Guia sobre Privacidade desde a Concepção e por Padrão

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0

Brasília, março de 2024

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

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Bruno Pierre Rodrigues de Sousa

Francisco Magno Felix Nobre

Ivaldo Jeferson De Santana Castro

Leonard Keyzo Yamaoka Batista

Rafael Da Silva Ribeiro

Raphael César Estevão

Equipe Técnica de Revisão

Adriano de Andrade Moura

Rodrigo Duran Lima

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
21/03/2024	1.0	Primeira versão do Guia sobre Privacidade desde a Concepção e por Padrão.	Equipe Técnica de Elaboração

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na adoção de medidas de privacidade desde a concepção e por padrão, em atendimento ao previsto no art. 46º, § 2º da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que, desde a fase de concepção do produto ou serviço até a sua execução, 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.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO), do *National Institute of Standards and Technology* (NIST) e de Autoridades de Proteção de Dados. Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e

e) caso o leitor deseje se certificar de que atende integralmente aos requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, à ABNT, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para a elaboração **deste documento**.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas **neste documento**.

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e as entidades da Administração Pública Federal, direta, autárquica e fundacional a adotar medidas de privacidade, desde a concepção e por padrão, no âmbito institucional.

Os Controles 24, 25 e 26 do Guia do Framework de Privacidade e Segurança da Informação (p. 63 a 65), estabelece que:

Controle 24: Minimização de Dados – *O órgão, dentro dos limites de suas competências legais, deve implementar ações para não coletar e tratar de forma inadequada ou excessiva os dados pessoais dos titulares de dados pessoais e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada.*

Controle 25: Gestão do Tratamento – *A gestão do tratamento visa a limitar o uso, a retenção e a divulgação de dados pessoais ao que for estritamente necessário para cumprir propósitos específicos, explícitos e legítimos.*

Controle 26: Acesso e Qualidade – *O acesso e qualidade visam a garantir que os direitos do titular, quanto ao tratamento de dados pessoais, sejam atendidos e assegurar que sejam feitos de forma exata, clara, relevante e atualizado de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Assegurar também o livre acesso aos titulares para consulta facilitada e gratuita sobre a integralidade de seus dados pessoais.*

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção dos Controles 24, 25 e 26 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 elaborado e publicado pela SGD. As medidas dos Controle 24, 25 e 26 que estão contempladas neste Guia são: 24.1, 24.2, 24.3, 24.4, 24.5, 24.6, 24.7, 24.8, 24.9, 24.10, 24.11, 24.12, 24.13, 24.14, 24.15, 25.1, 25.2, 25.3, 25.4, 25.5, 25.6, 25.7, 25.8, 25.9, 26.1, 26.2, 26.3, 26.4, 26.5, 26.6, 26.7, 26.8, 26.9, 26.10, 26.11 e 26.12.

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 15/03/2024.

A Privacidade desde a Concepção e por Padrão abrange um conjunto de ações que os agentes de tratamentos devem implementar com o intuito de garantir a privacidade dos titulares de dados pessoais desde o início do projeto até a sua execução conforme disposto no § 2º do Art. 46º da LGPD.

> *"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."*

Além disso, deve ser salientado que a privacidade dos titulares de dados pessoais deve ser adotada por padrão, garantindo que os usuários finais não necessitem tomar qualquer providência para protegerem seus dados pessoais.

Este Guia está organizado nos seguintes capítulos que descreverão informações sobre Privacidade desde a Concepção e por Padrão:

- Capítulo 1: Trata dos termos e definições;
- Capítulo 2: Aborda o conceito e os princípios fundamentais;
- Capítulo 3: Associa os princípios da LGPD aos princípios da privacidade desde a concepção;
- Capítulo 4: Descreve as metas de proteção de privacidade;
- Capítulo 5: Apresenta as estratégias de privacidade;
- Capítulo 6: Discorre sobre as técnicas de privacidade.

Os tópicos apresentados não são restritivos e o objetivo buscado não é sua adoção rigorosa. Como cada serviço possui características e especificidades próprias, o modelo deve ser adaptado para cada caso específico.

TERMOS E DEFINIÇÕES

Para auxílio na leitura deste guia, serão adotados os seguintes termos e definições no que se refere à temática de Privacidade desde a Concepção e por Padrão.

AGENTES DE TRATAMENTO: Controlador e Operador de dados pessoais.

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.

ANPD: sigla de Autoridade Nacional de Proteção de Dados.

APF: sigla de Administração Pública Federal.

BANCO DE DADOS: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

COMPUTAÇÃO EM NUVEM: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

CRIPTOGRAFIA: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

DADO PESSOAL: informação relacionada à pessoa natural identificada ou identificável.

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).

LGPD - sigla de Lei Geral de Proteção de Dados Pessoais.

MEDIDAS DE SEGURANÇA: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

PdC – Privacidade desde a Concepção.

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.

1. CONCEITO E PRINCÍPIOS FUNDAMENTAIS

As primeiras ideias de "Privacidade desde a Concepção (PdC)[2]" foram expressas na década de 1970, por meio de uma série de estudos que desencadeou em um código de práticas para preservar a privacidade de indivíduos cujos dados são tratados; e foram incorporadas na década de 1990 na diretiva de proteção de dados RL 95/46/CE[3], de acordo com o considerando 46 desta diretiva.

O termo Privacidade desde a Concepção (derivado do inglês *Privacy by Design*, *PbD*), bastante difundido e utilizado atualmente, refere-se a uma metodologia[4] constituída por um conjunto de princípios formulados na década de 1990 pela canadense e ex-comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian. A ex-comissária se embasou no FIPPs (*Fair Information Practices Principles*), uma coleção de princípios amplamente aceitos na comunidade de privacidade a serem observados no tratamento de dados pessoais. A metodologia prevê que qualquer projeto que envolva o processamento de dados pessoais deve garantir que a privacidade e a proteção de dados pessoais sejam incorporadas durante todo o seu ciclo de vida.

A metodologia desenvolvida por Cavoukian é pautada por 7 princípios[5] relacionados à privacidade desde a concepção, divididos da seguinte forma:

- proativo e não reativo; preventivo e não corretivo;
- privacidade por padrão;
- privacidade incorporada ao projeto;
- funcionalidade total;
- segurança fim a fim;
- visibilidade e transparência;
- respeito pelo usuário de privacidade.

Dentre os princípios, podemos destacar a privacidade por padrão (*privacy by default*) que significa que as configurações mais seguras de privacidade deverão ser

[2] https://gdpr-info.eu/issues/privacy-by-design/
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[4] https://www.ipc.on.ca/resource/privacybydesign/
[5] https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

aplicadas automaticamente por padrão, sem nenhuma intervenção ou providência do usuário para proteger seus dados pessoais.

Seguir os princípios de privacidade desde a concepção de um serviço/projeto reduz os riscos de privacidade e gera mais confiança, por se tratar de medidas proativas, em vez de reativas. Os princípios listados têm como objetivo evitar a ocorrência de infrações; e não de resolver infrações que tenham ocorrido. Logo, privacidade desde a concepção vem antes do fato ocorrer; e não depois.

Ao longo deste Guia serão detalhados cada um desses princípios e outras informações relacionadas a esse assunto.

1.1. PROATIVO E NÃO REATIVO; PREVENTIVO, NÃO CORRETIVO

O princípio se refere à necessidade de agir proativamente com a implementação de rotinas e metodologias de trabalho que previnam os riscos à privacidade.

Qualquer projeto, que utilize dados pessoais, deve proteger os dados desde a sua concepção, identificando os possíveis riscos aos direitos e liberdades das partes interessadas e minimizando-os para que não cheguem a resultar em danos.

