# Guia Sobre Privacidade Desde a Concepção e Por Padrão

MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Programa de Privacidade e Segurança da Informação
**PPSI 2.0**

**Versão 1.0**
**Brasília, 31 de agosto de 2026**

## GUIA SOBRE PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO

**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**
Rejane Monique Brelaz Castro
Thainan Cardoso Rezende

**EQUIPE DE REVISÃO**
Anderson Souza de Araújo
Denis Marcelo de Oliveira

## Histórico de versões

| Versão | Data | Descrição | Autor |
|---|---|---|---|
| 1.0 | 31/08/2026 | Elaboração do conteúdo. | Equipe Técnica de Elaboração |

# Sumário

## Licença *Creative Commons*



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

# Medida do *framework* do PPSI 2.0 apoiada por este documento

| Id | Medida |
|---|---|
| 20.4 | O órgão possui um processo para promover a privacidade desde a fase de concepção do produto ou do serviço até a sua execução? |

# 1 Introdução

**Privacidade desde a concepção e por padrão** consiste em um conjunto de medidas, princípios e práticas que objetivam incorporar a proteção de dados pessoais desde a fase inicial de concepção de produtos, serviços e sistemas, bem como assegurar que as configurações de privacidade mais seguras sejam aplicadas automaticamente, sem necessidade de intervenção do titular.

A adoção da Privacidade desde a Concepção e por Padrão cumpre, fundamentalmente, a determinação legal disposta no § 2º do art. 46 da Lei nº 13.709, de 14 de agosto de 2018 – **Lei Geral de Proteção de Dados Pessoais (LGPD)** [1]: "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" [1, art. 46, § 2º].

Para além da medida 20.4, disposta na Tabela de medidas do *framework* do PPSI 2.0 apoiada por esse documento, as recomendações apresentadas neste Guia também estão diretamente relacionadas aos controles 24 (Minimização de Dados), 25 (Gestão do Tratamento) e 26 (Acesso e Qualidade) do **Guia do *Framework* de Privacidade e Segurança da Informação** [2]. Esses controles estabelecem a necessidade de limitar a coleta, o uso, a retenção e a divulgação de dados pessoais ao estritamente necessário, bem como de assegurar os direitos dos titulares. Além disso, a abordagem está alinhada aos princípios da prevenção, necessidade, segurança e transparência, previstos no art. 6º da LGPD [1], bem como às diretrizes do **Programa de Privacidade e Segurança da Informação (PPSI 2.0)** [3] e da **Política de Proteção de Dados Pessoais (PPDP)** de cada órgão ou entidade.

Nesse sentido, os órgãos e entidades da administração pública devem adotar e manter práticas, controles e processos que assegurem a privacidade desde a concepção e por padrão em todos os seus projetos, serviços e sistemas que envolvam o tratamento de dados pessoais, de modo que a proteção de dados seja pensada proativamente e incorporada ao desenho das soluções, e não tratada como um complemento posterior.

Para fins deste Guia, o público-alvo compreende os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional (APF) que concebem, contratam, desenvolvem, operam ou avaliam sistemas, serviços digitais ou processos que tratem dados pessoais.

.

# 2 Princípios da privacidade desde a concepção e por padrão

As primeiras ideias de "**Privacidade desde a Concepção**" (em inglês, *Privacy by Design* – PbD) foram expressas na década de 1970, por meio de uma série de estudos que resultaram em um código de práticas para preservar a privacidade de indivíduos cujos dados são tratados.

O termo refere-se a uma metodologia constituída por um conjunto de princípios formulados na década de 1990 pela ex-comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian. Baseia-se nos *Fair Information Practices Principles* (FIPPs), amplamente aceitos na comunidade de privacidade. Ela preconiza que qualquer projeto que envolva o processamento de dados pessoais deve assegurar que a privacidade e a proteção de dados pessoais sejam incorporadas durante todo o seu ciclo de vida, de forma proativa e não reativa [5].

Na legislação brasileira, a obrigatoriedade da abordagem desde a concepção está expressa no § 2º do art. 46 da Lei nº 13.709/2018 (LGPD) [1]. Internacionalmente, destaca-se o art. 25 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), que trata especificamente da *Data Protection by Design and by Default*, exigindo que os controladores implementem medidas técnicas e organizacionais adequadas para garantir a proteção de dados desde a concepção e por padrão [6, 7].

A metodologia desenvolvida por Cavoukian é pautada por sete princípios relacionados à privacidade desde a concepção, assim enumerados:

1. proativo e não reativo; preventivo, não corretivo;
2. privacidade por padrão;
3. privacidade incorporada ao projeto;
4. funcionalidade total (soma positiva, não soma-zero);
5. segurança fim a fim;
6. visibilidade e transparência; e
7. respeito pela privacidade do usuário.

Para além dos sete princípios da **Privacidade desde a Concepção e por Padrão**, a proteção da informação fundamenta-se na tríade da segurança da informação — confidencialidade, integridade e disponibilidade (CID). No contexto da privacidade, essas metas são complementadas por objetivos específicos voltados à proteção dos titulares, especialmente a desvinculação, a transparência e a intervenção. Em conjunto, essas metas fornecem uma visão integrada dos objetivos que orientam a aplicação prática dos princípios apresentados neste guia [8]. A **Figura 1** apresenta essa correlação.

As metas apresentadas na **Figura 1** complementam os princípios da Privacidade desde a Concepção e por Padrão, servindo como referência para a adoção dos mecanismos técnicos, administrativos e organizacionais descritos ao longo deste capítulo. Cada princípio contribui, em maior ou menor grau, para o atendimento dessas metas, promovendo uma abordagem integrada de proteção de dados pessoais.


**Figura 1**: princípios da privacidade desde a concepção e por padrão e as metas de segurança da informação e objetivos voltados à proteção dos titulares

Os princípios apresentados neste capítulo constituem a base estrutural deste guia. Nas seções subsequentes, cada princípio será detalhado e relacionado às medidas, estratégias, técnicas, padrões, tecnologias e mecanismos de avaliação que contribuem para sua implementação prática no contexto da APF, em alinhamento com a LGPD, o PPSI 2.0 e as melhores práticas nacionais e internacionais.

