) Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa); c) Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa); d) Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços); e) Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver; f) Volume de dados pessoais tratados e número de titulares envolvidos no tratamento; g) Fonte de coleta; h) Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado); i) Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver); j) Política de armazenamento (descrever os prazos de retenção e métodos de descarte).
Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento.
Análise de princípios da LGPD.
Riscos identificados ao titular.
Resultado apurado com base na metodologia utilizada pelo agente de tratamento: a) Descrição do risco e do impacto para o titular; b) Probabilidade; c) Impacto; d) Risco total.
Medidas, salvaguardas e mecanismos de mitigação de risco: a) Risco; b) Tratamento do risco (*descrever as medidas adotadas para mitigação do risco*); c) Risco após o tratamento; d) Risco residual.
Comentários e aprovações.

É importante destacar que o RIPD deverá apresentar detalhadamente as medidas de mitigação tomadas, sinalizando devidamente os riscos inerente e residual. É mister que o documento contenha as explicações detalhadas sobre os processos analisados para que a Autoridade fiscalizadora possa fazer uma análise de adequação.

A importância da elaboração minuciosa das análises de risco no RIPD foi recentemente evidenciada no âmbito do Processo SEI nº 00261.000730/2022-53[26], sobre a divulgação de microdados do censo escolar e do Exame Nacional do Ensino Médio (ENEM) pelo INEP. Nesta ocasião, a ANPD observou o devido embasamento legal para a realização das atividades de tratamento de dados pessoais, a pertinência das medidas de segurança tomadas pelo INEP frente o caso concreto, a descrição das atividades capazes de gerar riscos às liberdades civis e aos direitos fundamentais e, ainda, a metodologia utilizada pelo Órgão para realizar suas operações de tratamento de dados pessoais.

Finalmente, vale mencionar as orientações[27] do EDPS quanto à elaboração de um Relatório de Impacto à Proteção de Dados, que menciona, entre outros aspectos, as seguintes informações:

- ✓ Fluxo do diagrama de processos;
- ✓ Descrição detalhada da finalidade do tratamento de dados pessoais;
- ✓ Descrição da interação com outros processos internos;
- ✓ Descrição da infraestrutura utilizada na rotina.

Resumidamente, o RIPD deverá apresentar: ***(i)*** a metodologia utilizada para análise de riscos; ***(ii)*** os riscos identificados em cada rotina, separadamente; ***(iii)*** os valores referentes aos riscos inerentes; ***(iv)*** as medidas de mitigação utilizadas para mitigar cada um dos riscos identificados; e ***(v)*** os valores referentes aos riscos residuais. Para elaborar o documento, o Controlador também possui à sua disposição algumas ferramentas criadas especificamente para este fim, como o *software*[28] criado pela autoridade de proteção de dados francesa, a *Commission Nationale de l'Informatique et des Libertés* (CNIL), disponibilizado em seu *site*.

[26] BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD publica Nota Técnica sobre divulgação de microdados pelo INEP: Coordenação-Geral de Fiscalização concluiu que Instituto cumpriu adequadamente medidas que reduzissem os riscos de violação da privacidade*. Governo Federal, 13 nov. 2023. Disponível em: <link>. Acesso em: 29 jan. 2024.
[27] UNIÃO EUROPEIA. European Data Protection Supervisor (EDPS). *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies – Part II: DPIAs and prior consultation*, p. 7. Publicado em: 16 jul. 2019. Disponível em: <link>. Acesso em: 08 mar. 2024.
[28] FRANÇA. Commission nationale de l'informatique et des libertés (CNIL). *The open source PIA software helps to carry out data protection impact assessment*. Publicado em: 30 jun. 2021. Disponível em: <link>. Acesso em: 13 mar. 2024.