Sendo assim, isso implica em:

- Um claro compromisso por parte da organização, que deve ser compreendido e promovido pela Alta Administração;
- O desenvolvimento de uma cultura de compromisso e melhoria contínua por parte de todos os colaboradores;
- Definição de deveres e responsabilidades específicas para cada membro da organização, para que todos saibam claramente suas funções ao se tratar de privacidade.

1.2. PRIVACIDADE POR PADRÃO

O princípio sugere que, quando as instituições disponibilizarem sistemas, produtos, serviços ou práticas de negócios, as configurações mais seguras de privacidade deverão ser aplicadas automaticamente por padrão, sem a necessidade de o titular tomar ações adicionais para proteger os seus dados pessoais. A privacidade deve ser a regra.

Este princípio deve ser integrado em todos os setores da organização e tornar-se uma parte intrínseca da rotina de negócios. Antes de iniciar um novo projeto, implementar novos fluxos ou controles, ou introduzir um serviço ou produto, é imperativo que a Privacidade desde a Concepção e por Padrão seja adequadamente atendida.

A Privacidade por Padrão é diretamente aplicável aos princípios fundamentais da proteção de dados:

- **Especificação da finalidade**: a finalidade para a qual os dados pessoais são coletados, utilizados, retidos e divulgados deve ser informada ao titular antes ou no momento da coleta.
- **Limitação da coleta**: a coleta de dados pessoais deve ser realizada de maneira justa, legal e restrita ao necessário para os propósitos especificados.
- **Minimização de dados**: a coleta de dados pessoais deve ser limitada ao mínimo estritamente essencial. Sempre que viável, a identificação e a possibilidade de vinculação entre dados pessoais devem ser reduzidas ao mínimo necessário.
- **Uso, retenção e limitação de divulgação**: devem ser restritas aos propósitos pertinentes previamente identificados para o titular e para os quais haja consentimento, exceto quando exigido por lei de outra maneira.

1.3. PRIVACIDADE INCORPORADA AO PROJETO (*DESIGN*)

O princípio requer que seja incorporada a proteção de dados na concepção e na arquitetura de quaisquer projetos ou práticas de negócios. Deve-se garantir que a proteção de dados faça parte das funções principais de qualquer sistema, serviço ou produto.

A Privacidade Incorporada ao Projeto deve compor as tecnologias, operações e arquiteturas de informação de maneira holística, integrada e criativa:

- deve ser uma abordagem holística, pois é necessário considerar contextos adicionais e mais amplos em todos os momentos;
- deve ser uma abordagem integrada, pois é necessário consultar todas as partes interessadas;

- deve ser uma abordagem criativa, pois incorporar a privacidade pode envolver a recriação das escolhas existentes sempre que alternativas forem viáveis.

Para assegurar que a privacidade integrada seja preservada desde as etapas iniciais do projeto, deve-se:

- Considerá-la como um requisito necessário no ciclo de vida dos sistemas e serviços, bem como no desenho dos processos da organização;
- Realizar uma análise dos riscos para os direitos e liberdades das pessoas titulares dos dados pessoais e, quando apropriado, realizar avaliações de impacto relativas à proteção de dados, como parte integrante da concepção de qualquer nova iniciativa de tratamento.

1.4. FUNCIONALIDADE TOTAL

Esse princípio é igualmente referido como "soma positiva, não soma-zero" e preconiza que todas as funcionalidades devem ser abrangentes e seguras, proporcionando benefícios tanto para o titular de dados pessoais quanto para a organização.

O propósito subjacente a esse princípio é buscar um equilíbrio ideal entre os requisitos estabelecidos em um projeto, uma vez que se entende que a privacidade é obtida às custas de outras funcionalidades, tais como dilemas entre privacidade e usabilidade, privacidade e funcionalidade, privacidade e benefício comercial, e até mesmo a dicotomia entre privacidade e segurança. Dessa forma, rejeita-se, por exemplo, a crença de que sistemas ou serviços só podem possuir ou privacidade ou segurança, e não ambas simultaneamente.

Para isso, desde as etapas iniciais do desenvolvimento de um projeto, uma organização deve:

- Assumir que podem coexistir interesses diferentes e legítimos, tanto da organização quanto dos usuários a quem prestam serviços, e que é necessário identificá-los, avaliá-los e equilibrá-los em conformidade.
- Estabelecer canais de comunicação para colaboração e consulta dos participantes, a fim de compreender e reunir múltiplos interesses que, à primeira vista, podem parecer divergentes.

- Caso as soluções propostas ameacem a privacidade, procurar alternativas para atingir as funcionalidades e finalidades pretendidas, mas nunca perdendo de vista que os riscos para a privacidade do titular de dados devem ser geridos de forma adequada.

Ao integrar a privacidade em tecnologia, processos ou sistemas, é imperativo fazê-la de maneira que não comprometa a funcionalidade plena e permita a otimização de todas as exigências tanto quanto possível.

1.5. SEGURANÇA FIM A FIM

A preservação da privacidade deve ser considerada desde a fase conceitual, antes da implementação do sistema e até mesmo antes da coleta do primeiro dado pessoal. Essa salvaguarda deve perdurar ao longo de todo o ciclo de vida dos dados em questão.

É essencial que sejam adotadas medidas fortes de segurança, desde o início do projeto, pois sem segurança, não é possível garantir a privacidade. A segurança da informação envolve a confidencialidade, integridade, disponibilidade, além da resiliência dos sistemas. Já a privacidade compreende a desvinculação, a transparência e a capacidade de intervenção e controle do titular dos dados pessoais no tratamento.

A privacidade necessita ser continuamente protegida em todo o ciclo de vida dos dados pessoais (coleta, registro, classificação, conservação, consulta, distribuição, limitação, destruição etc.) no projeto, produto ou sistema. Para cada caso, devem ser minuciosamente analisadas e implementadas as medidas mais adequadas para a proteção dos dados pessoais, entre as quais estão:

- Técnicas de pseudonimização ou anonimização;
- Classificação, organização e acesso aos dados e operações de tratamento com base em perfis de acesso;
- Criptografia padrão para que o estado “natural” dos dados, quando perdidos ou roubados, seja "ilegível";
- Destruição segura e garantida da informação no final do ciclo da sua vida útil.

1.6. VISIBILIDADE E TRANSPARÊNCIA

A promoção da visibilidade e da transparência é crucial para demonstrar conformidade e responsabilidade proativa perante a Autoridade Nacional de Proteção de Dados Pessoais; e como medida de confiança perante os sujeitos cujos dados são tratados. Visa a garantir que todos os participantes no processamento de dados pessoais estejam efetivamente aderindo aos princípios e objetivos declarados, sujeitos à verificação independente por parte do titular dos dados pessoais, de maneira a informá-los sobre quais dados estão sendo processados e com qual finalidade.

Para fins de auditoria, o órgão deve dar ênfase aos seguintes critérios:

a) **Prestação de contas**: a coleta de dados pessoais requer uma responsabilidade cuidadosa para garantir sua proteção. A responsabilidade por todas as políticas e procedimentos relativos à privacidade deve ser devidamente registrada e comunicada conforme necessário. Ao transferir dados pessoais para terceiros, é fundamental garantir uma proteção de privacidade equivalente por meio de acordos contratuais ou outros mecanismos adequados.

b) **Abertura**: a chave para a responsabilidade reside na abertura e transparência. As informações sobre políticas e práticas relacionadas ao tratamento de dados pessoais devem ser prontamente disponibilizadas aos titulares.

c) **Conformidade**: é fundamental implementar um mecanismo de reclamação e avaliação, com todas essas informações sendo comunicadas aos titulares, inclusive instruções sobre como apresentar reclamações à ANPD. São necessárias medidas adequadas para monitorar, avaliar e verificar o cumprimento das políticas e procedimentos de privacidade.