## 2.1 Proativo e não reativo; preventivo, não corretivo

Este princípio exige que os agentes de tratamento atuem de forma proativa na implementação de rotinas e metodologias de trabalho que previnam riscos à privacidade, em vez de esperar que incidentes ocorram para então reagir. Qualquer projeto que utilize dados pessoais deve proteger esses dados desde a sua concepção, identificando possíveis riscos aos direitos e liberdades dos titulares e minimizando-os antes que possam resultar em danos [5].

A implementação deste princípio requer que a proteção da privacidade seja incorporada desde as fases iniciais do tratamento de dados pessoais, por meio da adoção de medidas organizacionais, técnicas e administrativas voltadas à prevenção de riscos, à governança e à melhoria contínua. Nesse contexto, destacam-se as seguintes estratégias:

- **Governança e compromisso institucional:** a atuação proativa depende do comprometimento da Alta Administração e da definição de mecanismos de governança que assegurem a implementação contínua das ações de privacidade. Para tanto, recomenda-se a formalização de políticas institucionais, a definição de papéis e responsabilidades e a adoção de mecanismos de responsabilização e prestação de contas, em conformidade com a LGPD e com o PPSI 2.0 [1, 2].
- **Avaliação prévia de riscos: o** Relatório de Impacto à Proteção de Dados Pessoais (RIPD) constitui um importante instrumento preventivo para identificar e tratar riscos antes do

início das atividades de tratamento, permitindo que medidas de mitigação sejam adotadas ainda na fase de concepção [9].

- **Monitoramento e melhoria contínua:** a realização de auditorias, avaliações periódicas e a utilização de indicadores de maturidade em privacidade permitem verificar continuamente a eficácia das medidas implementadas, promovendo o aperfeiçoamento permanente dos controles de privacidade [2].
- **Políticas, normas e procedimentos:** o estabelecimento e o cumprimento de políticas, normas e procedimentos relacionados à privacidade e à proteção de dados pessoais compatíveis com os requisitos legais, por meio de mecanismos técnicos e organizacionais.
- **Adequação de contratos e instrumentos congêneres:** a inclusão de cláusulas de proteção de dados pessoais nos contratos com operadores e analisar evidências de conformidade [1].
- **Capacitação e conscientização:** a implementação deste princípio também depende da promoção de uma cultura organizacional voltada à privacidade. Para isso, recomenda-se a realização contínua de ações de conscientização e treinamento dos agentes de tratamento, de forma a fortalecer a adoção de boas práticas [1, 2].

Esses mecanismos concretizam a aplicação do princípio proativo e preventivo ao promover a identificação antecipada de riscos, fortalecendo a governança da privacidade e reduzindo a necessidade de ações corretivas após a ocorrência de incidentes.

## 2.2 Privacidade por padrão (*Privacy by default*)

A privacidade por padrão significa que, quando instituições disponibilizam sistemas, produtos, serviços ou práticas de negócio, as configurações mais seguras de privacidade devem ser aplicadas automaticamente, sem necessidade de o titular tomar qualquer ação adicional para proteger seus dados pessoais [5]. A privacidade deve ser a regra, não a exceção. Nesse contexto, destacam-se as seguintes estratégias:

- **Especificação da finalidade:** o titular deve ser informado antes ou no momento da coleta sobre a finalidade do tratamento [9].
- **Limitação da coleta:** os dados coletados devem ser restritos ao necessário para as finalidades especificadas [9].
- **Minimização de dados:** restringir ao mínimo necessário a quantidade de dados pessoais tratados, evitando coleta excessiva e limitando possíveis impactos à privacidade [1]. Por exemplo, coletar apenas a faixa etária, e não a data de nascimento exata, quando a finalidade for apenas verificar maioridade. Algumas estratégias para minimização de dados incluem:
    - **Supressão:** abster-se de processar dados pessoais total ou parcialmente (ex.: lista de bloqueio – *denylist*). Em um sistema de agendamento, não armazenar, por exemplo, o nome completo se apenas o CPF já for o suficiente para identificação;

  - **Seleção**: decidir quais dados pessoais serão utilizados, escolhendo apenas o estritamente necessário. Por exemplo, coletar apenas a faixa etária, e não a data de nascimento exata, quando a finalidade for apenas verificar maioridade;
  - **Eliminação:** eliminar logicamente os dados pessoais não mais necessários, com prazo de retenção predefinido. Por exemplo, após a conclusão de um processo de consulta pública, eliminar os dados de identificação dos participantes, mantendo apenas respostas anônimas;
  - **Descarte:** destruir, inclusive de *backups*, os dados pessoais de maneira segura e irreversível. Por exemplo, utilizar ferramentas de *wipe* seguro ou destruição física de mídias ao final do prazo de guarda de prontuários de saúde.

