Guia para Elaboração do Registro das Operações de Tratamento

MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Programa de Privacidade e Segurança da Informação
PPSI 2.0

Versão 1.0

Brasília, 01 de julho de 2026

GUIA PARA ELABORAÇÃO DO REGISTRO DAS OPERAÇÕES DE TRATAMENTO

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL
Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE
Marta Juvina de Medeiros
Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO
Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO
Ricardo Borges Almeida

EQUIPE DE REVISÃO
Anderson Souza de Araújo
Marta Juvina de Medeiros

Histórico de versões

Data	Versão	Descrição	Autor
01/07/2026	1.0	Construção do Guia para Elaboração do Registro das Operações de Tratamento (PPSI 2.0)	Equipe Técnica de Elaboração

Sumário

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

Medidas do *framework* do PPSI 2.0 apoiadas por esse documento

Controle	Id	Medida	Segmento
19	19.1	O órgão elabora e mantém processo para registrar as operações de tratamento de dados pessoais?	Privacidade
19	19.2	O órgão inclui no registro das operações de tratamento a descrição do fluxo dos dados pessoais?	Privacidade
19	19.3	O órgão inclui no registro das operações de tratamento de dados pessoais os agentes, os compartilhamentos, as transferências internacionais e as abrangências geográficas do tratamento?	Privacidade
19	19.4	O órgão inclui no registro das operações de tratamento de dados pessoais os tipos de dados tratados e as categorias de titulares?	Privacidade

1 Termos e definições

Algumas definições relevantes ao entendimento do conteúdo exposto neste Guia são apresentadas a seguir. Demais termos utilizados neste Guia podem ser encontrados na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 [1], na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) [2], ou no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021 [3].

Aviso de privacidade: documento voltado aos titulares que objetiva informar como os dados pessoais são tratados e para quais finalidades, quais os direitos dos titulares e como podem exercê-los, além de outras características que garantam ao titular a transparência em relação ao tratamento de seus dados pessoais, facilmente acessível e escrito em linguagem clara e simples.

Política de Proteção de Dados Pessoais (PPDP): instrumento normativo que estabelece diretrizes institucionais para o tratamento de dados pessoais no âmbito do órgão ou entidade, com o objetivo de assegurar os direitos fundamentais de liberdade, de intimidade e de privacidade dos titulares de dados pessoais.

2 Introdução

O Registro das Operações de Tratamento de Dados Pessoais (ROPA, do inglês *Records of Processing Activities*) é o documento institucional que descreve, de forma estruturada, todas as operações de tratamento de dados pessoais realizadas por um órgão ou entidade. Trata-se de obrigação legal expressa no art. 37 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) [1], aplicável tanto ao controlador quanto ao operador, e constitui um dos mecanismos centrais para a demonstração do cumprimento das normas de proteção de dados pessoais, nos termos do inciso X do art. 6º (princípio da responsabilização e prestação de contas).

Mais do que um requisito formal de conformidade, o ROPA é o instrumento que permite ao órgão conhecer o próprio universo dos tratamentos de dados pessoais que realiza, e serve de subsídio para identificar riscos, fundamentar decisões e responder tempestivamente aos titulares, à Agência Nacional de Proteção de Dados (ANPD) e aos órgãos de controle. A inexistência de um registro estruturado tem se mostrado um obstáculo concreto para a plena execução de outras atividades do **Programa de Governança em Privacidade (PGP)**, como a elaboração de **avisos de privacidade**, a realização de **Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)** e a atuação tempestiva diante de incidentes.

Este Guia integra o conjunto de documentos orientativos do **Programa de Privacidade e Segurança da Informação (PPSI 2.0)** e foi elaborado para fornecer subsídios práticos à elaboração e à manutenção do ROPA por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), em consonância com a LGPD, com as resoluções da ANPD e com o controle 19 do *framework* do PPSI 2.0.

O objetivo principal deste Guia é responder, de forma fundamentada, a duas perguntas centrais: (i) quais informações devem constar do registro das operações de tratamento de dados pessoais; e (ii) como organizar o processo institucional de elaboração e atualização do registro ao longo do tempo. O Guia adota, deliberadamente, uma abordagem independente de tecnologia. As orientações apresentadas podem ser implementadas em planilhas, formulários, interfaces *web* ou ferramentas *low-code*/*no-code*. O capítulo 6 discute as implicações de cada uma dessas escolhas, mas o conteúdo informacional do registro, descrito nos capítulos 3 e 4, é independente do meio em que é mantido.

3 Fundamentos do registro das operações de tratamento

Este capítulo apresenta as bases que justificam a obrigatoriedade e a centralidade do ROPA no PGP e está organizado em três seções: a primeira trata da natureza da obrigação no ordenamento jurídico brasileiro; a segunda descreve os propósitos e funções que o ROPA cumpre, combinando o mandato legal com a contribuição prática reconhecida pela literatura especializada; a terceira, por sua vez, articula o ROPA com os demais instrumentos do PPSI 2.0.

3.1 Natureza da obrigação

A obrigação de manutenção do registro das operações de tratamento de dados pessoais decorre, no ordenamento brasileiro, do art. 37 da LGPD [1], que estabelece que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. A redação do dispositivo é deliberadamente ampla: a obrigação não está condicionada a uma hipótese legal específica, a um porte mínimo de organização ou a um volume mínimo de dados pessoais tratados. A menção ao legítimo interesse cumpre função de reforço, não de delimitação da obrigação.

No caso dos órgãos e entidades do poder público, a obrigação conjuga-se com o regime específico previsto no Capítulo IV da LGPD (art. 23 a art. 32), que reforça a necessidade de transparência sobre as hipóteses, finalidades e procedimentos de tratamento. O art. 23, inciso I, ao exigir que sejam informadas as hipóteses em que, no exercício de competências, são realizados tratamentos de dados pessoais, pressupõe a existência de um registro interno minimamente organizado, função que o ROPA, em sua forma sistematizada, cumpre. As orientações da ANPD para o setor público complementam a interpretação desse regime [4].

A Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, que aprova o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte [5], reconhece o ROPA como obrigação de todos os agentes, embora preveja forma simplificada para agentes de pequeno porte; para os órgãos da administração pública federal, que não se enquadram nessa categoria, aplica-se o regime geral. A Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela ANPD [6], inclui, entre os critérios de avaliação da boa-fé do agente, a existência de mecanismos de governança que demonstrem o esforço de cumprimento da Lei, entre os quais o ROPA ocupa posição central.

3.2 Propósitos e funções do ROPA

O conjunto de funções aqui apresentado articula o mandato legal estabelecido pela LGPD com a contribuição prática reconhecida pela literatura especializada, em particular, Blum, Vainzof e Moraes (2020) [7]. As funções não são alternativas entre si, o ROPA cumpre todas elas simultaneamente.

3.2.1 Demonstração do cumprimento do princípio da responsabilização e prestação de contas

O ROPA é o documento que materializa, de forma sistemática, o princípio da responsabilização e prestação de contas previsto no inciso X do art. 6º da LGPD. Sem registro estruturado, o órgão não dispõe de meio idôneo para demonstrar que conhece os tratamentos de dados pessoais que realiza e que age de modo informado a seu respeito, pressuposto de qualquer prestação de contas [7]. Esta função é, conceitualmente, a primeira e dela derivam todas as demais.

3.2.2 Subsídio à fiscalização pela ANPD

O ROPA é instrumento direto de fiscalização pela ANPD. O art. 37 da LGPD estabelece a obrigação de manutenção do registro, e a competência da ANPD para fiscalizar seu cumprimento e requisitar informações de agentes de tratamento decorre do art. 55-J da mesma Lei. Na prática regulatória, o ROPA tende a ser um dos primeiros documentos requisitados em apurações, e sua qualidade afeta de modo significativo a forma como a fiscalização desenvolve-se [7]. Sua ausência ou inconsistência, por si só, pode constituir indício de inadequação do programa de privacidade, com possíveis reflexos no regime de dosimetria de sanções [6].

3.2.3 Suporte ao cumprimento do princípio da transparência e à elaboração de avisos de privacidade

O ROPA constitui base informacional direta para a elaboração de avisos de privacidade e demais instrumentos de transparência, em atenção ao art. 6º, inciso VI, e ao art. 9º da LGPD. Os elementos que devem constar dos avisos, como finalidade específica, hipótese legal, identificação dos controladores e operadores, compartilhamentos e transferências realizadas são, em grande medida, projeções externas das informações registradas internamente no ROPA [7]. Sem registro estruturado, a elaboração de avisos tende a ser fragmentada, inconsistente entre tratamentos e suscetível a omissões.

3.2.4 Atendimento ao direito à confirmação de tratamento e ao direito de acesso

Os incisos I e II do art. 18 da LGPD asseguram ao titular o direito à confirmação da existência de tratamento e o direito de acesso aos dados pessoais tratados. O atendimento tempestivo desses direitos, nos prazos estabelecidos pelo art. 19 da LGPD (acesso imediato em formato simplificado e até quinze dias para a declaração completa), depende também de o órgão dispor de visão organizada dos tratamentos que realiza, dos tipos de dados pessoais envolvidos e dos sistemas em que tais dados residem. O ROPA é, em geral, o primeiro instrumento consultado para responder a tais requisições [7].

3.2.5 Atribuição da hipótese legal das operações de tratamento (base legal)

A rigorosa atribuição da hipótese legal a cada operação de tratamento – exigência decorrente dos art. 7º, art. 11 e art. 23 da LGPD – é tarefa que demanda análise individualizada; tal análise deve garantir a adequabilidade da hipótese à finalidade da operação e a consistência da

fundamentação normativa específica. O ROPA é o espaço em que o resultado da análise, qual seja, a hipótese legal identificada, é documentado, tornando a base legal verificável e revisável ao longo do tempo e minimizando a probabilidade de enquadramentos equivocados.

3.2.6 Subsídio à adoção de medidas adequadas de proteção

A obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais (art. 46 da LGPD) é proporcional à natureza, ao escopo e ao risco do tratamento. O ROPA, quando adequadamente elaborado, pode fornecer os elementos para essa avaliação de proporcionalidade: tipos de dados pessoais envolvidos, categorias de titulares, volume de dados pessoais tratados, criticidade do tratamento, quantidade de agentes de tratamento envolvidos, fluxos de compartilhamento e transferência [7]. A escolha de controles sem observância do ROPA é, em regra, uma escolha cega, incapaz de demonstrar adequação ao risco efetivo.

3.2.7 Identificação dos tipos de dados envolvidos em cada operação

O ROPA é o instrumento que permite ao órgão registrar, com precisão, quais categorias e tipos de dados pessoais são tratados em cada operação, com especial atenção à presença de dados pessoais sensíveis (LGPD, art. 5º, II) e de dados de crianças e adolescentes (LGPD, art. 14) ou vulneráveis. Esse conhecimento é pressuposto da aplicação do regime diferenciado previsto pela LGPD para tais categorias e condição para que o órgão possa responder, com fidedignidade, a perguntas como "este sistema trata dados pessoais sensíveis?" – pergunta cuja resposta intuitiva, sem o respaldo do registrado no ROPA, é possivelmente equivocada.

3.2.8 Suporte à elaboração do PGP orientado a risco

A maturação de um PGP não pode ser linear ou homogênea: priorizar tratamentos de maior risco é, ao mesmo tempo, exigência de proporcionalidade e de eficiência. O ROPA é a base sobre a qual se identifica esse risco: ao registrar informações sobre os dados pessoais tratados, vulnerabilidade dos titulares, volume tratado, escopo dos compartilhamentos e transferências, ele permite construir um plano de conformidade orientado a risco, em substituição a planos genéricos ou baseados apenas em impressões.