4.2. IMPLEMENTAÇÃO DAS MEDIDAS DE MITIGAÇÃO DE RISCOS

Sabe-se que os riscos eventualmente identificados durante a etapa de análise deverão ser mitigados na medida do que for factível e que estas informações deverão constar no Relatório de Impacto à Proteção de Dados Pessoais. De acordo com o *Project Management Institute* (PMI)[29], as propostas de mitigação de riscos devem levar em consideração diversos elementos, como:

- ✓ Recursos disponíveis;
- ✓ Formas de evolução;
- ✓ Metodologia e processos utilizados;
- ✓ Ferramentas e técnicas utilizadas;
- ✓ Infraestrutura de suporte;
- ✓ Revisão e frequência de atualização;
- ✓ Requisitos de relatórios.

Um ponto extremamente importante e que exige a flexibilidade e compreensão multidisciplinar dos agentes de tratamento e de suas Equipes de Encarregado sobre o RIPD é o da razoabilidade e adaptabilidade das medidas às circunstâncias concretas de cada organização. O RIPD, tal como a LGPD sinaliza, é um tópico complexo, multidisciplinar e que exige expertises não apenas legais, mas de processos e de tecnologia da informação.

De um lado, recomendações extremamente teóricas e que recaiam em zonas de conforto (ex.: criptografar determinado arquivo em repouso, ainda que ele seja utilizado por diversos operadores do agente de tratamento e possua risco considerado baixo) podem prejudicar a exequibilidade do projeto. De outro, recomendações excessivamente pragmáticas e que acolham tão somente a perspectiva da facilidade e custo do agente de tratamento, deixando em segundo plano a salvaguarda de direitos e liberdades dos titulares, podem tornar o RIPD um documento com pouca profundidade e eficiência questionável.

[29] PROJECT MANAGEMENT INSTITUTE (PMI). *The Standard for Risk Management in Portfolios, Programs and Projects*, p. 31. Pensilvânia, Estados Unidos: Project Management Institute Inc., 2019.

Portanto, é imprescindível que as equipes envolvidas com as tomadas de decisão abrangidas em um RIPD sejam multidisciplinares e que argumentos bem embasados e razoáveis sejam aventados de modo a equilibrar todos os componentes desta equação.

Cumpre ressaltar, ainda, que deverão ser consideradas as eventuais normas regulamentares existentes que versem sobre a administração dos documentos utilizados na rotina. Logo, aqui o apoio operacional de pessoas habituadas à referida rotina é essencial para a correta identificação do arcabouço legal envolvido.

A título exemplificativo, tem-se que as Instituições de Ensino devem observar as Tabelas de Temporalidade e Destinação do Ministério da Educação (MEC)[30]. Assim, por exemplo, caso uma das medidas de mitigação de riscos recomendada pela Instituição de Ensino Superior seja a de eliminação de determinados tipos de documento, deve-se assegurar que esta operação não contrarie a normativa do Órgão público supramencionado. Para mais detalhes, consulte o **Guia de Proteção de Dados Pessoais: jornada acadêmica**.

Assim, quanto às medidas de mitigação recomendadas, a ABNT NBR ISO 3100:2018 estabelece[31] que as informações fornecidas no plano de trabalho incluam:

- ✓ A justificativa para a seleção das opções de tratamento, incluindo os benefícios esperados;
- ✓ As pessoas responsabilizáveis e responsáveis por aprovar e implementar o plano;
- ✓ As ações propostas;
- ✓ Os recursos requeridos, incluindo contingências;
- ✓ As medidas de desempenho;
- ✓ As restrições;
- ✓ Os relatos e monitoramento requeridos;
- ✓ Quando se espera que ações sejam tomadas e concluídas.

[30] BRASIL. Ministério da Educação. *Tabela de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Fim das Instituições Federais de Ensino Superior – IFES*. Disponível em: <link>. Acesso em: 13 mar. 2024.
[31] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 31000:2018: Gestão de riscos — Diretrizes*, p.15. 2ª edição. Rio de Janeiro: ABNT, 2018.

