Orientações para Privacidade desde a Concepção

Ministério da Gestão e da Inovação em Serviços Públicos

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Ministra da Gestão e da Inovação em Serviços Públicos
Esther Dweck

Secretaria Executiva
Cristina Kiomi Mori

Secretaria de Serviços Compartilhados
Cilair Rodrigues de Abreu

Diretoria de Gestão Estratégica
Wanessa Queiroz de Souza Oliveira

Coordenação-Geral de Proteção de Dados Pessoais
Luiz Fernando Bastos Coura
Maria Clara Souza Caribé Frutuoso
Andreia Queiroz Correia Dummar
Lucilene Ferreira da Silva Lopes
Julierme Rodrigues da Silva
Mário Jorge Pereira
Simone Gonçalves de Alencar
Sheila Cristina Soares Vieira

Comitê de Privacidade e Proteção de Dados Pessoais

TITULARES	SUBSTITUTOS
Cristina Kiomi Mori	Adauto Modesto Júnior
Luiz Fernando Bastos Coura	Maria Clara Souza Caribé Frutuoso e Andreia Queiroz Correia Dummar
Fernanda Tsunematsu	Miriam Barbuda Fernandes Chaves
Kimberly Coutinho Paes Leme de Castro	Carlos Eduardo Portella Sturm
Rodrigo Morais Lima Delgado	André Luiz Lara Resende Saraiva
Leonardo Rodrigo Ferreira	Marta Juvina de Medeiros
Antonio Fiuza de Sousa Landim	Rogério Mendes Meneguim
Lair Maria de Oliveira	Edi Damasceno Maciel
Gustavo Fernando Frohlich	Luciana de Almeida Toldo
Clauber Teixeira Rodrigues	Ronny Peterson Guimarães
Fabio Valotto	Rudson Pereira Costa da Silva
Alex Pereira de Holanda	Bruno de Freitas Tavares da Silva
Francisco Eduardo de Holanda Bessa	Dilson Gonzaga Pereira Neto
Ana Carolina Quintanilha dos Santos Loriato	Rildo Pereira Peixoto
Érica Bezerra Queiroz	Anderson Moreno Luz

Equipe Técnica de Elaboração
Coordenação-Geral de Proteção de Dados Pessoais – CGPDP/SSC/MGI

Julho de 2025

Histórico de versões

Data	Versão	Descrição	Autor
11/03/2025	v.0.1	Orientações para Privacidade desde a Concepção – Minuta	Equipe Técnica de Elaboração
18/06/2025	v.0.2	Revisão final para envio ao CPDP	Equipe Técnica de Elaboração

Sumário

1 Introdução

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) trouxe novos desafios para empresas e órgãos públicos. Um dos principais é garantir a proteção de dados pessoais em todas as áreas: tecnologia da informação, infraestrutura, processos internos, práticas de negócios e até no *design* de espaços físicos. Essa abordagem é conhecida como ***Privacy by Design***, ou **Privacidade desde a Concepção**.

Esse conceito começou a ser discutido nos anos 1990 pela Dra. **Ann Cavoukian**, ex-Comissária de Informação e Privacidade de Ontário no Canadá. Em 2010, ganhou força ao ser formalmente reconhecido pela comunidade científica na **Resolução sobre *Privacy by Design*** pela comunidade científica.

Com o avanço da tecnologia e os novos riscos à privacidade, essa abordagem se tornou ainda mais importante. Ela mostra que apenas criar leis e políticas não é suficiente – é preciso incorporar a proteção de dados desde o início de qualquer projeto ou iniciativa.

Este documento apresenta **orientações práticas para aplicar a Privacidade desde a Concepção**. O objetivo é ajudar a garantir que a proteção de dados pessoais seja considerada desde o planejamento até o encerramento do ciclo de vida de projetos, políticas públicas e outras ações.

1.1 Motivação

Este documento, chamado **Orientações para a Privacidade desde a Concepção (OPdC)**, integra o **Programa de Governança em Privacidade (PGP)** do Ministério da Gestão e Inovação em Serviços Públicos (MGI). Ele foi elaborado em conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD)** – Lei nº 13.709, de 14 de agosto de 2018 – e aprovado pelo **Comitê de Proteção de Dados Pessoais (CPDP)** do MGI.

A criação do OPdC-MGI atende à ação "**ID 21 - Elaborar Orientações Privacy By Design - MGI**", prevista no Plano de Ações PGP-MGI 2024/2025. Essa ação tem como objetivo apoiar a implementação dos **Controles 24, 25 e 26** do **Guia do Framework de Privacidade e Segurança da Informação**, que tratam de:

- **Controle 24 – Minimização de Dados**: orientar os órgãos a coletar e tratar apenas os dados pessoais estritamente necessários para atingir suas finalidades legais;
- **Controle 25 – Gestão do Tratamento**: garantir que o uso, a retenção e o compartilhamento de dados pessoais sejam limitados ao necessário, com base em propósitos específicos e legítimos; e

- **Controle 26 – Transparência e Acesso**: assegurar que os titulares tenham acesso facilitado às informações sobre o tratamento de seus dados pessoais.

Além disso, o documento contribui para o atendimento ao item 10.1 do autodiagnóstico do TCU sobre a implementação da LGPD nos órgãos públicos.

A importância de considerar a privacidade desde o início também está prevista no **artigo 46 da LGPD**, que estabelece:

> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
> *(...)*
> *§ 2º As medidas de que trata o caput deste artigo **deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução**.* (grifos nossos)

Essas diretrizes reforçam a importância de considerar a privacidade desde o início de qualquer projeto, garantindo que a proteção de dados pessoais seja parte integrante do planejamento e da execução de políticas públicas, sistemas e serviços.

1.1.1 Proteção de dados pessoais como direito fundamental

A proteção de dados pessoais passou a ser reconhecida como um **direito fundamental** na **Constituição Federal de 1988**, com a promulgação da **Emenda Constitucional nº 115**, em 10 de fevereiro de 2022, (BRASIL, 2022) pelo Congresso Nacional.

Com essa mudança, a proteção de dados deixou de ser apenas uma questão de privacidade. Passou a abranger também outros aspectos importantes, como o risco de uso indevido de informações pessoais que possam limitar direitos ou restringir o acesso a serviços. Isso reforça a importância de garantir que os dados pessoais sejam tratados com responsabilidade e segurança, como parte da proteção dos direitos fundamentais de cada cidadão.

1.1.2 Política de Proteção de Dados Pessoais do MGI

A **Política de Proteção de Dados Pessoais** do Ministério da Gestão e da Inovação em Serviços Públicos Instituída pela **Resolução CEPPDP/ME nº 7, de 22 de fevereiro de 2022** (BRASIL. ME, 2022a). Essa política define os deveres e responsabilidades do órgão em relação à proteção de dados pessoais.

Entre os principais pontos, destacam-se os seguintes deveres do Ministério, quando atua como **controlador** de dados:

- **Art. 6º, inciso I** - observar os fundamentos, princípios de proteção de dados e os deveres impostos ao controlador pela Lei nº 13.709, de 2018, e pela legislação correlata, **ao decidir sobre um futuro tratamento** ou realizá-lo;
- **Art. 6º, inciso IV** - Adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais sob sua responsabilidade, desde a fase de concepção até a execução de produtos ou serviços.

Quando o Ministério atua como **operador** de dados, também deve cumprir obrigações específicas, como:

- **Art. 7º, inciso IV** - Observar os princípios definidos no art. 6º da LGPD e os deveres atribuídos ao operador durante o tratamento de dados pessoais.

Essas diretrizes reforçam o compromisso institucional com a proteção de dados pessoais em todas as etapas dos processos e serviços públicos, alinhando-se aos princípios da LGPD e à abordagem de **Privacidade desde a Concepção**.

2 Objetivo

Este documento foi desenvolvido para apoiar as unidades organizacionais do **Ministério da Gestão e da Inovação em Serviços Públicos (MGI)** na implementação de boas práticas de **tratamento de dados pessoais**. Ele serve como referência para projetos internos, criação de novos serviços, adaptação de processos de trabalho ou qualquer outra iniciativa que envolva o uso de informações pessoais.

Sua elaboração teve como base o **Guia sobre Privacidade desde a Concepção e por Padrão** (BRASIL, 2024) da **Secretaria de Governo Digital (SGD)**, além da primeira versão lançada pela antiga **Resolução CEPPDP/ME nº 04/2022** (BRASIL. ME, 2022b) e publicações da **OCDE** (2023) e da **Autoridade Nacional de Proteção de Dados (ANPD)** (BRASIL. ANPD, 2024). Seu objetivo não é esgotar o tema, mas **difundir tecnologias e metodologias** capazes de aprimorar a proteção dos dados pessoais, promovendo a **Privacidade desde a Concepção**.

3 Definições

Para facilitar a aplicação das orientações apresentadas neste documento, é importante compreender alguns termos fundamentais:

Agentes de tratamento: o controlador e o operador (LGPD, Art. 5º, IX).

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (LGPD, Art. 5º, XI).

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade (Instrução Normativa GSI/PR nº 93/2021).

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, acessível e escrito em linguagem clara e simples (Resolução CEPPDP/ME nº 7, de 22 de fevereiro de 2022, Art. 2º, XVII).

Confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados (Instrução Normativa GSI/PR nº 93/2021).

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (LGPD, Art. 5º, VI).

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável (LGPD, Art. 5º, I).

Disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados (Instrução Normativa GSI/PR nº 93/2021).

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (Lei nº 13.709/2018).

Integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental (Instrução Normativa GSI/PR nº 93/2021).

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, Art. 5º, VII).

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (LGPD, Art. 13, § 4º).

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (LGPD, art. 6º, VII).

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de

tratamento (LGPD, Art. 5º, V).

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

Unidade responsável ou Unidade: unidade organizacional do MGI gestora do serviço ou sistema ofertado ao titular.

Usuário: pessoa física ou jurídica que pode fazer uso individual do serviço (Portaria SGD nº 548, de 24 de janeiro de 2022, art. 2º, inciso I).

4 Privacidade desde a Concepção (PdC)

A **Lei Geral de Proteção de Dados Pessoais (LGPD)** determina que devem ser adotadas medidas preventivas para evitar danos decorrentes do tratamento de dados pessoais. Isso significa que os riscos devem ser identificados e mitigados **antes mesmo do início do tratamento**.