Na prática, a promoção da visibilidade e transparência envolve a adoção de uma série de medidas que adotem uma abordagem organizacional que alcance determinados resultados, tais como:

a) Publicar as políticas de privacidade e proteção de dados que regem o funcionamento do órgão ou entidade;
b) Desenvolver, adotar e publicar uma política com cláusulas informativas concisas, claras e inteligíveis, de fácil acesso e entendimento, que permita aos interessados compreenderem o âmbito do tratamento dos dados, os riscos a que podem estar expostos, bem como a forma de fazerem valer os direitos que regem a proteção de seus dados;
c) Embora não seja obrigatório para todos os responsáveis, tornar pública, ou pelo menos facilmente acessível aos interessados, a lista dos tratamentos realizados no órgão ou entidade;
d) Divulgar a identidade e contacto do responsável pelo órgão ou entidade sobre assuntos de privacidade; e
e) Garantir que a identidade e as informações de contato dos responsáveis pelo órgão ou entidade, sobre assuntos de privacidade, estejam disponíveis e publicadas tanto dentro quanto fora da organização.

1.7. RESPEITO PELO USUÁRIO DE PRIVACIDADE

O objetivo deste princípio é garantir os direitos e liberdades dos titulares de dados pessoais cujos dados estão sendo processados pela organização, de modo que qualquer medida adotada deve ser direcionada para assegurar sua privacidade. Isso implica em projetar processos, aplicações, produtos e serviços com o titular de dados pessoais em mente, antecipando-se às suas necessidades. Para tais garantias recomenda-se: manter o projeto sempre centrado no titular de dados pessoais.

Instruir ao titular o desempenho de um papel ativo na gestão de seus próprios dados pessoais pode ser o critério mais eficaz contra abusos e usos inadequados desses dados. Sua inatividade não deve resultar em prejuízo à privacidade, retomando um dos princípios mencionados anteriormente que advoga por uma configuração padrão de privacidade que ofereça o mais alto nível de proteção.

São critérios a serem observados na garantia dos direitos e liberdades dos titulares de dados pessoais:

- **Consentimento**: é imprescindível obter o consentimento livre e específico do titular para a coleta, uso ou divulgação de dados

pessoais, salvo quando a lei de outra forma permitir. À medida que a sensibilidade dos dados aumenta, a clareza e especificidade requeridas para o consentimento também aumentam. Se necessário, o consentimento poderá ser revogado posteriormente.

- **Qualidade dos dados**: os dados pessoais devem ser precisos, completos e atualizados na medida necessária para cumprir a finalidade de seu tratamento.
- **Acesso**: os titulares têm o direito de acessar seus dados pessoais e serem notificados sobre seus usos e divulgações. Eles devem ter a capacidade de contestar a precisão e a integridade dos dados, buscando as devidas alterações, quando necessário.
- **Conformidade**: as instituições devem implementar mecanismos de reclamação e reparação, fornecendo informações ao público sobre esses processos, inclusive instruções para apresentar reclamações adicionais, se necessário.

2. PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Privacidade desde a Concepção e por Padrão é referenciada na LGPD em seu art. 46, no § 2º, determinando que medidas de segurança técnicas e administrativas sejam adotadas desde a fase de concepção do produto ou do serviço até a sua execução. Além disso, em seu art. 6º, são elencados os princípios a serem observados durante as atividades de tratamento de dados pessoais. Esses princípios foram derivados dos princípios da GDPR *(General Data Protection Regulation),* dos FIPPs e de outros conjuntos de princípios existentes desenvolvidos por organizações internacionais que têm influenciado diversas legislações mundiais acerca da temática de privacidade. Podemos correlacionar os princípios da Privacidade desde a Concepção com a LGPD da seguinte forma:

<table>
<tr><th>PdC</th><th>LGPD</th></tr>
<tr><td colspan="2">Princípios</td></tr>
<tr><td rowspan="2">Proativo e não reativo; preventivo e não corretivo</td><td>Segurança (Artigo 6º, VII): 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;</td></tr>
<tr><td>Prevenção (Artigo 6º, VIII): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.</td></tr>
<tr><td colspan="2">Considerações</td></tr>
<tr><td colspan="2">O primeiro princípio da metodologia PdC propõe a prevenção da concretização de cenários de risco, advogando pela adoção de uma abordagem proativa a fim de evitar ou minimizar a probabilidade de incidentes de violação à privacidade. Da mesma forma, a LGPD, por meio de dois princípios, estabelece que sejam adotadas medidas preventivas, incluindo aquelas de segurança técnica e administrativa, de modo a prevenir a materialização de situações de risco em virtude de tratamento de dados pessoais. Portanto, pode-se inferir que ambos os conjuntos de princípios destacam a importância de se evitar a efetivação dos riscos que envolvem a violação à privacidade.</td></tr>
</table>

PdC	LGPD
Princípios	
Privacidade por padrão	Finalidade (Artigo 6º, I): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Adequação (Artigo 6º, II): compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
	Necessidade (Artigo 6º, III): limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
	Prevenção (Artigo 6º, VIII): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Transparência (Artigo 6º, VI): garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Considerações	
O segundo princípio da PdC visa a garantir que as configurações e/ou práticas que objetivam maximizar a privacidade sejam habilitadas por padrão na disponibilização do sistema ou serviço, sem necessidade de ações adicionais. Essas configurações e práticas compreendem diversas ações, tais como a especificação da finalidade de forma explícita e informada ao titular, a coleta, uso, retenção e compartilhamento dos dados, de forma limitada, proporcional e não excessiva à finalidade do tratamento, bem como o acesso facilitado, de forma clara, adequada e ostensiva, às informações sobre o tratamento realizado. A LGPD prevê, por meio de cinco princípios, a observação de diversas dessas ações.	

PdC	LGPD
Princípios	
Privacidade incorporada ao projeto	Prevenção (Artigo 6º, VIII): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Segurança (Artigo 6º, VII): 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.
	Transparência (Artigo 6º, VI): garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a

	realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Considerações	
O terceiro princípio da PdC sugere que a privacidade e a proteção da dados pessoais sejam incorporados de forma holística, integrada e criativa como requisitos necessários ao ciclo de vida do desenvolvimento de um projeto. A LGPD estabelece requisitos importantes a serem observados nas atividades de tratamento de dados pessoais, tais como a prevenção a ocorrência de danos aos titulares por meio da adoção de medidas de segurança técnicas e administrativas para proteção dos dados pessoais, com garantia de transparência aos titulares sobre a realização do tratamento. Estes requisitos compreendem no mínimo três dos princípios elencados pela LGPD.	

PdC	LGPD
Princípios	
Funcionalidade total	Prevenção (Artigo 6º, VIII): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Segurança (Artigo 6º, VII): 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.
Considerações	
O quarto princípio da PdC preconiza que todos os requisitos estabelecidos pelas partes interessadas devem ser satisfeitos simultaneamente. Dois dos principais requisitos voltados à privacidade e estabelecidos pela LGPD são a prevenção a ocorrência de danos aos titulares e a adoção de medidas de segurança que visam a proteção dos dados pessoais. Estes requisitos podem ser satisfeitos em conjunto com requisitos de funcionalidade, usabilidade e benefícios comerciais.	