As medidas de mitigação podem ter várias áreas de aplicação. Assim, elas podem ter as seguintes naturezas: técnica, ou seja, pautadas em questões relacionadas a modificações na infraestrutura tecnológica da Instituição; jurídica, ou seja, que versem sobre questões de direito, como a elaboração de cláusulas contratuais ou termos de compromisso e responsabilidade; gerencial ou administrativa, isto é, quando se tratarem de medidas que incidam sobre o comportamento padrão do gestor/analista/técnico durante a execução de atividades que impliquem o tratamento de dados pessoais; entre outras formas.

Neste ponto, é de vital importância a **comunicação com os setores responsáveis pela implementação das medidas de mitigação recomendadas**. O PMI entende que são fatores de sucesso para o plano de mitigação de riscos: ***(i)*** a aceitação pelas partes interessadas; ***(ii)*** a identificação de certas tendências e as formas de correção das mesmas; ***(iii)*** Alinhamento sobre as restrições internas e externas, bem como sobre as prioridades; ***(iv)*** Balanceamento entre custo ou esforço da medida e seu benefício; e ***(v)*** Integridade em relação às necessidades do processo de gestão de riscos.

5. REVISÃO PERIÓDICA DO MAPEAMENTO

O mapeamento é um processo cíclico e deve ser revisto com uma determinada frequência para que ele esteja sempre condizente com a realidade de um determinado setor. É normal que ocorram mudanças na estrutura da Instituição, bem como a mudança dos sistemas utilizados e a forma de gestão e o registro destas informações deve estar sempre atualizado.

Sobre este tema, a ANPD se manifestou, por meio de sua Coordenação-Geral de Fiscalização (CGF), sobre a necessidade de atualização dos processos de mapeamento no âmbito da divulgação dos microdados do censo escolar e do Exame Nacional do Ensino Médio (ENEM) pelo Instituto Nacional de Estudos e Pesquisas Anísio Teixeira (INEP), conforme o texto[32] extraído a seguir:

> (...) Outrossim, **a CGF recomenda ao INEP a revisão contínua dos RIPDs apresentados, em especial, quando houver fatos novos que possam ensejar mudanças nos riscos identificados**, tais como alteração nas operações de

[32] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Nota Técnica nº 12/2023/CGF/ANPD, 2023. Disponível em: <link>. Acesso em: 14 mar. 2023.

> 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. Recomenda-se, ainda, a expansão e o aprimoramento dos canais de acesso controlado às bases de microdados destinados aos pesquisadores externos e demais cadastrados (...)

Conforme a ABNT NBR ISO 3100:2018[33], o monitoramento e análise crítica têm como principal finalidade "assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo". Logo, o constante acompanhamento das áreas mapeadas fortalece a cultura de proteção de dados e, ainda, evita situações de desconformidade com a LGPD. Oportunamente, apresenta-se abaixo o esquema gráfico apresentado pelo EDPS sobre o fluxo[34] do processo de mapeamento:

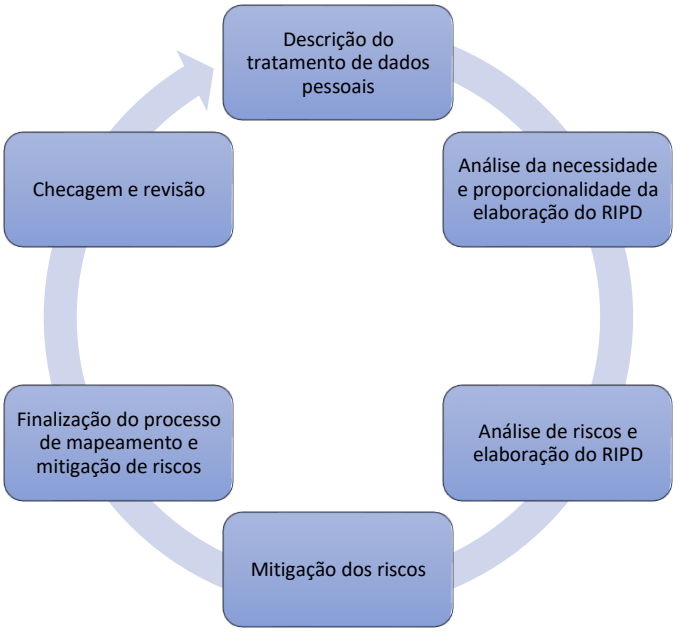

Figura 1. Representação do processo cíclico do mapeamento conforme o EDPS.