Nesse contexto, aplica-se o conceito de **Privacidade desde a Concepção (PdC)** — do inglês *Privacy by Design (PbD)* — desenvolvido por **Ann Cavoukian** na década de 1990 Esse conceito surgiu como uma resposta aos desafios trazidos pelos avanços das tecnologias da informação e comunicação e pelo uso crescente de dados pessoais em larga escala.

Em 2009, Cavoukian consolidou a abordagem em seu artigo intitulado “The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices” (CAVOUKIAN, 1990). No ano seguinte, em 2010, esses princípios foram reconhecidos como um componente essencial da proteção da privacidade durante a 32ª Conferência Internacional de Comissários de Privacidade e Autoridades de Proteção de Dados(“Resolution on Privacy by Design”, 2010).

Para alcançar o objetivo de tornar a proteção da privacidade um elemento essencial e integrado aos processos, a PdC se baseia em sete princípios fundamentais, que serão detalhados nas subseções 6.1 a 6.7 deste documento.

5 Princípios de PdC, LGPD e FIPP

Para compreender melhor a abordagem da **Privacidade desde a Concepção (PdC)**, é útil relacionar seus princípios não apenas aos previstos no **art. 6º da LGPD**, mas também

aos **Princípios das Práticas de Informações Justas**, conhecidos como *Fair Information Practices Principles (**FIPP**)* (GELLMAN, 2014).

Os FIPPs surgiram a partir de estudos estudos realizados na década de 1970 e propõem um conjunto de boas práticas para proteger a privacidade de indivíduos cujos dados são processados por sistemas automatizados. Essa abordagem foi formalizada pela **Organização para a Cooperação e Desenvolvimento Econômico (OCDE)** em 1980, por meio da publicação de **oito princípios** voltados à coleta, uso e proteção de dados pessoais.

Embora os FIPPs não façam parte de uma legislação específica, eles influenciaram significativamente diversas leis de proteção de dados ao redor do mundo — especialmente nos Estados Unidos — e continuam sendo uma referência importante para a construção de políticas e práticas de privacidade.

5.1 Princípios da Privacidade desde a Concepção (PdC)

5.1.1 Primeiro princípio - Proativo e não reativo; preventivo e não corretivo

O primeiro princípio da **Privacidade desde a Concepção (PdC)** enfatiza a importância de adotar uma postura proativa e preventiva, em vez de reativa e corretiva. Isso significa **agir antes que ocorram incidentes de privacidade**, buscando evitar ou reduzir ao máximo os riscos.

A PdC não se propõe a oferecer soluções para lidar com violações já ocorridas, como resposta, contenção ou recuperação. Seu foco está em **evitar que os riscos se concretizem**.

Para aplicar esse princípio, é essencial que o **MGI** reconheça o valor de práticas de privacidade sólidas, adotadas de forma antecipada e consistente pelos responsáveis por processos e serviços que envolvam dados pessoais. Isso envolve:

Comprometimento da alta gestão, com o estabelecimento e a aplicação de padrões elevados de privacidade;

Engajamento das equipes e partes interessadas, promovendo uma cultura organizacional voltada à melhoria contínua;

Uso de métodos estruturados para identificar projetos com falhas de privacidade, antecipar práticas inadequadas e corrigir impactos potenciais antes que se tornem problemas reais — de forma sistemática, inovadora e preventiva.

Exemplos práticos de aplicação desse princípio incluem:

- Projetar sistemas que **evitem a coleta de dados desnecessários**;
- Implementar **medidas de segurança desde o início** do desenvolvimento de sistemas e serviços;
- Adotar **políticas de retenção de dados** que excluam automaticamente informações após um período definido.

5.1.2 Segundo princípio - Privacidade por padrão

Esse princípio estabelece que **proteção dos dados pessoais** deve ser garantida por padrão, ou seja, independentemente de qualquer ação do titular. Em qualquer sistema de tecnologia da informação ou prática de negócios do MGI, a privacidade deve estar incorporada desde o início.

Para cumprir esse princípio, é essencial que:

- As **finalidades do tratamento de dados** sejam claras, específicas e compatíveis com o contexto;
- Essas finalidades sejam **comunicadas ao titular** antes ou no momento da coleta dos dados.

Dessa forma, recomenda-se:

a. **Limitação da coleta**

Coletar apenas os dados **estritamente necessários** e **autorizados por lei ou regulamento**.

b. **Minimização de dados**

Evitar a coleta de dados excessivos. Deve-se coletar somente o mínimo necessário para cumprir a finalidade informada.

c. **Limitação de uso, retenção e divulgação:**

1. Usar os dados **apenas para a finalidade informada ao titular**;
2. **Eliminar os dados** quando não forem mais necessários; e
3. **Evitar o compartilhamento** dos dados, salvo quando for indispensável para atingir a finalidade para a qual foram coletados.

d. **Segurança**

Adotar medidas técnicas e organizacionais adequadas para garantir a **autenticidade**, **confidencialidade**, **integridade** e **disponibilidade** dos dados pessoais.

Além disso, o armazenamento dos dados deve ocorrer **somente pelo tempo necessário** para cumprir a finalidade declarada. Após esse período, os dados devem ser eliminados de forma segura.

Por fim, recomenda-se que as **configurações padrão dos sistemas e serviços priorizem a proteção da privacidade**, limitando ao máximo a exposição dos dados pessoais.

5.1.3 Terceiro princípio - Privacidade incorporada ao projeto

Este princípio estabelece que a privacidade deve ser incorporada desde o início do desenvolvimento de qualquer sistema, serviço ou processo. Ela deve estar presente na **arquitetura dos sistemas de TI** e nas **práticas de negócios**, sendo um componente essencial desde a concepção de novos projetos.

Ou seja, **não se deve esperar** que a privacidade seja integrada em etapas posteriores, como durante a execução do projeto ou após sua entrada em operação.

Essa incorporação deve ser feita de forma:

Holística

- Contextos adicionais e mais amplos devem sempre serem considerados

Integrativa

- Todas as partes interessadas devem ser consultadas

Criativa

- Incorporar privacidade pode significar reinventar as escolhas existentes visto as alternativas não se mostrarem adequadas

Para aplicar esse princípio, recomenda-se:

- Adotar uma **abordagem sistemática**, baseada em **padrões reconhecidos**, que permita revisões e auditorias externas;
- Realizar **avaliações de impacto e risco à privacidade**, sempre que necessário, documentando os riscos identificados e as medidas adotadas para mitigá-los;
- Garantir que os impactos à privacidade sejam **minimizados desde o início** e que não possam ser facilmente comprometidos por erros de configuração, uso inadequado ou falhas operacionais.

5.1.4 Quarto princípio - Funcionalidade total ou funcionalidade integral

Este princípio defende que **privacidade e funcionalidade não devem ser vistas como opostas**, mas sim como elementos que podem e devem coexistir. A abordagem da **Privacidade desde a Concepção (PdC)** propõe que os interesses legítimos de todas as partes envolvidas — tanto do MGI quanto dos titulares dos dados — sejam atendidos de forma equilibrada.

Em vez de tratar a privacidade como um obstáculo à eficiência ou à inovação, a PdC promove uma **solução de soma positiva**, em que é possível **garantir a privacidade sem comprometer a funcionalidade** dos sistemas, serviços ou processos.

A aplicação desse princípio implica:

- **Evitar conflitos entre privacidade e segurança**, buscando soluções que atendam a ambos os objetivos;
- **Projetar tecnologias e processos** que incorporem a privacidade sem limitar sua eficácia;
- **Otimizar todos os requisitos relevantes**, garantindo que a privacidade seja um valor agregado e não um custo.

A PdC, portanto, atua como uma **facilitadora dupla**: protege os direitos dos titulares e, ao mesmo tempo, permite que o MGI alcance resultados práticos, eficientes e benéficos para todos os envolvidos.

5.1.5 Quinto princípio - Segurança de ponta a ponta

Este princípio reforça que a **segurança deve estar presente em todas as etapas do ciclo de vida dos dados pessoais** — desde a coleta e o processamento até o arquivamento e a eliminação. A proteção deve ser contínua, ou seja, **de ponta a ponta**.

A aplicação de medidas de segurança robustas é essencial para garantir a privacidade. Isso inclui a **análise de riscos**, a definição de controles adequados e a eliminação segura dos dados após o cumprimento de suas finalidades.

O **MGI** deve assumir a responsabilidade pela segurança dos dados pessoais, adotando medidas proporcionais ao grau de sensibilidade das informações e alinhadas a **normas e padrões reconhecidos**. Essas medidas devem assegurar a **autenticidade, confidencialidade, integridade e disponibilidade** dos dados ao longo de todo o tratamento.

Entre os métodos recomendados, destacam-se:

- Registro e controle de acesso;

- Criptografia de dados pessoais sensíveis;
- Anonimização e pseudonimização;
- Eliminação segura dos dados.

Como destacou Ann Cavoukian (2009): “a ausência de medidas técnicas de segurança é um impeditivo para que a privacidade seja fomentada”. Ou seja, privacidade e segurança são inseparáveis — uma depende da outra para garantir a proteção efetiva dos dados pessoais dos titulares.

5.1.6 Sexto princípio - Visibilidade e transparência

Este princípio destaca a importância de **garantir transparência e visibilidade desde a concepção** de qualquer sistema ou processo que envolva o tratamento de dados pessoais. A ideia central é assegurar que todos os envolvidos — titulares, gestores e demais partes interessadas — sejam informados de forma clara e acessível sobre como os dados estão sendo tratados.

A **Privacidade desde a Concepção (PdC)** busca garantir que as práticas de negócios e as tecnologias adotadas estejam alinhadas com os compromissos e objetivos declarados, promovendo confiança e responsabilização (CAVOUKIAN, 2009).

Para aplicar esse princípio, é essencial que:

- As **políticas e procedimentos de privacidade** sejam documentados, comunicados e de fácil acesso;
- Ao compartilhar dados com terceiros, sejam adotadas **medidas formais de proteção**, como contratos ou acordos específicos;
- Os **titulares tenham acesso às informações** sobre como seus dados são tratados, incluindo canais para manifestação e solicitação de direitos;
- A unidade responsável pelo tratamento estabeleça **mecanismos de monitoramento, avaliação e verificação da conformidade** com as políticas de privacidade.

A **abertura e a transparência** são fundamentais para a prestação de contas e para fortalecer a confiança dos titulares no tratamento de seus dados pessoais.