- **Uso, retenção e limitação de divulgação:** os dados só podem ser utilizados e mantidos conforme as finalidades informadas e a hipótese legal aplicável, salvo determinação legal em contrário [1, 9].
- **Configuração adequada de sistemas e aplicações:** sistemas governamentais, como portais de serviços ou aplicativos de cidadania, devem vir configurados com as opções de privacidade já ativadas, por exemplo:
  - não compartilhamento automático de dados;
  - coleta mínima de metadados, limitada aos registros tecnicamente indispensáveis para segurança, auditoria e prestação do serviço;
  - prazos de retenção reduzidos por padrão [10, 11].
- **Ocultação de dados pessoais:** estratégia para reduzir a exposição dos dados pessoais, restringindo seu acesso e dificultando sua identificação por pessoas não autorizadas [9]. Entre as estratégias recomendadas estão a restrição de acesso baseada em perfis, criptografia, ofuscação, dissociação e demais técnicas destinadas à proteção da confidencialidade dos dados. Algumas estratégias de ocultação incluem:
  - **Restrição**: prevenir o acesso não autorizado a dados pessoais. Implementar controle de acesso em perfis (RBAC) e necessidade de conhecimento (*need-to-know)*.
  - **Embaralhamento:** processar dados aleatoriamente dentro de um grupo suficientemente grande para reduzir correlação. Em pesquisas de satisfação, exibir as respostas em ordem aleatória antes da análise agregada.
  - **Criptografia:** criptografar dados em trânsito e em repouso. Utilizar TLS 1.3 para comunicação e AES-256 para armazenamento de dados sensíveis em bancos governamentais.
  - **Ofuscação:** tornar os dados pessoais incompreensíveis para impedir sua decifração. Substituir parte de um número de telefone ou CPF por asteriscos em interfaces de atendimento.
  - **Dissociação:** remover a correlação entre diferentes partes de dados pessoais. Armazenar *logs* de acesso sem o identificador direto do usuário, usando *hashes* temporários.
- **Desvinculação:** processar os dados pessoais de forma que estes não possam ser associados a outras fontes de dados, ou que tal associação demande um esforço considerável (em termos de tempo, custo ou tecnologia). Essa meta reduz o risco de uso indevido de dados pessoais, de formação de perfis não autorizados (*profiling*) e de

correlação indevida entre bases de dados distintas. A desvinculação está alinhada aos princípios da LGPD de adequação (art. 6º, II), finalidade (art. 6º, I), necessidade (art. 6º, III), segurança (art. 6º, VII) e prevenção (art. 6º, VIII) [1]. Na Administração Pública federal, a desvinculação é particularmente relevante quando se integram dados de diferentes sistemas governamentais (ex.: CadÚnico, CNIS, sistemas de saúde, educação, tributação). Algumas estratégias de desvinculação incluem:

  - Utilizar identificadores diferentes para o mesmo titular em contextos distintos, evitando chaves comuns (como CPF) quando não estritamente necessário;
  - Adotar pseudonimização ou anonimização sempre que a finalidade do tratamento não exigir a identificação direta;
  - Manter bases de dados separadas e com controles de acesso independentes, aplicando a estratégia “separar”.

- **Separação:** tem por objetivo distribuir o tratamento de dados pessoais em compartimentos separados em vez de centralizar, evitando a combinação indevida de diferentes fontes. A separação deve ser acompanhada de controles de acesso, criptografia, registro de operações e regras de integração para impedir recombinação indevida ou concentração de dados em outros pontos da cadeia de tratamento [9]. Algumas estratégias de separação incluem:

  - **Distribuição:** particionar dados pessoais de modo que sejam necessárias múltiplas autorizações para acessá-los integralmente. Separar dados cadastrais (nome, CPF) de dados de saúde (diagnóstico) em bancos distintos, com controles de acesso independentes.
  - **Isolamento:** processar partes de dados pessoais de forma independente, sem correlação com outras partes. Utilizar identificadores diferentes para o mesmo cidadão em sistemas de assistência social e de educação, evitando vinculação por padrão.

Os mecanismos apresentados concretizam a aplicação deste princípio ao assegurar que sistemas adotem, desde sua configuração inicial, práticas que reduzam a exposição e o tratamento desnecessário de dados pessoais, garantindo que a privacidade seja protegida por padrão.

## 2.3 Privacidade incorporada ao projeto (*Privacy by design*)

Este princípio requer que a proteção de dados pessoais seja incorporada à concepção e à arquitetura de quaisquer projetos ou práticas de negócio, desde a fase de requisitos até a desativação. A privacidade deve fazer parte das funções principais de qualquer sistema, serviço ou produto [5].

A incorporação deve ser:

- **Holística:** considera contextos mais amplos, interações com outros sistemas e o ciclo de vida completo dos dados;
- **Integrada**: envolve todas as partes interessadas (titulares, controladores, operadores, encarregado, áreas de TI, jurídico, auditoria);

- **Criativa:** busca soluções inovadoras que atendam à privacidade sem sacrificar a funcionalidade.

No âmbito da APF, isso significa, por exemplo, que, ao desenvolver ou contratar um novo sistema de atendimento ao cidadão, a equipe de projeto deve realizar avaliação de riscos de privacidade e, quando aplicável, elaborar o RIPD ainda na fase de levantamento de requisitos, antes do início das atividades de tratamento, com revisões periódicas sempre que necessário, cabendo ao controlador, com apoio do encarregado, conduzir sua elaboração e documentar os riscos identificados e as medidas mitigadoras adotadas [9].

Nesse contexto, os sistemas devem ser concebidos de forma a permitir que os titulares exerçam seus direitos previstos na LGPD de maneira simples e efetiva. Para isso, recomenda-se disponibilizar mecanismos que possibilitem acesso, correção, eliminação, oposição e demais formas de intervenção previstas na legislação. A possibilidade de intervenção assegura que os titulares dos dados pessoais, bem como os controladores em relação a seus operadores, possam intervir no tratamento sempre que necessário, implementando medidas de correção, limitação, oposição ou eliminação. Os direitos dos titulares elencados no art. 18 da LGPD conferem essa capacidade de intervenção [1].

A possibilidade de intervenção também está associada aos princípios da LGPD de qualidade dos dados (art. 6º, V) e responsabilização e prestação de contas (art. 6º, X) [1]. Melhores práticas como a ISO/IEC 29100:2024 (princípio do “acesso e retificação”) [8] também abordam a intervenção como requisito fundamental. Algumas estratégias de intervenção incluem:

- Formulários digitais de requisição de direitos (acesso, correção, exclusão, portabilidade, oposição, revogação de consentimento) integrados à identidade GOV.BR.
- Interface de Programação de Aplicações (*Application Programming Interfaces* – APIs) de atendimento de direitos que permitam a interoperabilidade entre sistemas de diferentes órgãos (ex.: ao solicitar exclusão de dados no órgão A, comunicar automaticamente os órgãos B e C que receberam cópias).
- Prazos automáticos e acompanhamento: o sistema deve registrar a data da solicitação, controlar o prazo de 15 dias (LGPD, art. 19) e permitir prorrogação justificada.
- Mecanismos de verificação de identidade que não exijam dados adicionais desproporcionais (ex.: usar o nível de confiança já existente no GOV.BR).
- Registro de consentimento (*consent receipt*): documento ou *hash* que comprove o consentimento dado, com data, finalidade e versão da política.