PdC	LGPD
Princípios	
Segurança de ponta a ponta	Prevenção (Artigo 6º, VIII): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Segurança (Artigo 6º, VII): 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.
	Responsabilização e Prestação de Contas (Artigo 6º, X): demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das

	normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
Considerações	
O quinto princípio da PdC propõe que sejam incorporadas medidas de segurança que venham a preservar a confidencialidade, a integridade e a disponibilidade de modo a proteger os dados pessoais e a privacidade do indivíduo em todo o ciclo de vida do projeto. De maneira equivalente, a LGPD estabelece que sejam observados os princípios da prevenção, segurança, responsabilização e prestação de contas a fim de garantir a confidencialidade, a integridade e a disponibilidade durante as atividades de tratamento de dados pessoais.	

PdC	LGPD
Princípios	
Visibilidade e transparência	Livre acesso (Artigo 6º, IV): garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
	Responsabilização e Prestação de Contas (Artigo 6º, X) demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
	Transparência (Artigo 6º, VI): garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Considerações	
O sexto princípio da PdC prevê que sejam asseguradas a visibilidade e transparência para todas as partes interessadas ao projeto. A visibilidade e transparência são essenciais para demonstração e comprovação da conformidade no cumprimento das normas de proteção de dados pessoais, estabelecendo a confiança entre as partes interessadas. A LGPD estabelece a observação deste pressuposto por meio dos princípios do livre acesso e transparência das informações sobre o tratamento e da responsabilização e prestação de contas pelos agentes de tratamento.	

PdC	LGPD
Princípios	
Respeito pela privacidade do usuário	Adequação (Artigo 6º, II): compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
	Finalidade (Artigo 6º, I): adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

	Livre acesso (Artigo 6º, IV): garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
	Necessidade (Artigo 6º, III): imitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
	Não discriminação (Artigo 6º, IX): impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
	Qualidade dos dados (Artigo 6º, V): garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
	Transparência (Artigo 6º, VI): garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Considerações	
O último princípio da PdC propõe que os interesses e necessidades, direitos e liberdades dos titulares de dados pessoais sejam primados durante todo o ciclo de vida do projeto. Este objetivo é previsto na LGPD por meio da observação dos princípios da adequação, finalidade, livre acesso, necessidade, não discriminação, qualidade dos dados e transparência.	

3. METAS DE PROTEÇÃO DE PRIVACIDADE

As metas de proteção de privacidade referem-se aos objetivos e diretrizes estabelecidos para garantir a proteção de dados pessoais e, consequentemente, a preservação da privacidade quando são tratados os dados pessoais dos titulares. Além disso, estabelece padrões que os órgãos devem seguir para que o tratamento de dados pessoais seja realizado com respeito e responsabilidade.

Tradicionalmente, os sistemas considerados seguros e confiáveis se baseiam na análise de riscos e na resposta a ameaças, adotando a tríade: confidencialidade, integridade e disponibilidade. Tais pilares da segurança da informação são amplamente aceitos como metas de segurança voltadas a privacidade.

• **confidencialidade**: evita o acesso não autorizado aos sistemas e serviços, e consequentemente, aos dados pessoais;

• **integridade:** protege os sistemas/serviços e dados contra modificações não autorizadas e impróprias, e

• **disponibilidade**: garante que os sistemas/serviços e dados estejam sempre disponíveis quando necessário.

Apesar de terem sido sugeridos diversos aprimoramentos e ajustes, essas metas fundamentais voltadas à proteção da privacidade se mantiveram constantes ao longo do tempo, servindo como inspiração para várias metodologias de privacidade e segurança.

Como complemento a essas metas de proteção, três objetivos específicos de privacidade foram propostos: desvinculação, transparência e possibilidade de intervenção. Esses objetivos foram aperfeiçoados e incorporados a um modelo padronizado de proteção de dados, sendo reconhecido por diversas autoridades de proteção de dados europeias.

- **Desvinculação:** O objetivo é processar os dados pessoais de forma que estes não possam ser associados a outras fontes de dados ou que esse relacionamento demande um esforço considerável. Esta meta de privacidade reduz o risco de uso indevido de dados pessoais e a formação de perfis através do relacionamento dos dados de diferentes bases,

assegurando os princípios da adequação, finalidade, necessidade, segurança, bem como o princípio da prevenção elencados na LGPD.

- **Transparência:** A transparência garante que todo o tratamento de dados pessoais possa ser compreendido. É uma garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. As informações de tratamento, como os objetivos e as condições legais, técnicas e organizacionais aplicáveis devem estar disponíveis antes, durante e após a realização do tratamento, minimizando assim os riscos de não observação aos princípios, constantes na LGPD, do livre acesso, não discriminação, transparência, responsabilização e prestação de contas.
- **Possibilidade de intervenção:** Assegura que as partes interessadas, tais como os titulares dos dados pessoais, possam intervir no tratamento sempre que for necessário a fim de implementar medidas de correção. A possibilidade de intervenção está relacionada diretamente ao princípio da qualidade dos dados e aos direitos dos titulares, como o direito de retificação e exclusão de dados, retirar o consentimento e o direito de realizar reclamações, elencadas na LGPD.

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.

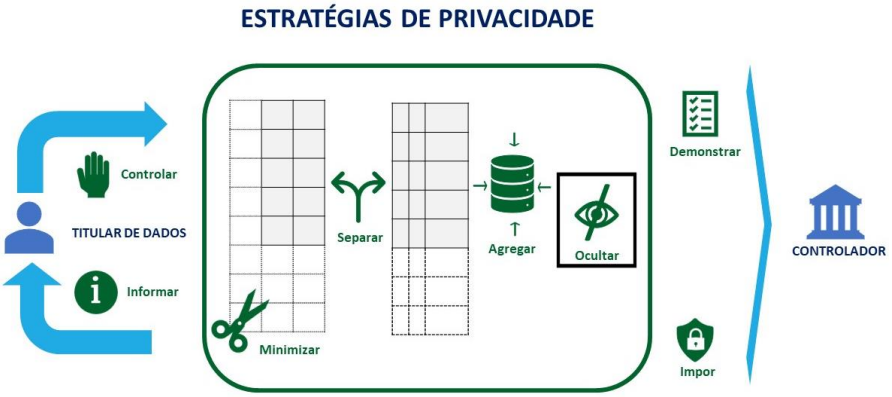
Essas três metas, mais as de segurança voltadas à privacidade, estabelecem uma estrutura de privacidade e proteção no tratamento de dados pessoais e

determinam o que o sistema/serviço deve atender no processo de privacidade desde a concepção e por padrão.

4. ESTRATÉGIAS DE PRIVACIDADE

As estratégias de privacidade têm o objetivo de descrever requisitos fundamentais para a proteção de dados pessoais e preservação da privacidade a serem definidos durante a fase de concepção de um produto ou serviço, para que possa atingir as metas de privacidade.

Com base em publicações internacionais[6] podemos mencionar oito estratégias de privacidade desde a concepção, as quais também se relacionam com os princípios do art. 6º da LGPD. A figura a seguir ilustra o relacionamento das estratégias de projeto de privacidade propostas neste guia.



Estas estratégias são divididas em duas categorias: estratégias orientadas a dados e estratégias orientadas a processos.

4.1. ESTRATÉGIAS ORIENTADAS A DADOS

As quatro estratégias orientadas a dados que podem apoiar tanto a intervenção quanto a desvinculação (citados na seção anterior), abordam principalmente os princípios da necessidade e qualidade dos dados presentes no Art. 6º da LGPD.

Tais estratégias não devem ser confundidas com os princípios fundamentais presentes na LGPD.

[6] Privacy and Data Protection by Design – from policy to engineering
Privacy Design Strategies ,Jaap-Henk Hoepman disponível em: https://arxiv.org/pdf/1210.6621.pdf

4.1.1. MINIMIZAR

O objetivo desta estratégia é restringir ao mínimo necessário a quantidade de dados pessoais a serem tratados, evitando assim o tratamento de dados pessoais desnecessários e limitando possíveis impactos na privacidade. Tal estratégia tem relação com os princípios da finalidade, qualidade dos dados e necessidade presentes no art. 6º da LGPD.