5.1.7 Sétimo princípio - Respeito pela privacidade do usuário

O último princípio da **Privacidade desde a Concepção (PdC)** reforça que os **interesses e direitos dos titulares de dados devem estar no centro de todas as decisões**. Isso significa adotar padrões elevados de privacidade, fornecer avisos claros e acessíveis,

e garantir interfaces fáceis de usar.

Os melhores resultados da PdC são alcançados quando os sistemas, serviços e processos são **conscientemente projetados em torno das necessidades e expectativas dos usuários** — os titulares dos dados pessoais (CAVOUKIAN, 2009).

Esse respeito se estende a todos os pontos de contato com o titular, incluindo:

- **Interfaces centradas no usuário**, que permitam decisões de privacidade de forma clara, simples e confiável;
- **Operações de negócios e arquiteturas físicas** que demonstrem o mesmo nível de consideração e cuidado com os direitos dos titulares;
- **Mecanismos que empoderem os titulares**, permitindo que tenham controle ativo sobre seus dados e possam gerenciar suas preferências de forma autônoma.

Ao colocar o titular no centro das operações, o MGI fortalece a confiança, reduz riscos e contribui para a prevenção de abusos e usos indevidos de dados pessoais.

5.1.8 Resumo dos princípios da PdC

Em resumo, o foco dos princípios da PdC são:

1. **Prevenção e proatividade** – evitar riscos antes que ocorram;
2. **Privacidade por padrão** – garantir proteção automática dos dados;
3. **Privacidade incorporada ao projeto** – integrar a privacidade desde a concepção, de forma holística, integrativa e criativa;
4. **Funcionalidade total** – equilibrar privacidade e funcionalidade, promovendo soluções de soma positiva que beneficiem tanto os titulares quanto a organização;
5. **Segurança de ponta a ponta** – aplicar medidas de segurança em todas as fases do ciclo de vida dos dados, desde a coleta até a eliminação;
6. **Visibilidade e transparência** – assegurar clareza, prestação de contas e acesso às informações sobre o tratamento de dados pessoais; e
7. **Respeito pela privacidade do usuário** – colocar o titular no centro das decisões, com interfaces acessíveis e mecanismos que permitam o controle sobre seus próprios dados.

5.2 Fundamentos e Princípios da LGPD

Embora existam diferenças conceituais entre os **princípios da Privacidade desde a**

Concepção (PdC), da **LGPD** e dos **Princípios das Práticas de Informações Justas (FIPPs)**, todos compartilham um objetivo comum: **garantir o direito à privacidade** e **à proteção dos dados pessoais**.

A LGPD, em seu artigo 2º, estabelece que a disciplina da proteção de dados pessoais se fundamenta nos seguintes pilares:

I – O respeito à privacidade - Reconhecimento da privacidade como um direito fundamental, que deve ser protegido em todas as atividades que envolvam o tratamento de dados pessoais.

II – A autodeterminação informativa - Direito de cada pessoa de controlar suas próprias informações, decidindo como, quando e por quem seus dados pessoais podem ser utilizados.

III – A liberdade de expressão, de informação, de comunicação e de opinião - Garantia de que a proteção de dados não será usada como justificativa para restringir direitos fundamentais relacionados à livre manifestação de ideias e informações.

IV – A inviolabilidade da intimidade, da honra e da imagem - Proteção contra o uso indevido de dados que possam afetar a vida privada, a reputação ou a imagem dos indivíduos.

V – O desenvolvimento econômico e tecnológico e a inovação - Promoção de um ambiente regulatório que incentive o uso responsável de dados pessoais, sem impedir o avanço tecnológico e a inovação.

VI – A livre iniciativa, a livre concorrência e a defesa do consumidor - Equilíbrio entre a proteção de dados e a liberdade econômica, assegurando também os direitos dos consumidores no uso de seus dados.

VII – Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais - Afirmação de que a proteção de dados está diretamente ligada à valorização da dignidade humana e ao pleno exercício da cidadania.

Os princípios da LGPD estão definidos no **art. 6º da Lei nº 13.709/2018** e devem ser observados em todas as atividades de tratamento de dados pessoais. Além da boa-fé, a LGPD estabelece os seguintes princípios:

5.2.1 Princípio da Finalidade

O tratamento deve ter **propósitos legítimos, específicos, explícitos e informados ao titular**, sem possibilidade de uso posterior de forma incompatível com essas

finalidades.

(LGPD, Art. 6º, I)

5.2.2 Princípio da Adequação

O tratamento deve ser **compatível com as finalidades informadas ao titular**, considerando o contexto em que os dados foram coletados.

(LGPD, Art. 6º, II)

5.2.3 Princípio da Necessidade

O tratamento deve se limitar ao **mínimo necessário** para atingir suas finalidades, com dados pertinentes, proporcionais e não excessivos.

(LGPD, Art. 6º, III)

5.2.4 Princípio do Livre Acesso

Os titulares devem ter **acesso facilitado e gratuito** às informações sobre a forma, duração e integralidade do tratamento de seus dados.

(LGPD, Art. 6º, IV)

5.2.5 Princípio da Qualidade dos Dados

Garante ao titular a **exatidão, clareza, relevância e atualização** dos dados, conforme a necessidade e a finalidade do tratamento.

(LGPD, Art. 6º, V)

5.2.6 Princípio da Transparência

As informações sobre o tratamento devem ser **claras, precisas e acessíveis**, respeitando os segredos comercial e industrial.

(LGPD, Art. 6º, VI)

5.2.7 Princípio da Segurança

Devem ser adotadas **medidas técnicas e administrativas** para proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas.

(LGPD, Art. 6º, VII)

5.2.8 Princípio da Prevenção

Devem ser adotadas **ações preventivas** para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais.

(LGPD, Art. 6º, VIII)

5.2.9 Princípio da Não Discriminação

É vedado o tratamento de dados para **fins discriminatórios, ilícitos ou abusivos**.

(LGPD, Art. 6º, IX)

5.2.10 Princípio da Responsabilização e Prestação de Contas

O agente de tratamento deve **demonstrar a adoção de medidas eficazes** para garantir o cumprimento da LGPD e a eficácia dessas medidas.

(LGPD, Art. 6º, X)

5.3 Princípios das Práticas de Informação Justas (FIPP)

Os **Princípios das Práticas de Informação Justas**, conhecidos como **FIPPs**, ou *Fair Information Practices Principles* (Gellman, 2022), foram desenvolvidos como um conjunto de boas práticas para proteger a privacidade de indivíduos em sistemas que tratam dados pessoais. A seguir, estão os oito princípios, com explicações simplificadas:

5.3.1 Princípio da Limitação de Coleta

A coleta de dados pessoais deve ter limites. Os dados devem ser obtidos de forma legal, justa e, sempre que possível, com o conhecimento ou consentimento da pessoa.

5.3.2 Princípio da Qualidade dos Dados

Os dados coletados devem ser relevantes para a finalidade pretendida e, sempre que necessário, devem estar corretos, completos e atualizados.

5.3.3 Princípio da Especificação da Finalidade

As finalidades para as quais os dados são coletados devem ser informadas no momento da coleta. O uso posterior deve estar de acordo com essas finalidades ou com outras compatíveis.

5.3.4 Princípio da Limitação de Uso

Os dados pessoais não devem ser usados ou compartilhados para outras finalidades além daquelas informadas, a menos que haja consentimento do titular ou obrigação legal.

5.3.5 Princípio das Salvaguardas de Segurança

Os dados devem ser protegidos contra riscos como perda, acesso não autorizado, uso indevido ou divulgação indevida, por meio de medidas de segurança adequadas.

5.3.6 Princípio da Abertura

As organizações devem manter políticas claras e acessíveis sobre como os dados são tratados. As pessoas devem poder saber quais dados estão sendo coletados,

para que são usados e quem é o responsável por eles.

5.3.7 Princípio da Participação Individual

As pessoas devem ter o direito de:

- Saber se seus dados estão sendo tratados;
- Acessar essas informações de forma clara e acessível;
- Contestar decisões ou negar acesso, com justificativa;
- Corrigir ou excluir dados incorretos.

5.3.8 Princípio da Responsabilidade

Quem trata os dados deve ser responsável por seguir todos os princípios acima e demonstrar que está em conformidade com essas práticas.

6 Metas de Proteção de Privacidade

As metas de proteção de privacidade são objetivos que ajudam a garantir que os dados pessoais sejam tratados com segurança e respeito. Elas servem como base para planejar e construir sistemas e serviços que protejam a privacidade das pessoas.

Essas metas se dividem em dois grupos principais: de segurança e de privacidade.

6.1 Metas de Segurança

Essas metas vêm da área de segurança da informação e ajudam a proteger os dados contra acessos indevidos, perdas ou alterações:

- **Confidencialidade**: Garante que só pessoas autorizadas possam acessar os dados.
- **Integridade**: Garante que os dados não sejam alterados de forma indevida.
- **Disponibilidade**: Garante que os dados estejam acessíveis quando forem necessários.

6.2 Metas Específicas de Privacidade

Essas metas foram criadas especialmente para proteger a privacidade dos titulares de dados:

- **Desvinculação:** Evita que os dados de uma pessoa sejam ligados a outras informações que possam identificá-la. Isso ajuda a impedir a criação de perfis detalhados sem necessidade.
- **Transparência:** Garante que as pessoas saibam como seus dados estão sendo usados, por quem e com qual finalidade.
- **Possibilidade de Intervenção:** Permite que as pessoas tenham controle sobre seus dados, podendo corrigi-los, excluí-los ou pedir explicações sobre o tratamento.

Essas metas estão diretamente ligadas aos princípios da LGPD, como finalidade, necessidade, segurança, qualidade dos dados, transparência e responsabilização.

A tabela a seguir correlaciona as metas de proteção de privacidade com os princípios estabelecidos na LGPD.

Metas de Proteção de Privacidade		
Desvinculação	**Transparência**	**Intervenção**
• Adequação; • Finalidade; • Necessidade; • Prevenção; • Segurança.	• Livre acesso; • Transparência; • Não discriminação.	• Qualidade dos dados; • Responsabilização e prestação de contas.

7 Estratégias de Privacidade

As estratégias de privacidade são formas práticas de alcançar as metas de proteção de privacidade. Enquanto as metas definem o que se deseja proteger — como a confidencialidade, a transparência e o controle pelos titulares — as estratégias mostram como isso pode ser feito na prática, desde o início do desenvolvimento de sistemas e serviços. Elas ajudam a garantir que a privacidade seja respeitada em todas as etapas do tratamento de dados.

