PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
DIRETORIA DE GESTÃO DE DOCUMENTOS, DA MEMÓRIA E DO CONHECIMENTO
COORDENADORIA DE GESTÃO DO CONHECIMENTO

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

STM SUPERIOR TRIBUNAL MILITAR

Brasília
2026

Relatório de Impacto à Proteção de Dados Pessoais

SUPERIOR TRIBUNAL MILITAR (2026)
Dra. Maria Elizabeth Guimarães Teixeira Rocha (*Ministra-Presidente*)
Ten Brig Ar Francisco Joseli Parente Camelo (*Ministro Vice-Presidente e Corregedor da JMU*)

Ministros
Ministro Dr. ARTUR VIDIGAL de Oliveira
Ministro Dr. José BARROSO Filho
Ministro Dr. PÉRICLES Aurélio Lima de Queiroz
Ministro Ten Brig Ar Carlos Vuyk de AQUINO
Ministro Alte Esq Leonardo PUNTEL
Ministro Alte Esq Celso Luiz NAZARETH
Ministro Ten Brig Ar Carlos Augusto AMARAL Oliveira
Ministro Alte Esq Cláudio Portugal de VIVEIROS
Ministro Gen Ex Lourival CARVALHO Silva
Ministro Gen Ex GUIDO Amin Naves
Ministra Dra. Verônica Abdalla Sterman
Ministro Gen Ex Anisio David de Oliveira Junior
Ministro Gen Ex Flavio Marcus Lancia Barbosa

Secretaria-Geral da Presidência
Marília Ramos Xavier (*Secretária-Geral da Presidência*)

Secretaria do STM
José Carlos Nader Motta (*Diretor-Geral*)

Diretoria de Gestão de Documentos, da Memória e do Conhecimento (DIDOC)
Maria Juvani Lima Borges (*Diretora*)

Coordenadoria de Gestão Documental (COGED)
Rafael Luiz Melo de Almeida (*Coordenador*)

Coordenadoria de Gestão do Conhecimento (COGES)
Luciana Lopes Humig (*Coordenadora*)

Coordenadoria de Gestão de Memória (COGEM)
Airton Guimaraes Xavier (*Coordenador*)

PODER JUDICIÁRIO

SUPERIOR TRIBUNAL MILITAR

DIRETORIA DE GESTÃO DE DOCUMENTOS, DA MEMÓRIA E DO CONHECIMENTO

COORDENADORIA DE GESTÃO DO CONHECIMENTO

Relatório de Impacto à Proteção de Dados Pessoais

STM SUPERIOR TRIBUNAL MILITAR

Brasília

2026

Pesquisa, levantamento dos dados e texto
Luciana Lopes Humig
Jonniery dos Santos Moreira

Chefia de editoração e revisão
Mosair Gomes Lima de Freitas

Projeto gráfico e Diagramação
Marcus Vinícius da Silva Teixeira

Revisão textual
Beatriz de Carvalho Santos

Ficha catalográfica
Jonniery dos Santos Moreira – CRB1 - 2689

Ficha catalográfica

BRASIL. Superior Tribunal Militar. Diretoria de Gestão de Documentos, da Memória e do Conhecimento. Relatório de Impacto à Proteção de Dados Pessoais. – Brasília, DF : Superior Tribunal Militar, Diretoria de Gestão de Documentos, da Memória e do Conhecimento, 2026.
21 p.

1. Proteção de dados pessoais. 2. Gestão de riscos. I. Título.

CDU 342.721

Impresso no Brasil / *Printed in Brazil*
Elaboração, distribuição e informações
Superior Tribunal Militar (STM)
Diretoria de Gestão de Documentos, da Memória e do Conhecimento (DIDOC)
Setor de Autarquias Sul – Praça dos Tribunais Superiores
Edifício-Sede – 10º Andar
CEP: 70098-900 Brasília-DF
Telefones: (61) 3313-9183/3313-9353/3313-9311
E-mail: didoc@stm.jus.br

SUMÁRIO

1. Contextualização

O presente Relatório de Impacto à Proteção de Dados Pessoais (RIPD) tem por finalidade apresentar a análise dos riscos inerentes ao tratamento[1] de dados pessoais relativos ao **Inventário de Tratamento de Dados**, elaborado pelo Superior Tribunal Militar (STM), em conformidade com o disposto na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

O RIPD é um instrumento previsto no art. 38 da LGPD e recomendado pela Agência Nacional de Proteção de Dados Pessoais (ANPD) como ferramenta para identificar, avaliar e mitigar riscos associados às operações de tratamento de dados pessoais.