Como exemplo, um cidadão que não quer mais receber comunicações de um serviço público pode, por meio do portal único, revogar essa opção e solicitar a eliminação de seus dados de contato para essa finalidade. O sistema deve processar a solicitação, confirmar a eliminação e, se for o caso, informar sobre dados que não podem ser excluídos em razão de obrigação legal (ex.: retenção para fins de auditoria tributária) [1].

Além do RIPD e do indicador usado para aferir a maturidade relacionada às medidas de privacidade do órgão ou entidade pública (iPriv) conforme previsto no PPSI [2], outras práticas de avaliação devem ser adotadas:

- **Auditorias internas e externas de privacidade:** permitem verificar a conformidade com políticas, processos e requisitos legais, bem como testar a efetividade dos controles implementados. Embora não haja uma determinação legal específica sobre a periodicidade de auditorias externas na LGPD, a realização dessas avaliações fortalece a *accountability* do órgão.
- **Avaliação de riscos:** é o processo estratégico de identificar, avaliar e mitigar as ameaças ao uso e tratamento de dados pessoais. Ao contrário da segurança da informação tradicional (que foca em proteger o dado contra invasões), a gestão de privacidade foca em **proteger o titular dos dados** contra impactos negativos causados pelo uso dessas informações (LGPD, art. 50) [1].
- **Metodologia de gestão de riscos de privacidade da ENISA:** a ENISA oferece referências e ferramentas que auxiliam organizações na avaliação de riscos e na seleção de tecnologias de aprimoramento da privacidade. O PETs Control Matrix facilita avaliações padronizadas e comparativas de ferramentas de privacidade, com critérios aplicáveis a categorias como mensagens seguras, VPNs, redes anônimas e ferramentas anti-rastreamento. Recomenda-se que os órgãos utilizem essa ferramenta na seleção de soluções de privacidade, observando a finalidade, a proporcionalidade e o risco do tratamento [12].

Por fim, a documentação sistemática de todas as atividades de avaliação é indispensável para comprovar conformidade, nos termos do princípio da responsabilização e prestação de contas da LGPD [1]. Recomenda-se que os órgãos mantenham atualizados e disponíveis para auditoria:

- Registro das Operações de Tratamento de Dados Pessoais (*Records of Processing Activities* – ROPA)): mapeamento de todos os tratamentos realizados, com finalidades, bases legais, fluxos e compartilhamentos [3].
- RIPD: em situações em que o tratamento passa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme a legislação aplicável e as determinações da ANPD [1, 9].
- Resultados do iPriv e planos de ação associados para melhoria da maturidade [3].
- Registros de incidentes com dados pessoais, com lições aprendidas.
- Relatórios de auditoria e respectivas evidências de implementação de recomendações.

Esses mecanismos concretizam a aplicação deste princípio ao assegurar que a privacidade seja trabalhada desde a fase de concepção de novos produtos ou serviços ofertados pelos órgãos ou entidades públicas.

## 2.4 Funcionalidade total (*Full functionality – positive-sum*)

Este princípio, também referido como “soma positiva, não soma-zero”, rejeita a falsa dicotomia de que se deve escolher entre privacidade ou funcionalidade, privacidade ou segurança, privacidade ou benefício comercial. Ao contrário, defende que todos os requisitos legítimos podem ser atendidos simultaneamente de forma equilibrada [5].

Na administração pública, dilemas comuns incluem: como oferecer um serviço personalizado sem coletar dados excessivos? Como assegurar transparência sem expor dados pessoais sensíveis? A solução está em buscar alternativas de desenho que conciliem os interesses, como o uso de pseudonimização, agregação estatística ou computação que preserva a privacidade (ex.: privacidade diferencial).

Ao projetar um serviço, recomenda-se:

- Identificar e documentar todos os interesses e requisitos legítimos da organização e dos titulares.
- Caso uma solução ameace a privacidade, buscar alternativas que alcancem a mesma finalidade com menor risco, documentando as escolhas.

Nesse contexto, é necessário tratar os dados pessoais no mais alto nível de agregação possível, com o mínimo de detalhes, preservando a utilidade estatística ou gerencial. A agregação pode ser implementada por diferentes formas de redução do nível de detalhamento dos dados, preservando sua utilidade para análises estatísticas ou gerenciais [8]. Algumas técnicas incluem:

- **Resumo:** extrair semelhanças e processar correlações em vez dos dados individuais. Por exemplo: converter datas de nascimento individuais em faixas etárias ou consolidar registros diários de frequência escolar em médias mensais por turma.
- **Agrupamento:** alocar dados pessoais em categorias comuns antes do processamento. Por exemplo: em relatórios de desempenho escolar, apresentar resultados por escola ou município, não por aluno.

Essas práticas permitem utilizar informações para fins analíticos e de gestão sem expor, de forma desnecessária, dados individualizados dos titulares.

A utilização de técnicas que permitem realizar operações matemáticas e estatísticas sobre dados sensíveis sem expor os dados subjacentes, ou seja, sem comprometer a confidencialidade também é uma boa prática [12]. Algumas técnicas comuns incluem:

- **Criptografia homomórfica:** permite computar sobre dados criptografados, obtendo resultado criptografado que, quando decifrado, é idêntico ao resultado que seria obtido sobre os dados em texto claro. Por exemplo, processamento de dados fiscais ou de saúde sem descriptografar individualmente.
- **Privacidade diferencial:** adiciona ruído controlado a consultas estatísticas, garantindo que a inclusão ou exclusão de um único indivíduo não altere significativamente o resultado. Por exemplo, publicação de estatísticas de censo, pesquisas de emprego, indicadores de saúde pública.
- **Computação multipartidária segura (MPC):** múltiplas partes calculam conjuntamente uma função sobre suas entradas privadas, sem revelá-las às outras. Por exemplo, consórcios entre entes federativos para cruzamento de dados sem compartilhar as bases brutas.