Segundo o **Guia sobre Privacidade desde a Concepção e por Padrão** da Secretaria de Governo Digital (SGD), essas estratégias se dividem em dois grupos: **orientadas a dados** e **orientadas a processos**.

7.1 Estratégias Orientadas a dados

Essas estratégias buscam reduzir a coleta e o uso excessivo de dados pessoais,

diminuindo os riscos para os titulares. Elas estão diretamente ligadas às metas de desvinculação e segurança, e aos princípios da necessidade e qualidade dos dados da LGPD. São quatro:

- **Minimizar**: Coletar e usar apenas os dados realmente necessários para cumprir a finalidade do serviço. Isso evita riscos desnecessários.
- **Ocultar**: Proteger os dados contra acessos indevidos, usando técnicas como criptografia, ofuscação e anonimização.
- **Separar**: Guardar os dados em locais diferentes ou tratá-los de forma isolada, para dificultar a criação de perfis completos de uma pessoa.
- **Agregar**: Usar dados agrupados (por exemplo, por região ou faixa etária) em vez de dados individuais, sempre que possível.

Essas estratégias estão ligadas aos princípios da LGPD, como necessidade, segurança, prevenção e qualidade dos dados.

7.2 Estratégias Orientadas a Processos

Essas estratégias tratam da forma como os dados são usados, com foco na transparência, no controle pelos titulares e na responsabilidade dos órgãos. Elas estão ligadas às metas de transparência e intervenção, e aos princípios da LGPD como responsabilização, prestação de contas e livre acesso. Incluem:

- **Informar:** Garantir que as pessoas saibam, de forma clara e acessível, como seus dados estão sendo usados, por quem e com qual finalidade.
- **Controlar:** Permitir que os titulares escolham o que pode ser feito com seus dados, como dar ou retirar consentimento, corrigir informações ou pedir a exclusão.
- **Impor:** Criar e aplicar regras internas que garantam o uso correto dos dados, de acordo com a LGPD.
- **Demonstrar:** Ter registros e provas de que as regras estão sendo seguidas, como relatórios, auditorias e políticas de privacidade.

8 Técnicas de Privacidade

As técnicas de privacidade são ferramentas práticas que ajudam a colocar em ação as estratégias e metas de proteção de dados. Elas são aplicadas no desenvolvimento e na operação de sistemas e serviços para garantir que os dados pessoais sejam tratados com segurança e respeito à privacidade.

A seguir, trazemos uma síntese das principais técnicas de privacidade descritas no **Guia sobre Privacidade desde a Concepção e por Padrão** da Secretaria de Governo Digital (SGD):

8.1 Autenticação

Verifica se a pessoa que está acessando um sistema é realmente quem diz ser. Pode ser

feita com senhas, biometria ou autenticação em duas etapas. Isso evita acessos indevidos aos dados.

8.2 Credenciais baseadas em atributos

Permitem que uma pessoa comprove uma informação (como idade ou vínculo com uma instituição) sem precisar revelar sua identidade completa. Isso reduz a exposição de dados.

8.3 Comunicações privadas seguras

Usam criptografia para proteger as informações trocadas entre sistemas ou pessoas. Isso impede que terceiros vejam ou alterem os dados durante a transmissão.

8.4 Anonimato e pseudônimo nas comunicações

Essas técnicas escondem quem está se comunicando com quem, protegendo os chamados metadados (como horário, localização e frequência de contatos). Isso evita rastreamentos e perfis indesejados.

8.5 Privacidade em banco de dados

Inclui métodos como:

- Supressão de informações sensíveis;
- Restrições de consulta;
- Mascaramento de dados;
- Geração de dados sintéticos.

Essas técnicas evitam que dados pessoais sejam acessados ou usados de forma indevida.

8.6 Privacidade de armazenamento

Garante que os dados guardados em servidores, nuvens ou dispositivos estejam protegidos contra acessos não autorizados, perdas ou alterações. Pode incluir criptografia, controle de acesso e destruição segura dos dados quando não forem mais necessários.

8.7 Cálculos que preservam a privacidade

Permitem fazer análises e cálculos com os dados sem revelar informações pessoais. Exemplos:

- Criptografia homomórfica;
- Privacidade diferencial;

- Computação multipartidária segura;
- Aprendizado federado.

Essas técnicas são úteis em pesquisas, estatísticas e inteligência artificial.

8.8 Técnicas de transparência

Ajudam os titulares a entenderem como seus dados estão sendo usados. Um exemplo são os painéis de privacidade, que mostram quais dados foram coletados, com quem foram compartilhados e permitem que a pessoa exerça seus direitos.

8.9 Técnicas de intervenção

Permitem que os titulares tenham controle sobre seus dados, como corrigir informações, pedir exclusão ou retirar consentimento. Essas técnicas devem ser apoiadas por sistemas que facilitem o acesso e a gestão dos dados pessoais.

9 Incorporação da Segurança e Privacidade em projetos

Ao longo deste documento, vimos como as metas de proteção de privacidade — como a confidencialidade, a desvinculação, a transparência e a possibilidade de intervenção — podem ser alcançadas por meio de estratégias bem definidas e técnicas aplicáveis desde a concepção de projetos. No entanto, para que essas metas e estratégias saiam do papel e se tornem realidade nos sistemas e serviços, é essencial contar com ferramentas tecnológicas que viabilizem sua implementação de forma eficaz, segura e escalável.

É nesse contexto que surgem as Tecnologias de Aprimoramento da Privacidade, conhecidas como PETs (Privacy Enhancing Technologies). Essas tecnologias atuam como facilitadoras da privacidade desde a concepção, oferecendo soluções técnicas que permitem aplicar, reforçar e automatizar os princípios da LGPD, da PdC e das FIPPs ao longo de todo o ciclo de vida dos dados. Elas ajudam a operacionalizar estratégias como minimizar, ocultar, separar e agregar, e viabilizam técnicas como anonimização, criptografia, controle de acesso, entre outras.

Mais do que ferramentas isoladas, as PETs representam uma abordagem integrada para fortalecer a proteção de dados pessoais, especialmente em um cenário de crescente complexidade tecnológica e exigências regulatórias. A seguir, exploraremos os principais tipos de PETs, suas aplicações e como podem ser utilizadas de forma estratégica para garantir a privacidade em projetos, serviços e políticas públicas.

9.1 Tecnologias de Aprimoramento da Privacidade (“PETs”)

As **Tecnologias de Aprimoramento da Privacidade** — conhecidas pela sigla em inglês **PETs (*Privacy-Enhancing Technologies*)** — surgiram como uma resposta ao desafio de

equilibrar **inovação tecnológica e proteção da privacidade** no tratamento de dados pessoais.

As PETs consistem em um conjunto de **técnicas e abordagens técnicas** que permitem a implementação de políticas de privacidade de forma mais proativa e eficaz. Elas possibilitam a **coleta, análise e processamento de dados** com maior segurança, protegendo tanto os dados pessoais quanto a privacidade dos titulares e informações sensíveis (OECD, 2023).

Segundo o **Guia sobre Privacidade desde a Concepção e por Padrão** da **Secretaria de Governo Digital (SGD)**, as PETs são definidas como:

"Um grupo organizado e coerente de soluções de TIC que reduzem os riscos de privacidade por meio da implementação de estratégias e padrões de projeto de privacidade previamente definidos, com tecnologia concreta, sem perda das funcionalidades do sistema de informação."

A adoção dessas tecnologias está alinhada aos **oito princípios das Práticas de Informações Justas (FIPPs)**, originalmente propostos pela OCDE para proteger os dados pessoais tratados por sistemas automatizados. Como vimos anteriormente, esses princípios também influenciaram legislações modernas e continuam sendo referência global.

Além disso, a LGPD impõe ao controlador a responsabilidade de adotar **medidas técnicas e administrativas adequadas** para proteger os dados pessoais. Nesse sentido, as PETs oferecem **estratégias práticas** para incorporar a privacidade diretamente nos sistemas e serviços, em conformidade com os princípios da **Privacidade desde a Concepção (PdC)**.

A aplicação das PETs deve ser pensada de forma **sistemática e baseada em riscos**, abrangendo todo o ciclo de vida dos sistemas de informação. Isso inclui desde o planejamento e desenvolvimento até a operação e descarte de dados, garantindo que a privacidade esteja integrada desde o início.

Como destacado no **quinto princípio da PdC — segurança de ponta a ponta**, a ausência de medidas técnicas adequadas compromete a efetividade da privacidade. Por isso, a segurança deve ser tratada como um elemento transversal, presente em todas as etapas e decisões relacionadas ao tratamento de dados.

Nesse contexto, as PETs se tornam ferramentas essenciais não apenas para o desenvolvimento de **sistemas tecnológicos**, mas também para aplicações mais complexas, como aquelas baseadas em **inteligência artificial (IA)**.

Para apoiar a implementação de padrões concretos de privacidade, a **OCDE propõe quatro categorias de PETs**, que serão apresentadas a seguir. Essas categorias também se alinham às **estratégias de privacidade** descritas no guia da SGD, como **minimizar**, **ocultar**, **separar** e **agregar**, que orientam a aplicação técnica das metas de proteção de privacidade.

Nota: Para enriquecer o presente documento com entendimentos atualizados, foram utilizados trechos do Estudo Preliminar da Autoridade Nacional de Proteção de Dados (ANPD) sobre Anonimização e Pseudonimização (ANPD, 2023), ainda sujeito a alterações. Recomenda-se o acompanhamento das futuras versões oficiais do documento, a fim de garantir alinhamento com as orientações mais recentes da ANPD.

9.2 Primeira Categoria de PETs: Ferramentas de Ofuscação de Dados

As **ferramentas de ofuscação de dados** são um grupo de tecnologias que alteram os dados para proteger a privacidade das pessoas. Elas funcionam adicionando ruído, removendo informações identificáveis ou processando os dados localmente — por exemplo, no próprio celular da pessoa, sem enviá-los para a nuvem (OECD, 2023).

Essas técnicas ajudam a proteger os dados pessoais e permitem que eles sejam usados com menor risco de exposição. A seguir, apresentamos as principais ferramentas dessa categoria.

