ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

ORIENTAÇÕES SOBRE PRIVACIDADE DESDE A CONCEPÇÃO

CARTILHA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)
ORIENTAÇÕES SOBRE PRIVACIDADE DESDE A CONCEPÇÃO
Agosto/2025

Assessoria Técnica (Astec)
Ana Carolina Motta Rezende

Gerência Técnica de Inovação e Informação
Vitor Mateus Silva Ramos

Equipe Técnica
Jessica Maria Borges Sales
Luiz Paulo Beltrão Frederico
Raquel Chamone Barbosa

Projeto Gráfico e Diagramação
Assessoria de Comunicação Social (Ascom)

Dúvidas, sugestões e críticas podem ser enviadas para o e-mail

encarregado.lgpd@anac.gov.br

Apresentação

A Lei n° 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais - LGPD, disciplina o tratamento de dados pessoais e foi criada para proteger os direitos fundamentais de liberdade, **privacidade** e a livre formação da personalidade de cada indivíduo.

De acordo com o art. 46, § 2°, da LGPD, é fundamental adotar medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, **desde a fase de concepção do produto ou do serviço até a sua execução**.

Essa diretriz está alinhada ao conceito de **Privacidade desde a Concepção** (*Privacy by Design*), que será detalhado a seguir, e que orienta a integração da proteção de dados pessoais em todas as fases do ciclo de vida de um projeto.

Conceitos

Privacidade desde a Concepção (*Privacy by Design*): estabelece que toda iniciativa que envolva o processamento de dados pessoais deve incorporar a privacidade e a proteção de dados pessoais em todo o seu ciclo de vida.

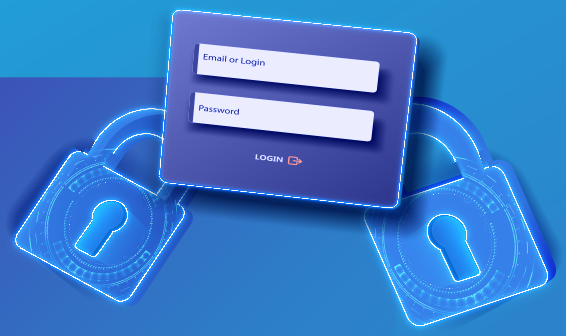
Essa abordagem prioriza medidas preventivas e proativas, e não apenas corretivas, promovendo a mitigação de riscos e garantindo maior segurança e confiança no tratamento de dados pessoais ao longo de todo o seu ciclo de vida.

***Privacy by Design* coloca a privacidade como prioridade em todas as etapas do desenvolvimento de um projeto, do planejamento à entrega final!**

Privacidade por Padrão (***Privacy by Default***): este é um dos sete princípios que compõem à Privacidade desde a Concepção, estabelece que as configurações mais protetivas à privacidade devem ser aplicadas automaticamente, sem a necessidade de ação prévia do usuário.
Em outras palavras, a coleta e o tratamento de dados pessoais devem ocorrer apenas quando estritamente necessários e, sempre que possível, com intervenção explícita do titular (ou consentimento explícito do titular).

Exemplo prático: a coleta de cookies em um site só deve ser habilitada quando o próprio usuário oferece essa permissão.

- por padrão, apenas os cookies estritamente necessários devem estar ativos, ou seja, aqueles que interferem no funcionamento correto do próprio site (configuração mais segura de privacidade); e
- os demais cookies, como os de marketing ou estatísticas, são habilitados quando o próprio usuário autorizar explicitamente.



Princípios

O termo Privacidade desde a Concepção foi formulado na década de 1990 pela Dra. Ann Cavoukian, então comissária de Informação e Privacidade da província de Ontário, no Canadá.

Essa abordagem é baseada em um conjunto de sete princípios fundamentais:

- **Proativo e não reativo; preventivo e não corretivo:** antecipar os riscos e adotar medidas para prevenir incidentes;
- **Privacidade por padrão:** adoção de configuração mais segura como padrão (explicado na seção anterior);
- **Privacidade incorporada ao projeto:** deve ser intrínseca ao projeto, fazendo parte de sua arquitetura, e não apenas um complemento;
- **Funcionalidade total:** conciliar privacidade e a plena funcionalidade do projeto;
- **Segurança de ponta a ponta:** proteção durante todo o ciclo de vida do projeto;
- **Visibilidade e transparência:** informações claras sobre a forma como os dados são tratados; e
- **Respeito à privacidade do usuário:** foco no titular.

