

Ofício nº 09-SG-GT-Ano/2024

Curitiba/PR, 26 de fevereiro de 2024

À Autoridade Nacional de Proteção de Dados (ANPD)

GABINETE DA PRESIDÊNCIA DA REPÚBLICA

Conselho Diretor

Esplanada dos Ministérios, Ministério da Economia, Bloco C, 2º andar, Brasília - DF,  
70297-400.

Ao Senhor Waldemar Gonçalves Ortunho Júnior – Diretor Presidente

Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos direitos fundamentais de privacidade e proteção de dados, bem como colaborar com o desenvolvimento de políticas públicas relacionadas a proteção de dados pessoais, o INPD vêm, respeitosamente, apresentar suas observações e recomendações quanto à Consulta **Pública** relacionada ao **Estudo Preliminar Anonimização e pseudonimização para a proteção de dados pessoais**, conforme exposto abaixo.

**Instituto Nacional de Proteção de Dados - INPD**

Atilio Augusto Segantin Braga

(Secretário Geral)

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

## Contribuição do Instituto Nacional de Proteção de Dados – INPD

### Consulta Pública – Estudo Preliminar Anonimização e pseudonimização para a proteção de dados pessoais

#### Grupo de Trabalho

O presente estudo foi elaborado pelo grupo técnico composto por alguns associados do IINPD e que analisou a sugestão de minuta apresentada pela Autoridade Nacional de Proteção de Dados – ANPD via – “Estudo Preliminar sobre Anonimização e Pseudonimização para a Proteção de Dados Pessoais”.

Para garantir uma análise aprofundada e abrangente, contamos com a participação dos seguintes membros do INPD que foram responsáveis pela elaboração do presente estudo:

- Atilio Augusto Segantin Braga
- Denise Nunes
- Martha Leal
- Matheus Passos
- Mitye Hirye
- Rafael Reis

#### Reconhecimento

Parabenizamos a Autoridade Nacional de Proteção de Dados – ANPD, bem como todos os servidores e colegas que participaram da elaboração do material objeto da presente consulta pública.

Percebe-se um grande esforço no sentido de buscar simplificar a compreensão do processo de Anonimização e Pseudonimização face a sua complexidade e impactos de ordem prática na esfera dos direitos individuais.

Assim, com o objetivo de contribuir e somar a esse esforço, tecemos aqui as contribuições do Instituto Nacional de Proteção de Dados sobre o tema, buscando aperfeiçoar o material, deixando-o mais completo, fluído e de fácil utilização, independente da área de formação de quem o esteja utilizando.

O estudo foi estruturado por tópico seguindo o racional do estudo preliminar.

As sugestões são precedidas da expressão [inclusão] quando o tema ou parágrafo não foi abordado no estudo original. Em se tratando de alterações, é citado o tópico, seção e item, precedido da transcrição do texto original seguindo da sugestão e justificativa de alteração.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

## Sumário

<b>2. Conceitos Básico</b> .....	4
<b>2.1. Glossário</b> .....	4
[inclusão].....	4
<b>2.2. Anonimização e Pseudonimização de Dados na LGPD</b> .....	6
[inclusão].....	6
<b>3. OS PROCESSOS DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS</b> .....	7
<b>3.1. ASPECTOS JURÍDICOS RELEVANTES</b> .....	7
<b>3.1.2 RISCOS DE REIDENTIFICAÇÃO DE DADOS ANONIMIZADOS</b> .....	7
[inclusão].....	7
<b>3.2. O PROCESSO DE ANONIMIZAÇÃO</b> .....	7
<b>3.2.2. Gestão do risco de reidentificação</b> .....	8
[inclusão].....	8
<b>3.3. O PROCESSO DE PSEUDONIMIZAÇÃO</b> .....	15
<b>6. APÊNDICES</b> .....	15
<b>APENDICE I. PRINCIPAIS ESCLARECIMENTOS</b> .....	15
Justificativa.....	16
<b>APENDICE II. CADERNO DE TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO</b> .....	16
<b>TÉCNICAS PARA ANONIMIZAR DADOS TEXTUAIS ESTRUTURADOS ( PAG. 30)</b> .....	16
<b>TÉCNICAS PARA ANONIMIZAR IMAGENS ( PAG. 34/35)</b> .....	16
<b>APENDICE IV. ESTUDO DE CASOS</b> .....	18
<b>Risco de Reidentificação mensurado (RRM)</b> .....	18

## 2. Conceitos Básico

### 2.1. Glossário

#### [inclusão]

**Minuta atual:** Não existe previsão

#### **Sugestão:**

**Atributo:** Também chamado de campo de dados, coluna de dados, ou variável. Uma informação que pode ser encontrada nos registros do conjunto de dados. Nome, gênero e endereço são exemplos de atributos.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos ser relevante incluir o conceito de um atributo para fins de clarificação do conceito e para não deixar dúvidas quanto ao seu significado.

