



CENTRO UNIVERSITÁRIO DE BRASÍLIA – UniCEUB
FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS/TI
CURSO DE CIÊNCIAS DA COMPUTAÇÃO

Elaborado por:
Gabrielle Gutierrez RA-22350026
Pedro Klein RA-22105154
Henrique Portal Lessa RA-22402204
Gabriel Marques RA-22451254
Matheus de Moraes RA-22352763
Thales Rassi RA-22400186

Brasília

2025

RELATÓRIO DE IMPACTO
À PROTEÇÃO DE DADOS PESSOAIS

Brasília
2025

Histórico de Revisões

Data	Versão	Descrição	Autor
03/12/2025	1.0	Conclusão da primeira versão do relatório	Matheus Jose de Morais Silva

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

GRUPO DE PESQUISA ACADÊMICA

Thales Rassi Porto de Matos - 22400186

Gabriel Marques da Rocha - 22451254

Gabrielle Gutierrez - 22350026

Pedro Klein - 22105154

Henrique Portal Lessa - 22402204

Matheus José de Moraes - 22352763

Orientadora:

Kadidja Valeria Reginaldo de Oliveira

Encarregado

Kadidja Valeria Reginaldo de Oliveira

E-mail Encarregado

kadidja.oliveira@ceub.edu.br

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Como regra geral, é recomendado elaborar o RIPD em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme Art. 5º, inciso XVII, e Art. 55-J, inciso XIII, da Lei nº 13.709/2018 (LGPD).

A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela Autoridade Nacional de Proteção de Dados (ANPD), como:

- nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);
- quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, §

- 3º);
- para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e
- para Controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam **dados pessoais sensíveis** (art. 38).

Portanto, haverá situações em que o **Controlador (Grupo de Pesquisa e Orientador)** elaborará o RIPD para atender à determinação da ANPD ou, em atenção ao princípio da **Responsabilização e Prestação de Contas** (art. 6º, X), ao verificar que o tratamento a ser realizado pode implicar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

Justificativa Específica do Projeto Acadêmico

A elaboração deste Relatório de Impacto se fundamenta, especificamente, na natureza dos dados e na finalidade do projeto, sendo essencial para o **Projeto Integrador I** da graduação em Ciência da Computação (FATECS/CEUB).

O tratamento de dados realizado pelo Grupo de Pesquisa visa o **Desenvolvimento de Dashboard**, utilizando dados abertos e descentralizados do **DATASUS**. Este tratamento exige a elaboração do RIPD pelos seguintes motivos:

1. **Dados Pessoais Sensíveis:** A fonte de dados (DATASUS) contém informações referentes à saúde, as quais são classificadas como **dados pessoais sensíveis** (Art. 5º, II da LGPD), mesmo que os dados sejam públicos e anonimizados/agregados na origem (sendo descritos como "dados descentralizados sem valor interpretativo"). O tratamento de dados sensíveis, mesmo para fins de estudo, impõe um dever de cautela e documentação.
2. **Conformidade na Finalidade:** O tratamento está amparado na base legal de "**Realização de estudos por órgão de pesquisa**" (Art. 7º, IV da LGPD), o que exige a garantia da anonimização e do compromisso com as medidas de segurança, as quais devem ser formalmente documentadas neste relatório.
3. **Princípios de Segurança e Prevenção:** O documento é a principal ferramenta para demonstrar a aplicação dos princípios de **Segurança e Prevenção** (Art. 6º, VII e VIII), atestando que o Grupo de Pesquisa adotou medidas de proteção técnica e administrativa (como a gestão de acesso e o descarte seguro) para mitigar o risco residual de reidentificação ou uso indevido no ambiente acadêmico.