Figura 1: Princípios da Privacidade desde a Concepção (*Privacy by Design*)

Sempre que iniciamos um projeto, seja para desenvolver um serviço, produto ou sistema, precisamos garantir que esses princípios estão sendo respeitados!

A adoção desses princípios não apenas promove conformidade com a LGPD, mas fortalece a confiança do cidadão na forma como seus dados são tratados.

Implementação

A implementação da Privacidade desde a Concepção envolve as seguintes etapas:

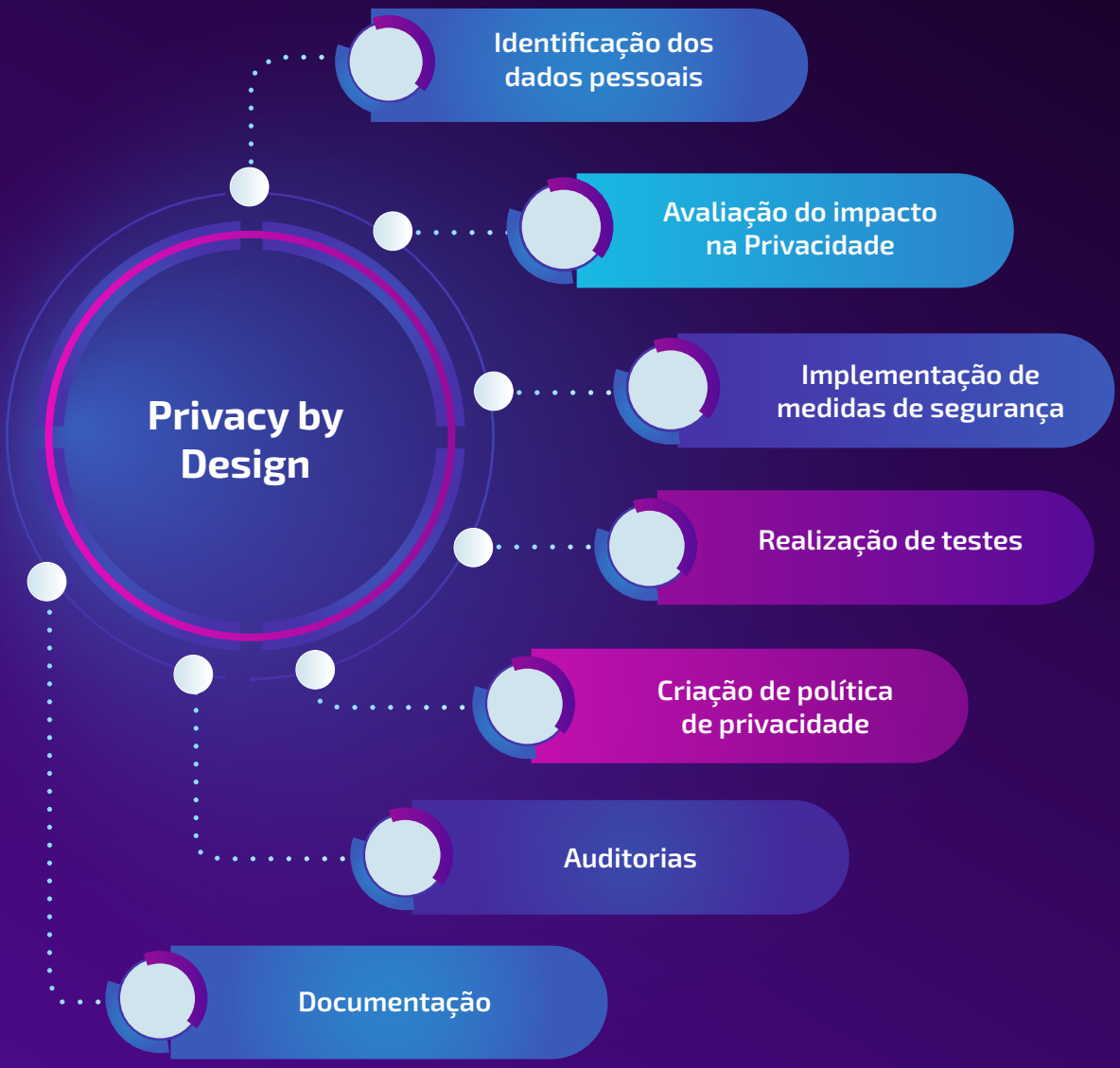


Figura 2: Etapas para implementação da Privacidade desde a Concepção (*Privacy by Design*)

• identificação dos dados pessoais coletados e seu tratamento:

- identifique os tipos de dados pessoais coletados e quem são os titulares;
- identifique e destaque os dados pessoais sensíveis;
- mapeie o fluxo de dados, identificando os pontos de coleta, armazenamento, processamento, compartilhamento e eliminação;
- analise a legislação aplicável (LGPD, entre outras); e
- verifique a finalidade específica de cada dado pessoal coletado e de cada operação de tratamento realizada.