3.2.9 Governança interna dos tratamentos

Além das funções diretamente vinculadas à LGPD, o ROPA cumpre função de governança interna. Ao estruturar o conhecimento sobre os tratamentos realizados, ele permite identificar redundâncias entre processos, dependências entre sistemas, áreas com maior exposição e oportunidades de racionalização. Em órgãos de grande porte, o próprio exercício de elaboração do ROPA frequentemente revela tratamentos não documentados, processos sobrepostos e fluxos de dados desconhecidos pelo órgão.

3.3 Articulação com o PPSI 2.0

No âmbito do Programa de Privacidade e Segurança da Informação (PPSI 2.0) [1], o ROPA é o instrumento direto de cumprimento do controle 19 (Registro das operações de tratamento de dados pessoais), primeiro controle do segmento de privacidade do *framework* [8].

O controle 19 prescreve que as operações de tratamento de dados pessoais do órgão sejam identificadas e registradas, em atendimento ao art. 37 da LGPD [1]. As orientações do guia do *framework* traduzem, em termos práticos e independentes de tecnologia, o conteúdo informacional necessário ao cumprimento desse controle.

Em um segundo momento, o ROPA articula-se com as demais medidas do segmento de privacidade do PPSI 2.0, funcionando como insumo direto para a sua implementação. Mantém relações funcionais relevantes com: (i) o RIPD, que aprofunda a análise dos tratamentos de maior risco identificados no ROPA; (ii) os avisos de privacidade e ações vinculadas aos direitos dos titulares, que projetam externamente parte das informações registradas; (iii) a gestão de incidentes envolvendo dados pessoais, em particular a comunicação à ANPD e aos titulares prevista no art. 48 da LGPD; e (iv) a gestão de operadores, contratos e instrumentos de compartilhamento e transferência internacional. A consistência entre o ROPA e os instrumentos citados é elemento de maturidade do PGP.

4 Conteúdo do registro das operações de tratamento

Este capítulo descreve, em nível de detalhe operacional, as informações que devem compor o registro das operações de tratamento de dados pessoais. Está organizado em uma introdução, que apresenta o critério metodológico de seleção das informações, e em seções temáticas que descrevem, bloco a bloco, os campos do registro.

Para cada campo, são indicados: a denominação sugerida, o fundamento normativo de sua inclusão, as orientações práticas de preenchimento e, quando aplicável, a correlação com os campos correspondentes do Formulário de Comunicação de Incidente de Segurança com Dados Pessoais (FCI) da ANPD [9]. Essa correlação cumpre duas funções: (i) evidencia que o ROPA é insumo direto para o atendimento ao art. 48 da LGPD, fornecendo, com antecedência, informações que de outro modo precisariam ser produzidas sob a pressão de um incidente; e (ii) orienta o desenho do ROPA de modo que seu conteúdo seja diretamente reaproveitável no formulário regulatório, reduzindo retrabalho e o risco de inconsistências.

A LGPD não enumera, de forma exaustiva, as informações que devem compor o registro das operações de tratamento. A leitura sistemática da Lei, complementada pelas resoluções da ANPD e por referências da literatura nacional e internacional [10], [11], [12], permite estabelecer um conjunto mínimo de informações necessárias para que o registro cumpra suas funções. As seções a seguir apresentam esse conjunto mínimo organizado em blocos temáticos. A organização em blocos não é prescritiva: o órgão pode adotar outra estrutura, desde que todas as informações descritas estejam contempladas. Os blocos refletem agrupamentos lógicos que facilitam o preenchimento por gestores das unidades.

Quando pertinente, são apresentadas observações sobre fontes complementares, em particular a literatura especializada e instrumentos correlatos como o art. 30 do Regulamento Geral sobre a Proteção de Dados da União Europeia – que, embora não vinculante no Brasil, oferece referência consolidada sobre o tema [13].

4.1 Identificação da operação de tratamento

Este bloco de informações reúne dados que permitem identificar inequivocamente a operação de tratamento e localizá-la na estrutura organizacional. Suas funções são dar individualidade ao registro de cada operação e estabelecer o vínculo entre o tratamento, o produto ou serviço objeto do ROPA e a unidade administrativa responsável. As informações deste bloco são, em regra, as primeiras a serem solicitadas no preenchimento, por seu caráter mais objetivo. Possui correlação com o art. 30(1), alíneas (a) e (b), do GDPR [10].

Correlação com o Formulário de Comunicação de Incidente da ANPD

- Identificação do processo afetado: a denominação do processo (4.1.2) e a unidade responsável (4.1.3) são utilizadas para localizar internamente o incidente, designar interlocutores e mobilizar a investigação técnica.

4.1.1 Identificador único do registro

Cada operação registrada deve receber um identificador único e estável, atribuído pelo órgão. A LGPD não exige expressamente um identificador, mas ele é decorrência prática da função de prestação de contas (LGPD, art. 6º, X) e da necessidade de manter a rastreabilidade ao longo das atualizações do registro. O identificador deve ser preservado entre versões e não deve ser reutilizado. Considerando o uso de tecnologias para apoiar a manutenção do ROPA, este campo possivelmente será gerado automaticamente, não havendo necessidade de instruções ao preenchedor.

4.1.2 Nome do produto ou serviço

Trata-se da denominação institucional do produto ou serviço no qual a operação de tratamento de dados pessoais está inserida. Sua inclusão é necessária para que o registro seja inteligível para terceiros (em particular a ANPD e órgãos de controle) e para que a operação possa ser vinculada à competência institucional que a fundamenta – exigência implícita na LGPD, art. 23, inciso I.

> **Orientação prática para o preenchedor**
> **Nome do produto ou serviço**: informe o nome do produto ou do serviço que realiza tratamento de dados pessoais. Exemplos: "Concessão de aposentadoria por idade"; "Análise de pedidos de bolsa de estudo"; "Cancelamento e renovação de registros sanitários". Evite siglas internas que não sejam reconhecidas fora da unidade.

4.1.3 Unidade administrativa responsável

Deve ser indicada a unidade administrativa do órgão responsável pelo produto ou serviço. Este campo cumpre função dupla: (i) operacionalizar o princípio da responsabilização (LGPD, art. 6º, X), distribuindo-a entre as unidades, e não a concentrando indevidamente no encarregado; e (ii) viabilizar o processo de manutenção do registro, ao identificar quem deve responder por atualizações.

> **Orientação prática para o preenchedor**
> **Unidade responsável:** indique a unidade que efetivamente executa o tratamento (não necessariamente a unidade que demanda o serviço). Se houver corresponsabilidade entre unidades, registre todas, com as respectivas atribuições, e indique a unidade principal.

4.1.4 Responsável pelo preenchimento

Identificação nominal de quem efetuou o preenchimento do registro, com indicação da unidade administrativa de lotação e da data do preenchimento; em caso de revisão posterior, registra-se também o responsável pela revisão e a respectiva data. A identificação tem duas funções complementares: (i) atribuir individualmente a autoria do registro e (ii) preservar o canal de interlocução em caso de dúvidas posteriores.

A informação não substitui a indicação da unidade responsável pelo processo de trabalho, a qual representa a área administrativa que executa o processo; o responsável pelo preenchimento é o servidor que documentou a operação no instrumento.

Orientação prática para o preenchedor
Responsável pelo preenchimento: informe nome completo, matrícula ou identificação funcional, unidade de lotação, cargo e data do preenchimento.
Responsável pela revisão: ao revisar o registro, mantenha o responsável original e acrescente o responsável pela revisão com a respectiva data.
Observação: em registros mantidos em ferramenta com autenticação, esta informação tende a ser capturada automaticamente. Confirmar se o sistema preserva o histórico ou apenas o último responsável. O histórico de responsabilidades é parte da trilha de auditoria do registro.

4.1.5 Situação do registro

Indicação do estado em que se encontra o registro no fluxo institucional de governança do ROPA. Recomenda-se que a tipologia de situações adotada pelo órgão contemple, no mínimo, as seguintes categorias:

- em andamento: preenchimento em curso pela unidade administrativa, ainda não finalizado para integrar o ROPA oficial. Registros em andamento devem estar visualmente distinguidos no instrumento;
- em revisão (quando aplicável): preenchimento concluído e submetido a etapa formal de revisão - seja por responsável superior, seja por instância de governança designada (comitê interno, área técnica de privacidade). Esta categoria deve ser adotada apenas pelos órgãos ou entidades cujo fluxo institucional preveja revisão formal antes da validação; inclui também registros já concluídos que passaram a ser revisados periodicamente, conforme calendário definido;
- concluído: registro validado e em vigor, descrevendo operação de tratamento atualmente ativa cuja documentação integra o ROPA oficial;
- descontinuado: registro mantido por preservação de histórico, referente a operação de tratamento que cessou, permanecendo como elemento de demonstração de conformidade pretérita;
- cancelado: registro criado por engano, em duplicidade ou que jamais correspondeu a tratamento efetivamente realizado. O cancelamento deve ser fundamentado e registrado no histórico de versões, e o registro cancelado deve permanecer recuperável para fins de auditoria.

A adoção da categoria "em revisão" é facultativa e deve refletir a realidade institucional do órgão ou entidade. Em estruturas com fluxo de governança mais leve - nas quais a responsabilidade pela qualidade do preenchimento recai diretamente sobre o preenchedor, os registros podem migrar diretamente de “em andamento” para “concluído”, sem passagem por etapa intermediária. Nestes casos, a categoria “em revisão” pode ser adotada exclusivamente em fluxos de revisão periódica. Em órgãos ou entidades com estrutura de governança mais robusta, a etapa de revisão tende a ser adotada como mecanismo formal de controle de qualidade.

A distinção entre descontinuado (tratamento cessou, registro preservado) e cancelado (registro criado indevidamente) é importante. Tratamentos descontinuados deixam pegada documental legítima; registros cancelados representam ajustes na própria gestão do ROPA. As duas situações têm consequências distintas em auditorias e em comunicações regulatórias.

A transição entre situações deve obedecer ao fluxo definido na governança do programa - incluindo, quando aplicável, a passagem pela etapa de revisão - e ser registrada no histórico de versões.

Orientação prática para o preenchedor
Situação do registro: ao criar ou revisar um registro existente, mantenha a situação atualizada.
Observação: sugere-se contemplar as definições das diferentes situações possíveis na ferramenta utilizada para apoio ao ROPA.

4.1.6 Versionamento e histórico de alterações

Indicação da versão atual do registro e do histórico das alterações realizadas, com identificação de cada versão anterior, da data e do responsável pela alteração e da síntese das modificações efetuadas. O versionamento atende a três finalidades: (i) demonstrar, em situações de auditoria ou fiscalização, que o registro reflete o tratamento à época do fato verificado, e não apenas a configuração atual; (ii) permitir a recuperação de versões anteriores em caso de alteração indevida ou de necessidade de reconstituir o estado do tratamento em data específica; e (iii) sustentar análises evolutivas do PGP (quantos registros foram criados, alterados ou descontinuados em cada ciclo).

Independentemente da periodicidade da revisão obrigatória do registro, conforme tratado no capítulo 6 deste Guia, qualquer alteração relevante na operação de tratamento – como mudança de finalidade, inclusão de novos tipos de dados pessoais, alteração de hipótese legal, mudança nos agentes de tratamento, alteração de período de retenção, alteração de medidas de segurança – deve produzir nova versão do registro.