O relatório integra o conjunto de ações de governança e conformidade em proteção de dados implementadas no âmbito da Justiça Militar da União, conforme previsto na Resolução STM nº 340/2023 e no Ato Normativo nº 691/2023.

A elaboração deste documento reforça o compromisso institucional desta Corte com a transparência, a responsabilidade e a segurança no tratamento de dados pessoais, observando os princípios da finalidade, adequação, necessidade, prevenção e não discriminação.

[1] Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X da LGPD).

2. Identificação dos Agentes de Tratamento e do Encarregado

Controlador
União / Superior Tribunal Militar (STM)
Endereço: Setor de Autarquias Sul – Praça dos Tribunais Superiores – Brasília/DF

Encarregado (DPO)
Ministro-Ouvidor Gen Ex Lourival Carvalho Silva
E-mail: ouvidoria@stm.jus.br

O Superior Tribunal Militar (STM), como órgão do Poder Judiciário da União, é responsável por zelar pela aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em todas as suas atividades administrativas e judiciais.

O Tribunal atua na qualidade de controlador[2] de dados pessoais, conforme definição do art. 5º, inciso VI da LGPD, cabendo-lhe determinar as finalidades e os meios de tratamento dos dados pessoais sob sua responsabilidade.

O Ministro-Ouvidor da Justiça Militar da União exerce a função de Encarregado pelo Tratamento de Dados Pessoais, nos termos do art. 41 da LGPD e do Ato Normativo n° 4.917/2025, sendo o ponto de contato entre o Tribunal, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

[2] Controlador, segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

3. Análise de princípios da Lei Geral de Proteção de Dados Pessoais (LGPD)

As atividades de tratamento de dados pessoais observam os princípios indicados no art. 6º da Lei nº 13.709/2018 (LGPD). A aplicação desses princípios assegura que o uso das informações sob responsabilidade do Tribunal ocorra de maneira transparente e compatível com o interesse público.

A *finalidade* orienta todas as ações de tratamento, garantindo que os dados pessoais sejam coletados e utilizados apenas para propósitos legítimos, específicos e relacionados diretamente com as funções administrativa e jurisdicional. Já a *adequação* garante ao titular dos dados que o tratamento seja feito observando-se a finalidade previamente informada.

O *princípio da necessidade* garante que os dados pessoais sejam tratados somente até o limite necessário para a realização das finalidades, atendendo sempre ao interesse público em todas as etapas de tratamento.

Já os *princípios do livre acesso e da transparência* se concretizam por meio da disponibilização de informações relacionadas ao tratamento de dados pessoais, no âmbito do Superior Tribunal Militar, na página da LGPD via portal da internet, onde podem ser encontrados o Inventário de Tratamento de Dados Pessoais e o Inventário de Compartilhamento de Dados Pessoais com Terceiros, além das informações sobre o exercício dos direitos do titular e sobre o Encarregado pelo Tratamento dos Dados (DPO).

Quanto à segurança, por meio da atuação das Coordenadorias de Gestão do Conhecimento e de Segurança Cibernética, são adotadas medidas para prevenir acessos indevidos, vazamentos e demais incidentes, bem como permitir controles de acesso e auditorias.

4. Descrição das Operações de Tratamento

O Tribunal realiza diversas operações de tratamento de dados pessoais, tanto em sua função administrativa quanto jurisdicional.

A coleta dos dados é feita pelas diversas unidades administrativas e judiciais, bem como por meio de solicitações encaminhadas por cidadãos aos serviços oferecidos, tais quais a emissão de certidões e os pedidos de informação.