#### **Minuta atual:**

**Banco de dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

#### **Sugestão:**

**Banco de Dados:** É uma coleção organizada de dados que permite o armazenamento, a recuperação e a manipulação de dados. Geralmente é controlado por um sistema de gerenciamento de banco de dados (DBMS). Pode conter vários conjuntos de dados e tem capacidade para consultar, inserir, atualizar e manipular dados. Um banco de dados também pode ser composto por tabelas, que por sua vez consistem em linhas e colunas. Cada linha representa uma entrada de dados específica e cada coluna representa um atributo ou característica dessa entrada. Os bancos de dados são geralmente usados em aplicações onde os dados precisam ser persistentes e manipulados por várias transações.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos que o conceito precisa ser mais abrangente.

**Minuta Atual:** Não existe previsão

#### **Sugestão:**

**Classe de equivalência:** Os registros em um conjunto de dados que partilham os mesmos valores com certos atributos, tipicamente identificadores indiretos.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

**Justificativa:** Entendemos ser relevante incluir o conceito de classe de equivalência para fins de clarificação do conceito e para não deixar dúvidas quanto ao seu significado.

**Minuta Atual:** Vide Banco de Dados.

**Sugestão:**

**Conjunto de Dados:** É uma coleção não estruturada ou estruturada de informações que pode estar contida em um arquivo ou em múltiplos arquivos. Pode ser composto por uma variedade de tipos de dados, como texto, números, imagens, vídeos, etc. Um conjunto de dados é usado em análises de dados e geralmente é extraído de um ou mais bancos de dados ou fontes de dados externas. Um conjunto de dados pode ser armazenado por exemplo em formatos como CSV, Excel, JSON, XML, entre outros.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Na nossa percepção há diferenças entre banco de dados e conjunto de dados, em especial pelo fato de que um conjunto de dados pode não estar necessariamente em um banco de dados no seu conceito literal.

**Minuta Atual:** Não existe previsão no glossário.

**Sugestão:**

**Conjunto de dados anonimizado:** O conjunto de dados resultante após as técnicas de anonimização terem sido aplicadas em combinação com a avaliação de risco adequada.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

**Minuta Atual:** Não existe previsão

**Sugestão:**

**Conjunto de dados original:** O conjunto de dados antes de qualquer técnica de anonimização ser aplicada.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

**Minuta Atual:** Não existe previsão

**Sugestão:**

**Identificabilidade vs Re-identificabilidade:** O grau ao qual um indivíduo pode ser

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

identificado em um ou mais conjuntos de dados que contêm identificadores diretos e indiretos, vs o grau ao qual uma pessoa natural pode ser identificada a partir de conjuntos de dados anonimizados.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

**Minuta Atual:** Não existe previsão

**Sugestão:**

**Não identificador:** Conjunto de dados que podem conter atributos de dados que não são categorizados como identificadores diretos nem indiretos. Tais atributos não precisam de ser sujeitos a anonimização.

**Fonte:** [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation\\_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

**Justificativa:** Entendemos ser relevante incluir o conceito para fins de clarificação e para não deixar dúvidas quanto ao seu significado.

## 2.2. Anonimização e Pseudonimização de Dados na LGPD

[inclusão]

**Minuta atual:** Não existe previsão

**Sugestão: APÓS O ITEM 22, inclusão do seguinte texto:**

A anonimização tem como objetivo a eliminação ou redução significativa dos riscos de reidentificação dos dados anonimizados, mas sempre preservando a veracidade dos resultados do seu tratamento. O processo de anonimização, além de evitar a identificação do titular de dados pessoais, deve garantir que o tratamento realizado após a anonimização não implique em uma distorção dos dados reais.