Orientação prática para o preenchedor
Versão: registre o número da versão atual (ex.: v1.0, v1.1, v2.0). Recomenda-se adotar versionamento semântico (incremento maior para alterações estruturais; incremento menor para ajustes pontuais ou correções).
Data da versão: registre a data em que a versão entrou em vigor – não confundir com a data do preenchimento original.
Síntese das alterações: para cada nova versão, descreva sucintamente o que foi alterado em relação à versão anterior (ex.: "v2.0 – inclusão de categoria de dados sensíveis (biometria facial); alteração da hipótese legal aplicável"). Esta síntese é o que torna o histórico utilizável.
Observação: deve-se assegurar que a tecnologia adotada preserva integralmente as versões anteriores e permite sua restauração. Em planilhas, isso requer disciplina manual (cópia da planilha antes de cada alteração). Em ferramentas *web*, *low-code* ou de mercado, em regra é capacidade nativa – confirme antes de adotar.
Reversão: caso necessário restaurar versão anterior, registre nova entrada no histórico com a indicação "v1.2 – reversão à v1.0 em razão de [motivação]"; jamais substitua o histórico.

4.2 Dados pessoais tratados

Este bloco visa descrever as categorias de titulares a quem se referem os dados pessoais objeto do tratamento e quais tipos de dados pessoais são tratados. A identificação precisa dos dados pessoais é necessária para a aplicação do princípio da necessidade (LGPD, art. 6º, III), para a avaliação de risco e para o tratamento adequado de dados pessoais sensíveis (LGPD, art. 11) e de dados de crianças e adolescentes (LGPD, art. 14) ou de outras categorias de vulneráveis, como idosos. É o bloco do ROPA com maior aderência direta ao FCI da ANPD: praticamente todos os campos sobre dados pessoais afetados pelo incidente espelham informações que devem estar previamente registradas aqui. Também possui correlação com o art. 30(1), alínea (c), do GDPR [10].

Correlação com o Formulário de Comunicação de Incidente da ANPD

- Campos "Quais as categorias de titulares foram afetadas pelo incidente?" e "Informe a quantidade de titulares afetados, por categoria": correspondem às categorias de titulares (4.2.1), com a estimativa de quantidade afetada pelo incidente.
- Campos sobre crianças, adolescentes e outros titulares vulneráveis afetados: correspondem à sinalização prevista em 4.2.2.
- Campo "Quais os demais tipos de dados pessoais violados?": espelha diretamente os tipos de dados pessoais em 4.2.3; a adoção de taxonomia compatível torna o preenchimento praticamente automático.
- Campo "Quais os tipos de dados pessoais sensíveis foram violados?": a indicação prévia da presença de dados sensíveis (4.2.4) permite resposta imediata e fidedigna.

4.2.1 Categorias de titulares

Identificação das categorias de titulares cujos dados pessoais são tratados no âmbito da operação, tais como servidores ativos, servidores inativos, pensionistas, contribuintes, beneficiários de programas sociais, fornecedores e candidatos a concurso público. Devem ser consideradas tanto as categorias que compõem o público-alvo do produto ou serviço quanto aquelas cujos dados pessoais também são objeto de tratamento em razão de suas atribuições de administração, gestão ou operação dos sistemas envolvidos.

Recomenda-se que o ROPA registre, além das categorias, a estimativa de quantidade de titulares por categoria. Essa informação é exigida pelo FCI da ANPD (campos "Qual a quantidade total de titulares cujos dados pessoais são tratados nas atividades afetadas pelo incidente?" e "Informe a quantidade de titulares afetados, por categoria") e raramente está disponível quando demandada sob pressão de tempo, caso não tenha sido previamente registrada.

Orientação prática para o preenchedor

Categorias de titulares: identifique as categorias de titulares cujos dados pessoais são tratados neste processo (por exemplo: servidores ativos, servidores inativos, pensionistas, contribuintes, beneficiários de programa social, fornecedores, candidatos a concurso, cidadãos atendidos). Registre também a estimativa de quantidade de titulares por categoria – essa informação será solicitada em situações de incidente.

4.2.2 Titulares que demandam proteção reforçada

Indicação expressa quando o tratamento envolver crianças, adolescentes, idosos ou outras categorias de titulares que demandem atenção diferenciada sob a perspectiva da proteção de dados pessoais. A LGPD estabelece proteção específica para crianças e adolescentes (art. 14). Além disso, a ANPD considera a utilização de dados pessoais de crianças, adolescentes e idosos como elemento relevante para a caracterização de tratamento de alto risco (Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, art. 4º, inciso II, alínea "d") [5] e atribui especial relevância a incidentes de segurança que envolvam dados dessas categorias de titulares (Resolução CD/ANPD nº 15, de 24 de abril de 2024) [14]. A identificação dessas situações auxilia na definição de salvaguardas proporcionais, na elaboração de avisos de privacidade adequados e na avaliação dos riscos decorrentes da atividade de tratamento.

Orientação prática para o preenchedor
Titulares que demandam proteção reforçada: caso sejam tratados dados pessoais de crianças, adolescentes, idosos ou de outras categorias de titulares cuja condição possa ampliar os riscos ou impactos decorrentes do tratamento de dados pessoais, identifique as categorias envolvidas e informe sua quantidade estimada, sempre que possível.

4.2.3 Tipos de dados pessoais

Relação dos tipos de dados pessoais efetivamente tratados pelo produto ou serviço, preferencialmente organizados em categorias. O registro tem por unidade o tipo de dado (por exemplo: nome completo, CPF, data de nascimento, e-mail corporativo, telefone funcional, número de matrícula), e não a mera indicação genérica da categoria (por exemplo: "dados de identificação"). A categorização é importante pois funciona como instrumento de organização e leitura, agrupando tipos afins sob rótulos comuns (dados básicos de identificação; dados de contato; dados financeiros; dados de autenticação; entre outros) – mas não elimina o registro tipo a tipo,

A escolha por registrar tipos, e não apenas categorias, tem três justificativas: (i) alinhamento direto com o FCI da ANPD [9], que opera com tipos específicos e cuja resposta em situação de incidente requer essa granularidade já previamente documentada; (ii) auxílio à reflexão do preenchedor sobre a real extensão dos dados pessoais tratados, particularmente relevante em produtos ou serviços com operações complexas, em que rótulos genéricos como "dados de contato" podem encobrir realidades distintas (endereço residencial vs. endereço comercial, telefone pessoal vs. corporativo, e-mails de natureza diversa); e (iii) coerência com o princípio da necessidade (inciso III do art. 6º da LGPD [2]), cujo controle prático supõe que se saiba concretamente quais dados pessoais são tratados, e não apenas a que famílias eles pertencem.

Recomenda-se que a taxonomia de categorias adotada pelo órgão seja compatível com aquela utilizada pela ANPD no FCI [9] – categorias comumente utilizadas incluem: dados básicos de identificação; documentos de identificação oficial; dados de contato; dados financeiros e meios de pagamento; dados protegidos por sigilo legal ou profissional; dados de autenticação; imagem, voz e localização geográfica; entre outros. A adoção dessa taxonomia comum reduz o esforço de tradução em situação de incidente e aumenta a consistência entre os instrumentos do PGP.

Orientação prática para o preenchedor
Tipos de dados pessoais (organizados por categoria): registre os tipos de dados pessoais efetivamente tratados, agrupados por categoria. O formato recomendado é "Categoria: tipo1; tipo2; tipo3" – por exemplo: "Dados básicos de identificação: nome completo; data de nascimento; CPF; RG; nacionalidade. Dados de contato: endereço residencial; telefone pessoal; e-mail pessoal; e-mail corporativo. Dados de autenticação: nome de usuário; senha (armazenada com hash); *token* de acesso".

4.2.4 Indicação de tipos de dados pessoais sensíveis

Quando o tratamento envolver dados pessoais sensíveis, tal qual definidos na LGPD, art. 5º, inciso II (dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural), o registro deve indicá-lo expressamente. Esta sinalização decorre diretamente do regime diferenciado estabelecido pelo art. 11 da LGPD e é determinante para a definição de medidas de segurança proporcionais.

A presença de dados pessoais sensíveis em uma operação afeta de forma direta a obrigação de comunicação de incidente: incidentes envolvendo dados pessoais sensíveis são, em regra, presumidamente capazes de acarretar risco ou dano relevante aos titulares (art. 48 da LGPD), atraindo maior probabilidade ao dever de comunicação à ANPD.

Orientação prática para o preenchedor
Tipos de dados pessoais sensíveis: caso sejam tratados dados pessoais sensíveis (saúde, biometria, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa/filosófica/política, dado genético, vida sexual), informe a(s) categoria(s) e, para cada uma, descreva quais são os tipos específicos. Exemplo: "Dados biométricos: biometria digital utilizada para ponto biométrico; biometria facial para autenticação no aplicativo do sistema".

4.3 Ciclo de vida dos dados

Este bloco reúne informações sobre como os dados pessoais são coletados, onde são armazenados, como são utilizados, qual o período de retenção e o que ocorre ao final do ciclo. Estas informações materializam o princípio da necessidade (LGPD, art. 6º, III), a transparência prevista no art. 9º e a obrigação de eliminação prevista no art. 16 da LGPD. Também fornecem elementos para o controle de proporcionalidade entre risco e medida de segurança e para a avaliação do impacto de eventual incidente sobre a disponibilidade dos dados.

Correlação com o Formulário de Comunicação de Incidente da ANPD
- Campo "Descrição do Incidente – Descreva, resumidamente, como ocorreu o incidente": a descrição do fluxo de tratamento descrito em 4.3.1, bem como as demais informações deste bloco, são insumos diretos, ao permitir caracterizar com precisão o ponto do fluxo em que o incidente ocorreu.

- Identificação do sistema afetado e localização do incidente: o local e meio de armazenamento (4.3.3) registrado no ROPA é o ponto de partida para localizar o incidente e dimensionar seu alcance.
- Avaliação da extensão temporal do incidente: o período de retenção (4.3.4) ajuda a estimar o conjunto histórico de dados potencialmente comprometidos.

4.3.1 Descrição do fluxo de tratamento

Descrição textual e sintética de como os dados pessoais são coletados, processados, armazenados, eventualmente compartilhados e descartados ao longo do processo. A descrição do fluxo é necessária para que a finalidade declarada (item 3.2.1) seja inteligível à luz das operações concretas executadas, e ampara a transparência exigida pelo art. 9º da LGPD.

Orientação prática para o preenchedor
Descrição do fluxo: descreva como (de que forma) os dados pessoais são tratados, desde a coleta, retenção/armazenamento, processamento/utilização até a sua eliminação. Caso haja fluxograma, anexá-lo facilita a leitura do registro por terceiros.

4.3.2 Origem dos dados pessoais

Indicação da origem dos dados pessoais utilizados na operação de tratamento, informando se a coleta ocorre diretamente junto ao titular ou por intermédio de outras fontes, tais como órgãos públicos, entidades privadas, bases de dados de acesso público. Devem ser identificados também os dados pessoais reutilizados a partir da coleta por outros produtos ou serviços, se são produzidos ou inferidos no decorrer do próprio tratamento. Essa informação é relevante para o cumprimento das obrigações de transparência previstas na LGPD, especialmente quando os dados não são obtidos diretamente do titular, e para a avaliação da conformidade e da legitimidade da atividade de coleta.

Orientação prática para o preenchedor
Fontes de dados: informe as fontes para obtenção dos dados pessoais utilizadas neste produto ou serviço (formulário preenchido pelo próprio titular; coleta por outro produto ou serviço; cadastro de outro órgão público; bases públicas; terceiros; produção interna). Quando houver mais de uma fonte, registre cada uma.

4.3.3 Local e meio de armazenamento

Descrição do local e do meio em que os dados são armazenados – por exemplo, sistema corporativo X, base de dados Y, repositório documental Z, arquivo físico. Esta informação é insumo para a avaliação de medidas de segurança proporcionais (LGPD, art. 46) e para a resposta a incidentes. Em situações de incidente, a indicação do local de armazenamento é o ponto de partida para a apuração técnica.

Orientação prática para o preenchedor

Meios de armazenamento: informe os meios de retenção/armazenamento dos dados pessoais (sistema corporativo, base de dados, repositório documental, planilhas, arquivo físico, nuvem corporativa etc.). Quando houver mais de um meio, registre todos. Esta informação será o ponto de partida para localizar o incidente em caso de comunicação à ANPD.