Abaixo, estão descritas as principais categorias de operações de tratamento mapeadas no **Inventário de Proteção de Dados Pessoais**, que servem como referência para a análise de riscos apresentada neste relatório, a qual se encontra disponível na página da LGPD do portal, por meio do link: https://www.stm.jus.br/lgpd/pag-inicial-lgpd/tratamento-de-dados-nostm.

4.1 Atividades Administrativas

- **Gestão de Pessoas**: registro funcional, folha de pagamento, gestão de benefícios e deveres, saúde ocupacional.
- **Capacitação e Desenvolvimento**: registro de participação em cursos e eventos.
- **Gestão Contratual**: cadastro e controle de fornecedores, dados de empresas contratadas, de prestadores de serviço e de fiscalização de contratos.
- **Segurança Institucional**: controle de acesso físico e lógico, identificação biométrica, videomonitoramento, cibersegurança, auditoria e *logs* de sistema.
- **Ouvidoria**: coleta e armazenamento dos dados pessoais dos solicitantes.
- **Gestão Orçamentária**: rol de responsáveis, atualização de informações no SIAFI, COMPRASNET, PNCP, cadastro de operadores no SIPOC e divulgação de dados voltados à transparência das contas públicas.
- **Tecnologia da Informação**: criação/alteração/exclusão de permissões para os usuários, cadastramento de informações pessoais e/ou sensíveis em sistemas internos e externos, bem como em formulários eletrônicos e desenvolvimento de soluções tecnológicas para coleta de dados pessoais, inclusive sensíveis.
- **Gestão Documental**: digitalização, armazenamento e eliminação de documentos e coleta de dados em pedidos de pesquisa.

4.2 Atividades Judiciais

- **Tramitação Processual**: registro e acompanhamento de processos judiciais.
- **Cadastro de juízes militares, conselhos, partes e advogados**: coleta de dados de identificação, endereço, CPF, OAB e informações de contato.

5. Finalidades e Bases Legais

As finalidades de tratamento de dados pessoais estão diretamente relacionadas ao cumprimento de suas atribuições legais e institucionais. O tratamento é sempre orientado por finalidade legítima e compatível com o interesse público, conforme quadro abaixo:

Finalidade	Base Legal (LGPD)	Atividade
Cumprimento de obrigação legal	Art. 7º, II	Envio de informações funcionais ao TCU e ao CNJ
Execução de políticas públicas	Art. 7º, III	Ações de equidade de gênero e de raça
Execução de contratos	Art. 7º, V	Gestão de contratos com empresas terceirizadas
Proteção da vida e da incolumidade física	Art. 7º, VII	Atendimento médico a servidor em serviço
Legítimo interesse da administração pública	Art. 7º, IX	Controle de acesso físico e segurança da informação
Tratamento de dados sensíveis	Art. 11, II	Dados de saúde

6. Tipos de Dados e Titulares

Os dados tratados abrangem: a) os **pessoais comuns**: nome, CPF, endereço, contatos, *e-mail*; b) os **sensíveis**: dados de saúde, biometria, raça/cor, gênero, filiação sindical; c) os **funcionais e financeiros**: informações de cargo, matrícula, lotação, remuneração, escolares e histórico funcional; e d) os **judiciais**: dados de partes, advogados, testemunhas e peritos.

Os titulares incluem magistrados, servidores (ativos e inativos), estagiários, militares a serviço do STM ou que sejam partes em processos judiciais, terceirizados e cidadãos que solicitem serviços nos canais disponíveis no site do Superior Tribunal Militar.

Além dos titulares acima informados, também é realizado o tratamento de dados pessoais de crianças e adolescentes, especialmente no contexto de cadastro de dependentes de servidores e magistrados, para fins de concessão de benefícios legais, assistência médica e previdenciária. Esse tratamento observa o disposto no art. 14 da Lei nº 13.709/2018 (LGPD), sendo realizado com base no melhor interesse da criança e do adolescente.

7. Compartilhamento e Transferência Internacional

O compartilhamento de dados pessoais é realizado de forma restrita, observando os princípios da finalidade, necessidade, adequação e segurança, conforme previsto na Lei nº 13.709/2018 (LGPD) e na Resolução STM nº 340/2023.