- **Aprendizado federado:** modelos de *machine learning* são treinados localmente em cada dispositivo ou servidor, e apenas os parâmetros agregados são compartilhados. Por exemplo, análise de padrões de uso de serviços públicos sem centralizar dados sensíveis dos cidadãos.

Também a **anonimização** e **pseudonimização** são boas práticas utilizadas, sempre que a finalidade do tratamento permitir, para reduzir a identificação direta dos titulares. A aplicação dessas técnicas possibilita a utilização dos dados pessoais para finalidades legítimas sem exposição desnecessária das pessoas naturais [1, 8].

Da mesma forma, a integração das três metas de segurança (confidencialidade, integridade, disponibilidade) com as três metas específicas de privacidade (desvinculação, transparência, intervenção), conforme demonstrado na **Figura 1**, é fundamental para o princípio da funcionalidade total [8]. Nesse contexto, a **Tabela 1** apresenta um conjunto de técnicas que podem ser utilizadas para correlação dessas metas.

**Tabela 1:** integração das metas de segurança e privacidade

| Categoria | Meta | Descrição operacional |
|---|---|---|
| Segurança da Informação | Confidencialidade | Impedir acessos não autorizados a dados pessoais (ex.: criptografia, RBAC, MFA). |
| Segurança da Informação | Integridade | Garantir que os dados pessoais não sejam alterados indevidamente (ex.: logs, *checksums*, validações). |
| Segurança da Informação | Disponibilidade | Assegurar que sistemas e dados estejam acessíveis quando necessários (ex.: redundância, *backup*, DRP). |
| Privacidade | Desvinculação | Evitar a correlação indevida de dados entre diferentes bases governamentais (ex.: pseudonimização, separação de contextos). |
| Privacidade | Transparência | Informar claramente sobre as atividades de tratamentos, finalidades e direitos (ex.: avisos de privacidade, painéis, encarregado acessível). |
| Privacidade | Intervenção | Permitir que o cidadão exerça seus direitos (acesso, correção, exclusão, oposição) de forma simples e rápida. |

Essas seis metas, quando implementadas de forma integrada desde a concepção, estabelecem uma estrutura robusta de privacidade e proteção de dados pessoais.

Além disso, a adoção de Tecnologias de Aprimoramento da Privacidade (*Privacy-Enhancing Technologies* – PETs) como **ofuscação**, **criptografia** e **descentralização,** também contribui para a implementação prática dos princípios da **Privacidade desde a Concepção e por Padrão** [12]. A **Tabela 2** apresenta exemplos de implementação dessas tecnologias.

**Tabela 2:** exemplos de tecnologias de aprimoramento da privacidade aplicáveis aos princípios deste guia

| Categoria | Problema que resolve | Exemplo |
|---|---|---|
| Ofuscação de dados | Evitar a identificação quando a finalidade do tratamento não exige a vinculação direta. | Publicar estatísticas de saúde por região em vez de dados individualizados (k-anonimato, l-diversidade). Utilizar pseudônimo em pesquisas de opinião pública. |
| Criptografia de dados | Garantir a confidencialidade e integridade, mesmo que o meio de armazenamento ou transmissão seja comprometido. | Criptografar comunicações com TLS 1.3; armazenar dados sensíveis com criptografia AES-256; utilizar criptografia homomórfica para processar dados sem descriptografá-los. |
| Descentralização de dados | Evitar a concentração excessiva de dados pessoais em um único controlador ou base centralizada. | Compartilhar apenas parâmetros agregados de modelos (aprendizado federado) em vez de mover dados brutos entre órgãos; processar dados localmente na ponta. |

Por fim, destaca-se que, para além das tecnologias voltadas diretamente à proteção dos dados pessoais, a implementação da **Privacidade Desde a Concepção e Por Padrão** também depende da adoção de mecanismos de governança e conformidade, como registros de tratamento, auditorias, **indicadores de maturidade** e **RIPDs**, abordados ao longo deste guia.

## 2.5 Segurança fim a fim (*End-to-end security*)

A privacidade não existe sem segurança. Este princípio estabelece que a proteção dos dados pessoais deve ser garantida desde a coleta até a eliminação, abrangendo todo o ciclo de vida. Sem medidas fortes de segurança, não é possível assegurar a confidencialidade, a integridade e a disponibilidade dos dados, requisitos básicos para a privacidade [5].

As medidas técnicas e administrativas recomendadas incluem:

- Pseudonimização ou anonimização sempre que a finalidade permitir;
- Controle de acesso baseado em perfis e no princípio do menor privilégio;
- Criptografia de dados em repouso, em trânsito e, sempre que possível, em uso (criptografia homomórfica);
- Destruição segura dos dados ao final de sua vida útil, incluindo *backups*.

No âmbito do SISP, a segurança fim a fim deve ser documentada em políticas de segurança da informação e verificada por auditorias periódicas, conforme disposto no PPSI 2.0 [2, 3] e na Estratégia Nacional de Segurança Cibernética (Decreto nº 12.573/2025) [8]. Dentre as estratégias utilizadas, destacam-se: autenticação, credenciais baseadas em atributos, comunicações privadas seguras, privacidade em banco de dados, privacidade de armazenamento e anonimato e pseudônimo nas comunicações.

**Autenticação**

Processo de verificação da identidade do usuário que tenta acessar uma área restrita de um sistema ou serviço. É a primeira linha de defesa para garantir que apenas o titular dos dados pessoais (ou partes autorizadas) possa acessar informações pessoais [12]. Algumas estratégias de autenticação incluem:

- Os protocolos de autenticação devem proteger as identidades contra captura por terceiros (ex.: evitar envio de credenciais em texto plano).
- Não devem permitir personificação (*spoofing*) ou dedução da identidade a partir da observação da sessão autenticada.
- Sempre que possível, adotar autenticação multifator (MFA), especialmente para serviços que tratam dados sensíveis ou que permitem exercício de direitos (acesso, correção, exclusão), em alinhamento com diretrizes atuais de identidade digital [12].