Em suma, uma análise massiva de dados anonimizados não poderá produzir resultado diferente daquela obtida através de dados não anonimizados.

### JUSTIFICATIVA DO ACRÉSCIMO:

A sugestão do acréscimo se dá em razão da necessidade de registrar que o objetivo final do processo de anonimização é a diminuição de riscos de identificação em nível razoável de segurança, evitando-se assim, o estímulo a processos que não possuam técnicas de segurança suficientes para garantir a desvinculação dos dados pessoais às pessoas físicas e a não reversão do processo.

Assegurar que o resultado do tratamento após a anonimização dos dados reflita fielmente o resultado que seria atingido sem a aplicação da anonimização também é de extrema relevância, a medida em que, além de não identificar o titular de dados é preciso reproduzir a realidade da análise de dados que teria sido obtida através dos dados não anonimizados.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion>

### 3. OS PROCESSOS DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS

#### 3.1. ASPECTOS JURÍDICOS RELEVANTES

##### 3.1.2 RISCOS DE REIDENTIFICAÇÃO DE DADOS ANONIMIZADOS

[inclusão]

**Minuta atual:** Não existe previsão

**Sugestão:** APÓS O ITEM 46, inclusão:

É recomendável que se realize uma análise de risco do processo de anonimização por parte do responsável pelo tratamento de dados, através da elaboração de um RIPD.

#### **JUSTIFICATIVA DO ACRÉSCIMO:**

A sugestão do acréscimo se dá em razão da constatação de que nenhuma técnica de anonimização poderá garantir em termos absolutos a impossibilidade de reidentificação e que deverá ser mitigada através da gestão de riscos.

<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion>

#### 3.2. O PROCESSO DE ANONIMIZAÇÃO

##### Item 54.

**Minuta atual:**

Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados. Isso implica que as organizações podem utilizá-los para finalidades, desde que compatíveis, que vão além daquelas para as quais foram originalmente coletados e esses dados podem ser mantidos indefinidamente.

**Sugestão:**

Convém ressaltar que os dados que tenham sido tornados irreversivelmente anonimizados deixam de ser considerados "dados pessoais" e o processamento desses dados não exige conformidade com a legislação de proteção de dados, desde que, tenham partido de um tratamento lícito e que a finalidade – anonimização - tenha sido informada ao titular.

**Justificativa:** A redação atual transmite a impressão de que a alegação por parte de um responsável pelo tratamento de dados de possuir um processo anonimização o

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

liberaria da obrigatoriedade de se adequar a Lei Geral de Proteção de Dados. Apesar do item 29 deixar claro que o processo de anonimização, deve na origem partir de um objeto legítimo de tratamento pelo tratamento, a leitura do item 54 transmite uma impressão equivocada no sentido de que o processo de anonimização isentaria o agente de tratamento quanto a regularidade do tratamento que antecede o processo de anonimização. Por isso, recomendamos que a premissa citada no item 29 fique reforçada logo depois do 54.

Em suma, o Agente de Tratamento de dados necessita possuir um processo lícito de tratamento já que a anonimização se inicia após a coleta, ou seja, é fruto de um processamento de dados que precede de atividades lícitas de tratamento.

## Item 55

### Minuta atual:

O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o agente identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los.

### Sugestão

O processo de anonimização, orientado por uma abordagem baseada em riscos, tem como objetivo fornecer um conjunto mínimo de etapas que podem servir de guia de boas práticas aos agentes de tratamentos de dados. Essas etapas sugerem que o **Controlador dos Dados** identifique e compreenda os riscos envolvidos em sua atividade, bem como adote medidas para mitigá-los, **podendo utilizar a metodologia do item 76 ou outra que melhor se adequar ao seu contexto.**

### Justificativa do acréscimo

Considerando que o Controlador é responsável pela tomada de decisões referente ao tratamento de dados pessoais, se faz necessário enfatizar a sua responsabilidade no processo de anonimização, visando a minimizar o risco de identificação do titular.