Para aplicar essa estratégia, é necessário avaliar se o tratamento de dados pessoais é proporcional em relação à finalidade e se não existem outros meios menos invasivos para atingir a mesma finalidade. A decisão de coletar dados pessoais pode ser tomada tanto na fase de projeto quanto na de execução e pode assumir diversas formas. Por exemplo, pode-se decidir não recolher qualquer informação sobre um determinado titular de dados ou coletar apenas um conjunto limitado de atributos.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Supressão	Abster-se de processar os dados pessoais de um titular de dados, parcial ou totalmente, da mesma forma que incluir na deny-list.
Seleção	Decidir sobre quais dados pessoais serão utilizados, selecionando apenas aquilo que for estritamente necessário à sua finalidade.
Eliminação	Eliminar logicamente (deletar, apagar) os dados pessoais não mais necessários e determinar previamente o tempo de utilização para que o dado seja excluído.
Descarte	Destruir, inclusive dos backups, os dados pessoais não mais necessários de maneira segura (irreversível), de modo a impossibilitar a recuperação.

4.1.2. OCULTAR

Esta estratégia tem como objetivo garantir a confidencialidade dos dados pessoais e suas inter-relações, fazendo com que eles não sejam visíveis para todos. A lógica por trás desta estratégia é que, ao ocultar os dados, eles não devem ser facilmente usados de forma indevida. Não há como especificar diretamente de

quem os dados devem ser ocultados, pois dependerá do contexto específico em que esta estratégia será aplicada. Tal estratégia tem relação com os princípios da segurança, prevenção e não discriminação presentes no art. 6º da LGPD.

A estratégia **OCULTAR** tem como objetivo alcançar a desvinculação dos dados e torná-los inobserváveis ou não rastreáveis. Neste contexto, garante que dois eventos não possam ser relacionados entre si.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Restrição	Prevenir o acesso não autorizado aos dados pessoais.
Embaralhamento	Processar dados pessoais aleatoriamente dentro de um grupo grande o suficiente para reduzir a correlação.
Criptografia	Criptografar dados (em trânsito ou em repouso).
Ofuscação	Tornar os dados pessoais incompreensíveis para impedir a capacidade de decifrá-los.
Dissociação	Remover a correlação entre diferentes partes de dados pessoais.

4.1.3. SEPARAR

A terceira estratégia exige que o tratamento de dados pessoais seja distribuído em compartimentos separados, sempre que possível, em vez de centralizado. Em particular, os dados provenientes de fontes distintas devem ser armazenados em bases de dados separadas e não devem estar interligados. Tal estratégia tem relação com os princípios da segurança e prevenção presentes no art. 6º da LGPD.

O objetivo desta estratégia é evitar, ou pelo menos minimizar, o risco de que diferentes dados pessoais possam ser combinados para criar um perfil completo do titular dos dados pessoais. Para isso, é necessário manter contextos de tratamento

independentes que dificultem a correlação de conjuntos de dados que deveriam ser desvinculados.

Sempre que possível, os dados devem ser tratados e armazenados localmente. As tabelas do banco de dados devem ser divididas quando existir a possibilidade. As linhas nessas tabelas devem ser difíceis de serem vinculadas entre si, por exemplo, removendo quaisquer identificadores ou usando pseudônimos específicos da tabela.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Distribuição	Particionar dados pessoais para que seja necessário mais acesso para processá-los.
Isolamento	Processar partes de dados pessoais de forma independente, sem acesso ou correlação com partes relacionadas.

4.1.4. AGREGAR

A quarta estratégia afirma que os dados pessoais devem ser tratados no mais alto nível de agregação e com o mínimo de detalhes possível em que, ainda, sejam úteis. Tal estratégia tem relação com o princípio da prevenção presente no art. 6º, VIII, da LGPD.

A agregação de informações sobre grupos de atributos ou grupos de indivíduos restringe a quantidade de detalhes nos dados pessoais que permanecem. Estes dados tornam-se, portanto, menos sensíveis se a informação for suficientemente granular e o tamanho do grupo sobre o qual é agregado for suficientemente grande.

Dados comuns significam que os itens de dados são suficientemente para que a informação armazenada seja válida para vários indivíduos, portanto, tal informação não pode ser atribuída a uma única pessoa, protegendo assim a sua privacidade.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Resumo	Extrair semelhanças em dados pessoais, encontrando e processando correlações ao invés dos próprios dados.
Agrupamento	Induzir menos detalhes de dados pessoais antes do processamento, alocando-os em categorias comuns.
Perturbação	Adicionar ruído ou aproximar o valor real de um item de dados.

4.2. ESTRATÉGIAS ORIENTADAS A PROCESSOS

As quatro estratégias que terão relação com as estratégias orientadas por processos podem apoiar tanto as metas de intervenção quanto a de transparência e abordam principalmente os princípios da transparência e o da responsabilização e prestação de contas presentes no art. 6º da LGPD.

4.2.1. INFORMAR

Esta estratégia tem como objetivo dar transparência aos titulares de dados pessoais sobre a realização do tratamento, garantindo que sejam adequadamente informados sempre que seus dados pessoais forem tratados. Tal estratégia tem relação principalmente com o princípio da transparência presente no art. 6º, VI da LGPD.

Sempre que os titulares de dados utilizem um sistema, é importante que eles sejam informados sobre quais dados pessoais estão sendo coletados, para qual finalidade e por quais meios. Devem constar informações sobre as medidas de segurança adotadas para proteger os dados e ser transparente sobre a segurança do sistema. Os titulares dos dados também devem ser informados sobre terceiros com os quais as informações são compartilhadas. Além disso, é importante informar aos titulares sobre seus direitos de acesso aos dados e como exercê-los.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Entrega	Disponibilizar amplos recursos sobre o processamento de dados pessoais, incluindo políticas, processos e riscos potenciais.
Notificação	Alertar os titulares dos dados sobre qualquer nova informação sobre o processamento de seus dados pessoais em tempo hábil.
Explicação	Detalhar as informações sobre o processamento de dados pessoais de forma concisa e compreensível.

4.2.2. CONTROLAR

A sexta estratégia estabelece que os titulares dos dados devem ter poder de decisão sobre o tratamento dos seus dados pessoais. Tal estratégia guarda relação com os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados e transparência presentes no art. 6º da LGPD.

As estratégias **INFORMAR** e **CONTROLAR** são complementares. Sem meios razoáveis de controlar a utilização dos dados pessoais, há pouca utilidade em informar o titular dos dados sobre o motivo dos dados pessoais serem coletados. O inverso também é válido: sem informação adequada, há pouca utilidade em pedir um consentimento, por exemplo. A LGPD, em seu artigo 18º, confere direitos ao titular dos dados como o de visualizar, atualizar e até solicitar a eliminação de seus dados pessoais.

A estratégia **CONTROLAR** também se refere aos meios pelos quais os titulares de dados podem decidir se desejam usar um determinado sistema e como controlam o tipo de dado que é tratado sobre eles. Além disso, fornece aos titulares controle direto sobre seus próprios dados pessoais, que pode aumentar a probabilidade de que eles corrijam erros. Como resultado, a qualidade dos dados pessoais tratados tende a melhorar.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Consentimento	Processar apenas os dados pessoais para os quais houve consentimento explícito, dado livremente e recebido.
Escolha granular	Permitir ao usuário selecionar ou excluir, de qualquer processamento, os dados pessoais, parcial ou totalmente.
Atualização	Fornecer aos titulares de dados os meios para manter seus dados pessoais precisos e atualizados.
Retirada	Respeitar o direito do titular dos dados à remoção completa de quaisquer dados pessoais em tempo hábil.