Como exemplo no setor público, podemos citar o uso do GOV.BR como provedor de identidade digital, com níveis de garantia adequados ao risco (bronze, prata, ouro), evitando a criação de credenciais locais separadas, que aumentam a superfície de ataque e dificultam a gestão de identidades.

**Credenciais baseadas em atributos**

Técnica de gerenciamento de identidades que permite autenticar de forma flexível e seletiva determinados atributos de uma entidade (ex.: “maior de 18 anos”, “servidor público”, “residente do DF”) sem revelar informações adicionais sobre a entidade [12]. Algumas estratégias de implementação incluem:

- Basear-se em provas de conhecimento zero (*zero-knowledge proofs*), em que o titular prova a posse de um atributo sem divulgar o atributo em si ou sua identidade completa.
- Armazenar os atributos em credenciais digitais emitidas por uma autoridade confiável, permitindo que sejam utilizados para comprovar informações específicas do titular durante o processo de autenticação.

Como exemplo no setor público podemos citar um serviço de vacinação em que o cidadão pode provar que pertence ao grupo prioritário (ex.: “idade ≥ 60 anos”) sem revelar sua data exata de nascimento ou nome completo. A aplicação recebe apenas a confirmação do atributo, minimizando a coleta de dados.

**Comunicações privadas seguras**

Métodos e tecnologias que garantem confidencialidade, integridade e autenticidade das informações trocadas entre duas partes, protegendo contra interceptação, manipulação ou divulgação indevida [13]. As principais tecnologias relacionadas incluem:

- Protocolo de Transferência de Hipertexto Seguro (*Hypertext Transfer Protocol Secure* – HTTPS) com a Segurança da Camada de Transporte (*Transport Layer Security* – TLS) versão 1.3 ou superior para as comunicações web.

- Rede Privada Virtual (*Virtual Private Network* – VPN) para tráfego entre redes internas governamentais, especialmente quando utilizado por servidores em teletrabalho.
- Assinaturas digitais para garantir autenticidade e não repúdio em mensagens ou documentos eletrônicos.
- Criptografia de ponta a ponta (*End-to-End Encryption* – E2EE) para aplicações de mensageria institucional.

Como exemplo no setor público podemos citar os portais e serviços digitais de um órgão que exigem HTTPS com TLS 1.3, configuração de HTTP Segurança Estrita de Transporte HTTP (HTTP *Strict Transport Security* – HSTS) e utilização de certificados digitais ICP-Brasil. Em APIs de integração entre sistemas, há o emprego do mutual TLS (mTLS) para autenticação mútua.

**Privacidade em banco de dados**

Conjunto de práticas e medidas para proteger dados pessoais armazenados em bancos de dados, garantindo que apenas pessoas autorizadas acessem as informações e que esses dados sejam utilizados conforme a finalidade [1, 15]. Algumas estratégias de privacidade em banco de dados incluem:

- **Proteção de dados tabulares**: supressão de célula, generalização, k-anonimato. Por exemplo, em bases de dados de pesquisas de saúde, suprimir valores raros (ex.: idade 107 anos) para evitar reidentificação.
- **Proteção de banco de dados consultável:** perturbação de consulta, restrição de consulta. Por exemplo, limitar o número de linhas retornadas por consulta ou adicionar ruído em contagens.
- **Proteção de microdados:** mascaramento de dados, síntese de dados. Por exemplo, substituir nomes por identificadores sequenciais, e datas por intervalos.
- **Mascaramento dinâmico (*dynamic data masking*):** para usuários que não precisam ver os dados completos.
- **Registros de eventos de banco de dados:** manter registros de eventos de acesso a bancos de dados que contenham dados pessoais, com trilha de auditoria.
- **Separação de banco de dados:** utilizar bancos de dados separados para contextos distintos (estratégia de separação).

Como exemplo no setor público, podemos citar um sistema de gestão de pessoas em que dados cadastrais, funcionais e financeiros dos servidores são armazenados de forma segregada, com acesso definido conforme o perfil do usuário. Informações sensíveis ou não necessárias à atividade desempenhada podem ser mascaradas, enquanto os acessos e consultas realizados são registrados para fins de auditoria.

**Privacidade de armazenamento**

Proteção da confidencialidade e integridade das informações armazenadas em dispositivos de armazenamento (discos rígidos, servidores, nuvens de dados), garantindo que apenas

usuários autorizados tenham acesso e que os dados permaneçam íntegros [13]. Algumas estratégias incluem:

- **Criptografia em repouso (ex.: AES-256):** para discos inteiros (full disk encryption) ou para arquivos/pastas específicas.
- **Armazenamento esteganográfico:** ocultar a existência dos dados (uso restrito e com justificativa).
- **Gerenciamento de chaves:** utilizar serviços de gerenciamento de chaves (KMS) com rotação periódica e segregação de funções.
- **Armazenamento privado em configurações remotas:** em nuvem pública, utilizar Criptografia do Lado do Cliente (*Client-Side Encryption* – CSE), de modo que o provedor de nuvem não tenha acesso às chaves.

Como exemplo no setor público podemos citar sistemas em nuvem cujos provedores oferecem criptografia gerenciada pelo cliente e demonstram conformidade com a LGPD e com a **Estratégia Nacional de Segurança Cibernética** [1, 16].

**Anonimato e pseudônimo nas comunicações**

Técnicas que protegem os metadados de comunicação (quem fala com quem, horário, volume, duração, localização) além do conteúdo da mensagem. Metadados podem comprometer a privacidade mesmo quando o conteúdo está criptografado [12]. Algumas estratégias incluem:

- **Proxies e VPNs únicos**: ocultam o endereço IP original, mas podem manter logs.
- **Roteamento em camadas (ex.: Tor):** a mensagem passa por múltiplos relays, cada um conhecendo apenas o nó anterior e seguinte, dificultando o rastreamento.
- **Redes mistas (mix networks):** embaralham a ordem e o timing das mensagens.
- **Pseudônimos descartáveis:** permitem que o cidadão interaja com o serviço sem revelar sua identidade permanente.