## 3.2.2. Gestão do risco de reidentificação

### [inclusão]

**Minuta atual:** Não existe previsão

**Sugestão: APÓS O ITEM 75, inclusão:**

É recomendável que no desenvolvimento de um processo de anonimização seja definida a equipe de trabalho com base em perfis e funções necessárias para o bom desempenho do projeto, bem como o detalhamento do escopo de cada atuação. Alguns perfis que devem ser considerados:

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

- Responsável pelo tratamento de dados;
- Encarregado de Dados;
- Responsável pelo tratamento de informações anonimizadas;
- Equipe de avaliação de risco;
- Equipe de pré-anonimização e de anonimização;
- Equipe do processo de segurança da informação.

#### **JUSTIFICATIVA DA SUGESTÃO DO ACRÉSCIMO:**

A sugestão de acréscimo se dá em função da necessidade de criação de uma equipe para definição do processo de anonimização e agentes envolvidos, garantido a segregação de funções, a confidencialidade e a criação de um inventário para orientação no planejamento do processo de anonimização.

<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion>

[inclusão]

#### **APÓS O ITEM 75, inclusão:**

Na hipótese de o processo de anonimização compreender dados pessoais sensíveis, art. 5, II da Lei Geral de Proteção de Dados, é recomendável que se constitua uma equipe para avaliar a viabilidade e riscos do processo de anonimização e elaboração de um relatório de viabilidade que conterà de forma detalhada as razões e condições específicas para a anonimização de dados pessoais sensíveis. A equipe responsável pela segurança da informação validará ou não a Análise de Impacto à Proteção de Dados- AIPD, e caso optem por não o fazer, devem emitir um parecer fundamentado.

#### **JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:**

A sugestão de acréscimo se dá em função da análise do potencial de riscos gerados por uma possível reidentificação de dados sensíveis anonimizados e impactos negativos. A comprovação por parte do responsável de tratamento de dados, na adoção de boas práticas e medidas preventivas na fase pré-anonimização se enquadra nos princípios de prestação de contas, segurança e prevenção do art. 6º. da LGPD e art. 40 da mesma norma legal .

[inclusão]

#### **ACRÉSCIMO DE ITEM, com a seguinte redação:**

É de extrema relevância o treinamento da equipe envolvida com o processo de anonimização e com dados anonimizados, especialmente no que tange aos requisitos de segurança da informação estabelecidos no art. 46 da LGPD.

O treinamento deverá compreender:

- Princípios e aplicação da política de anonimização;
- Objetivos definidos na gestão de riscos;

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

- Estrutura e responsabilidade da equipe de trabalho envolvida no processo de anonimização;
- Objetivos e finalidade da informação anonimizada;
- Variáveis de anonimização: identificação e classificação;
- Técnicas de anonimato utilizadas;
- Termos de uso e acesso a informações anonimizadas;
- Medidas de controle para pessoal com acesso a informações anonimizadas;
- Obrigações e deveres em caso de quebra da cadeia de anonimização que acarrete reidentificação dos titulares de dados.

#### **JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:**

A justificativa da sugestão de acréscimo se dá em função da importância da adoção de boas práticas por parte do responsável de tratamento que optar pela anonimização dos dados com a finalidade de prevenção e mitigação de riscos. O treinamento da equipe humana envolvida com o processo é elementar para que se evitem e mitiguem riscos.

<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonizacion>

[inclusão]

#### **ACRÉSCIMO DE ITEM, com a seguinte redação:**

Tendo em vista que o processo de anonimização não garante de forma absoluta a possibilidade de reidentificação do titular de dados, algumas garantias para preservar os direitos dos interessados são recomendáveis de adoção, por parte do responsável pelo processo de anonimização. São elas:

- Acordos de confidencialidade envolvendo o responsável pelo tratamento, o responsável pelo processo de anonimização, o responsável pelo tratamento de dados anonimizados e pelas pessoas com acesso às informações anonimizadas.
- Termo de Compromisso do destinatário da informação em manter a informação anônima e a obrigação de informar o responsável pelo tratamento em caso de suspeita de reidentificação.
- Realização de auditorias pelo responsável de tratamento ao responsável pelo tratamento de dados anonimizados.