4.2.3. IMPOR

A sétima estratégia preconiza que deve estar em vigor uma política de privacidade e proteção de dados pessoais compatível com os requisitos legais. Tal estratégia tem relação com os princípios da segurança e prevenção presentes no art. 6º da LGPD.

Essa estratégia é um passo importante para garantir que durante as atividades de tratamento sejam observadas as diretrizes que dizem respeito à preservação da privacidade do titular de dados pessoais. A política deve ser compatível com os requisitos legais estabelecidos. Para garantir que a política seja aplicada, é necessário a existência de mecanismos técnicos de proteção adequados que impeçam violações das diretrizes estabelecidas nesta política. Além disso, também devem ser estabelecidas estruturas de governança adequadas para fazer cumprir a política em caso de reclamações ou problemas.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Reconhecimento	Reconhecer o valor da privacidade e decidir sobre políticas que a habilitem e processos que respeitem os dados pessoais.

Fundamento	Considerar a privacidade ao projetar ou modificar recursos e atualizar políticas e processos para proteger melhor os dados pessoais.
Dever	Garantir que as políticas sejam respeitadas, tratando os dados pessoais como um ativo, e a privacidade como um objetivo a ser incentivado como um recurso crítico.

4.2.4. DEMONSTRAR

Esta estratégia exige que um responsável pelo tratamento de dados pessoais seja capaz de demonstrar a conformidade com a política de privacidade e quaisquer requisitos legais aplicáveis. Esta estratégia está apoiada no princípio da responsabilização e prestação de contas do art. 6º, X, da LGPD.

A estratégia **DEMONSTRAR** é mais rigorosa do que a estratégia **IMPOR**. Ela exige que o responsável pelo tratamento dos dados prove que está no controle e seja capaz de demonstrar a eficácia da política de privacidade e proteção de dados pessoais implementada no âmbito da organização. Em caso de reclamações ou problemas, ela deverá ser capaz de determinar imediatamente a extensão de quaisquer possíveis violações de privacidade.

Como implementar

Formas comuns que implementam esta estratégia são:

Táticas associadas	
Registro	Rastrear todo o processamento de dados, sem revelar dados pessoais, protegendo e revendo a informação recolhida para quaisquer riscos.
Auditoria	Examinar todas as atividades do dia a dia em busca de quaisquer riscos aos dados pessoais e responder seriamente a quaisquer discrepâncias.
Relatório	Analisar as informações coletadas em testes, auditorias e registros periodicamente para revisar as melhorias na proteção de dados pessoais.

Abaixo é demonstrada a relação entre as Metas de Privacidade e as Estratégias de Privacidade:

Metas de Privacidade	Estratégias orientadas por dados	Estratégias orientadas por processos
Desvinculação	Minimizar	
	Ocultar	
	Separar	
	Agregar	
Intervenção	Minimizar	Controlar
	Ocultar	Impor
	Separar	Demonstrar
	Agregar	
Transparência		Informar

5. TÉCNICAS DE PRIVACIDADE

Uma vez estabelecidas e definidas as metas e estratégias de privacidade, procede-se a implementação de técnicas de privacidade específicas que visem a integração das metas e estratégias ao projeto.

A seguir, são apresentadas as principais técnicas de privacidade que podem ser utilizadas na implementação das estratégias descritas anteriormente.

5.1. Autenticação

Autenticação é o processo de verificar a identidade do usuário que está tentando acessar uma determinada área de um sistema/serviço que envolva acesso restrito a informações ou funcionalidades. Essa técnica é fundamental para proteger os sistemas digitais e geralmente é o primeiro passo para usar um serviço e então realizar o controle de acesso.

Os protocolos de autenticação devem fornecer proteções para evitar que terceiros alcancem as identidades das partes autenticadoras, não divulguem essas identidades através de personificação, e não deduzam as identidades das partes em uma sessão segura.

A autenticação forte pode ser um mecanismo fundamental de privacidade quando usada para garantir que apenas o titular dos dados pessoais, ou partes autorizadas, possam acessar informações pessoais.

5.2. Credenciais baseadas em atributos

Credenciais baseadas em atributos é uma técnica voltada para a implementação de um gerenciamento de identidades que permite autenticar de forma flexível e seletiva diferentes atributos sobre uma entidade sem revelar informações adicionais sobre a entidade (propriedade de conhecimento zero).

Esta técnica permite que um usuário prove de forma segura e privada a propriedade de um atributo a um provedor. Geralmente, os atributos são armazenados em um contêiner seguro chamado credencial.

5.3. Comunicações privadas seguras

Todas as comunicações do usuário devem ser protegidas com criptografia, com o objetivo de mitigar a possibilidade de um atacante extrair informações sobre

o titular de dados pessoais que possam ser usadas para uma ação maliciosa (vazamento de dados, criação de perfil falso etc.).

As comunicações privadas seguras referem-se a métodos e tecnologias que garantem a confidencialidade, integridade e autenticidade das informações trocadas entre duas partes. Essa abordagem visa proteger as comunicações contra acessos não autorizados, interceptação, manipulação ou divulgação indevida.

Alguns métodos e tecnologias comuns utilizados para garantir a comunicação privada segura incluem protocolos criptográficos (por exemplo, SSL/TLS para comunicações web), redes privadas virtuais (VPNs), assinaturas digitais, autenticação forte e práticas de segurança da informação. A implementação adequada desses elementos contribui para um ambiente de comunicação confiável e seguro.

5.4. Anonimato e pseudônimo nas comunicações

A técnica que emprega o anonimato e pseudônimos nas comunicações visa a proteger os metadados expostos a terceiros durante o processo de comunicação. Os metadados são informações “sobre” a comunicação, como quem está falando com quem, o horário e o volume das mensagens, a duração das sessões ou chamadas, a localização e possivelmente a identidade dos pontos finais da rede.

A exposição de metadados pode ter um impacto devastador na privacidade. Descobrir que um jornalista está a falar com alguém dentro de uma organização ou departamento governamental pode comprometê-lo como fonte jornalística, mesmo que os detalhes do conteúdo da mensagem não sejam recuperáveis. Os metadados também podem revelar informações sobre estilo de vida que não são imediatamente óbvias para as partes comunicantes.

Existem diversos tipos de técnicas para comunicação anônima, dentre as quais pode-se destacar os proxies e VPNs únicos, o roteamento em camada, as redes mistas e os esquemas de transmissão broadcast.

5.5. Privacidade em banco de dados

A privacidade em bancos de dados refere-se às práticas e medidas adotadas para a proteção e controle dos dados pessoais e dados pessoais sensíveis

armazenados em um banco de dados. O objetivo é garantir que apenas as pessoas autorizadas tenham acesso a determinadas informações e que esses dados sejam utilizados de maneira adequada, respeitando as leis e regulamentações relacionadas à privacidade.

Existem diversos tipos de tecnologias para a privacidade em banco de dados, dentre as quais pode-se destacar:

- a proteção de dados tabulares por meio de técnicas de supressão de célula, por exemplo;
- a proteção de banco de dados consultável por meio de perturbação de consulta e restrição de consulta; e
- a proteção de microdados por meio de mascaramento de dados e síntese de dados.

5.6. Privacidade de armazenamento

A privacidade de armazenamento refere-se à proteção da confidencialidade e integridade das informações armazenadas em dispositivos de armazenamento, como discos rígidos, servidores, nuvens de dados, e outros meios de retenção de dados, de forma que apenas usuários autorizados tenham acesso aos dados sensíveis e que esses dados permaneçam íntegros ao longo do tempo.