As hipóteses de compartilhamento decorrem de obrigações legais ou regulamentares, bem como da execução de contratos administrativos e da necessidade de envio de informações aos sistemas de controle e transparência públicas.

O inventário de compartilhamento de dados com terceiros pode ser consultado no portal institucional, por meio do endereço: https://www.stm.jus.br/lgpd/pag-inicialIgpd/compartilhamento-de-dados-pessoais.

Entre os principais destinatários do compartilhamento de dados estão órgãos como o Tribunal de Contas da União (TCU), o Conselho Nacional de Justiça (CNJ) e as instituições bancárias conveniadas para gestão de folha de pagamento, além das empresas contratadas, na condição de operadoras de dados, para execução de serviços ligados à área de saúde e bem-estar, de manutenção de sistemas de informação, de armazenamento em nuvem, de gestão de frota de veículos, etc.

Nesses casos, os contratos administrativos contêm cláusulas específicas de proteção de dados pessoais, que determinam as responsabilidades das partes, o dever de confidencialidade, a eliminação de dados após o término do vínculo contratual e a obrigatoriedade de comunicação de eventuais incidentes de segurança.

8. Avaliação de Riscos e Tratamento

A gestão de riscos aplicada ao tratamento de dados pessoais no Superior Tribunal Militar segue as diretrizes da Resolução STM nº 343/2023, que institui a Política de Gestão de Riscos da Justiça Militar da União e observa os limites de exposição definidos pelo Ato Normativo nº 819/2025, o qual estabelece o apetite a riscos da JMU.

Em conformidade com tais normativos, a avaliação de riscos foi conduzida de forma estruturada, considerando as etapas de estabelecimento do contexto, como identificação, análise, avaliação, tratamento e monitoramento contínuo, alinhadas às orientações da ANPD e às melhores práticas previstas pela ISO 31000:2018.

8.1 Tratamento de Riscos e Monitoramento

I. Proteger os direitos fundamentais dos titulares de dados pessoais;
II. Garantir o tratamento adequado, seguro e transparente;
III. Prevenir incidentes de segurança e reduzir riscos associados ao tratamento;
IV. Assegurar conformidade com a LGPD, diretrizes da ANPD, Resolução CNJ nº 363/2021 e normativos internos.

8.2 Estabelecimento do Contexto

O tratamento de dados pessoais no STM ocorre em ambiente complexo, envolvendo sistemas informatizados, múltiplos agentes de tratamento, atividades judiciais e administrativas, compartilhamentos com outros órgãos públicos e operadores contratados, além da necessidade de realizar atividades de transparência ativa em conformidade com a Lei de Acesso à Informação.

Para compreender adequadamente esse cenário, foram analisados:

Contexto Interno

- Alto volume de dados pessoais e sensíveis tratados rotineiramente;
- Entrada e saída frequente de militares, estagiários e colaboradores, o que impacta a gestão de acessos;
- Necessidade de publicação de atos administrativos e judiciais com atenção aos requisitos de proteção de dados; e
- Presença de processos de contratação envolvendo operadores.

Contexto Externo

- Crescente sofisticação de ataques cibernéticos;
- Exigências normativas do CNJ e da ANPD;
- Necessidade de envio de informações a outros órgãos (CNJ, TCU);
- Exposição reputacional em casos de incidentes de segurança; e
- Exigências de transparência pública somadas às obrigações de proteção da privacidade.

Esse levantamento permitiu delimitar o escopo da avaliação de riscos: compreender como os eventos relacionados ao tratamento de dados pessoais podem afetar a privacidade, integridade, disponibilidade e confidencialidade das informações, bem como o cumprimento das finalidades institucionais do STM.

8.3 Identificação e Análise dos Riscos

A identificação dos riscos considerou as informações consolidadas no Mapa de Riscos (SEI n° 4657053), resultado de reuniões técnicas entre a Coordenadoria de Gestão do Conhecimento (COGES) e a Coordenadoria de Governança e Gestão Socioambiental (CGOVE), além da análise dos Inventários de Tratamento de Dados Pessoais e de Compartilhamento de Dados Pessoais do STM, ambos disponíveis no portal da LGPD no site do Superior Tribunal Militar.