3 – DESCRIÇÃO DO TRATAMENTO

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

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

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

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

3.1 – NATUREZA DO TRATAMENTO

Tópico	Descrição Específica do Projeto
Coleta	Os dados são coletados diretamente da base pública do DATASUS (Sistema de Informações de Saúde - TABNET) , conforme referência bibliográfica. O processo de coleta é realizado por meio de <i>download</i> dos arquivos brutos disponíveis no formato DBF/DBC e posterior conversão para formatos tabulares (ex: CSV, Excel).
Armazenamento	Os dados brutos e os arquivos de trabalho são armazenados em dispositivos de propriedade dos membros do Grupo de Pesquisa e em serviço de nuvem institucional (ou pessoal) . São adotadas medidas de segurança básicas, como a utilização de senhas nos dispositivos e a utilização de autenticação de dois fatores (2FA) no acesso à nuvem.
Processamento/Tratamento	O tratamento dos dados consiste em: 1) Limpeza e Filtro: remoção de dados inconsistentes ou desnecessários. 2) Agregação e Anonimização: criação de novas variáveis e agrupamento de registros para garantir que nenhum indivíduo possa ser singularizado. 3) Análise: geração de estatísticas e visualizações para o <i>Dashboard</i> conforme o objetivo da pesquisa.
Compartilhamento	Não há compartilhamento dos dados brutos com terceiros ou entidades externas à instituição. O compartilhamento está restrito aos membros do Grupo de Pesquisa e ao Professor Orientador, para fins exclusivos de supervisão e desenvolvimento do trabalho acadêmico.
Destino/Término do Tratamento	Após a conclusão e defesa do Projeto Integrador (prevista para o final do semestre/curso), os dados brutos e as bases de dados processadas serão excluídos de forma segura de todos os dispositivos e contas de <i>backup</i> do Grupo de Pesquisa,

	mantendo-se apenas o produto final (Dashboard/Relatório) com as informações agregadas e estatísticas.
--	--

3.2 – ESCOPO DO TRATAMENTO

Tipos de Dados Pessoais Tratados:

- Natureza: Dados de Saúde/Clínicos (referente ao CID de doenças, procedimentos, etc.).
- Características: Dados Públicos, Desidentificados e Agregados na fonte (DATASUS).
- Exemplos de Campos Tratados: Idade (faixas), Sexo, Município de Residência (ou Região de Saúde), Data de Ocorrência (Agregada por ano/mês), e dados de procedimentos/diagnósticos (CID).
- Observação: Não foram tratados dados diretamente identificáveis (Nome, CPF, Endereço completo). Os dados utilizados são classificados como "dados descentralizados sem valor interpretativo" no seu formato de origem.

Volume de Dados: (Descreva a escala) Ex: "Dados referentes a X milhões/milhares de registros de internações/nascidos vivos", ou "Volume total de dados processados é considerado Moderado no contexto acadêmico".

Extensão/Frequência do Tratamento: O tratamento é realizado de forma pontual e intermitente ao longo da disciplina Projeto Integrador I (semestre letivo).

3.3 – CONTEXTO DO TRATAMENTO

O tratamento é realizado em um contexto de **pesquisa e estudo acadêmico**, sob a supervisão de um Professor Orientador, no âmbito de uma instituição de ensino superior (CEUB/FATECS). O ambiente de tratamento é o do laboratório ou dispositivos pessoais dos alunos, sendo regido pelas normas e políticas internas de conduta ética da instituição e pelos requisitos da LGPD para fins de estudo.

3.4 – FINALIDADE DO TRATAMENTO

Finalidade Primária:

"Desenvolvimento de um **Dashboard de Acompanhamento** para gerar valor acadêmico, social e prático, permitindo a análise e visualização de dados epidemiológicos (ex: evolução do indicador X na região Y) com base nas informações públicas do DATASUS."

Base Legal (LGPD):

Art. 7º, IV: "Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis." (Se a sua faculdade for classificada como "órgão de pesquisa"). **Art. 7º, § 5º:** Se o dado for manifestamente público.

Reforce que: A base legal primária é a **realização de estudos e pesquisa**, e que a anonimização ou desidentificação original dos dados é o principal mecanismo de proteção.

4 – PARTES INTERESSADAS CONSULTADAS

Campo	Descrição Específica do Projeto
Pessoa/Unidade Consultada	Professor Orientador/Supervisor do Projeto (Prof. Kadidja Valeria Reginaldo de Oliveira)
Motivo da Consulta	Supervisão da metodologia de pesquisa, validação das fontes de dados (DATASUS) e definição das medidas de segurança e controle de acesso aos arquivos brutos.
Parecer Emitido/Informações Relevantes	O Professor Orientador validou o uso dos dados públicos do DATASUS para fins de pesquisa, desde que garantidas a desidentificação e a adoção de medidas de segurança (criptografia, controle de acesso) para a base de dados em posse do grupo, conforme detalhado na Seção 7.
Outras Partes	Não se aplica.
Observação	A elaboração deste RIPD foi conduzida pelo Controlador (Grupo de Pesquisa) sob orientação da Professora Responsável pela disciplina. Não foram consultados o Encarregado de Dados ou o Comitê de Segurança da Informação Institucional devido à natureza e ao escopo limitado do projeto.