A privacidade de armazenamento é uma parte essencial na proteção da privacidade, especialmente considerando o aumento na quantidade de dados pessoais e dados pessoais sensíveis armazenados digitalmente.

Práticas relacionadas à privacidade de armazenamento incluem medidas para proteger dados pessoais contra acesso não autorizado, perda, roubo ou danos. Dentre as quais pode-se citar: controles de sistema operacional, armazenamento local de dados criptografados, criptografia com a preservação de formato, armazenamento esteganográfico, armazenamento privado em configurações remotas e pesquisa em dados criptografados.

5.7. Cálculos que preservam a privacidade

Cálculos que preservam a privacidade referem-se a técnicas e métodos utilizados para realizar operações matemáticas e estatísticas sobre dados sensíveis

ou privados sem comprometer a confidencialidade dessas informações. O objetivo é permitir a análise de dados sem a necessidade de divulgar detalhes específicos sobre indivíduos ou informações sensíveis subjacentes.

Essas técnicas são aplicadas em diversos campos, como ciência de dados, pesquisa médica, aprendizado de máquina e análise estatística, para permitir análises valiosas sem comprometer a privacidade dos dados subjacentes. Dentre as diversas técnicas, pode-se citar a criptografia homomórfica, a privacidade diferencial, computação multipartidária segura, a máscara de bit e o aprendizado federado.

5.8. Técnicas de aprimoramento da transparência

A transparência visa à compreensão dos titulares ao tratamento de seus dados pessoais e aos riscos relacionados para que seja fornecido uma base solida para a autodeterminação. O inciso VI do art. 6º da LGPD garante que os titulares possam ter informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Diversas técnicas foram propostas com o objetivo de aumentar a transparência, permitindo assim que os titulares compreendam melhor quais dados pessoais são coletados e como são utilizados. Dentre essas técnicas, destaca-se os painéis de privacidade que informam aos titulares quais tipos de dados pessoais foram coletados e/ou compartilhados. Essas técnicas podem incorporar diversas características que favorecem a privacidade e a proteção de dados pessoais, como:

- fornecimento de informações sobre o tratamento atual ou pretendido de dados pessoais e os riscos relacionados.
- visão geral de quais dados pessoais foram compartilhados, incluindo o órgão e sob quais políticas.
- auxílio ao titular para que ele possa analisar e entender melhor as informações relacionadas à privacidade, principalmente quando se trata de agrupamento de perfis.

Uma funcionalidade extra é a integração de um recurso que permite ao titular acessar suas informações pessoais e exercer seus direitos, tais como revogar o

consentimento, solicitar a correção de dados, e o bloqueio e eliminação de informações pessoais.

5.9. Técnicas de aprimoramento da capacidade de intervenção

A intervenção foi apresentada na seção 4 - metas de proteção de privacidade - e se refere à possibilidade de interferência no tratamento de dados pessoais. Pode ser realizada tanto pelo titular de dados pessoais quanto pelo controlador que contrata operadores para atuarem em seu nome. São diversas as possibilidades de intervenção por parte dos titulares, conforme elencados no Art. 18 da LGPD. Já o controlador pode intervir para garantir que o tratamento esteja em conformidade com as normas vigentes, aceitar reclamações dos titulares e receber comunicados da ANPD nos termos dos incisos I e II do art. 41 da LGPD, respectivamente.

Na privacidade desde a concepção, é de suma importância que o titular seja devidamente informado a respeito de seus direitos. Além disso, é crucial oferecer suporte ao titular para que este direito seja exercido.

Pode-se facilmente constatar que as técnicas de intervenção muitas vezes não podem ser implementadas apenas a nível técnico, em vez disso, muitos processos, em particular dos sistemas jurídicos, contribuem para uma intervenção eficaz. Ainda assim, existem algumas possibilidades de suporte tecnológico dos processos que devem ser realizados pelos agentes de tratamento para permitir que os titulares exerçam os seus direitos. Dentre os suportes técnicos, destaca-se aqueles que fornecem aos titulares funcionalidades on-line para acessar seus dados pessoais e realizar solicitações relativas à retificação e remoção dos dados.

6. PADRÕES DE PRIVACIDADE

Padrões de projeto são estratégias consolidadas e comprovadas para solucionar problemas recorrentes em nível de *design*, independentemente do contexto. Exemplos de padrões de projeto, amplamente conhecidos, são aqueles adotados na estruturação de um sistema de software, fornecendo recursos para a organização e a manutenção do software, além de promover a reutilização de soluções eficazes.

Em condição semelhante, os padrões de projeto de privacidade são diretrizes específicas que visam abordar desafios relacionados à proteção de dados e privacidade que aparecem repetidamente em um contexto específico durante o desenvolvimento de sistemas ou serviços. Esses padrões oferecem soluções para questões como controle de acesso, anonimização de dados, consentimento do usuário e gerenciamento de informações sensíveis. Ao implementar padrões de projeto de privacidade, os profissionais podem garantir que seus sistemas atendam às regulamentações de privacidade e proteção de dados, além de proteger a confidencialidade e a integridade das informações dos usuários.

Cada padrão de projeto de privacidade descreve a sua finalidade (incluindo o problema a ser tratado), seu contexto de aplicação, objetivos, estrutura e implementação (incluindo a solução recomendada), as consequências de sua aplicação e usos conhecidos. A solução recomendada em cada padrão de projeto de privacidade é geralmente composta por uma ou mais técnicas de privacidade apresentadas na seção anterior.

Um padrão de projeto de privacidade pode ser usado para resolver um problema de privacidade implementando uma ou mais estratégias de privacidade. Existem diversas coleções ou catálogos de padrões de projeto de privacidade, como exemplo pode-se citar o PRIPARE (Preparing Industry to Privacy by design by supporting its Application in Research), um projeto financiado pela União Europeia que desenvolveu um catálogo com 26 padrões de projeto de privacidade[7]. Outro exemplo semelhante é o projeto desenvolvido pela Vienna University of Economics

[7] https://privacypatterns.eu/

and Business que classifica 40 padrões de projeto de privacidade pelos 11 princípios de proteção de dados pessoais definidos por a norma ISO/IEC 29100:2011[8]. Um último exemplo é uma iniciativa colaborativa entre vários centros de pesquisa e universidades que mantém um catálogo de padrões com o objetivo de operacionalizar requisitos legais em soluções específicas, padronizar a linguagem da privacidade, documentar e compilar soluções comuns para problemas concretos e ajudar projetistas de sistemas e aplicações a identificar problemas de privacidade e respondê-los[9].

Abaixo, como exemplo, são listados alguns desses padrões de projeto de privacidade que foram publicados em sítios eletrônicos como resultado das iniciativas anteriormente mencionadas, com um breve resumo do objetivo de cada padrão e da estratégia de projeto de privacidade a ser suportada.