#### **JUSTIFICATIVA DA SUGESTÃO DE ACRÉSCIMO:**

A justificativa da sugestão do acréscimo se dá em função de que as garantias adotadas pelo responsável do tratamento, além de configurarem boas práticas com caráter preventivo, serão consideradas em eventual realização de DPIA, como salvaguardas destinadas a minimizar danos em caso de eventual reidentificação de dados pessoais.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

## Item 81. 9

### Minuta atual:

9. Registro e Documentação: mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

### SUGESTÃO

9. Registro e Documentação: mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

**A informação sobre o tipo de pseudonimização poderá ser informado no RIPD, sendo seu preenchimento de responsabilidade do controlador que realizou a pseudonimização .**

### Justificativa:

\*\*\* Não ficou claro papéis e responsabilidades.

Visto que foi indicado uma métrica para validar o nível de proteção à técnica utilizada (RRA, RRM, quem será o responsável por medir e eficácia da métrica e onde essa informação será utilizada. Ex.: Uma vez feito um RIPD da atividade, essa métrica deverá constar no relatório?

## Minuta atual: Item 83

83. Desenvolver uma metodologia eficaz de pseudonimização de dados pessoais, alinhada com as melhores práticas de mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais.

Figura 3: Metodologia Eficaz de Pseudonimização.

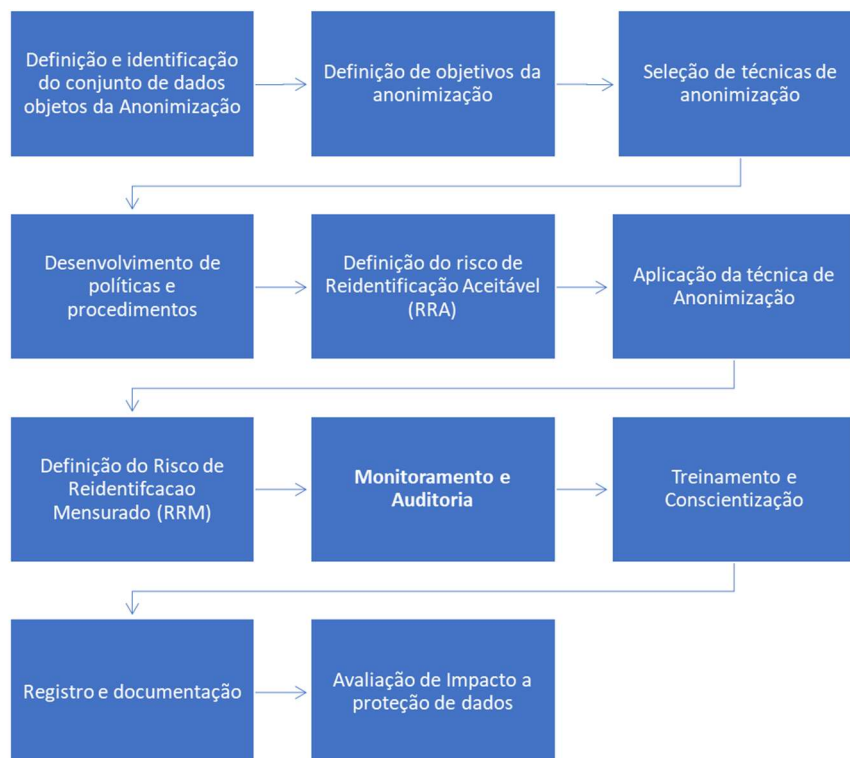


Fonte: Elaboração própria.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

### Sugestão:

Desenvolvimento de uma metodologia eficaz de anonimização de dados pessoais pelo controlador de dados, alinhada com as melhores práticas do mercado e em conformidade com os princípios da LGPD é fundamental para garantir a privacidade e a segurança das informações pessoais:



### Justificativa conjunta ao final (item 83 e 84)

#### Minuta atual: Item 84 – PÁGS. 23-25

**84.** Conforme ilustração acima (Figura 3), para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:

- 1. Avaliação Inicial e Identificação dos Dados Objeto da Pseudonimização:** inicie com uma avaliação abrangente de quais dados pessoais serão coletados e tratados. Identifique quais dados pessoais serão objeto da pseudonimização, considerando os riscos e o tratamento realizado, dando ênfase a dados considerados sensíveis, como por exemplo, dados de saúde, origem racial ou étnica, convicção religiosa, opinião política, entre outros.
- 2. Definição de Objetivos da Pseudonimização:** estabeleça claramente os objetivos da pseudonimização, incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

**3. Seleção de Técnicas de Pseudonimização:** escolha as técnicas de pseudonimização apropriadas com base na natureza dos dados. Isso pode incluir o mascaramento de informações pessoais, o uso de tokenização, o embaralhamento de dados ou a criptografia, dentre outros. A escolha dependerá das características específicas dos dados e dos riscos associados.