4.3.4 Período de retenção

Tempo durante o qual os dados pessoais permanecem sob tratamento pelo órgão ou entidade, bem como o fundamento normativo que justifica sua retenção. O registro dessas informações decorre dos art. 15 e art. 16 da LGPD, que disciplinam o término do tratamento e as hipóteses de conservação de dados pessoais. A definição de prazos ou critérios de retenção contribui para demonstrar a observância dos princípios da necessidade e da responsabilização, além de auxiliar na identificação de tratamentos que possam demandar revisão periódica. A inexistência de prazo ou critério definido para a retenção dos dados pessoais constitui elemento relevante para a avaliação da conformidade da operação de tratamento. Esta informação possui correlação com o art. 30(1), alínea (f), do GDPR [10].

Orientação prática para o preenchedor
Período de retenção: informe por quanto tempo os dados pessoais permanecem sob tratamento ou quais critérios determinam o encerramento de sua retenção. A informação pode ser apresentada de diferentes formas, tais como: (a) período determinado ("5 anos a partir da coleta" ou "5 anos após o encerramento do vínculo"); (b) data específica ("até 31 de dezembro de 2030"); ou (c) condição ou evento que marque o término da retenção ("enquanto durar o vínculo contratual" ou "até a conclusão do processo administrativo"). Sempre que houver norma legal, regulamentar, contratual ou outra obrigação que justifique a retenção dos dados, indique-a de forma expressa.

4.3.5 Forma de eliminação ou destinação final

Indicação da forma de eliminação, anonimização, conservação ou outra destinação conferida aos dados pessoais após o término da finalidade que justificou o tratamento. O registro dessa informação permite verificar a observância dos art. 15 e art. 16 da LGPD, que disciplinam o término do tratamento e as hipóteses em que os dados pessoais podem ser conservados, tais como para cumprimento de obrigação legal ou regulatória pelo controlador, realização de estudos por órgão de pesquisa, transferência a terceiro mediante observância dos requisitos legais ou uso exclusivo do controlador, vedado seu acesso por terceiro e desde que os dados sejam anonimizados sempre que possível. Quando aplicável, deve ser indicada também a destinação dos documentos ou registros que contenham dados pessoais, inclusive sua preservação permanente, observada a legislação arquivística pertinente.

Orientação prática para o preenchedor
Forma de eliminação ou destinação final: informe o que ocorre com os dados pessoais após o término do tratamento. Descreva se os dados são eliminados, anonimizados, conservados com base em hipótese legal ou submetidos a outra forma de destinação, indicando, sempre que possível, o procedimento adotado (por exemplo: eliminação automática pelo sistema, expurgo periódico, destruição física de documentos, anonimização ou preservação permanente de documentos) e o fundamento que justifica a destinação adotada.

4.3.6 Frequência do tratamento

Indicação da periodicidade com que a operação de tratamento é realizada, distinguindo-se, quando aplicável, entre atividades contínuas, periódicas ou eventuais. O registro desta informação não é exigido pela LGPD e sua adoção deve ser avaliada pelo órgão ou entidade conforme o caso concreto - em operações de tratamento dinâmicas, integradas a sistemas em tempo real ou sujeitas a janelas operacionais específicas, o registro da frequência tende a ser elemento relevante para a compreensão da dinâmica da operação, para a avaliação da exposição dos dados pessoais a riscos e para o planejamento de medidas técnicas ou administrativas de privacidade e segurança da informação. Já em operações pontuais, estáticas ou de baixa variabilidade temporal, o registro pode acrescentar pouco valor informacional, cabendo ao órgão decidir, à luz da sua realidade institucional e da natureza do tratamento, sobre a pertinência de mantê-lo.

Orientação prática para o preenchedor
Frequência do tratamento: informe com que regularidade a operação de tratamento é realizada, considerando a natureza da atividade e a ocorrência das diferentes etapas do tratamento. A frequência pode ser descrita, por exemplo, como contínua, diária, semanal, mensal, anual ou eventual. Quando houver diferenças relevantes entre as etapas da operação, estas podem ser detalhadas de forma complementar. Exemplos: "coleta contínua e atualização mensal"; "tratamento realizado apenas durante o período de inscrições"; ou "processamento eventual, mediante solicitação do titular".

4.4 Finalidade e fundamentação do tratamento

As informações reunidas neste bloco permitem compreender por que os dados pessoais são tratados e qual é o fundamento jurídico que autoriza o tratamento. Esses elementos decorrem diretamente dos princípios da finalidade e da transparência, bem como das hipóteses legais de tratamento previstas na LGPD (art. 6º, inciso I, art. 7º, art. 11 e art. 23). O conjunto de informações deste bloco possui relação com o art. 30(1), alínea (b), do GDPR [10].

A correta identificação da finalidade, da hipótese legal aplicável e da respectiva previsão normativa constitui requisito essencial para demonstrar a conformidade da operação de tratamento, assegurar a transparência perante os titulares e viabilizar a prestação de contas perante órgãos de controle e supervisão. A consistência entre esses elementos deve ser verificada periodicamente, especialmente quando houver alterações no produto ou serviço prestado, na política pública executada ou na base normativa que sustenta o tratamento.

Correlação com o Formulário de Comunicação de Incidente da ANPD
- Campo "Riscos e Consequências aos Titulares": a finalidade declarada para o tratamento constitui referência para a avaliação dos impactos decorrentes de eventual incidente de segurança, especialmente quando o uso indevido dos dados puder resultar em tratamento incompatível com as finalidades originalmente informadas.
- Campo "Atividades de tratamento submetidas a regulações setoriais": a previsão normativa específica (4.4.3) registrada no ROPA contém parte das informações requeridas, evitando reconstrução em situação de urgência.

4.4.1 Finalidade do tratamento

Descrição específica, explícita e legítima dos objetivos que justificam o tratamento dos dados pessoais, em conformidade com o princípio da finalidade previsto inciso I do art. 6º da LGPD. A finalidade deve expressar o resultado que se pretende alcançar com o tratamento e permitir a compreensão de sua necessidade pelos titulares, pelos agentes envolvidos e pelos órgãos de controle.

A finalidade não deve ser genérica nem se confundir com a descrição do produto ou serviço, da política pública ou do sistema utilizado. Deve responder, de forma clara, à pergunta: "para que os dados pessoais são necessários?". Em operações simples, que envolvem um único fluxo, uma única hipótese legal, um único público e poucos sistemas, uma única finalidade geral tende a ser suficiente. Em operações complexas, recomenda-se desdobrar a descrição em finalidades específicas, especialmente quando o tratamento envolver: (i) múltiplas hipóteses legais aplicáveis a diferentes etapas; (ii) públicos distintos sujeitos a fluxos diferenciados; (iii) compartilhamentos que ocorrem apenas em parte das etapas; (iv) tratamento de dados pessoais sensíveis em apenas parte dos fluxos; ou (v) integração com múltiplos sistemas com regras de acesso distintas. Nesses casos, a criação de entradas distintas no ROPA, com maior granularidade na finalidade, promove maior qualidade no registro, facilita a sua manutenção e demais ações de conformidade sustentadas pelo ROPA.

Orientação prática para o preenchedor
Finalidades: descreva de forma objetiva para qual propósito os dados pessoais são tratados. A finalidade deve indicar o resultado pretendido pelo tratamento e justificar a necessidade da utilização dos dados pessoais. Registre cada finalidade separadamente, quando houver mais de uma. Evite expressões genéricas como "fins administrativos", "gestão institucional", "cumprimento da legislação" ou "execução das competências do órgão". O nível de detalhamento e granularidade das finalidades deve ser avaliado conforme a complexidade do tratamento - evite tanto o excesso de generalidade quanto o excesso de fragmentação. Descreva concretamente a finalidade, por exemplo: "conceder aposentadorias e pensões" pode ser desdobrado em (i) "analisar e autorizar aposentadorias e pensões a servidores", (ii) "analisar e autorizar aposentadorias e pensões a dependentes", (iii) "manter o pagamento de benefícios concedidos" e (iv) "realizar comprovação de vida e recadastramento periódico de beneficiários"

4.4.2 Hipótese legal de tratamento

Indicação da hipótese legal que autoriza o tratamento dos dados pessoais, nos termos dos art. 7º ou art. 11 da LGPD, conforme a natureza dos dados e das categorias de titulares envolvidas, especialmente considerando as disposições do art. 14 da LGPD para crianças e adolescentes. A hipótese legal deve guardar correspondência com a finalidade declarada e refletir a efetiva justificativa jurídica para a realização do tratamento.

Para os órgãos e entidades da administração pública federal, são frequentemente aplicáveis as hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador (LGPD, art. 7º, inciso II) e de execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (LGPD, art. 7º, inciso III), observadas as disposições do art. 23 da LGPD.

Orientação prática para o preenchedor
Hipóteses de tratamento: identifique a hipótese prevista na LGPD que autoriza a realização do tratamento para cada finalidade registrada. Verifique se a hipótese selecionada é compatível com a natureza dos dados pessoais tratados, a finalidade informada e o contexto da operação.

4.4.3 Previsão normativa específica

Indicação da norma jurídica que fundamenta concretamente a realização do tratamento, especialmente quando este decorrer do exercício de competências legais, da execução de políticas públicas, do cumprimento de obrigação legal ou regulatória ou de outras atividades disciplinadas por norma específica.

Esse campo complementa a hipótese legal de tratamento, permitindo verificar de forma objetiva a existência do fundamento normativo que sustenta a atividade. Na administração pública, assume especial relevância por demonstrar a vinculação do tratamento às competências legais do órgão ou entidade e às normas que disciplinam a política pública, o serviço ou o processo administrativo correspondente.

A indicação da previsão normativa contribui para a transparência, a rastreabilidade das decisões e a demonstração da conformidade da operação de tratamento.

Observação: nos casos em que a hipótese legal for o consentimento (art. 7º, inciso I, ou art. 11, inciso I, da LGPD), o registro deve indicar o instrumento ou mecanismo utilizado para sua obtenção e gestão, bem como os meios disponibilizados para sua revogação, em conformidade com o art. 8º da LGPD.

Orientação prática para o preenchedor
Previsões normativas: informe os dispositivos legais, regulamentares ou administrativos que respaldam a finalidade do produto ou serviço. Sempre que possível, indique a norma específica e os respectivos artigos, incisos ou dispositivos relevantes. Quando se tratar de execução de competência institucional, é desejável citar o ato que atribuiu a competência ao órgão. A indicação deve ser suficientemente precisa para permitir a verificação do fundamento declarado, evitando referências genéricas a leis ou regulamentos sem a identificação dos dispositivos pertinentes.

4.5 Agentes de tratamento

Este bloco identifica os agentes de tratamento envolvidos na operação e suas respectivas responsabilidades, em conformidade com os conceitos e atribuições previstos na LGPD. O registro dessas informações permite compreender quem participa da operação de tratamento, quem define suas finalidades e meios essenciais e quem executa atividades de tratamento em nome do controlador, contribuindo para a adequada atribuição de responsabilidades e para a transparência da operação. Estas informações também são identificadas no art. 30(1), alínea (a), e ao art. 30(2) do GDPR [10].

A correta identificação dos agentes de tratamento é particularmente relevante em operações que envolvam o compartilhamento de dados pessoais, a execução conjunta de políticas públicas, a contratação de serviços de tecnologia da informação ou outras formas de

cooperação entre órgãos e entidades. Também contribui para a gestão de riscos, para a supervisão das atividades de tratamento e para a adoção de medidas de resposta em caso de incidentes de segurança.