Como exemplo no setor público podemos citar pesquisas de opinião ou coleta de denúncias (ex.: ouvidorias) nas quais se pode permitir o envio anônimo ou com pseudônimo, sem exigir autenticação com o GOV.BR. Os logs de acesso devem ser minimizados ou anonimizados.

**Atenção**: o anonimato pode conflitar com a necessidade de responsabilização em certos contextos (ex.: processos administrativos). A escolha da técnica deve considerar a finalidade e a base legal.

## 2.6 Visibilidade e transparência

A promoção da visibilidade e da transparência é essencial para demonstrar conformidade e responsabilidade (*accountability*) quanto ao tratamento de dados pessoais, bem como para gerar confiança nos titulares. Este princípio garante que todas as partes envolvidas no tratamento de dados pessoais possam verificar, de forma independente, se as práticas declaradas estão sendo efetivamente seguidas. A transparência está diretamente ligada aos

princípios da LGPD de livre acesso (art. 6º, IV), transparência (art. 6º, VI) e não discriminação (art. 6º, IX), bem como ao princípio da responsabilização e prestação de contas (art. 6º, X) [1].

Na prática, os órgãos devem assegurar:

- Publicação e manutenção atualizada de políticas de proteção de dados pessoais e avisos de privacidade;
- Identificação do encarregado pelo tratamento de dados pessoais e disponibilização pública de seus canais de contato [17];
- Mecanismos de prestação de contas, como relatórios de impacto (RIPD) e auditorias independentes.

A transparência também se estende ao desenho das interfaces eletrônicas, devendo ser evitados padrões obscuros (*dark patterns*) que induzam o titular a decisões prejudiciais à sua privacidade [10].

A transparência garante que todo o tratamento de dados pessoais possa ser compreendido pelos titulares e pela sociedade em geral. É a garantia de informações claras, precisas, acessíveis e atualizadas sobre a realização do tratamento, os agentes envolvidos, as finalidades, os riscos e os direitos dos titulares, observados os segredos comercial e industrial e a segurança institucional. Nesse contexto, algumas estratégias incluem:

- **Entrega:** disponibilizar amplos recursos sobre o processamento, incluindo políticas e riscos. Por exemplo, publicar o aviso de privacidade no canal de disponibilização do serviço.
- **Notificação:** alertar os titulares sobre qualquer nova informação relevante sobre o tratamento. Por exemplo, enviar comunicado por e-mail ou *push* quando houver alteração no **aviso de privacidade**.
- **Explicação:** detalhar as informações sobre o processamento de forma concisa e compreensível. Utilizar linguagem clara, exemplos e ícones nos avisos de privacidade.

Na prática, para promover a transparência recomenda-se:

- Avisos de privacidade disponibilizados em linguagem clara e em múltiplos canais (portal, aplicativo, atendimento presencial);
- Painéis de privacidade (*privacy dashboards*) que permitam ao cidadão visualizar, de forma agregada, quais dados pessoais são tratados, por qual fundamento legal, com quem são compartilhados e por quanto tempo são retidos;
- Publicação da identidade e das informações de contato do Encarregado pelo Tratamento de Dados Pessoais, bem como dos meios para exercício de direitos (arts. 18 a 22 da LGPD) [1, 17];
- RIPD, quando exigidos.

Existem outras técnicas que visam dar aos titulares uma compreensão ainda mais clara de quais dados pessoais são coletados, como são utilizados, com quem são compartilhados e por

quanto tempo são retidos, conforme exigido pelos princípios da transparência (LGPD, art. 6º, VI) e livre acesso (art. 6º, IV) [1].

As principais técnicas incluem:

- **Painéis de privacidade (*privacy dashboards*):** interfaces que consolidam informações de tratamento e permitem ao titular exercer direitos (acesso, correção, exclusão). Exemplo: um painel mostrando quais órgãos acessaram seus dados, quando e para qual finalidade.
- **Notificações de privacidade proativas:** envio de alertas quando houver alteração no aviso de privacidade, compartilhamento com novos terceiros ou detecção de comportamento incomum.
- **Ícones e rótulos de privacidade (*nutrition labels*):** representação gráfica simplificada que indica, com ícones e cores, as práticas de coleta, uso e compartilhamento.
- **Formatos legíveis por máquina** (ex.: JSON com estrutura padronizada) para que agentes automatizados possam comparar e avaliar políticas.

Como exemplo no setor público podemos citar um órgão cujo portal “orgao.gov.br/servicos” exibe, antes do login, um resumo conciso (tópicos ou ícones) de quais dados serão tratados, se haverá compartilhamento e quais os direitos do cidadão, com link para o aviso de privacidade completo.

Por fim, a transparência também exige que os órgãos mantenham documentação capaz de demonstrar a conformidade das atividades de tratamento de dados pessoais, incluindo registros, relatórios e demais evidências que possam ser apresentados à ANPD ou aos titulares quando necessário. A demonstração de conformidade também pode ser fortalecida por meio da manutenção de registros atualizados das avaliações realizadas, incluindo relatórios de impacto, auditorias e indicadores de maturidade, de forma a evidenciar a evolução contínua das práticas de privacidade perante a organização e os órgãos de controle e de fiscalização [1, 2].

Esses mecanismos concretizam a aplicação deste princípio ao assegurar visibilidade e transparência desde a fase de concepção de novos produtos ou serviços ofertados pelos órgãos ou entidades públicas.

## 2.7 Respeito pela privacidade do usuário

O sétimo princípio coloca os direitos e liberdades dos titulares no centro de qualquer projeto. Significa projetar produtos e serviços com o titular em mente, antecipando suas necessidades e garantindo meios efetivos para que ele exerça controle sobre seus dados [5].