**4. Desenvolvimento de Políticas e Procedimentos:** crie políticas e procedimentos claros para garantir a pseudonimização adequada. Isso inclui diretrizes sobre como realizar a pseudonimização, armazenar chaves criptográficas de forma segura e garantir a rastreabilidade e o acesso somente a pessoal autorizado.

**5. Implementação da Pseudonimização:** implemente as técnicas de pseudonimização de acordo com as políticas e procedimentos estabelecidos. Certifique-se de que todos os dados pessoais sejam adequadamente pseudonimizados antes de serem armazenados ou processados. Em alguns casos, técnicas diferentes podem ser aplicadas, concomitantemente, para produzir uma pseudonimização eficiente.

**6. Proteção das Chaves e Algoritmos:** garanta que as chaves e algoritmos utilizados no processo de pseudonimização, como por exemplo, chaves criptográficas, senhas de acesso a sistemas ou a arquivos, códigos-fonte, dentre outros, sejam armazenadas de forma segura e acessíveis apenas a pessoal autorizado. Os registros de auditoria devem ser mantidos, documentando quando as chaves foram usadas, quem as utilizou e com que finalidade. Isso é valioso para conformidade regulatória, registro de operações e investigações de segurança. É fundamental garantir que os dados possam ser revertidos quando necessário de forma segura, pelo controlador.

Como uma boa prática para o gerenciamento de chaves, técnicas como a implementação de logs de eventos e sistemas de monitoramento podem ser empregados para facilitar a rastreabilidade no uso das chaves, e ainda, as chaves podem ser armazenadas de forma segura usando práticas como a criptografia de chaves mestras e Módulos de Segurança em Hardware (HSMs).

**7. Monitoramento e Auditoria:** implemente sistemas de monitoramento e auditoria para verificar continuamente a eficácia da pseudonimização e garantir o cumprimento das políticas e procedimentos. Realize revisões e auditorias regulares a fim de acompanhar as mudanças regulatórias, tecnológicas e melhores práticas de mercado relacionadas à pseudonimização e ajuste sua metodologia conforme necessário.

**8. Treinamento e Conscientização:** forneça treinamento regular aos colaboradores que lidam com dados pessoais para garantir que compreendam a importância da pseudonimização e saibam como aplicá-la corretamente.

**9. Registro e Documentação:** mantenha registros detalhados de todas as atividades de pseudonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

**10. Relatório de Impacto à Proteção de Dados:** realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à pseudonimização e garantir a conformidade com a LGPD.

**11. Comunicação com os Titulares:** esteja preparado para informar de forma transparente e acessível aos titulares sobre a pseudonimização e os direitos de acesso e correção de suas informações pessoais, conforme exigido pela LGPD.

**12. Plano de resposta a Incidentes de Segurança:** desenvolva um plano de resposta a incidentes de segurança com dados pessoais que inclua procedimentos para lidar, entre outras situações, com acessos não autorizados e tratamentos inadequados ou ilícitos, incluindo as ações de mitigação apropriadas para reverter ou mitigar os efeitos dos prejuízos gerados.

### Sugestão:

**84.** Conforme ilustração acima, para o desenvolvimento dessa metodologia algumas etapas devem ser observadas:

**1. Definição e identificação do banco de dados objetos da Anonimização:** Inicie com a definição e identificação do conjunto de dados que serão objeto de anonimização, considerando os riscos, tratamento realizado e finalidade.

**2. Definição de Objetivos da Anonimização :** estabeleça claramente os objetivos da Anonimização , incluindo a proteção da privacidade do titular dos dados, a redução do risco de violações de dados e o cumprimento da LGPD.

**3. Seleção de técnicas de anonimização:** escolha as técnicas de anonimização apropriadas com base na natureza dos dados. A escolha dependerá das características específicas dos dados e dos riscos associados.

**4. Desenvolvimento de Políticas e Procedimentos:** crie políticas e procedimentos claros para garantir a anonimização adequada.