Conforme destacado pela ANPD em seu Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado [15], a qualificação de um agente como controlador ou operador deve ser analisada em relação à operação de tratamento específica, podendo uma mesma organização desempenhar diferentes papéis em contextos distintos.

Correlação com o Formulário de Comunicação de Incidente da ANPD

- Bloco "Dados do Controlador": a identificação do controlador – razão social, CNPJ, dados de contato – é reaproveitada integralmente.
- Campos “Caso o incidente tenha sido comunicado ao controlador por um operador, informe os dados abaixo do Operador”: pressupõe que o controlador conheça e mantenha contato ativo com seus operadores, o que demanda o registro prévio dessa relação.

4.5.1 Controladores

Identificação do órgão na condição de controlador, quando aplicável. Em regra, o órgão da administração pública federal é controlador dos tratamentos que realiza no exercício de suas competências legais e institucionais, conforme a LGPD, art. 5º, VI. Todavia, a identificação do controlador deve ser realizada considerando a operação de tratamento específica e a efetiva competência para definir suas finalidades e meios essenciais.

Quando a operação envolver múltiplos controladores, devem ser identificados todos estes agentes que participam das decisões referentes ao tratamento, bem como, sempre que possível, os instrumentos normativos, contratuais ou de cooperação que disciplinam a distribuição de responsabilidades.

Orientação prática para o preenchedor

Controladores: identifique o órgão ou entidade responsável pelas decisões referentes às finalidades e aos meios essenciais da operação de tratamento. Em regra, o controlador será o órgão ou entidade responsável pela política pública, pelo serviço, pelo processo administrativo ou pela atividade que justifica o tratamento. Sendo assim, informe a razão social, CNPJ, endereço, contato com unidade responsável pelo produto ou serviço e responsabilidades do controlador.
Nos casos em que mais de um órgão ou entidade participe da definição das finalidades e dos meios essenciais do tratamento, identifique todos os controladores envolvidos e informe, sempre que possível, os instrumentos que disciplinam a relação entre eles, tais como acordos de cooperação, convênios, termos de execução descentralizada ou instrumentos equivalentes.
Importante distinguir compartilhamento de dados pessoais da relação controlador–operador: o operador trata os dados sob instruções do controlador, em nome dele; um terceiro com quem se compartilham dados pessoais, em regra, atua como controlador.

4.5.2 Operadores

Identificação dos operadores que realizam operações de tratamento de dados pessoais em nome do controlador e de acordo com suas instruções, nos termos do inciso VII do art. 5º da LGPD.

A identificação dos operadores permite compreender a cadeia de tratamento associada à operação, apoiar a supervisão das atividades executadas por terceiros e demonstrar a observância das disposições da LGPD relativas à atuação do operador. Também contribui para a gestão de riscos na cadeia de suprimentos, ou seja, riscos decorrentes da terceirização de atividades de tratamento e para a definição das responsabilidades dos agentes envolvidos.

Sempre que aplicável, devem ser registradas informações que permitam identificar a relação existente entre controlador e operador, bem como o instrumento que disciplina a execução das atividades de tratamento.

Orientação prática para o preenchedor
Operadores: identifique as pessoas naturais ou jurídicas que realizam operações de tratamento de dados pessoais em nome do órgão ou entidade e de acordo com suas instruções. Sempre que possível, informe a razão social ou nome completo, CPF ou CNPJ, a responsabilidade do operador e o instrumento que fundamenta a relação, como contrato administrativo, acordo de cooperação, convênio, termo de execução descentralizada ou instrumento equivalente.
São exemplos frequentes de operadores os fornecedores de serviços de hospedagem, processamento, sustentação ou desenvolvimento de sistemas, centrais de atendimento, prestadores de serviços especializados e outras organizações que tratem dados pessoais exclusivamente para viabilizar atividades do controlador. Servidores, empregados, estagiários e demais colaboradores não são operadores para fins da LGPD.

4.6 Compartilhamento e transferência internacional de dados pessoais

Neste bloco são registradas as hipóteses em que os dados pessoais são compartilhados com outros órgãos, entidades ou organizações, bem como os casos de transferência internacional de dados pessoais. Essas informações contribuem para a compreensão do fluxo dos dados pessoais ao longo do seu ciclo de vida no fornecimento do produto ou serviço, refletindo na identificação de agentes de tratamento e principalmente para a verificação da conformidade destas ações.

O registro dos compartilhamentos e transferências internacionais encontra fundamento, entre outros dispositivos, nos art. 26, art. 27 e art. 33 a art. 36 da LGPD. No âmbito da administração pública, essas informações são particularmente relevantes para demonstrar a compatibilidade do tratamento com as finalidades da operação, a observância das competências institucionais dos órgãos envolvidos e a existência de base jurídica.

O **Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público** [4] da ANPD destaca que o compartilhamento de dados entre órgãos e entidades públicas constitui prática frequente para a execução de políticas públicas, prestação de serviços públicos e exercício de competências legais, devendo observar os princípios da LGPD, com atenção à finalidade, necessidade, transparência e segurança. O registro dessas informações no ROPA contribui para a rastreabilidade dos fluxos de dados pessoais e para a demonstração da conformidade da operação de tratamento.

Correlação com o Formulário de Comunicação de Incidente da ANPD

- Avaliação da extensão do incidente: o mapeamento prévio dos compartilhamentos e transferências internacionais permite identificar se o incidente potencialmente afeta dados pessoais já compartilhados com terceiros, ampliando o escopo da apuração.

4.6.1 Compartilhamento de dados pessoais

Identificação dos órgãos, entidades ou organizações com os quais os dados pessoais são compartilhados, indicando a finalidade do compartilhamento e o fundamento que o autoriza. Tais informações possuem alinhamento com o art. 30(1), alínea (d), do GDPR [10].

O compartilhamento pode ocorrer entre órgãos e entidades da Administração Pública, entre diferentes esferas de governo ou com entidades privadas, observadas as disposições da LGPD e demais normas aplicáveis. Em todos os casos, recomenda-se registrar informações suficientes para permitir a compreensão da necessidade do compartilhamento, dos agentes envolvidos e do instrumento jurídico ou normativo que o fundamenta.

Quando aplicável, devem ser identificados os instrumentos que disciplinam o compartilhamento, tais como acordos de cooperação técnica, convênios, termos de execução descentralizada, contratos, instrumentos congêneres ou previsões legais específicas.

Orientação prática para o preenchedor
Compartilhamento de dados pessoais: identifique os órgãos, entidades ou organizações com as quais os dados pessoais são compartilhados no contexto do produto ou serviço objeto do ROPA. Para cada compartilhamento, informe, sempre que possível:

- o destinatário dos dados pessoais – nome completo ou razão social, CPF ou CNPJ (demais informações devem constar na identificação dos controladores);
- a finalidade do compartilhamento;
- os tipos de dados pessoais compartilhados;
- o fundamento legal ou normativo aplicável; e
- o instrumento que disciplina a relação, quando existente.

Inclua tanto os compartilhamentos realizados com outros órgãos ou entidades públicas quanto aqueles realizados com entidades privadas. Caso existam diferentes destinatários para finalidades distintas, registre cada compartilhamento separadamente.
Não registre nestes campos os acessos realizados por operadores que tratem os dados exclusivamente em nome do controlador e de acordo com suas instruções, os quais devem ser identificados nos campos destinados aos operadores.

4.6.2 Transferência internacional

Identificação das operações que envolvam transferência internacional de dados pessoais, nos termos dos art. 33 a art. 36 da LGPD e da Resolução CD/ANPD nº 19, de 23 de agosto de 2024, que aprovou o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais [16]. No GDPR, tais informações são solicitadas no ROPA em conformidade com o art. 30(1), alínea (e) [10].

Nos termos da regulamentação da ANPD, considera-se transferência internacional a operação de tratamento por meio da qual um agente de tratamento transmite, compartilha ou disponibiliza acesso a dados pessoais a outro agente de tratamento localizado em país

estrangeiro ou organismo internacional. A caracterização da transferência internacional deve ser analisada à luz das circunstâncias concretas da operação, observados os conceitos e definições estabelecidos pela regulamentação vigente.

Quando houver transferência internacional, devem ser registrados os países ou organismos internacionais de destino, os destinatários dos dados, os tipos de dados pessoais transferidos e o mecanismo jurídico que a fundamenta. Entre os mecanismos previstos pela LGPD e pela regulamentação da ANPD estão as decisões de adequação, as cláusulas contratuais específicas, as cláusulas-padrão contratuais aprovadas pela ANPD, as normas corporativas globais e as demais hipóteses previstas no art. 33 da LGPD.

O registro dessas informações contribui para a avaliação dos riscos associados à circulação internacional dos dados pessoais, para a demonstração da conformidade da operação de tratamento e para o atendimento aos deveres de transparência e prestação de contas previstos na LGPD.

Orientação prática para o preenchedor
Transferência internacional: informe se a operação envolve a transmissão, o compartilhamento ou a disponibilização de acesso a dados pessoais para agente de tratamento localizado em país estrangeiro ou organismo internacional. Em caso positivo, registre, sempre que possível:

- o destinatário dos dados – nome completo ou razão social, CPF ou CNPJ (demais informações devem constar na identificação dos agentes de tratamento);
- o país ou organismo internacional de destino;
- os tipos de dados pessoais transferidos;
- o mecanismo de transferência internacional utilizado; e
- o instrumento contratual, normativo ou administrativo que discipline a operação, quando aplicável.

A caracterização da transferência internacional deve observar os critérios estabelecidos pela LGPD e pela Resolução CD/ANPD nº 19/2024.

4.7 Síntese das informações do registro

Esta seção consolida, em formato de tabela, o conjunto mínimo de informações descrito ao longo das seções 4.1 a 4.6, indicando o fundamento normativo principal de cada uma. A finalidade da síntese é dupla: oferecer uma visão de conjunto que apoie a implantação inicial do ROPA e funcionar como instrumento de auditoria periódica do registro, permitindo verificar, item a item, se a operação está adequadamente documentada.

A Tabela 1 está organizada por bloco temático (correspondente às seções 4.1 a 4.6), seguindo a sequência apresentada neste capítulo. Recomenda-se que esta síntese sirva como lista de verificação no processo de implantação e de auditoria do registro.

Tabela 1: conjunto mínimo de informações do ROPA

Bloco	Informação	Fundamento principal
4.1 Identificação	Identificador único do registro	Função de inteligibilidade e gestão do registro

Bloco	Informação	Fundamento principal
	Nome do produto ou serviço	Função de inteligibilidade e gestão do registro
	Unidade administrativa responsável	Art. 6º, X (responsabilização)
	Responsável pelo preenchimento	Art. 6º, X (responsabilização aplicada à gestão do registro)
	Situação do registro	Função de inteligibilidade e gestão do registro
	Versionamento e histórico de alterações	Função de inteligibilidade e gestão do registro
4.2 Dados pessoais tratados	Categorias de titulares (com estimativa quantitativa)	Arts. 17 a 22 (direitos do titular)
	Titulares que demandam proteção reforçada	Art. 14 e demais hipóteses de vulnerabilidade
	Tipos de dados pessoais (organizados por categoria)	Art. 6º, III (necessidade)
	Indicação de tipos de dados pessoais sensíveis	Art. 11 e gestão de riscos
4.3 Ciclo de vida dos dados	Descrição do fluxo de tratamento	Arts. 6º, I e 9º (transparência)
	Origem dos dados pessoais	Art. 9º (transparência)
	Local e meio de armazenamento	Boa prática (rastreabilidade)
	Período de retenção	Arts. 15 e 16
	Forma de eliminação ou destinação final	Art. 16
	Frequência do tratamento	Boa prática (gestão de risco)
4.4 Finalidade e fundamentação	Finalidade do tratamento	Art. 6º, I; art. 9º, I e V
	Hipótese legal de tratamento	Arts. 7º, 11 e 14
	Previsão normativa específica	Art. 7º, II; Art. 11, II, a; Art. 23, I
4.5 Agentes de tratamento	Controladores (singular ou múltiplos)	Art. 9º, V; Art. 18, VII
	Operadores	Art. 9º, VI; Art. 6º, VI; Art. 39
	Compartilhamento de dados pessoais	Art. 9º, V; Art. 18, VII; Art. 26

Bloco	Informação	Fundamento principal
4.6 Compartilhamento e transferência	Transferência internacional	Arts. 33 a 36; Resolução CD/ANPD nº 19/2024

5 Processo do registro das operações de tratamento de dados pessoais

Tão importante quanto definir o conteúdo do ROPA é estabelecer um processo institucional sustentável para sua elaboração e manutenção. Embora a qualidade do conteúdo informacional seja um elemento relevante, os desafios enfrentados em iniciativas de ROPA na administração pública também podem estar relacionados à ausência de processos estruturados, à indefinição de papéis e responsabilidades e à falta de mecanismos institucionais que assegurem a atualização contínua dos registros.