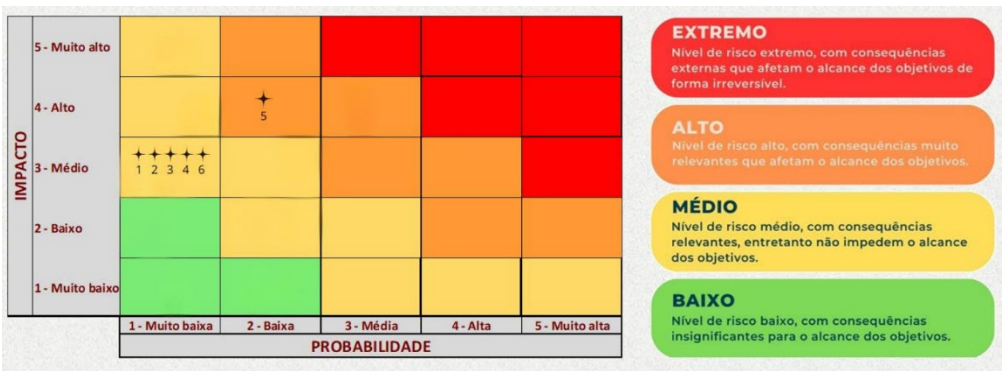
Cada risco foi avaliado segundo sua probabilidade de ocorrência e impacto sobre os direitos dos titulares, bem como às atividades institucionais do STM.

O Mapa de Riscos é composto pelas etapas do processo de avaliação dos riscos preconizado pela norma ISO 31000:2018 e consolida o registro dos riscos para as atividades de tratamento de dados pessoais no âmbito do Superior Tribunal Militar, seus componentes, causas, eventos e consequências, bem como os controles preventivos e reativos existentes para mitigá-los, quando for o caso.

Após a etapa de análise, 6 (seis) riscos foram identificados, sendo 5 (cinco) riscos classificados com nível médio e 1 (um) risco com nível alto, conforme descriminado abaixo.

N°	Evento de Risco
1	Acesso por pessoa não autorizada a dados pessoais em sistemas internos
2	Acessos aos sistemas de informação mantidos após o desligamento de colaboradores
3	Dados pessoais compartilhados com operador não autorizado, em excesso, fora das finalidades informadas aos titulares ou por tempo superior ao previsto
4	Vazamento de dados sensíveis nos sistemas da JMU
5	Publicação de dados pessoais nos portais da internet e intranet em desconformidade com a legislação sobre o tema
6	Operador não cumpre cláusulas contratuais de proteção de dados pessoais

Os riscos analisados foram representados na Matriz de Classificação de Riscos, ferramenta utilizada na gestão de riscos para auxiliar no processo decisório, uma vez que possibilita visualizar todos os riscos e priorizar ações de acordo com a importância de cada evento.



8.4 Tratamento de Riscos e Monitoramento

As medidas definidas para controle e redução dos riscos identificados foram consolidadas no Plano de Ações – Tratamento de Riscos (SEI n° 4657036), elaborado de acordo com as diretrizes da Política de Gestão de Riscos da Justiça Militar da União (Resolução STM nº 343/2023), do Apetite a Riscos da JMU (Ato Normativo nº 819/2025) e das normas e recomendações relacionadas com a proteção de dados pessoais.

O Plano traduz, em ações concretas, as iniciativas necessárias para reduzir a probabilidade e o impacto dos eventos avaliados acima do nível aceitável, definindo atividades, responsáveis, prazos, status e forma de acompanhamento para cada um dos riscos avaliados como passíveis de tratamento. São eles:

- ✓ **Evento de risco 2** - Acessos aos sistemas de informação mantidos após o desligamento de colaboradores;
- ✓ **Evento de risco 5** - Publicação de dados pessoais nos portais da internet e intranet em desconformidade com a Lei Geral de Proteção de Dados Pessoais e normas correlatas; e
- ✓ **Evento de risco 6** - Operador não cumpre cláusulas contratuais de proteção de dados pessoais.

Dessa forma, é possível pensar o tratamento individualizado de cada risco, garantindo clareza na distribuição de responsabilidades e facilitando o monitoramento das ações de mitigação.