9.2.1 Anonimização de Dados

Segundo o **estudo preliminar da ANPD (2023)**, a anonimização deve ser entendida como um **processo contínuo e baseado em riscos**, e não como uma técnica única ou definitiva. Isso significa que:

- A anonimização **não garante risco zero** de reidentificação.
- O processo deve considerar o **contexto do tratamento**, a **finalidade dos dados**, e o **nível aceitável de risco**.
- A **reversibilidade** da anonimização pode ocorrer com o tempo, à medida que novas tecnologias e dados auxiliares se tornam disponíveis.

A LGPD estabelece que dados anonimizados **não são considerados dados pessoais**, exceto se o processo puder ser revertido com **meios próprios** ou com **esforços razoáveis** (art. 12). A ANPD esclarece que:

- **Meios próprios** são os recursos disponíveis ao próprio agente de tratamento.
- **Esforços razoáveis** envolvem uma análise objetiva de custo, tempo e viabilidade técnica para reverter a anonimização.

Entre as técnicas mais comuns de anonimização, destacam-se:

- **Generalização:** substituição de valores específicos por categorias amplas (ex: idade exata por faixa etária).
- **Supressão:** remoção de atributos ou registros.
- **Adição de ruído:** alteração de valores numéricos para dificultar a identificação.
- **Permutação:** embaralhamento de dados entre registros.
- **K-anonimização:** garantia de que cada registro seja indistinguível de pelo menos outros K-1 registros.

A escolha da técnica deve considerar o equilíbrio entre utilidade dos dados e nível de anonimização, conforme ilustrado no próprio guia da ANPD.

9.2.2 Pseudonimização de Dados

A pseudonimização, conforme o artigo 13, § 4º da LGPD, é o processo de separar

informações que podem identificar uma pessoa das demais informações. Os dados identificáveis são mantidos em um ambiente seguro e separado.

A pseudonimização substitui dados identificáveis por códigos ou pseudônimos. Diferente da anonimização, os dados ainda podem ser reidentificados se forem combinados com informações adicionais mantidas separadamente.

Essa técnica reduz o risco de exposição direta e é reconhecida pela LGPD como uma medida de segurança útil, mas os dados pseudonimizados continuam sendo considerados dados pessoais.

A **pseudonimização** é uma técnica que visa dificultar a identificação direta de uma pessoa a partir de seus dados, sem eliminá-la completamente. De acordo com o §4º do art. 13 da **LGPD**, pseudonimização é o tratamento no qual um dado perde a possibilidade de associação direta ou indireta a um indivíduo, **exceto** pelo uso de uma informação adicional que deve ser mantida **separadamente** e em **ambiente seguro** pelo controlador.

Segundo o **estudo preliminar da ANPD (2023)**, a pseudonimização:

- **Não transforma os dados em anônimos**, ou seja, os dados pseudonimizados continuam sendo considerados **dados pessoais.**
- **Permite a reversibilidade**, desde que o controlador tenha acesso à chave ou informação adicional que possibilite a reidentificação.
- **Reduz riscos**, mas não elimina a possibilidade de identificação, especialmente se combinada com outras fontes de dados.

A pseudonimização é recomendada em diversos contextos, como:

- **Minimização de riscos** em compartilhamento de dados com terceiros
- **Prevenção de acessos indevidos** por equipes internas
- **Implementação de medidas de segurança** e de "privacidade desde a concepção" (*Privacy by Design*)
- **Preparação para eventual anonimização posterior**

Entre as técnicas mais comuns de pseudonimização, destacam-se:

- **Substituição por códigos:** troca de identificadores por valores únicos (ex: CPF → código aleatório)
- **Tokenização:** uso de tokens que não têm valor fora do sistema
- **Cifração (criptografia):** transformação dos dados em formato ilegível, reversível apenas com chave
- **Mascaramento:** ocultação parcial dos dados (ex: mostrar apenas os últimos dígitos de um CPF)
- **Hashing com sal (salting):** aplicação de funções criptográficas com valores aleatórios para dificultar ataques

Importante: A pseudonimização **não substitui** outras medidas de segurança e **não isenta** o controlador das obrigações previstas na LGPD. A informação adicional que permite a reidentificação deve ser protegida com rigor técnico e organizacional.

A ANPD recomenda que a pseudonimização seja parte de uma **estratégia mais**

ampla de proteção de dados, com políticas claras, controle de acesso, monitoramento, auditoria e avaliação de impacto (RIPD), quando aplicável.

9.2.3 Uso de Dados Sintéticos

Essa técnica cria dados artificiais que imitam as características estatísticas dos dados reais. Os dados sintéticos são gerados por modelos que simulam padrões semelhantes aos dos dados originais (OECD, 2023).

Dados sintéticos são gerados artificialmente com base em padrões estatísticos de dados reais. Eles são úteis para testes, treinamentos de modelos de IA e pesquisas, pois imitam os dados reais sem expor informações sensíveis.

Apesar disso, há risco de reidentificação se os dados sintéticos forem muito parecidos com os originais ou se o registro dos dados de origem aparecerem nos dados sintéticos. Por isso, é essencial avaliar a qualidade e a segurança dos modelos usados para gerar esses dados.

Segundo a **OCDE (2023)**, os dados sintéticos são uma ferramenta promissora para:

- **Treinar modelos de inteligência artificial**
- **Testar sistemas e softwares**
- **Compartilhar dados com menor risco de reidentificação**
- **Produzir estatísticas e análises em contextos sensíveis**

Apesar de úteis, esses dados podem, em alguns casos, permitir a reidentificação de pessoas, especialmente se os dados reais forem muito específicos e acabarem sendo replicados nos dados sintéticos.

Existem três tipos principais de dados sintéticos:

- **Totalmente sintéticos:** todos os registros são gerados artificialmente.
- **Parcialmente sintéticos:** apenas alguns atributos são substituídos por dados artificiais.
- **Híbridos:** combinação de dados reais e sintéticos, com controle sobre quais partes são preservadas.

Importante: A geração de dados sintéticos deve ser acompanhada de uma **avaliação de risco de reidentificação**, especialmente em contextos de dados sensíveis. A ANPD recomenda que os agentes de tratamento adotem uma abordagem baseada em risco e documentem as decisões tomadas.

Vantagens:

- Redução do risco de exposição de dados reais
- Preservação de padrões estatísticos
- Possibilidade de uso em ambientes de teste e desenvolvimento

Limitações:

- Risco de reidentificação se os dados sintéticos forem muito semelhantes aos reais ou se o registro dos dados de origem aparecerem nos dados sintéticos
- Perda de fidelidade em análises específicas
- Necessidade de validação rigorosa dos modelos geradores

9.2.4 Privacidade Diferencial

A **privacidade diferencial** é uma técnica que busca proteger a identidade dos indivíduos em um conjunto de dados ao adicionar **ruído estatístico controlado**. O objetivo é garantir que a presença ou ausência de uma pessoa em um banco de dados **não afete significativamente os resultados de uma análise**, preservando a utilidade dos dados agregados.

Segundo a **OCDE (2023)**, essa técnica é amplamente utilizada em contextos como:

- Pesquisa estatística
- Desenvolvimento de produtos com base em dados agregados
- Compartilhamento de dados com terceiros
- Treinamento de modelos de IA com dados sensíveis

A técnica é mencionada no **estudo preliminar da ANPD (2023)** como um dos paradigmas possíveis para anonimização de dados, ao lado da generalização. No entanto, o documento **não aprofunda sua aplicação nem fornece diretrizes específicas** sobre seu uso. Assim, qualquer implementação deve ser cuidadosamente avaliada à luz dos princípios da LGPD e das boas práticas de proteção de dados.

A privacidade diferencial pode ser aplicada de duas formas:

- Centralizada: o ruído é adicionado por um controlador central antes da divulgação dos dados.
- Distribuída: o ruído é adicionado no dispositivo do usuário (por exemplo, no próprio celular), antes do envio dos dados.

Exemplo prático: A Apple utiliza privacidade diferencial para coletar dados de uso de seus dispositivos sem identificar os usuários individualmente.

Vantagens:

- Protege a identidade individual mesmo em grandes conjuntos de dados
- Permite análises estatísticas úteis
- Reduz riscos em ambientes de dados abertos ou compartilhados

Desafios:

- Definir o nível adequado de ruído (parâmetro de privacidade)
- Risco de perda de precisão em análises detalhadas
- Necessidade de orientações regulatórias claras sobre sua aplicação

9.2.5 Prova de Conhecimento Zero

A técnica conhecida como **Zero-Knowledge Proofs (ZKP)** permite que uma parte comprove a veracidade de uma informação sem revelar a informação em si.

Por exemplo, é possível confirmar que alguém tem autorização para acessar um sistema sem precisar mostrar seus dados pessoais. Essa técnica é útil para validar informações de forma segura e privada (OECD, 2023).

As **Provas de Conhecimento Zero** (do inglês *Zero-Knowledge Proofs – ZKP*) são técnicas criptográficas que permitem a uma parte (o "proponente") provar a outra (o "verificador") que uma determinada informação é verdadeira, **sem revelar a informação em si**.

Essa abordagem é especialmente útil em situações em que é necessário validar uma condição — como idade mínima, renda ou credencial — sem expor os dados pessoais para os casos em que a resposta de validação não constitui o próprio dado pessoal.

Segundo a OCDE (2023), os ZKPs são considerados ferramentas promissoras para:

- Verificação de identidade e idade
- Autenticação em sistemas digitais
- Gestão de credenciais em carteiras de identidade digitais
- Aplicações em blockchain e criptomoedas

Como funciona?

- O proponente possui uma informação (por exemplo, sua data de nascimento).
- Ele passa essa informação por um algoritmo que valida que essa informação atende a um critério (por exemplo, "possuir mais de 18 anos").
- O verificador valida essa prova sem ter acesso à informação original.

Vantagens:

- Reduz drasticamente a exposição de dados pessoais
- Fortalece o princípio da minimização de dados
- Pode ser integrado a sistemas de identidade digital descentralizada

Desafios:

- Complexidade técnica e custo computacional
- Pouca maturidade em aplicações fora do setor financeiro
- Necessidade de padronização e interoperabilidade

Nota: Embora os ZKPs ainda estejam em fase inicial de adoção em larga escala, já são considerados uma das tecnologias mais promissoras para **privacidade desde a concepção** (*Privacy by Design*), especialmente em ambientes digitais complexos.

9.3 Segunda Categoria de PETs: Ferramentas de Criptografia de Dados

A segunda categoria de Tecnologias de Aprimoramento da Privacidade (PETs) inclui as **ferramentas de criptografia de dados**. Essas tecnologias têm como objetivo proteger os dados pessoais por meio da **codificação das informações**, tornando-as inacessíveis para pessoas não autorizadas.