Este capítulo aborda o processo institucional de elaboração e manutenção do ROPA, com ênfase nas particularidades da administração pública federal: ciclos de planejamento institucional, alta rotatividade de servidores e dirigentes, descontinuidade administrativa decorrente de transições de governo, heterogeneidade de maturidade entre unidades e limitação de equipes dedicadas à privacidade.

O capítulo está organizado em cinco seções: governança do processo, estratégias de implantação inicial, calendário e ciclo regular, capacitação e suporte e manutenção do registro atualizado.

5.1 Governança do processo

Esta seção descreve a distribuição de papéis e responsabilidades necessária para que o processo do ROPA seja sustentável e para que a responsabilização seja efetivamente distribuída no órgão ou entidade, evitando a concentração indevida de atribuições no encarregado ou na unidade de privacidade.

Nos termos do art. 37 da LGPD, os agentes de tratamento devem manter registro das operações de tratamento de dados pessoais que realizam. Embora o dispositivo legal atribua essa obrigação ao agente de tratamento, sua execução prática depende da atuação das diversas unidades administrativas que realizam operações de tratamento no âmbito de suas competências. Assim, a responsabilidade institucional pela manutenção do ROPA concretiza-se por meio da participação das unidades responsáveis pelos tratamentos, sob coordenação e governança adequadas.

Desta forma, como subsídio para reflexão pelo órgão ou entidade, é apresentada a seguir uma possível distribuição de papéis e responsabilidades:

- Comitê de governança de privacidade e segurança (ou equivalente): aprova as diretrizes institucionais relacionadas ao ROPA, incluindo estratégia de implantação, responsabilidades, cronograma e critérios de priorização; valida o escopo de cada ciclo de levantamento e delibera sobre conflitos de prioridade ou questões de governança que exijam decisão colegiada;
- Encarregado e equipe de apoio: podem conduzir tecnicamente o processo, mantendo o padrão metodológico institucional, desenvolvendo orientações, materiais de apoio e ações de capacitação, e prestando suporte técnico às unidades responsáveis pelo preenchimento dos registros. A coordenação operacional do processo também pode

ser atribuída à unidade de privacidade, quando existente, preservando-se a atribuição do encarregado de orientar os agentes de tratamento, nos termos da LGPD, art. 41, § 2º, III. Quando exercida pelo encarregado, a coordenação metodológica e processual não implica a definição de meios e finalidades sobre o tratamento de dados pessoais decorrentes do ROPA - atribuição que permanece, por força do art. 5º, VI, da LGPD, do controlador, materializada institucionalmente por meio de norma interna articulada à PPDP aprovada pelo comitê ou instância equivalente;

- Unidades administrativas: elaboram, validam e mantêm atualizados os registros das operações de tratamento realizadas no exercício de suas atribuições. Como são essas unidades que conhecem os processos de negócio e executam os tratamentos de dados pessoais, cabe a elas a responsabilidade primária pela completude, precisão e atualização das informações registradas. O encarregado e a unidade de privacidade exercem função de orientação e supervisão metodológica, mas não substituem as unidades na identificação e descrição de seus tratamentos. Para conferir maior clareza e responsabilização ao processo, é recomendável que a responsabilidade seja atribuída formalmente a ocupantes de cargos de gestão, como coordenadores-gerais, coordenadores ou equivalentes, observada a estrutura organizacional de cada órgão ou entidade;
- Pontos focais de privacidade nas unidades: o órgão ou entidade pode designar servidores para atuar como interlocutores diretos junto ao encarregado ou à unidade de privacidade. Esses pontos focais facilitam a coleta e atualização das informações, apoiam a disseminação das orientações institucionais e contribuem para a sustentabilidade do processo ao longo do tempo.

Recomenda-se que essa distribuição de papéis seja formalizada em norma interna, preferencialmente em articulação com a Política de Proteção de Dados Pessoais (PPDP) do órgão ou entidade. Recomenda-se, ainda, que o responsável pela coordenação do processo mantenha atualizada a relação das unidades responsáveis pelos registros e dos respectivos pontos focais de privacidade, quando designados.

5.2 Estratégias de implantação inicial

A elaboração da primeira versão do ROPA é o momento de maior desafio do processo. A escolha da estratégia de implantação deve considerar a maturidade do órgão em proteção de dados pessoais, o porte da administração, o nível de adesão das chefias e os recursos disponíveis.

Esta seção discute as alternativas estratégicas para a primeira elaboração do ROPA, com ênfase no equilíbrio entre amplitude (cobertura do órgão ou entidade) e profundidade (detalhamento dos registros). A seguir são apresentadas três configurações típicas, além da recomendação geral de realização de projeto-piloto antes da implantação em larga escala.

5.2.1 Estratégia em ondas de profundidade crescente (estratégia horizontal)

Nesta estratégia, todas as unidades do órgão ou entidade são mobilizadas simultaneamente, mas o conjunto de informações solicitadas inicialmente é reduzido a um núcleo mínimo. Em ondas subsequentes, novas informações são incorporadas, refinando progressivamente o registro.

Exemplo de progressão:

- **onda 1:** identificação do processo, finalidade, hipótese legal e tipos de dados pessoais (objetivo: registrar a existência de tratamentos).
- **onda 2:** ciclo de vida (origem, armazenamento, retenção, eliminação) e categorias de titulares.
- **onda 3:** agentes de tratamento, compartilhamentos e transferências.
- **onda 4:** revisão geral.

Dentre as vantagens desta estratégia, pode-se destacar: gera, desde a primeira onda, uma visão panorâmica de todo o órgão ou entidade; cria cultura institucional homogênea; a curva de aprendizado para as unidades é gradativa, respeitando as ondas – informações mais simples são solicitadas nas primeiras ondas. Entretanto, há limitações: exige forte capacidade de coordenação central; e pode gerar registros superficiais nas primeiras ondas, que precisam ser controlados como provisórios.

5.2.2 Estratégia em profundidade unidade a unidade (estratégia vertical)

Nesta estratégia, o órgão é trabalhado por conjunto de unidades – uma por vez, ou um pequeno grupo por vez –, com o conteúdo completo de informações sendo necessário desde o primeiro momento. O preenchimento do ROPA de cada conjunto de unidades encerra-se com a consolidação dos registros contemplando todas as operações de tratamento de dados pessoais, e o trabalho avança para o conjunto seguinte de unidades.

Essa abordagem tende a produzir registros de alta qualidade desde o início e permite construir conhecimento detalhado da unidade, gerando benefícios que extrapolam o ROPA, como o fornecimento de subsídios para a elaboração de RIPDs, avisos de privacidade e controles de segurança. Em contrapartida, a visão panorâmica do órgão somente é consolidada ao final das iterações com todas as unidades; além disso, os registros das áreas trabalhadas nas etapas iniciais podem estar desatualizados ao final do preenchimento pelas últimas unidades, e sua adoção depende de uma priorização inicial adequadamente fundamentada.

5.2.3 Estratégia mista

Outra possibilidade é a adoção de uma estratégia mista, que combina elementos das abordagens horizontal e vertical. Neste modelo, realiza-se inicialmente um levantamento abrangente de todas as unidades do órgão ou entidade por meio de ondas de profundidade crescente, ao mesmo tempo em que são priorizadas para aprofundamento imediato aquelas unidades cujas atividades envolvam operações de tratamento potencialmente mais relevantes ou de maior risco.

Essa priorização normalmente recai sobre unidades que tratam dados pessoais sensíveis, dados de crianças, adolescentes ou outros grupos em situação de vulnerabilidade, realizam tratamentos em larga escala ou executam atividades consideradas críticas para a missão institucional. Enquanto o aprofundamento dessas unidades produz registros mais completos e gera insumos para iniciativas correlatas – como RIPDs, avisos de privacidade e definição de medidas de segurança da informação – as ondas de levantamento garantem a construção

gradual de uma visão panorâmica do conjunto dos tratamentos realizados pelo órgão ou entidade.

Entre as principais vantagens dessa estratégia estão a obtenção precoce de uma visão institucional ampla, a possibilidade de direcionar esforços para os tratamentos mais relevantes e a distribuição mais equilibrada da carga de trabalho ao longo do tempo. Como contrapartida, sua implementação demanda critérios claros de priorização, mecanismos de governança capazes de coordenar frentes de trabalho com ritmos distintos e cuidados adicionais para assegurar a consistência metodológica entre os registros produzidos em diferentes níveis de profundidade.

5.2.4 Projeto-piloto antes da implantação ampla

Independentemente da estratégia adotada, recomenda-se a realização de um projeto-piloto envolvendo um conjunto reduzido e representativo de unidades antes da implantação em larga escala. Essa etapa permite testar e aperfeiçoar a metodologia de levantamento, validar o instrumento de coleta de informações e verificar a adequação dos conceitos, orientações e exemplos disponibilizados às unidades participantes.

Além de contribuir para a identificação de dúvidas recorrentes e inconsistências interpretativas, o projeto-piloto fornece subsídios para ajustar a comunicação institucional, aperfeiçoar materiais de apoio e capacitação e calibrar os mecanismos de governança e acompanhamento do processo. Também possibilita estimar com maior precisão o esforço necessário para execução das atividades, incluindo a dedicação das equipes envolvidas, os prazos de preenchimento e validação dos registros e a capacidade da equipe coordenadora.

Os aprendizados obtidos nessa etapa reduzem o risco de retrabalho durante a implantação ampla e aumentam a probabilidade de obtenção de registros consistentes e comparáveis entre as diferentes unidades do órgão ou entidade.

5.3 Calendário e ciclo regular

A manutenção do ROPA exige a adoção de um ciclo institucional regular, com responsabilidades, prazos e eventos de revisão previamente definidos. A ausência de um calendário formal tende a transformar o registro em uma iniciativa pontual, comprometendo sua atualização e utilidade para a governança da proteção de dados pessoais.

Recomenda-se que o comitê, ou instância equivalente, aprove periodicamente um calendário de elaboração, revisão e atualização do ROPA, contemplando, no mínimo:

- uma janela periódica de revisão geral dos registros por todas as unidades administrativas, em período previamente definido e estável, de modo a facilitar o planejamento das atividades e a consolidação de uma rotina institucional;
- revisões extraordinárias sempre que ocorrer alteração relevante em uma operação de tratamento, tais como mudança de finalidade, inclusão de novos tipos de dados pessoais, ampliação de compartilhamentos, contratação ou substituição de operador, modificação dos prazos de retenção ou alterações significativas no fluxo de tratamento;

- revisão obrigatória das operações envolvidas em incidentes de segurança ou em eventos que revelem inconsistências nos registros existentes, como parte das atividades de análise e tratamento pós-incidente;
- agenda periódica de orientação e suporte às unidades administrativas, conduzida pelo encarregado e equipe de apoio, por meio de encontros regulares destinados ao esclarecimento de dúvidas e à discussão de questões relacionadas ao ROPA e às demais obrigações decorrentes da LGPD.