5 – NECESSIDADE E PROPORCIONALIDADE

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

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do GRUPO DE PESQUISA ACADÊMICA (LGPD, art. 10), demonstrar que:
 - esse tratamento de dados pessoais é indispensável;
 - não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
 - esse processamento de fato auxilia no propósito almejado.
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
- Como estão implementadas as medidas que asseguram o direito de o titular de dados pessoais obter do GRUPO DE PESQUISA ACADÊMICA o previsto pelo art. 18 da LGPD.

- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Quais são as salvaguardas para as transferências internacionais de dados.>

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do GRUPO DE PESQUISA ACADÊMICA ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

5.1-Necessidade do Tratamento

Tópico	Descrição Específica do Projeto
O tratamento é legalmente exigido ou estritamente necessário para uma finalidade legítima?	Sim. O tratamento é estritamente necessário para a finalidade acadêmica e científica de Desenvolvimento de Dashboard de Acompanhamento, com o objetivo de gerar valor prático e social. A finalidade do tratamento se baseia na hipótese legal de "Realização de estudos por órgão de pesquisa" (Art. 7º, IV da LGPD).
Os dados coletados são essenciais para atingir a finalidade?	Sim. Os dados específicos de saúde pública e epidemiologia, referentes aos indicadores de interesse do projeto, são essenciais para o desenvolvimento do dashboard e para o cumprimento dos objetivos do Projeto Integrador I.
Há alternativa ao tratamento que cause menos impacto à privacidade?	Não. O uso dos dados do DATASUS é a alternativa que causa o menor impacto à privacidade, pois esses dados já são públicos, desidentificados e agregados na fonte. Coletar dados diretamente dos titulares ou usar fontes privadas teria um impacto de privacidade muito maior.

5.2-Proporcionalidade do Tratamento

Tópico	Descrição Específica do Projeto
As expectativas dos titulares foram consideradas?	Sim. O Grupo de Pesquisa realizou uma curadoria dos dados, selecionando apenas as variáveis e campos estritamente necessários para calcular e apresentar os indicadores no dashboard (ex: ano, sexo, município, CID). Campos excessivos foram descartados ou não foram baixados, em alinhamento com o princípio da Minimização de Dados (Art. 6º, III).

As expectativas dos titulares foram consideradas?	Sim. A expectativa do titular (a população cujos dados de saúde geraram as estatísticas) é que seus dados de saúde sejam utilizados de forma segura e ética, especialmente para pesquisa em saúde pública. O uso de bases desidentificadas e a garantia da exclusão segura do arquivo bruto respeitam essa expectativa.
O tratamento está em conformidade com o princípio da Não Discriminação?	Sim. A pesquisa é de caráter estatístico/epidemiológico e não visa a individualização, exclusão, discriminação ou desvantagem indevida de qualquer titular.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

6.1. Matriz de Avaliação de Riscos

Id	Risco referente ao tratamento de dados pessoais	P ¹	I ²	Nível de Risco (P x I) ³
R01	Acesso não autorizado: Acesso aos arquivos de dados brutos por terceiros (fora do Grupo/Orientador) devido a falha de segurança no dispositivo ou nuvem.	10 (Improvável)	15 (Catastrófico)	150 (Alto)
R03	Perda dos Dados: Perda dos arquivos devido a falha de hardware, erro humano ou corrupção de <i>backup</i> (o que compromete a integridade da pesquisa).	5 (Raro)	10 (Grave)	50 (Moderado)
R12	Vinculação/Associação Indevida (Reidentificação): Risco de os dados, mesmo que desidentificados, serem cruzados com outras informações e permitirem a identificação de um indivíduo.	5 (Raro)	15 (Catastrófico)	75 (Moderado)
R15	Não Exclusão no Prazo: Falha em garantir a exclusão segura dos dados brutos após a defesa/conclusão do projeto, levando à retenção desnecessária.	10 (Improvável)	10 (Grave)	100 (Alto)