Segundo **Machado e Doneda** (2018), a criptografia é "a ciência da escrita secreta com o objetivo de esconder o significado de uma mensagem". As técnicas criptográficas modernas são utilizadas como mecanismos de **confidencialidade** em segurança computacional, cifrando informações de modo que apenas o destinatário da comunicação ou o detentor da chave possa acessá-las.

Esse tipo de proteção é especialmente relevante em ambientes de **inteligência artificial (IA)**, onde grandes volumes de dados sensíveis são processados. O uso de criptografia — especialmente em suas formas avançadas, como criptografia homomórfica e ambientes de execução confiável — pode **contribuir significativamente** para a proteção desses dados, permitindo seu uso em análises e modelos sem comprometer a privacidade. No entanto, sua eficácia depende do contexto, da arquitetura do sistema e da combinação com outras medidas de segurança e governança.

A **Autoridade Nacional de Proteção de Dados (ANPD)** esclarece, em seu estudo preliminar (2023), que:

"Criptografia típica não é anonimização — criptografia é uma técnica de pseudonimização. Como a informação original precisa estar acessível, as transformações aplicadas pelos algoritmos criptográficos são projetadas para serem reversíveis, no que é conhecido como descriptografia. Entretanto, vários algoritmos criptográficos (simétricos, assimétricos e de hash) podem realizar processamentos unidirecionais. Nesses casos, atendem aos requisitos da anonimização, desde que os dados cifrados sejam úteis."

Esse esclarecimento reforça que a criptografia, embora poderosa, não substitui a anonimização, mas pode ser usada como parte de uma estratégia de proteção de dados, especialmente quando a reversibilidade é necessária — como no caso de dados que precisam ser acessados posteriormente por agentes autorizados.

Principais características da criptografia como PET:

- **Confidencialidade**: impede o acesso não autorizado aos dados.
- **Integridade**: garante que os dados não foram alterados durante a transmissão.
- **Autenticidade**: permite verificar a origem dos dados.

As subseções a seguir detalham as principais abordagens criptográficas utilizadas como PETs, com destaque para suas funcionalidades, aplicações práticas e limitações. São elas: a criptografia homomórfica, a computação multipartidária segura (MPC) e os ambientes de execução confiável (TEE).

9.3.1 Criptografia Homomórfica

A **criptografia homomórfica** é uma técnica avançada que permite realizar operações matemáticas sobre dados criptografados **sem a necessidade de descriptografá-los**. Isso significa que é possível processar informações sensíveis mantendo-as protegidas durante todo o ciclo de tratamento — desde o armazenamento até a análise.

Essa abordagem é especialmente útil em contextos em que os dados precisam ser processados por terceiros ou em ambientes de nuvem, mas sem que esses agentes tenham acesso ao conteúdo original dos dados.

Segundo a **OCDE (2023)**, essa técnica permite que os dados sejam criptografados pelo próprio titular — com uma chave que apenas ele possui — antes de serem enviados ao processador de dados. O processador, por sua vez, pode realizar cálculos simples (e progressivamente mais complexos) sobre os dados criptografados, gerando um resultado que também permanece cifrado. Apenas o titular dos dados pode descriptografar esse resultado final.

Exemplo prático: Um hospital pode enviar dados de pacientes criptografados a um centro de pesquisa, que realiza análises estatísticas diretamente sobre os dados cifrados. O centro nunca acessa os dados em claro, mas ainda assim obtém os resultados desejados.

Esse processo aprimora a privacidade e a proteção de dados ao permitir que as informações permaneçam criptografadas **mesmo enquanto estão em uso** — algo que tradicionalmente exigiria sua exposição. Com isso, titulares ou controladores mantêm **estrita confidencialidade** sobre os dados, reduzindo significativamente os riscos de segurança associados ao uso e processamento de dados sensíveis.

Vantagens:

- Garante a privacidade dos dados durante o processamento
- Permite terceirização segura de análises e cálculos
- Reduz o risco de exposição em ambientes de nuvem

Desafios:

- Alto custo computacional e tempo de processamento
- Complexidade na implementação e na escolha dos esquemas criptográficos
- Limitações quanto ao tipo e à complexidade das operações suportadas (alguns esquemas permitem apenas somas ou multiplicações, enquanto outros são totalmente homomórficos)

9.3.2 Computação Multipartidária Segura

A **Computação Multipartidária Segura** (*Secure Multi-Party Computation – MPC*) é uma técnica criptográfica que permite que duas ou mais partes realizem cálculos conjuntos sobre seus dados, **sem que nenhuma delas precise revelar suas informações para as demais**. Cada participante mantém seus dados em sigilo, mas ainda assim

contribui para o processamento coletivo, obtendo um resultado final compartilhado.

Essa abordagem é especialmente útil em contextos de **cooperação entre organizações**, como instituições financeiras, órgãos públicos ou centros de pesquisa, que desejam realizar análises conjuntas sem comprometer a confidencialidade dos dados sob sua responsabilidade.

Exemplo prático: Dois hospitais podem calcular estatísticas conjuntas sobre seus pacientes (como taxas de recuperação ou prevalência de doenças) sem compartilhar os dados individuais entre si.

Segundo a **OCDE (2023)**, a MPC é uma das PETs mais promissoras para **viabilizar o uso colaborativo de dados sensíveis**, especialmente em setores como saúde, finanças, segurança pública e pesquisa científica. Ela permite que os dados permaneçam protegidos durante todo o processo de cálculo, reduzindo os riscos de exposição e vazamento.

Essa técnica também está alinhada com os princípios e estratégias descritos no **Guia sobre Privacidade desde a Concepção e por Padrão** da **Secretaria de Governo Digital (SGD)**:

- **Estratégia "Ocultar"** (seção 4.1.2): ao impedir que os dados sejam visíveis para os participantes, a MPC garante a confidencialidade e reduz o risco de uso indevido.
- **Meta de "Desvinculação"** (seção 3): ao evitar a associação direta entre dados e indivíduos durante o processamento, a MPC contribui para a proteção contra reidentificação.
- **Princípio da "Segurança fim a fim"** (seção 1.5): a MPC assegura que os dados estejam protegidos desde a coleta até o processamento, mantendo a privacidade em todas as etapas do ciclo de vida.

Como funciona?

- Cada parte divide seus dados em fragmentos criptográficos (ou "compartimentos").
- Esses fragmentos são distribuídos entre os participantes.
- Os cálculos são realizados de forma distribuída, sem que nenhum participante tenha acesso ao dado completo.
- O resultado final é reconstruído a partir dos fragmentos, sem revelar os dados originais.

Vantagens:

- Permite colaboração entre entidades sem troca de dados sensíveis
- Garante confidencialidade durante o processamento
- Reduz riscos legais e regulatórios associados ao compartilhamento de dados

Desafios:

- Alto custo computacional e complexidade técnica
- Necessidade de sincronização entre as partes envolvidas
- Limitações em cenários com muitos participantes ou dados altamente dinâmicos

Nota: A MPC é especialmente útil quando a confiança entre as partes é limitada, mas há interesse mútuo em cooperar com segurança. Sua adoção vem crescendo em projetos de análise federada, consórcios de pesquisa e sistemas de IA distribuída.

9.3.3 Intersecção de Conjuntos Privados

A **Intersecção de Conjuntos Privados (Private Set Intersection – PSI)** é uma técnica criptográfica que permite que diferentes organizações comparem **bases de dados** para identificar elementos comuns, sem expor ou compartilhar diretamente os dados individuais dos titulares. Essa abordagem reduz significativamente os **riscos de privacidade**, garantindo que apenas as informações relevantes sejam utilizadas para correspondências sem revelar detalhes sensíveis.

Como funciona?

O PSI utiliza algoritmos criptográficos para permitir que duas ou mais partes verifiquem **quais elementos** estão presentes em **ambas as bases**, sem que os dados completos sejam compartilhados. Isso significa que cada organização mantém **seus dados protegidos**, evitando exposição indevida, enquanto ainda colabora na identificação de correspondências.

Exemplo prático:

Durante a pandemia da **Covid-19**, o PSI foi utilizado em larga escala para **notificar usuários** sobre contatos próximos com indivíduos contaminados. Os sistemas comparavam listas de pessoas infectadas sem expor diretamente a identidade dos envolvidos, permitindo que os titulares recebessem alertas de forma segura e privada.

Principais aplicações do PSI:

- **Proteção de dados em colaborações entre instituições** (ex.: cruzamento de registros hospitalares sem revelar pacientes individuais).
- **Combate a fraudes** em setores como bancos e seguradoras, verificando se um cliente já está cadastrado em outra instituição sem expor seus dados completos.
- **Verificação de credenciais** sem que um sistema precise conhecer todas as informações sobre um usuário.

Vantagens do PSI:

- Protege a **privacidade dos titulares** ao evitar exposição direta dos dados.
- Permite o **uso colaborativo de dados** sem violar normas de proteção.
- Reduz riscos de **vazamento** e uso indevido por terceiros.

Desafios do PSI:

- Exige **capacidade computacional** significativa para comparação de grandes conjuntos de dados.
- Pode demandar **acordos regulatórios** entre partes envolvidas na troca de informações.
- Necessita de implementação cuidadosa para evitar **reidentificação acidental**.

Nota: A OCDE (2023) reconhece o **PSI** como uma tecnologia promissora para aprimorar **privacidade e segurança de dados** em diversos setores, especialmente no contexto de compartilhamento responsável de informações.

9.3.4 Ambientes Seguros

Os **Ambientes de Execução Confiável (Trusted Execution Environments – TEEs)** são áreas isoladas dentro de um **processador**, projetadas para proteger **dados pessoais e confidenciais** contra acessos não autorizados, inclusive do próprio sistema operacional. Essa abordagem garante que informações sensíveis permaneçam inacessíveis a aplicativos externos ou processos não autorizados, mesmo em situações de comprometimento do sistema principal.

Como funciona?

Os **TEEs** criam um **espaço seguro** dentro do processador, onde os dados armazenados são protegidos contra leitura ou modificação por agentes externos. Esse ambiente funciona como uma **zona de confiança**, permitindo que **cálculos sensíveis** sejam realizados com maior segurança, sem que terceiros tenham acesso às informações utilizadas.

Aplicações dos TEEs:

Proteção de **credenciais e autenticação segura**. Segurança em **pagamentos digitais** e transações financeiras. Isolamento de **dados biométricos** para verificação de identidade. Proteção de **chaves criptográficas** utilizadas na comunicação segura.