NOME	OBJETIVO	ESTRATÉGIAS SUPORTADAS
Ofuscação com Ruído Adicionado (*Added Noise Measurement Obfuscation*)	Modifica as medidas detalhadas de uso ou qualquer outro atributo de um serviço adicionando valores de ruído que mascaram dados reais para evitar a dedução de padrões e comportamentos por terceiros não autorizados que possam interceptar a comunicação.	Agregar Minimizar Ocultar
Agregação no Tempo (*Aggregation in Time*)	Consiste na coleta de dados de diferentes momentos e no tratamento de dados de forma agregada para proteger a privacidade.	Agregar
Granularidade de Localização Dinâmica (*Dynamic Location Granularity*)	Utiliza a técnica de k-anonimato para reduzir a precisão da localização do titular em serviços baseados em localização, mas mantém um equilíbrio no que diz respeito ao uso dos dados necessários à prestação do serviço.	Agregar Minimizar
Obtendo Consentimento Explícito (*Obtaining Explicit Consent*)	Para determinados processos, o responsável pelo tratamento de dados pessoais deve obter o consentimento informado do titular. A implementação	Controlar

[8] https://privacypatterns.wu.ac.at:8443/catalog/
[9] https://privacypatterns.org/

	deste padrão garante a exibição de um aviso claro, conciso e compreensível antes da recolha de dados e início do tratamento onde, ao utilizar o serviço, o titular consente no tratamento dos dados pessoais solicitados e está ciente das possíveis consequências. Os detalhes completos sobre o tratamento devem ser facilmente acessíveis para que o titular possa decidir se deseja utilizar o serviço ou não.	
Controle de Acesso (*Access Control*)	Estabelece mecanismos para controlar o acesso à informação com base na "necessidade de saber", para que os dados sejam tratados legalmente e pelas partes autorizadas.	Impor
Auditoria (*Auditing*)	Consiste em realizar auditorias periódicas para examinar a eficácia dos mecanismos de conformidade com leis, políticas e outros procedimentos.	Demonstrar
Registro (*Logging*)	A aplicação deste padrão permite ao responsável pelo tratamento demonstrar a sua conformidade com o princípio da responsabilização e que os regulamentos relevantes de proteção de dados pessoais foram devidamente implementados.	Demonstrar
Termos e Condições Resumidos (*Abridged Terms and Conditions*)	Seu objetivo é que os titulares de dados pessoais compreendam melhor os termos e condições de uma política de privacidade (riscos, direitos, transferências etc.), apresentando-os de forma concisa, abreviada e compreensível.	Informar
Padrão de Confinamento de Dados do Usuário (*User Data Confinement Pattern*)	É habitual desenvolver sistemas centralizados onde o tratamento de dados pessoais é realizado num único sistema ou entidade na qual o titular é obrigado a confiar e até a partilhar dados sensíveis. Este padrão evita o tratamento de dados pessoais de forma centralizada, transferindo uma parte	Separar

	dele para ambientes de confiança dos titulares (como seus próprios dispositivos), permitindo-lhes controlar os dados exatos que são compartilhados com prestadores de serviços.	

7. TECNOLOGIAS DE PRIVACIDADE

As Tecnologias de Privacidade (*Privacy Enhancing Technologies - PETs*) são um grupo organizado e coerente de soluções TIC (Tecnologia da Informação e Comunicação) 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.

Existem diversas classificações de PETs, a maioria delas baseadas em características técnicas. Dentre estas classificações, destacam-se dois grupos listados a seguir. O primeiro grupo combina ferramentas e tecnologias que protegem ativamente a privacidade durante o tratamento de dados pessoais (por exemplo, ocultando dados pessoais ou eliminando a necessidade de identificação). O segundo grupo trata de ferramentas e tecnologias que apoiam procedimentos relacionados à gestão da privacidade, mas não operam ativamente nos dados.

CATEGORIA	SUBCATEGORIA	DESCRIÇÃO
Proteção de Privacidade	Ferramentas de pseudonimização	Permitem transações sem pedir informações pessoais.
	Produtos e serviços de anonimização	Fornecem acesso aos serviços sem exigir a identificação do titular dos dados.
	Ferramentas de criptografia	Protegem que documentos e transações sejam visualizados por terceiros.
	Filtros e bloqueadores	Evitam e-mails e conteúdo da web indesejados.
	Anti-rastreadores	Eliminam um possível rastreamento digital do titular de dados pessoais.
Gerenciamento de Privacidade	Ferramentas de informação	Criam e verificam políticas de privacidade e políticas proteção de dados pessoais.
	Ferramentas administrativas	Gerenciam a identidade e as permissões do usuário do sistema.

Existem inúmeros catálogos de ferramentas e tecnologias PET. Embora a SGD não endosse nenhum fornecedor, tecnologia ou ferramenta, é recomendável que o órgão esteja ciente das possíveis tecnologias a serem adotadas na implementação de soluções que protegem os dados pessoais e consequentemente preservem a privacidade. Dentre os diversos catálogos, destaca-se um estudo realizado pela ENISA (*European Union Agency for Cybersecurity*) sobre ferramentas de privacidade online para o público em geral[10].

[10]https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public/at_download/fullReport

8. MEIOS DE AVALIAÇÃO

O fato de implementar técnicas de privacidade, por si só, não garante que os produtos e serviços entregues possuam os níveis de proteção de dados e privacidade desejados pela organização. Desta forma, o órgão pode utilizar de alguma metodologia de avaliação de riscos de privacidade para obter informações importantes sobre vulnerabilidades e ameaças para a privacidade dos titulares de dados pessoais que seus serviços e produtos possuem, e assim, priorizar os aspectos e funcionalidades para possíveis melhorias em processos, com o objetivo de atender os requisitos de privacidade e proteção de dados previamente estipulados. É importante salientar que as avaliações de risco também devem passar por um processo periódico de revisão, visando garantir plena conformidade com diretrizes normativas e de boas práticas que possam surgir com o passar do tempo.

Algumas entidades europeias utilizam de selos de privacidade para demonstrar a garantia da privacidade desde a concepção em seus serviços ou produtos. Tais selos funcionam como uma forma de demonstrar que a organização protege a privacidade dos titulares de dados pessoais sob sua responsabilidade, gerando assim, maior confiança em seus clientes e usuários. No Brasil, esta cultura de selos ainda não é aplicada de forma ampla, porém os órgãos públicos da APF podem utilizar dos níveis de iPriv (Indicador de Maturidade em Privacidade) do Framework de Privacidade e Segurança da Informação (pág. 84), para demonstrar os níveis de proteção à privacidade de seus sistemas e serviços.

É de suma importância que a organização registre e armazene todos os procedimentos e operações que envolvam o tratamento de dados pessoais, como por exemplo o Inventário de Dados Pessoais (IDP) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Tal ação pode ser utilizada para realizar auditorias internas, buscando obter informações para adequar as estratégias de entrega de sistemas e serviços para o titular de dados pessoais com níveis satisfatórios de privacidade e proteção de dados pessoais. Da mesma forma, esta ação auxiliará ao órgão em caso de solicitação da ANPD ou outras organizações sobre possíveis investigações, para que

os responsáveis por alguma violação de privacidade sejam devidamente responsabilizados.

REFERÊNCIAS BIBLIOGRÁFICAS

_____. **ABNT NBR ISO/IEC 27701:2019**: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 10 nov. 2023

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93, outubro de 2021**. Aprova o glossário de segurança da informação.** Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 >. Acesso em: 15 nov. 2023

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Novembro 2022**. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 06 nov. 2023.

GUIA DE RESPOSTA A INCIDENTES DE SEGURANÇA – DPSI/SGD. Guia de Resposta a Incidentes de Segurança. Março 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf>. Acesso em: 19 nov. 2023.

ESPANHA. GUÍA DE PRIVACIDAD DESDE EL DISEÑO RESPOSTA A INCIDENTES DE SEGURANÇA – DPSI/SGD. **Guia de Privacidade Desde el Diseño. Outubro 2019**. Disponível em: <https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf>. Acesso em: 16 nov. 2023.

ENISA Privacy and Data Protection by Design – from policy to engineering. Privacy and Data **Protection by Design – from policy to engineering. Dezembro 2014.** Disponível em: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>. Acesso em: 16 nov. 2023.

_____. **ISO/IEC 27018:2014**: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Genebra, 2014.

_____. **ISO/IEC ISO/IEC 29100:2011**: Information technology — Security techniques — Privacy framework. Genebra, 2011.

_____. **ISO/IEC 29134:2017**: Information technology – Security techniques – Guidelines for privacy impact assessment. Genebra, 2017.

_____. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.