**5. Definição do risco de Reidentificação Aceitável (RRA):** definir o risco de reidentificação aceitável (RRA), para um certo conjunto de dados, considerando o contexto do agente de tratamento.

**6. Aplicação da técnica de anonimização:** implemente as técnicas de anonimização de acordo com as políticas e procedimentos estabelecidos. Certifique-se de que todos os dados pessoais sejam adequadamente anonimizados antes de serem armazenados ou processados.

**7. Definição do Risco de Reidentificação Mensurado (RRM):** definir o risco de reidentificação aceitável (RRA), para um certo conjunto de dados, considerando o contexto do agente de tratamento.

**8. Monitoramento e Auditoria:** implemente sistemas de monitoramento e auditoria para verificar continuamente a eficácia da anonimização e garantir o cumprimento das políticas e procedimentos. Realize revisões e auditorias regulares a fim de acompanhar as mudanças regulatórias, tecnológicas e melhores práticas de mercado relacionadas à anonimização e ajuste sua metodologia conforme necessário.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

**9. Treinamento e Conscientização:** forneça treinamento regular aos colaboradores que lidam com dados pessoais para garantir que compreendam a importância da anonimização e saibam como aplicá-la corretamente.

**10. Registro e documentação:** mantenha registros detalhados de todas as atividades de anonimização, incluindo datas, técnicas utilizadas, responsáveis e propósitos. Isso é importante para fins de prestação de contas, rastreabilidade e registro de operações.

**11. Avaliação de Impacto a proteção de dados :** realize a avaliação de impacto sobre a proteção de dados, elaborando o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando apropriado, a fim de avaliar os riscos associados à anonimização e garantir a conformidade com a LGPD. Considere a elaboração do RIPD sempre que o tratamento envolve alto risco.

### Justificativa da inclusão

A sugestão do acréscimo se dá em virtude da identificação da necessidade de uma metodologia para as etapas do desenvolvimento das atividades no processo de anonimização, contribuindo para a conformidade com a legislação, mitigação de gaps e prestação de contas para demonstração de aplicação da eficácia das medidas adotadas.

A redação atual não deixa claro papéis e responsabilidades, visto que indica uma métrica para validar o nível de proteção à técnica utilizada (RRA, RRM, quem será o responsável por medir a eficácia da métrica e onde essa informação será utilizada. Ex. Uma vez feito, um RIPD da atividade, essa métrica deverá constar no relatório? Abordaremos o tema com mais profundidade em item específico (item 9).

### 3.3. O PROCESSO DE PSEUDONIMIZAÇÃO

## 6. APÊNDICES

### APENDICE I. PRINCIPAIS ESCLARECIMENTOS

#### Minuta atual:

i) A anonimização, geralmente, não reduz a probabilidade de reidentificação de um conjunto de dados a zero - a anonimização não impossibilita a reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de riscos de reidentificação.

#### SUGESTÃO

i) A anonimização, **geralmente, reduz** a probabilidade de reidentificação de um conjunto de dados de forma significativa - a anonimização **se aplicada com meios apropriados** impossibilita a reidentificação de um conjunto de dados; o processo de anonimização e a forma como é implementado terão influência direta na probabilidade de riscos de reidentificação.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

## **Justificativa**

Segundo LGPD no seu art. 5º Para os fins desta Lei, considera-se:

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Porém aqui, leva o leitor a concluir de forma equivocada que não existe anonimização real, uma vez que diz que a anonimização não impossibilita a reidentificação de um conjunto de dados.

Especialmente considerando-se a própria definição de anonimização da 29100: “processo pelo qual dados pessoais são irreversivelmente alterados, de forma que um titular de dados pessoais não mais pode ser identificado, direta ou indiretamente, seja por um controlador apenas ou em colaboração com qualquer outra parte”.

\*\*\* Falta esclarecer melhor esta definição.

Ref.: ABNT NBR ISO/IEC 29100:2020

### 4.4.4 Dados pseudonimizados

Os processos de anonimização.... mas destroem a capacidade de vinculação.

## **APENDICE II. CADERNO DE TÉCNICAS PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO**

### **TÉCNICAS PARA ANONIMIZAR DADOS TEXTUAIS ESTRUTURADOS ( PAG. 30)**

**Minuta atual:** (Pág. 30)

Para as colunas Idade e Quantidade filhos o valor do ruído foi trucando

#### **SUGESTÃO**

Para as colunas Idade e Quantidade filhos o valor do ruído foi trucando => Confirmar o sentido da palavra “trucando” ou corrigir se for erro de digitação.