Exemplo prático:

Grandes fabricantes de chips, como **ARM, Intel e Qualcomm**, e empresas de tecnologia, como **Apple, Google e Samsung**, implementaram **TEEs** em seus dispositivos para garantir maior segurança. Essa técnica é aplicada em recursos como **Face ID, Secure Enclave e Trusted Platform Module (TPM)**, usados para proteger credenciais e autenticação de usuários.

Vantagens dos TEEs:

- Proporcionam **isolamento confiável** entre dados sensíveis e aplicações comuns.
- Reduzem a possibilidade de **vazamento de informações** em ambientes comprometidos.
- Permitem execução segura de cálculos e operações sigilosas.

Desafios dos TEEs:

- Dependem do suporte de **hardware dedicado** e integração adequada nos sistemas.
- Exigem **modelos de confiança** bem definidos entre as aplicações e o processador.
- Ainda são pouco acessíveis para **desenvolvedores independentes**, devido à complexidade técnica.

Nota: A **OECD (2023)** recomenda o uso de **TEEs desde a fase inicial do desenvolvimento de sistemas**, garantindo que os dados sejam protegidos desde a concepção, reforçando a segurança e minimizando riscos futuros.

9.4 Terceira Categoria de PETs: Ferramentas de Descentralização de Dados

As **Ferramentas de Descentralização de Dados** são uma abordagem inovadora para **processamento e análise distribuída**, permitindo que grandes volumes de dados sejam tratados **sem a necessidade de centralização em um único servidor**. Em vez de os dados serem coletados em um **repositório central**, o processamento ocorre **localmente em múltiplos dispositivos** (**nós**), que realizam cálculos de forma distribuída e, posteriormente, enviam resultados agregados para um servidor de referência.

Como funciona?

A técnica permite que o treinamento de **modelos de inteligência artificial (IA)** ocorra **diretamente nos dispositivos dos usuários**, como celulares, computadores ou sensores inteligentes. Em vez de transferir grandes volumes de **dados brutos** para um servidor central, cada **nó** processa localmente suas informações e compartilha apenas **aprendizados** com o modelo global, garantindo maior privacidade e redução no fluxo de dados sensíveis.

Exemplo prático:

Essa abordagem é utilizada para **reconhecimento facial** distribuído, onde os dados dos usuários **permaneçam armazenados em seus próprios dispositivos** enquanto participam do treinamento de um sistema de IA. Os padrões aprendidos são então compartilhados com um **servidor central**, que integra os modelos sem nunca acessar diretamente os dados brutos dos dispositivos individuais.

Principais aplicações das Ferramentas de Descentralização:

- **Treinamento de IA distribuído**, preservando a privacidade dos dados individuais.
- **Processamento de dados sensíveis** em dispositivos locais, evitando exposição em ambientes externos.
- **Sistemas de recomendação personalizadas**, sem compartilhamento direto de dados entre usuários.

Vantagens:

- Redução na transferência de **dados sensíveis** para servidores externos.
- Maior **segurança e privacidade**, pois os dados permanecem no dispositivo do titular.
- Eficiência no processamento de **grandes volumes de dados** sem sobrecarga de infraestrutura centralizada.

Desafios:

- Necessidade de **sincronização** entre os dispositivos para garantir a acurácia do modelo global.
- Dependência de **recursos computacionais** distribuídos nos dispositivos dos usuários.

- Potenciais **limitações na precisão** devido à fragmentação dos dados entre os nós.

Nota: Segundo a **OECD (2023)**, essa abordagem vem sendo cada vez mais adotada por **empresas de tecnologia e pesquisas avançadas**, permitindo maior eficiência e privacidade no tratamento de dados pessoais.

9.5 Quarta Categoria de PETs: Ferramentas de Accountability

As ferramentas de **responsabilização de dados** oferecem novos mecanismos para **controlar a coleta, o uso e a transparência** das transações envolvendo dados pessoais. Embora não sejam consideradas **PETs em sentido estrito**, por não focarem diretamente na **confidencialidade** dos dados, essas ferramentas desempenham um papel essencial no aprimoramento da **privacidade e governança de dados** (OECD, 2023).

Essas soluções permitem que organizações e indivíduos **exijam e apliquem regulamentações** sobre o tratamento de dados, fortalecendo a **autonomia e o controle** dos titulares. A seguir, são apresentadas algumas das principais tecnologias utilizadas nessa categoria.

9.5.1 Accountability Systems

Os **sistemas de prestação de contas** são ferramentas voltadas para **gerenciar a responsabilidade das organizações** em relação ao tratamento de dados pessoais. Seu objetivo é garantir que empresas e instituições **possam responder por suas ações** e decisões envolvendo o uso e o compartilhamento de informações pessoais (OECD, 2023).

Esses sistemas são fundamentais para **monitorar a conformidade** com normas de privacidade, **controlar os processos de tratamento** e **acompanhar como os dados são coletados, processados e utilizados** ao longo do tempo.

Apesar de sua relevância, a **OECD** destaca que os sistemas de accountability ainda enfrentam desafios para **ganhar escala**, principalmente devido à sua **complexidade de implementação**, o que os mantém, por ora, em **fase de testes ou pilotos**.

9.5.2 Threshold Secret Sharing

O **Threshold Secret Sharing**—ou **compartilhamento de segredos de limite**—é uma técnica criptográfica que **divide uma chave** entre múltiplas partes distintas, permitindo que os dados só sejam acessados **quando um número predeterminado de chaves** for utilizado em conjunto (OECD, 2023).

Esse mecanismo possibilita que **autoridades regulamentadoras estabeleçam condições** para o acesso aos dados, garantindo maior controle sobre sua utilização.

Uma analogia útil para entender essa abordagem é imaginar uma **caixa segura**

trancada com várias fechaduras separadas, onde as chaves estão distribuídas entre diferentes pessoas. Somente quando **todas as partes concordam em utilizar suas chaves**, a caixa pode ser aberta—o que reforça a segurança e evita acessos indevidos.

Essa técnica pode ser empregada para:

- **Proteção de dados altamente sensíveis**, garantindo que seu acesso dependa de múltiplas autorizações.
- **Implementação de regras rigorosas de privacidade**, permitindo que o desbloqueio dos dados ocorra apenas sob condições previamente definidas.
- **Segurança aprimorada em sistemas financeiros, jurídicos e de identificação digital**, fortalecendo a proteção contra fraudes e acessos indevidos.

9.5.3 Armazenamentos de dados pessoais/Sistemas de Gestão de Informações Pessoais

Os **sistemas de armazenamento de dados pessoais (PDS)** oferecem uma abordagem alternativa ao modelo tradicional de **coleta e armazenamento centralizado de informações pessoais**. Em vez de um único agente controlador manter grandes volumes de dados, essas ferramentas permitem que **os próprios titulares tenham controle sobre seus dados** e decidam **como, quando e com quem** compartilhá-los (OECD, 2023).

Esses sistemas contribuem para a **privacidade e proteção de dados**, pois possibilitam:

- **Maior autonomia e autodeterminação informacional** por parte dos titulares de dados.
- **Implementação dos direitos de portabilidade**, permitindo que usuários transfiram seus dados entre serviços sem precisar depender exclusivamente dos controladores.
- **Redução da exposição desnecessária dos dados**, minimizando riscos de acesso indevido ou uso abusivo.

Porém, um dos principais desafios para a adoção dessa abordagem é a **divisão de responsabilidades** entre os titulares dos dados e os agentes de tratamento. É necessário garantir que **os usuários compreendam** o impacto de suas decisões de compartilhamento e que **os agentes de tratamento respeitem os princípios de segurança e conformidade** estabelecidos pelas regulamentações.

10 Aplicação Prática da PdC no MGI

A implementação dos princípios de **Privacidade desde a Concepção (PdC)** no **Ministério da Gestão e da Inovação em Serviços Públicos (MGI)** deve ocorrer sempre que houver um **novo tratamento de dados pessoais** ou uma **alteração em um processo já existente**. A responsabilidade por essa análise (A1) cabe à **Unidade Responsável**, pois a identificação do tratamento ocorre dentro dessa área.

O primeiro passo é verificar se o **processo ou serviço realiza o tratamento de dados pessoais**. Caso a resposta seja positiva, os dados do processo devem ser cadastrados no **ColaboraDap** (A2), o **Sistema de Gestão Responsável de Tratamento de Dados Pessoais do MGI**. Durante esse cadastramento, a **Unidade Responsável** deve avaliar se **precisa de apoio técnico para validar a aderência aos princípios da PdC**.

Se **não houver necessidade de apoio técnico**, a unidade deve verificar se o processo **coleta dados diretamente do titular**. Caso isso ocorra, o princípio da **transparência** exige o envio de uma solicitação ao **Encarregado** para a elaboração do **Termo de Uso e Aviso de Privacidade (TUAP)** (A3). Essa solicitação deve ser feita pelo email cgpdp.mgi@gestao.gov.br. O **Encarregado** analisará a solicitação (A4) e, se necessário, elaborará o **TUAP** em conjunto com a Unidade Responsável (P1) usando o **Modelo de Termo de Uso e Aviso de Privacidade – TUAP** disponível no **SEI**. Após a finalização do **TUAP**, a **Unidade Responsável** deve registrar essa alteração no ColaboraDap (A2) e seguir o fluxo.

Caso o TUAP já tenha sido elaborado e atualizado, mas a **avaliação de Alto Risco** ainda não tenha sido realizada, a Unidade Responsável deve conduzir essa **avaliação** no **ColaboraDap** (A7). Esse procedimento segue a **metodologia da Autoridade Nacional de Proteção de Dados (ANPD)** e determina se o processo é classificado como de **"Alto Risco"** ou não.

Se o processo for **classificado como de alto risco**, a unidade deve verificar se já existe um **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** e se é necessário atualizá-lo. O RIPD deve ser revisado sempre que houver **alterações no processo ou serviço que envolva o tratamento de dados pessoais**, garantindo conformidade e segurança. Para isso, a **Unidade Responsável** deve solicitar apoio ao **Encarregado** (A9) pelo email cgpdp.mgi@gestao.gov.br. Após análise (A4), se necessário, o Encarregado elaborará o **RIPD** (P2) em conjunto com a unidade, por meio da **abertura de processo SEI sigiloso e de acesso reservado**, utilizando o Modelo de **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** disponível no SEI.