[33] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000:2018: Gestão de riscos — Diretrizes, p.16. 2ª edição. Rio de Janeiro: ABNT, 2018.
[34] UNIÃO EUROPEIA. European Data Protection Supervisor (EDPS). *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies – Part II: DPIAs and prior consultation*, p. 6. Publicado em: 16 jul. 2019. Disponível em: <link>. Acesso em: 08 mar. 2024.

Sobre a revisão periódica dos processos, o PMI[35] estabelece que (tradução livre):

> (...) Os objetivos principais do processo de monitoramento são rastrear os riscos identificados e manter a viabilidade dos planos de resposta. Além de monitorar e gerenciar as ações de resposta aos riscos, a eficácia de todos os processos de gestão de riscos é revisada periodicamente para proporcionar melhorias na gestão do trabalho atual, bem como trabalhos futuros com lições aprendidas (...)

O referido Instituto também menciona que o plano de gerenciamento de riscos é focado em um processo de melhoria a longo prazo e, ainda, apresenta como alguns fatores-chave para o sucesso da conscientização sobre os riscos: ***(i)*** monitoramento integrado dos riscos; ***(ii)*** o monitoramento contínuo das condições que ativam situações de risco; e ***(iii)*** a manutenção de um estado de atenção para os riscos que eventualmente podem se apresentar.

Em conclusão, o processo de revisão periódica dos mapeamentos feitos e das medidas de mitigação implementadas gera mais segurança para um processo de adequação estável e promove a conscientização coletiva sobre a importância dos procedimentos de segurança adotados para proteger os dados pessoais nas operações de tratamento.

6. CONSIDERAÇÕES FINAIS

Neste documento foram abordados os principais pontos que envolvem a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais sob a égide da LGPD.

No Capítulo 2 constam os aspectos gerais do RIPD, como a sua definição, sobre quem recai a responsabilidade de sua elaboração, os tipos de rotinas que devem constar no documento e o momento ideal para sua elaboração;

No Capítulo 3 foram abordados os tópicos referentes às etapas prévias à elaboração do RIPD, como o mapeamento, o registro das operações das atividades de tratamento de dados pessoais, as análises de risco e a necessidade da apresentação da metodologia escolhida;

[35] PROJECT MANAGEMENT INSTITUTE (PMI). *The Standard for Risk Management in Portfolios, Programs and Projects*, p. 40. Pensilvânia, Estados Unidos: Project Management Institute Inc., 2019.

No Capítulo 4 foram trazidos os aspectos referentes à elaboração do RIPD propriamente dito, como sua estruturação, os principais pontos que devem ser mencionados no referido documento, a implementação das medidas de mitigação e a importância do envolvimento multidisciplinar de todos os envolvidos na rotina, como advogados, gerentes e gestores de tecnologia da informação.

Por fim, no Capítulo 5 é possível verificar a importância da revisão periódica do mapeamento e os fatores-chave para o sucesso do monitoramento da implementação das medidas de mitigação de riscos.

Este Guia se destinou a oferecer algumas diretrizes e boas práticas, especialmente no que se refere às Instituições Educacionais e suas mantenedoras que, na realização de suas atividades, poderão vislumbrar a necessidade de elaborar um Relatório de Impacto à Proteção de Dados Pessoais.

Este Guia é suscetível de constante mudança e atualização.

FGV DCI

DIRETORIA DE
CONTROLES INTERNOS