### **TÉCNICAS PARA ANONIMIZAR IMAGENS ( PAG. 34/35)**

#### **SUGESTÃO DE EXCLUSÃO DO EXEMPLO DE TÉCNICA DE ANONIMIZAÇÃO IMAGENS:**

As Técnicas de Desfoque Gaustiano ( blur) e pixelização descritas no Guia da ANPD, como ilustrações de técnicas válidas de anonimização, não podem ser admitidas, uma vez que vão de encontro com o disposto na norma legal, especialmente em seu art. 12º.

#### **JUSTIFICATIVA DA SUGESTÃO DE EXCLUSÃO:**

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

A sugestão de exclusão de recomendação das técnicas de anonimização de imagens trazidas no estudo preliminar da ANPD se dá em função de que contraria o disposto na LGPD, especificamente na conceituação do dado anonimizado e do grau de razoabilidade de um processo de anonimização, dispostos nos artigos 5º, III e art. 12º, Caput e Parágrafo Primeiro, senão vejamos:

“Art. 5, III- Dado anonimizado: dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.”

“Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

&1º. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios....”

Observe-se que as imagens disponibilizadas no estudo preliminar da ANPD, como dados anonimizados, não podem assim ser entendidas, uma vez que do simples olhar da figura já é possível identificar o indivíduo, especialmente se aqueles que a veem já o conhecem. E não se diga, nem por mera hipótese, que o processo de reidentificação do dado anonimizado, não possa se dar através de um terceiro que já tenha tido algum contato visual prévio com o titular de dados que sofreu a técnica de anonimização, objeto de contestação. Pois, a própria norma legal define o dado anonimizado como sendo aquele que não identifica o seu titular.

Apenas, por mero exercício, no improvável contexto de acatarmos as figuras da página 35 do Guia como sendo dados anonimizados, precisaríamos enfrentar o disposto no art. 12, Caput e Parágrafo Primeiro.

A lei condiciona o processo de anonimização a dois critérios: i) quando forem utilizados esforços razoáveis para a anonimização; ii) e que esses esforços razoáveis para a reversão do processo levem em conta tempo, custo e tecnologias disponíveis.

Pois bem, partindo da premissa de que o processo de anonimização requer técnicas seguras e que contenham um grau considerável de confiabilidade de não reversão da anonimização, demonstramos a singeleza do processo que levou a reidentificação da imagem em questão.

O aplicativo “face.api.js playground” disponibilizado na internet e de forma gratuita, permite que ao se inserir a imagem das fls. 35 se reverta a imagem a sua forma original, identificando o titular de dados.

Portanto, impõe-se por medida de segurança e evitando a indução de técnicas e processos de anonimização que não sejam seguros, seja suprimido os exemplos de imagens anonimizadas apresentados equivocadamente no Guia.

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)



## APENDICE IV. ESTUDO DE CASOS

**Caso 03: Compartilhamento de dados educacionais – Supressão, generalização, mascaramento, adição de ruídos e permutação.**

### Esclarecimentos:

Quando, em quais situações, devemos aplicar a métrica RRA/RRM?

### Risco de Reidentificação mensurado (RRM)

Item 7. (Acompanhamento do RRM/RRA) - pág. 48

- 1) Como acompanhar?
- 2) Se o compartilhamento envio dos dados for feito uma única vez?
- 3) Se o compartilhamento for periódico, deve-se toda vez recalculer o RRM? É isso? Não ficou claro.

### Minuta atual:

**Classificação:** INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)

07. De acordo com o processo proposto, é necessário acompanhar o risco mensurado de reidentificação para que ele sempre se mantenha abaixo do risco de reidentificação aceitável.

### **SUGESTÃO**

07. De acordo com o processo proposto, é necessário acompanhar o risco mensurado de reidentificação para que ele sempre se mantenha abaixo do risco de reidentificação aceitável. **Neste caso é responsabilidade do órgão que coleta os dados realizar periodicamente o cálculo do RRM para verificar sua efetividade.**

### **Justificativa:**

Não está claro como deve ser executado.

\*\*\*