Nota: O RIPD deve ser inserido em **processo sigiloso** e de acesso controlado por credencial, pois contém informações sobre **fragilidades do processo/serviço**, além das medidas de controle recomendadas para mitigação de riscos.

Após a elaboração e assinatura do **RIPD** (**P2**), o **Encarregado** encaminhará as orientações à **Unidade Responsável** (**A5**), que deverá implementar os ajustes necessários (A6) e reiniciar o fluxo (**A2**).

Concluída a avaliação de **Alto Risco** e elaborado o **RIPD**, a unidade deve **realizar o cadastro completo do inventário** no **ColaboraDap** (**A8**) para finalizar o fluxo. Se o processo não for classificado como processo de **Alto Risco**, o cadastro completo também deve ser realizado (A8).

***Dica*: O inventário completo no ColaboraDap** permite ao **Encarregado** e equipe analisar os processos (**P4**) e verificar se estão **aderentes aos princípios da PdC** para **publicação dos dados no Aviso de Privacidade Institucional** (**A13**).

Caso o **Encarregado** conclua que o processo ou serviço está aderente aos princípios da PdC, ele **solicitará autorização** à **Unidade Responsável** para **publicação dos dados no Aviso de Privacidade Institucional do MGI** (**A13**).

Se a Unidade Responsável aprovar a publicação, todo o fluxo de PdC será concluído com sucesso.

Se a Unidade Responsável optar por não publicar, o processo será encerrado com pendência de publicação e transparência.

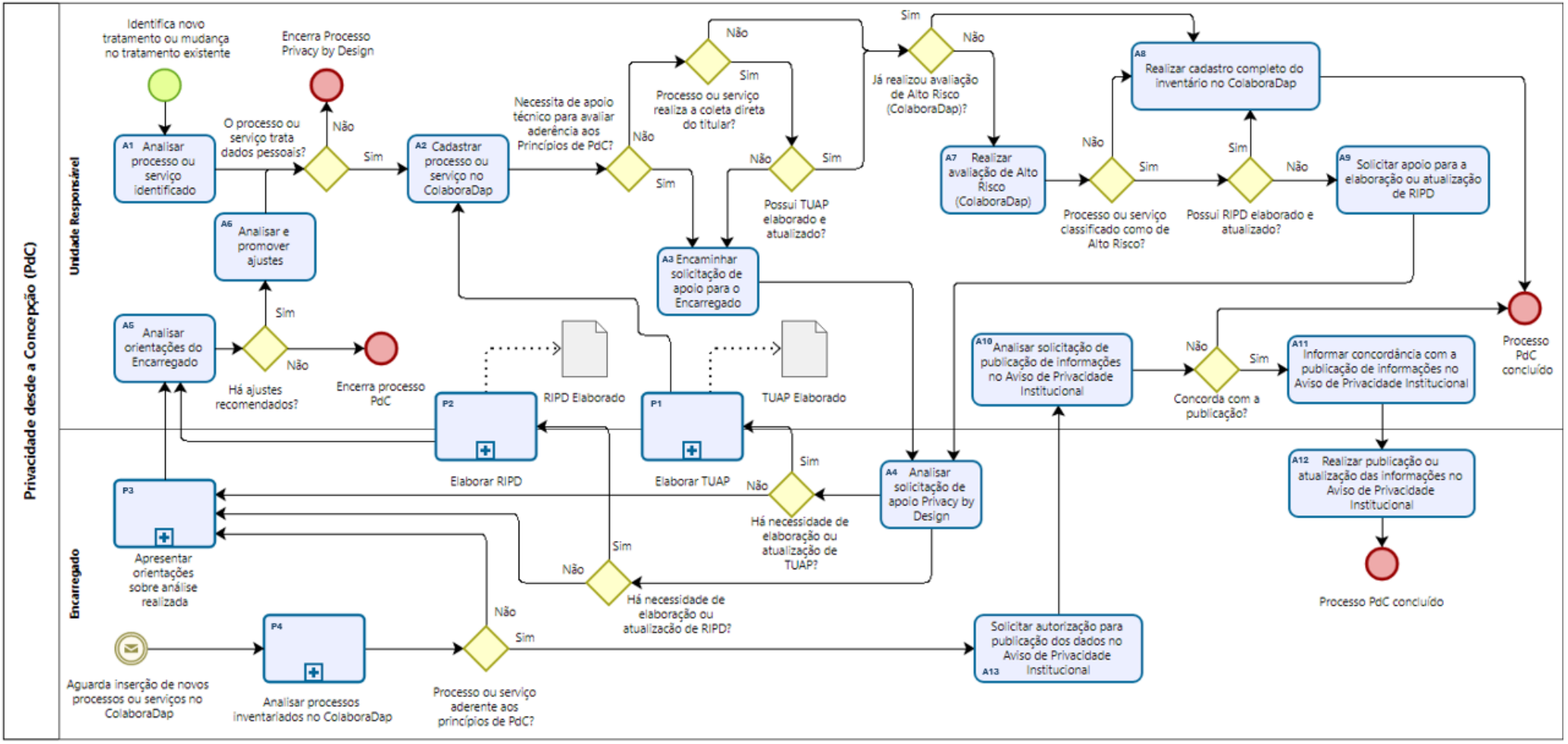

Figura 1 - Fluxo de Processo Privacidade desde a Concepção no MGI

O fluxo de aplicação prática da **Privacidade desde a Concepção (PdC)**, apresentado na **Figura 1**, destaca a **importância da participação da Unidade Responsável**, seja na implementação de um **novo projeto**, seja na adequação de um **processo já existente** que envolva o tratamento de dados pessoais. Para garantir que cada etapa siga os princípios da PdC, é essencial que as unidades **avaliem corretamente o impacto de seus processos** e mantenham o compromisso com a **transparência e segurança dos dados**. Caso surjam dúvidas na aplicação prática desses princípios, a **Unidade Responsável** poderá solicitar **orientação ao Encarregado pelo Tratamento de Dados Pessoais do MGI**, conforme disposto no **inciso III do § 2º do art. 41 da LGPD**.

11 Considerações finais

Este documento consolidou diretrizes fundamentais para a **Privacidade desde a Concepção (PdC)**, promovento um tratamento de dados pessoais no **Ministério da Gestão e da Inovação em Serviços Públicos (MGI)** alinhado às melhores práticas internacionais e às exigências da **Lei Geral de Proteção de Dados (LGPD)**. Ao longo dos capítulos, abordamos desde os princípios estruturantes da **PdC**, **LGPD** e **FIPP**, passando por metas, estratégias, técnicas de proteção e aplicação prática da governança de dados no **MGI**, até chegarmos ao **fluxo operacional** que orienta as unidades responsáveis a seguirem as diretrizes de conformidade e transparência.

Nosso compromisso não se limita apenas à adequação regulatória, mas visa fortalecer a **confiança dos titulares de dados**, garantindo que suas informações sejam protegidas desde o momento da concepção de qualquer projeto, serviço ou iniciativa. Ao implementar as práticas detalhadas neste documento, buscamos mitigar riscos, assegurar **responsabilização** e promover um modelo de gestão que prioriza **segurança, transparência e inovação**.

A importância da privacidade e da proteção de dados tem sido amplamente reconhecida em diferentes países e organismos internacionais. Como ressalta a **OCDE** em suas diretrizes sobre Tecnologias de Aprimoramento da Privacidade (**Privacy-Enhancing Technologies – PETs**), "as medidas de proteção de dados devem ser integradas desde o início, garantindo que segurança e inovação caminhem lado a lado". Essa visão reforça que a **Privacidade desde a Concepção** não é apenas uma exigência regulatória, mas um diferencial estratégico que pode aprimorar a prestação de serviços públicos e fortalecer os direitos fundamentais dos cidadãos.

Com este documento, esperamos colher frutos significativos na **qualidade do tratamento de dados pessoais**, criando um ambiente mais seguro, transparente e eficiente para todos os titulares. A privacidade deve ser vista como um **pilar central da governança digital**, e o **MGI** segue comprometido com a evolução contínua desse processo.

.

12 Referências bibliográficas

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm>. Acesso em: 19 jul. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 mar. 2023.

BRASIL. ANPD, A. N. DE P. DE D. *Estudo Preliminar - Anonimização e pseudonimização para proteção de dados*. Disponível em: <https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados>. Acesso em: 18 jun. 2025.

BRASIL, M., Ministério da Gestão e da Inovação em Serviços Públicos. *Guia sobre Privacidade desde a Concepção e por Padrão*. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf>. Acesso em: 18 jun. 2025.

BRASIL. ME, M. DA E. *Resolução CEPPDP-ME nº 7, de 22 de fevereiro de 2022. Aprova a Política de Proteção de Dados Pessoais no âmbito do Ministério da Economia.* . [S.l: s.n.]. Disponível em: <https://www.gov.br/gestao/pt-br/acesso-a-informacao/estrategia-e-governanca/estrutura-de-governanca/cpdp/resolucao-ceppdp-me-no-7-2022-atualizada>. Acesso em: 17 set. 2023a. , 22 fev. 2022

BRASIL. ME, M. DA E. *Resolução CEPPDP-ME nº 12, de 04 de outubro de 2022. Aprova as Orientações para Privacidade desde a Concepção no âmbito do Ministério da Economia.* . [S.l: s.n.]. . Acesso em: 17 set. 2023b. , 4 out. 2022

CAVOUKIAN, A. Privacy by Design The 7 Foundational Principles. 1990.

GELLMAN, R. Fair Information Practices: A Basic History. *SSRN Electronic Journal*, 2014. Disponível em: <http://www.ssrn.com/abstract=2415020>. Acesso em: 18 jun. 2025.

MACHADO, D.; DONEDA, D. C. M. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Regulação da criptografia no direito brasileiro*, 1 jan. 2018. Disponível em: <https://www.academia.edu/38168713/Prote%C3%A7%C3%A3o_de_dados_pessoais_e_criptografia_tecnologias_criptogr%C3%A1ficas_entre_anonimiza%C3%A7%C3%A3o_e_pseudonimiza%C3%A7%C3%A3o_de_dados>. Acesso em: 18 jun. 2025.

OCDE, O. PARA A C. E D. E. *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*. , OECD Digital Economy Papers.OECD Digital Economy Papers, nº 351. [S.l: s.n.], 8 mar. 2023. Disponível em: <https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html>. Acesso em: 18 jun. 2025.

Resolution on Privacy by Design. 29 out. 2010.