A manutenção de canais permanentes de orientação é particularmente relevante na administração pública. Em muitos casos, a qualidade dos registros depende menos da realização de ações pontuais de capacitação e mais da existência de mecanismos contínuos de apoio às unidades responsáveis pelo preenchimento e atualização das informações. A previsibilidade desse suporte reduz inseguranças interpretativas, incentiva a atualização tempestiva dos registros e contribui para a consolidação de uma cultura organizacional de proteção de dados pessoais.

5.4 Capacitação e suporte

A qualidade e a sustentabilidade do ROPA dependem diretamente da capacidade de as unidades administrativas compreenderem os conceitos envolvidos, identificar corretamente suas operações de tratamento e manter os registros atualizados ao longo do tempo. Por essa razão, recomenda-se a implementação de um modelo de capacitação e suporte que combine ações estruturadas de treinamento com mecanismos permanentes de orientação.

Esse modelo pode contemplar, entre outros elementos:

- capacitação inicial específica sobre o ROPA, abordando conceitos fundamentais, responsabilidades institucionais, metodologia adotada pelo órgão ou entidade e utilização prática do instrumento de registro, preferencialmente com exemplos extraídos de situações reais ou semelhantes à realidade organizacional;
- disponibilização de materiais de referência permanentes, tais como guias, manuais, perguntas frequentes, glossários, modelos de preenchimento e exemplos comentados de registros, de forma a promover maior uniformidade na interpretação dos conceitos e na elaboração das informações;
- atendimento individualizado às unidades administrativas em momentos críticos do ciclo de gestão do ROPA, especialmente durante a implantação inicial, os períodos de revisão, a consolidação dos registros ou sempre que houver mudanças significativas nos tratamentos realizados;
- integração das ações relacionadas ao ROPA com o programa de capacitação em proteção de dados pessoais do órgão ou entidade, reforçando a compreensão de que o registro das operações de tratamento constitui instrumento de governança e prestação de contas, conectado a outras atividades, como gestão de riscos, elaboração de RIPDs, transparência e implementação de controles de segurança.

A combinação entre capacitação estruturada, materiais de apoio acessíveis e canais permanentes de orientação produz resultados mais consistentes do que iniciativas isoladas de treinamento. Além de melhorar a qualidade dos registros, essa abordagem contribui para

a disseminação do conhecimento sobre proteção de dados pessoais e reduz a dependência de poucos especialistas para a manutenção do processo.

5.5 Manutenção do registro atualizado

A elaboração inicial do ROPA representa apenas a primeira etapa de um processo de gestão contínua deste instrumento, inserido no PGP. Um registro que não acompanha a evolução dos processos de trabalho, dos sistemas de informação e das estruturas organizacionais perde progressivamente sua capacidade de refletir a realidade dos tratamentos realizados pelo órgão ou entidade, comprometendo sua utilidade como instrumento de conformidade, gestão de riscos e prestação de contas.

Na prática, a manutenção contínua do registro está entre os maiores desafios dos programas de governança em proteção de dados pessoais. A desatualização do ROPA decorre, principalmente, de três fatores: alterações em tratamentos já existentes, criação de novos tratamentos sem integração ao processo de governança da privacidade e mudanças organizacionais decorrentes de transições de gestão ou rotatividade de equipes.

5.5.1 Alterações em produtos ou serviços existentes

Alterações em produtos ou serviços que envolvam tratamento de dados pessoais devem resultar na revisão correspondente dos registros existentes. Mudanças em processos de trabalho, sistemas, fluxos operacionais, compartilhamentos, operadores contratados, prazos de retenção ou outras características relevantes do tratamento podem tornar o registro inconsistente caso não sejam refletidas tempestivamente no ROPA.

O principal desafio não é técnico, mas institucional. Em muitos órgãos, essas mudanças são conduzidas pelas áreas de negócio ou de tecnologia da informação sem que exista mecanismo formal que assegure o envolvimento da governança de privacidade.

Para mitigar esse risco, recomenda-se:

- incorporar verificações obrigatórias de impacto sobre o ROPA nos fluxos de aprovação de mudanças organizacionais, tecnológicas ou contratuais que envolvam tratamento de dados pessoais;
- integrar os processos de governança de tecnologia da informação ao processo de manutenção do ROPA, de modo que demandas relacionadas à aquisição de sistemas, desenvolvimento de soluções, integrações, compartilhamentos de dados pessoais ou alterações relevantes em ambientes tecnológicos incluam a análise dos registros potencialmente afetados;
- estabelecer critérios objetivos para caracterização de alterações significativas que exijam atualização imediata do registro, independentemente do ciclo periódico de revisão;
- orientar gestores e pontos focais para que a atualização do ROPA seja tratada como etapa obrigatória dos processos de mudança, e não como atividade posterior ou facultativa.

5.5.2 Novos tratamentos: privacidade desde a concepção e por padrão

A criação de novos processos que envolvam tratamento de dados pessoais é, ao mesmo tempo, oportunidade e risco. Oportunidade, porque permite incorporar requisitos de privacidade desde o início – privacidade desde a concepção e por padrão (*privacy by design and by default*), em conformidade com o § 2º do art. 46 da LGPD. Risco, porque, sem mecanismo institucional, novos tratamentos tendem a entrar em operação sem o correspondente registro.

As duas dimensões – desde a concepção e por padrão – são complementares, mas distintas. A privacidade desde a concepção (*by design*) significa que os requisitos de proteção de dados pessoais devem orientar as decisões de arquitetura, modelagem de dados e configuração de produtos e serviços desde a fase inicial do projeto, e não como adaptação posterior. Já a privacidade por padrão (*by default*) exige que, entre as configurações possíveis de um produto ou serviço, a menos invasiva à privacidade seja adotada como configuração inicial.

A integração entre o ROPA e a privacidade desde a concepção e por padrão opera em mão dupla: o ROPA é insumo para a avaliação de privacidade de novos produtos e serviços (permitindo verificar se já existe tratamento equivalente em outra unidade), e a avaliação prévia produz o registro inicial da nova operação. Recomenda-se que o órgão estabeleça, em sua PPDP ou em norma específica, a obrigatoriedade de avaliação prévia de privacidade para novos processos que envolvam dados pessoais, com produção concomitante do registro no ROPA.

5.5.3 Mudanças de equipe e transições de governo

A administração pública está sujeita a mudanças periódicas de dirigentes, reestruturações organizacionais e rotatividade de servidores. Sem mecanismos adequados de institucionalização, essas mudanças podem comprometer a continuidade do processo de manutenção do ROPA e provocar perda de conhecimento acumulado.

A sustentabilidade do registro depende, portanto, da existência de estruturas, procedimentos e responsabilidades formalizadas que reduzam a dependência de pessoas específicas e garantam a preservação da memória organizacional.

Nesse contexto, recomenda-se:

- formalizar responsabilidades, procedimentos e fluxos relacionados ao ROPA em normativos internos e instrumentos permanentes de governança;
- manter atualizada a relação dos responsáveis pelos registros e dos pontos focais de privacidade designados em cada unidade, incluindo a definição de suplentes sempre que possível;
- incorporar informações sobre o programa de privacidade, incluindo o ROPA e os tratamentos considerados críticos aos processos formais de transição de gestão e sucessão de responsáveis;
- vincular a manutenção do registro a instrumentos institucionais permanentes, tais como políticas, planos de gestão, planejamento estratégico, programas de integridade e mecanismos de prestação de contas.

5.5.4 Indicadores de qualidade do registro

A manutenção do ROPA deve ser acompanhada por indicadores que permitam avaliar sua qualidade, grau de atualização e efetividade como instrumento de governança. O monitoramento periódico desses indicadores auxilia na identificação de fragilidades, orienta ações corretivas e fornece evidências objetivas para fins de prestação de contas.

Entre os indicadores que podem ser adotados destacam-se:

- cobertura: proporção entre os produtos ou serviços registrados no ROPA e o total estimado, pelas unidades administrativas, de produtos ou serviços que envolvem tratamento de dados pessoais;
- atualidade: percentual de registros revisados dentro do período definido pela norma institucional de atualização;
- completude: percentual de registros com todos os campos obrigatórios preenchidos e validados;
- tratamentos de alto risco identificados: número absoluto e percentual de operações que envolvem dados pessoais sensíveis, grupos vulneráveis, muitos tipos de dados pessoais, vários agentes de tratamento, monitoramento sistemático, tratamento em larga escala ou outras características que indiquem maior potencial de impacto aos titulares;
- tratamentos com RIPD vinculado: percentual dos tratamentos classificados como de maior risco que possuem relatório de impacto elaborado ou em elaboração;
- participação das unidades: percentual de unidades administrativas que realizaram suas revisões periódicas dentro dos prazos estabelecidos.

Os indicadores devem ser reportados periodicamente às instâncias de governança, possivelmente o comitê ou estrutura equivalente, responsáveis pela supervisão do programa de privacidade e podem integrar relatórios gerenciais e outros instrumentos de prestação de contas do órgão ou entidade.

6 Considerações sobre a escolha de tecnologia

Este capítulo apresenta considerações sobre o instrumento tecnológico de implantação do ROPA, sem indicar ou excluir soluções específicas. Está organizado em três seções: a primeira (6.1) estabelece critérios gerais para avaliação da tecnologia; a segunda (6.2) descreve, em termos de características gerais, quatro famílias de alternativas comumente adotadas; e a terceira (6.3), por sua vez, sintetiza recomendações de orientação geral.

Este Guia adota como premissa que o conteúdo do registro é independente da tecnologia em que ele é mantido. Não obstante, a escolha do instrumento tecnológico afeta significativamente a sustentabilidade do processo, a qualidade dos registros e o esforço de manutenção. A tecnologia adequada é, em regra, aquela que se ajusta ao processo institucional já estabelecido, e não o contrário.

6.1 Critérios para avaliação da tecnologia

Esta seção apresenta um conjunto de critérios que devem ser considerados na escolha do instrumento tecnológico de manutenção do ROPA, ordenados pela centralidade que ocupam em geral nas decisões de órgãos da administração pública federal. Neste sentido, recomenda-se que os seguintes critérios sejam considerados:

- aderência ao conteúdo informacional: a tecnologia deve permitir registrar todas as informações descritas no capítulo 4 deste Guia, com a estrutura adequada (campos com múltiplos valores, vínculos entre registros, indicação de dados sensíveis, anexos);
- usabilidade pelos gestores: o instrumento deve ser preenchível por servidores das unidades. A presença de orientações contextuais (ajuda por campo, exemplos, listas de opções controladas) reduz erros e o custo de suporte;
- suporte à colaboração e ao versionamento: o ROPA é “documento vivo”; a tecnologia deve preservar histórico de versões, permitir trabalho concorrente entre unidades e segregar permissões;
- capacidade de restauração de versões anteriores: requisito particularmente relevante. Recomenda-se que a solução tecnológica adotada preserve não apenas o conteúdo histórico de cada versão (para fins de consulta), mas também a possibilidade de reverter o registro a uma versão anterior, total ou parcialmente, mediante decisão fundamentada;
- capacidade de extração e relatório: o registro deve ser consultável para subsidiar respostas a titulares, ANPD e órgãos de controle. Funcionalidades de filtro, exportação e geração de relatórios reduzem drasticamente o esforço operacional;
- segurança da informação: a própria base do ROPA contém informações relevantes sobre como os dados pessoais são tratados; a tecnologia deve oferecer controles de acesso adequados, registros de auditoria e proteção contra perda;
- sustentabilidade institucional: a manutenção da tecnologia ao longo do tempo deve ser viável com os recursos do órgão, sem dependência crítica de fornecedores únicos ou de servidores específicos;

- interoperabilidade: a tecnologia deve permitir, sempre que possível, integração com outros instrumentos do programa (RIPD, gestão de incidentes, avisos de privacidade) e a exportação em formatos abertos.