Níveis de Risco

Probabilidade (P)	Impacto (I)	Nível de Risco (P x I)
-------------------	-------------	------------------------

10 - Improvável	15 - Catastrófico (Dano sério à reputação, multas, violação de direitos fundamentais)	< 75: Baixo
5 - Raro	10 - Grave (Dano significativo, impacto legal)	75 a 125: Moderado
1 - Quase Impossível	5 - Significativo (Dano relevante, impacto nos projetos)	> 125: Alto

6.2. Análise dos Riscos

R01 - Acesso não autorizado (Risco Alto): A probabilidade é baixa devido ao controle de acesso do Grupo de Pesquisa, mas o impacto é máximo porque envolve dados sensíveis de saúde. O vazamento de um arquivo de dados do DATASUS, mesmo que desidentificado, pode gerar desconfiância na instituição e violar os princípios da LGPD.

R12 - Vinculação/Associação Indevida (Risco Moderado): Embora os dados sejam desidentificados na origem, sempre há um risco teórico de que, em posse de terceiros, eles possam ser combinados com outras bases (risco de *linkage attack*). A probabilidade é baixa, mas o impacto seria catastrófico.

R15 - Não Exclusão no Prazo (Risco Alto/Moderado): O risco não é o vazamento em si, mas a violação do princípio da LGPD de limitação do tempo de retenção. A retenção desnecessária dos dados brutos após a finalidade (defesa do trabalho) é uma falha de conformidade que deve ser evitada por meio de processos claros de descarte.

7 – MEDIDAS PARA TRATAR OS RISCOS

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

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

7.1. Medidas, Salvaguardas e Mecanismos de Mitigação de Risco

Risco Referente ao Tratamento	Medida (Controle) Adotada	Efeito sobre o Risco	Risco Residual (Após o Controle)
R01 (Acesso não autorizado)	C1: Controle de Acesso e Senhas Fortes: Todos os	Reduzir a probabilidade de acesso não	Moderado (10 x 10 = 100)

	dispositivos utilizados para armazenar os dados brutos possuem senha de acesso forte ao sistema operacional (PC/Notebook). Além disso, os arquivos de dados brutos são armazenados em serviço de nuvem com Autenticação de Dois Fatores (2FA) ativada, para controle de acesso remoto.	autorizado por software ou remotamente.	
R01 (Acesso não autorizado)	C2: Segregação de Arquivos: Manter o arquivo de dados brutos separado dos demais documentos do projeto e protegido por senhas adicionais (se o software permitir), dificultando o acesso acidental ou incidental.	Reduzir a probabilidade de acesso acidental.	Moderado (10 x 10 = 100)
R12 (Reidentificação)	C3: Anonimização e Agregação: Não manipulação ou criação de variáveis que possam, em conjunto, singularizar um titular. A pesquisa se limita a variáveis já agregadas (faixas etárias, municípios) conforme o princípio da Minimização .	Evitar que o risco se concretize.	Baixo (1 x 15 = 15)
R03 (Perda dos Dados)	C4: Rotina de Backup: Manter cópias de segurança dos arquivos de dados e da análise em, pelo menos, dois locais distintos (Ex: dispositivo local e	Reduzir o impacto da perda ou erro.	Baixo (5 x 5 = 25)

	nuvem protegida por 2FA), prevenindo a perda accidental.		
R15 (Não Exclusão no Prazo)	C5: Termo de Descarte: Elaboração de um Termo de Compromisso de Descarte de Dados Brutos, assinado pelos integrantes do Grupo e pelo Orientador, com previsão de exclusão segura imediatamente após a conclusão do projeto.	Reduzir a probabilidade de retenção prolongada.	Baixo (5 x 10 = 50)

8 – APROVAÇÃO

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

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

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<p>_____</p> <p>Matheus José de Moraes</p> <p>Matrícula: 22352763</p> <p>Data :</p>	<p>_____</p> <p>Kadidja Valeria Reginaldo de Oliveira</p> <p>Data:</p>

Integrantes do Grupo de Pesquisa	Assinatura
----------------------------------	------------

Thales Rassi Porto de Matos	
Gabriel Marques da Rocha	
Gabrielle Gutierres	
Pedro Klein	
Henrique Portal Lessa	
Matheus José de Moraes	