8.5 Controles Aplicáveis

Os controles são ações e procedimentos implementados pela gestão para diminuir os riscos e assegurar o alcance dos objetivos organizacionais.

Durante a análise dos riscos relacionados ao tratamento de dados pessoais, foram identificados os controles já existentes no Tribunal, bem como definidos novos mecanismos necessários para mitigar os riscos classificados como prioritários, conforme detalhado no Plano de Ações – Tratamento de Riscos (SEI n° 4657036).

Controles Existentes	
Riscos analisados	6 (seis) riscos
Controles existentes	35 (trinta e cinco) controles existentes

Controles Propostos	
Riscos priorizados	6 (seis) riscos
Riscos priorizados	4 (quatro) controles existentes

Os riscos mapeados e os controles propostos permanecerão sob monitoramento contínuo, com revisões periódicas ou sempre que ocorrer alteração significativa nas operações de tratamento. Essas ações visam garantir que a gestão de riscos em proteção de dados pessoais mantenha-se coerente com os normativos internos de gestão de riscos, e às diretrizes da Lei nº 13.709/2018 (LGPD), assegurando conformidade, transparência e governança no tratamento de dados pessoais.

9. Considerações Finais

Há comprometimento contínuo com os princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no ano de 2025, quando foram implementadas ações estruturantes voltadas à conscientização e capacitação de servidores e colaboradores, bem como à consolidação de procedimentos relacionados ao tratamento e à proteção dos dados pessoais sob responsabilidade institucional.

Entre as medidas adotadas, destacam-se os mapeamentos realizados pela Seção de Atendimento ao SEI e Proteção de Dados Pessoais (SEIPD), pela Coordenadoria de Gestão do Conhecimento (COGES) e pelo Comitê Executivo de Privacidade, Segurança Cibernética e Dados Abertos (CESDA), que resultaram na elaboração do Inventário de Tratamento, do Inventário de Compartilhamento de Dados Pessoais e deste Relatório de Impacto à Proteção de Dados Pessoais.

Também integram esse esforço a elaboração de normativos específicos sobre privacidade e segurança da informação e a adoção de melhores práticas identificadas por meio de *benchmarking* com outras instituições públicas, visando ao aperfeiçoamento contínuo da governança em proteção de dados. Esses instrumentos são fundamentais para o fortalecimento da governança, da transparência e da segurança da informação no âmbito institucional.

Merece destaque, ainda, a reformulação da página dedicada à proteção de dados no portal institucional, que passou a reunir conteúdos atualizados e organizados por tópicos, em conformidade com os princípios da transparência e do livre acesso, previstos no art. 6º da LGPD, além das ações contínuas de capacitação e sensibilização de servidores e colaboradores sobre boas práticas em proteção de dados pessoais.

O presente Relatório de Impacto à Proteção de Dados Pessoais representa não apenas um registro técnico, mas um instrumento de gestão e aprimoramento contínuo da cultura de privacidade, cuja revisão deverá ocorrer periodicamente e sempre que houver alterações relevantes nas operações de tratamento, na base legal aplicável ou na adoção de novas tecnologias.

10. Normativos Relacionados

Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

Resolução CNJ nº 363/2021 – Política de Governança de Privacidade e Proteção de Dados Pessoais no Poder Judiciário;

Resolução STM nº 340/2023 – Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento no âmbito da JMU;

Resolução STM nº 343/2023 – Política de Gestão de Riscos da Justiça Militar da União;

Ato Normativo STM nº 691/2023 – Plano Operacional de Gestão e Privacidade de Dados Pessoais;

Ato Normativo nº 819/2025 – Estabelece o apetite a riscos na JMU;

Ato STM nº 4917/2025 – Designa o Encarregado pelo Tratamento de Dados Pessoais, no âmbito do Superior Tribunal Militar;

Guia Orientativo da ANPD - Atuação do encarregado de dados pessoais (2022);

Guia Orientativo da ANPD – Tratamento de Dados Pessoais pelo Poder Público (2023);

Relatório de Impacto à Proteção de Dados Pessoais do Banco Central do Brasil (2023).