6.2 Alternativas tecnológicas: características gerais

As alternativas tecnológicas para manutenção do ROPA podem assumir diferentes formas, variando desde instrumentos simples de registro até plataformas especializadas de governança de privacidade. Cada abordagem apresenta vantagens, limitações e requisitos distintos de implantação e manutenção.

As características descritas nas subseções seguintes representam tendências observadas em cada família de soluções e não devem ser interpretadas como atributos obrigatoriamente presentes em todos os produtos ou ferramentas. O objetivo é fornecer parâmetros para a tomada de decisão institucional, sem prescrever ou excluir tecnologias específicas.

6.2.1 Planilhas e documentos estruturados

Planilhas eletrônicas e documentos estruturados figuram entre as alternativas mais frequentemente adotadas em fases iniciais de implantação do ROPA. Sua principal vantagem reside na baixa barreira de adoção, uma vez que normalmente utilizam ferramentas já disponíveis no ambiente institucional e familiares aos usuários.

Entre suas limitações mais comuns estão a dificuldade de controle de versões, a maior propensão à fragmentação das informações em múltiplos arquivos, a limitação de mecanismos de validação automática e os desafios relacionados à consolidação e consulta dos registros quando há grande volume de informações ou múltiplas unidades participantes. Dependendo da ferramenta utilizada, também podem surgir dificuldades para controlar permissões de acesso, histórico de alterações e fluxos formais de revisão.

Apesar dessas limitações, essa abordagem pode ser adequada para órgãos ou entidades de menor porte, para projetos-piloto ou para fases iniciais de programas de governança em privacidade, especialmente quando acompanhada de procedimentos claros de manutenção e atualização.

6.2.2 Interfaces web próprias

Soluções desenvolvidas especificamente para atender às necessidades do órgão ou entidade permitem elevado grau de aderência aos processos internos e aos requisitos definidos para o ROPA. Entre suas principais vantagens estão a possibilidade de implementação de regras de negócio específicas, fluxos de aprovação, validações automáticas e integrações com sistemas corporativos já existentes.

Por outro lado, essa alternativa normalmente exige investimento em desenvolvimento, manutenção evolutiva, sustentação tecnológica e gestão do ciclo de vida da aplicação. Também pode gerar dependência de equipes internas ou fornecedores especializados e demandar períodos mais longos para levantamento de requisitos, implementação e disponibilização da solução em ambiente produtivo.

Em geral, essa abordagem tende a ser mais atrativa quando o órgão ou entidade já possui requisitos relativamente consolidados e capacidade institucional para sustentar a evolução contínua da ferramenta.

6.2.3 Plataformas low-code/no-code corporativas

Plataformas de desenvolvimento de aplicações com baixo volume de programação podem representar uma alternativa intermediária entre planilhas e soluções desenvolvidas integralmente sob medida. Quando já disponíveis no ambiente corporativo, permitem a criação relativamente rápida de formulários, fluxos de trabalho, painéis gerenciais e mecanismos de validação.

Entre suas vantagens estão a redução do tempo de implantação, a maior flexibilidade para ajustes incrementais e a possibilidade de participação mais direta das áreas de negócio na evolução da solução. Dependendo da plataforma adotada, também podem ser disponibilizados recursos de integração, controle de acesso, automação e geração de relatórios.

Como limitações, destacam-se a dependência da plataforma utilizada, a necessidade de capacitação específica para sua manutenção e evolução, eventuais restrições técnicas impostas pelo ambiente tecnológico e o risco de dependência tecnológica de longo prazo.

6.2.4 Soluções de mercado especializadas

Soluções comerciais voltadas à governança de privacidade frequentemente oferecem funcionalidades integradas para gestão do ROPA, elaboração de RIPDs, gestão de incidentes, atendimento aos titulares e outras atividades relacionadas à conformidade em proteção de dados pessoais.

Entre suas principais vantagens estão a disponibilização de funcionalidades já estruturadas, a incorporação de boas práticas consolidadas de mercado e a possibilidade de utilização de uma plataforma integrada para diferentes processos de governança.

Por outro lado, a adoção dessas soluções pode envolver custos de licenciamento, implantação, customização e suporte. Também deve ser avaliada a aderência do modelo conceitual adotado pela ferramenta às necessidades do órgão ou entidade e ao contexto normativo brasileiro, especialmente quando a solução tiver sido concebida originalmente para outros regimes regulatórios internacionais. No contexto da administração pública, devem ainda ser considerados os requisitos e prazos associados aos processos de contratação e gestão contratual.

Outro aspecto a ser considerado é a curva de aprendizado associada à adoção da solução. Embora plataformas especializadas frequentemente ofereçam funcionalidades avançadas e modelos previamente estruturados, sua utilização eficaz pode demandar capacitação dos usuários responsáveis pelo preenchimento e manutenção dos registros, bem como da equipe responsável pela administração da ferramenta. Dependendo da complexidade da solução adotada, o órgão ou entidade poderá necessitar de recursos dedicados para configuração, parametrização, suporte aos usuários e interlocução com o fornecedor, fatores que devem

ser considerados na avaliação do custo total de propriedade e da sustentabilidade da solução ao longo do tempo.

6.3 Recomendações

A escolha da tecnologia para manutenção do ROPA deve ser orientada pelas necessidades institucionais, pela maturidade do programa de privacidade e pela capacidade de sustentação da solução ao longo do tempo. Independentemente da alternativa adotada, recomenda-se observar as seguintes diretrizes:

- a definição do conteúdo informacional do registro deve preceder a escolha da tecnologia. O órgão ou entidade deve primeiro estabelecer quais informações serão registradas, como serão mantidas e quais processos de governança darão suporte ao ROPA;
- a complexidade da solução tecnológica deve ser proporcional à maturidade do processo institucional e às necessidades efetivas de gestão. Em muitas situações, instrumentos mais simples podem atender adequadamente às necessidades iniciais do programa;
- a solução adotada deve possibilitar a exportação dos registros em formatos abertos ou amplamente utilizados, de modo a preservar a portabilidade das informações e reduzir riscos de dependência tecnológica;
- devem ser considerados, desde a fase de seleção, aspectos relacionados à manutenção evolutiva, sustentabilidade operacional, segurança da informação, gestão de acessos e continuidade do serviço;
- a tecnologia deve atuar como elemento de apoio à governança do processo. A qualidade e a atualização do ROPA dependem fundamentalmente da definição de responsabilidades, da existência de rotinas institucionais e do comprometimento das unidades responsáveis pelos registros.

7 Considerações finais

O registro das operações de tratamento de dados pessoais, previsto no art. 37 da LGPD, constitui mais do que uma obrigação legal. Trata-se de um instrumento fundamental de governança que permite aos agentes de tratamento conhecer, documentar, monitorar e demonstrar como realiza o tratamento de dados pessoais no exercício de suas atribuições. Sua elaboração e manutenção contribuem para a concretização do princípio da responsabilização e prestação de contas previsto no inciso X do art. 6º da LGPD, ao fornecer evidências objetivas das medidas adotadas para assegurar a conformidade com a legislação.

Ao longo deste Guia, buscou-se demonstrar que a efetividade do ROPA depende menos da ferramenta utilizada e mais da existência de processos institucionalizados, responsabilidades claramente definidas, mecanismos de governança adequados e rotinas permanentes de atualização. A qualidade do registro está diretamente relacionada à capacidade do órgão ou entidade de integrar a proteção de dados pessoais aos seus processos de trabalho e às suas estruturas de gestão.

A elaboração e a manutenção do ROPA devem ser compreendidas como atividades contínuas e iterativas. Registros inicialmente incompletos tendem a amadurecer à medida que as unidades aprofundam seu conhecimento sobre os tratamentos realizados e incorporam a proteção de dados pessoais às suas práticas de gestão. Nesse contexto, a revisão periódica do registro não representa uma evidência de falha, mas um elemento natural do processo de melhoria contínua e de prestação de contas.

As correlações apresentadas neste Guia entre o ROPA e outros instrumentos de governança evidenciam que o registro não constitui um fim em si mesmo. As informações nele consolidadas subsidiam atividades como a elaboração de RIPD, a produção de avisos de privacidade, a gestão de riscos, a implementação de medidas de segurança da informação, a gestão de incidentes, o atendimento a demandas de órgãos de controle e da ANPD, entre outras. Quanto maior a qualidade e a atualização do registro, maior tende a ser a eficiência dessas atividades e menor o risco de inconsistências entre diferentes instrumentos de governança.

As orientações apresentadas neste Guia não esgotam o tema. A evolução das atividades do órgão ou entidade, o amadurecimento de seu programa de privacidade e a consolidação das orientações regulatórias e interpretativas poderão demandar revisões periódicas das práticas aqui descritas. Recomenda-se, portanto, que cada órgão ou entidade adapte estas orientações à sua realidade organizacional e formalize suas decisões institucionais – especialmente aquelas relacionadas à governança, às responsabilidades, aos ciclos de revisão e aos instrumentos de apoio – em normativos internos articulados às demais políticas e normas de proteção de dados pessoais e de segurança da informação.

Em última análise, o sucesso do ROPA não deve ser medido pela existência de um documento ou sistema, mas pela capacidade do órgão ou entidade de manter uma visão confiável, atualizada e institucionalizada de seus tratamentos de dados pessoais. É essa capacidade que permite transformar uma obrigação legal em um instrumento efetivo de governança, transparência e proteção dos direitos dos titulares.

8 Referências bibliográficas

[1] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. **Institui o Programa de Privacidade e Segurança da Informação (PPSI 2.0)** no âmbito dos órgãos e entidades integrantes do SISP. Brasília, DF, 2025.

[2] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 mai. 2026.

[3] BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprova o Glossário de Segurança da Informação. Brasília, DF: GSI/PR, 2021.

[4] BRASIL. Agência Nacional de Proteção de Dados. **Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público**. Brasília, DF: ANPD, 2022 (e atualizações).

[5] BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2022.

[6] BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023.

[7] BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

[8] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia do *Framework* de Privacidade e Segurança da Informação** - Programa de Privacidade e Segurança da Informação (PPSI 2.0). Versão 1.2 (e atualizações). Brasília, DF: SGD/MGI, janeiro de 2026.

[9] BRASIL. Agência Nacional de Proteção de Dados. **Formulário de Comunicação de Incidente de Segurança com Dados Pessoais**. Brasília, DF: ANPD (versão vigente).

[10] RYAN, Paul; BRENNAN, Rob. **Support for Enhanced GDPR Accountability with the Common Semantic Model for ROPA (CSM-ROPA)**. SN Computer Science, v. 3, n. 3, p. 224, 2022.

[11] RYAN, Paul; PANDIT, Harshvardhan; BRENNAN, Rob. **A Common Semantic Model of the GDPR Register of Processing Activities**. SN Computer Science, 2020.

[12] PANDIT, Harshvardhan. Simple now, Complex later: **The Questionable Efficacy of Diluting GDPR Article 30(5)**. Social Science Research Network, 2025.

[13] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - **Regulamento Geral sobre a Proteção de Dados** (RGPD/GDPR).

[14] BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024.

[15] BRASIL. Agência Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: ANPD, 2021 (e atualizações).

[16] BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 19, de 23 de agosto de 2024**. Aprova o Regulamento de Transferência Internacional de Dados e conteúdo das cláusulas-padrão contratuais. Brasília, DF: ANPD, 2024.

gov.br

Dúvida?

Entre em contato

conosco

Sítio PPSI:

PPSI 2.0 - Governo Digital