Para atender a este princípio, os órgãos e entidades devem observar:

- a qualidade dos dados, no sentido de exatidão, clareza, relevância e se estão atualizados;
- o acesso facilitado ao titular quanto às informações sobre dados pessoais tratados, bem como os usos e compartilhamentos realizados;

- os mecanismos de reclamação e reparação, com instruções claras sobre como acionar o encarregado pelo tratamento de dados pessoais e a ANPD.

Nesse contexto, algumas estratégias incluem:

- **Hipótese legal e finalidade adequada:** processar dados pessoais com hipótese legal válida e finalidade específica, nunca genérica, vinculada a dispositivo legal relacionado às competências do órgão ou entidade pública.
- **Escolha granular:** quando aplicável, permitir ao usuário aceitar, recusar ou personalizar, de forma granular, o tratamento de seus dados, podendo autorizar ou excluir determinadas finalidades parcial ou totalmente. As opções devem ser apresentadas de forma clara, equilibrada e sem indução à escolha de determinada alternativa.
- 
- **Atualização:** fornecer meios para que os titulares mantenham seus dados pessoais precisos e atualizados. Disponibilizar painel de autoatendimento (“Minhas informações”) no portal institucional.
- **Eliminação:** respeitar o direito do titular à eliminação dos dados pessoais em tempo hábil, quando aplicável, observadas as hipóteses legais de conservação. Implementar processo automatizado para solicitação de exclusão, com confirmação e cumprimento no prazo legal (art. 18 da LGPD) [1].
- **Exercício dos direitos do titular:** os produtos e serviços devem ser concebidos de forma a permitir que os titulares exerçam, de maneira simples e efetiva, os direitos previstos na LGPD, incluindo acesso, correção, anonimização, bloqueio, eliminação, portabilidade, revogação do consentimento e oposição ao tratamento, quando aplicáveis.
- **Qualidade e acesso aos dados:** os órgãos e entidades devem assegurar que os dados pessoais tratados permaneçam exatos, claros, relevantes e atualizados, bem como disponibilizar mecanismos que permitam aos titulares consultar as informações tratadas, conhecer seus compartilhamentos e solicitar correções sempre que necessário. Os órgãos e entidades devem disponibilizar mecanismos de autoatendimento que permitam aos titulares manter seus dados pessoais atualizados e exercer seus direitos de forma simples e acessível.
- **Canais de atendimento ao titular:** os titulares devem dispor de canais acessíveis para exercer seus direitos, apresentar reclamações e obter informações sobre o tratamento de seus dados pessoais, incluindo os canais de contato do encarregado pelo tratamento de dados pessoais e orientações para comunicação com a ANPD.

## 2.8 Recomendações finais

A implementação da privacidade desde a concepção e por padrão não se limita à adoção de controles específicos ou ao atendimento de requisitos normativos. Trata-se de uma abordagem de governança que busca incorporar a proteção de dados pessoais como elemento permanente do planejamento, desenvolvimento, operação e melhoria dos serviços públicos.

Nesse contexto, os princípios, estratégias e mecanismos apresentados neste Guia devem ser continuamente avaliados e aperfeiçoados pelos órgãos e entidades, considerando seus riscos, sua realidade institucional e seu estágio de maturidade em privacidade. Instrumentos como o RIPD, o iPriv, as auditorias de privacidade e as autoavaliações de riscos podem apoiar esse processo, fornecendo subsídios para a identificação de oportunidades de melhoria e para o fortalecimento da conformidade.

A utilização de ciclos contínuos de planejamento, implementação, avaliação e aperfeiçoamento contribui para consolidar uma cultura organizacional orientada à proteção de dados pessoais, fortalecendo a confiança da sociedade e promovendo a efetividade das ações de privacidade na Administração Pública Federal.

# Referências bibliográficas


1. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 jun. 2026.

2. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (Brasil). **Guia do Framework de Privacidade e Segurança da Informação (PPSI 2.0)**. Brasília, DF: MGI, 2026. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0. Acesso em: 26 jun. 2026.

3. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025**. Institui o Programa de Privacidade e Segurança da Informação no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Diário Oficial da União: seção 1, Brasília, DF, 2025. Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 28 jul. 2026.

4. BRASIL. **Decreto nº 7.579, de 11 de outubro de 2011**. Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, do Poder Executivo Federal. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm. Acesso em: 27 jul. 2026.

5. CAVOUKIAN, Ann. **Privacy by Design**: The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario, 2011. Disponível em: https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd-1.pdf. Acesso em: 26 jun. 2026.

6. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 26 jun. 2026.

7. EUROPEAN DATA PROTECTION BOARD. **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default**. Versão final. Bruxelas: EDPB, 2020. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. Acesso em: 26 jun. 2026.

8. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 29100:2024**: Security techniques – Privacy framework. Genebra: ISO, 2024. Disponível em: https://www.iso.org/standard/85938.html. Acesso em: 26 jun. 2026.

9. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, DF: ANPD, [2023]. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 26 jun. 2026.

10. EUROPEAN DATA PROTECTION BOARD. **Guidelines 3/2022 on Dark patterns in social media platform interfaces**: how to recognise and avoid them. Versão final. Bruxelas: EDPB, 2023.

Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Acesso em: 26 jun. 2026.

11. INFORMATION COMMISSIONER'S OFFICE (UK). **Data protection by design and by default**. Wilmslow: ICO, [2026]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/. Acesso em: 26 jun. 2026.

12. EUROPEAN UNION AGENCY FOR CYBERSECURITY. **PETs controls matrix**: A systematic approach for assessing online and mobile privacy tools. Atenas: ENISA, 2016. Disponível em: https://www.enisa.europa.eu/publications/pets-controls-matrix. Acesso em: 26 jun. 2026.

13. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2022**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Genebra: ISO, 2022. Disponível em: https://www.iso.org/standard/27001.html. Acesso em: 26 jun. 2026.

14. BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 26 jun. 2026.

15. BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 18, de 16 de julho de 2024**. Aprova o Regulamento sobre a indicação do Encarregado pelo tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 17 jul. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd. Acesso em: 26 jun. 2026.

gov.br

# Dúvida?

**Entre em contato conosco**

Sítio do PPSI:
PPSI 2.0 — Governo Digital