O Anexo I apresenta um exemplo de esquema para auxiliar a execução dessa etapa.

• **avaliação do impacto do sistema/processo à privacidade - *Privacy Impact Assessment* - PIA**;

» identifique os riscos potenciais, como acessos não autorizados, vazamento de dados ou uso inadequado de informações; e

» avalie os riscos, classificando-os de acordo com seu impacto e probabilidade.

O Anexo II apresenta um exemplo de tabela para auxiliar a execução dessa etapa.

• **implementação de medidas de segurança para mitigar riscos:**

» controles de acesso;

» minimize os tratamentos de dados (colete apenas o necessário);

» adote anonimização e pseudonimização sempre que possível;

» estabeleça critérios para retenção e descarte seguro de dados;

» utilize logs e trilhas de auditoria para rastreamento do uso de dados; e

» utilize criptografia para proteger informações sensíveis, entre outras medidas.

• realização de testes para identificar vulnerabilidades e avaliar a eficácia das medidas adotadas:

» realize testes de segurança e privacidade de forma periódica; e

» verifique o cumprimento dos princípios da Privacidade desde a Concepção.

• criação de políticas de privacidade claras para garantir transparência aos titulares:

» permita que os usuários gerenciem suas preferências de privacidade; e

» evite o uso de padrões obscuros ou confusos que induzam o compartilhamento excessivo de informações;

» garanta acesso facilitado às informações sobre o tratamento de dados pessoais; e

» utilize linguagem clara e acessível.

Exemplo: Política de Privacidade do SuperApp, disponível através do link:

https://www.gov.br/anac/pt-br/acesso-a-informacao/politica-de-privacidade_superapp.

- **acompanhamento por meio de auditorias e novos testes:**
  - » estabeleça um processo de monitoramento contínuo para assegurar a conformidade com as normas e práticas de privacidade; e
  - » realize ajustes no sistema sempre que surgirem novas regulamentações, riscos ou vulnerabilidades identificadas.

- **documentação:**
  - » elabore relatórios e registre as decisões tomadas para mitigar os riscos.

Conclusão

O conceito de Privacidade desde a Concepção (*Privacy by Design*) tem como objetivo assegurar a proteção dos dados pessoais desde as etapas iniciais em qualquer projeto, garantindo ao titular maior controle sobre suas informações. Tudo isso sem comprometer a funcionalidade ou usabilidade da solução.

Para que sua implementação seja eficaz, é essencial compreender todo o fluxo de dados pessoais no sistema ou processo, identificar e avaliar os riscos à privacidade e adotar medidas técnicas e administrativas adequadas para mitigá-los.

Por fim, é fundamental reforçar que todo tratamento de dados pessoais deve manter o foco no **titular**, assegurando a centralidade de seus direitos e a transparência na forma como suas informações são utilizadas.

Referências

Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

Guia sobre Privacidade desde a Concepção e por Padrão. Programa de privacidade e Segurança da Informação - PPSI. Secretaria de Governo Digital - SGD. Versão 1.0. Março, 2024.

Anexos

Anexo I

A seguir, apresentamos um exemplo de esquema para etapa de identificação dos dados pessoais:

	Vamos entender o sistema/processo sobre o ponto de vista da privacidade?			Nome do sistema/processo:		
Observações	**Quais os dados pessoais tratados?** exemplos: nome, CPF, endereço, telefone, e-mail	**E os dados pessoais sensíveis?** exemplos: cor da pele, tipo sanguíneo, informações sobre saúde; foto; dados de crianças, Adolescentes e idosos	**Qual a fonte dos dados?** exemplos: o próprio titular fornece os dados? O dado é coletado via sou.gov?	**Quais os tipos de tratamento realizados?** exemplos: coleta, armazenamento, processamento, extração, compartilhamento, arquivamento, eliminação	**Qual a finalidade do tratamento?** exemplos: conceder licença ao piloto, conceder licença capacitação para um servidor	**Quais normativos aplicáveis?** (pode ser normativos internos ou externos, como Resolução, IS, leis...)
	Qual a finalidade de cada dado coletado? (Todos são necessários?) exemplos: nome e CPF para identificação, endereço, telefone e e-mail para contato	**Qual a base legal do tratamento?** exemplos: consentimento do titular, cumprir obrigação legal ou regulatória, realização de política pública	**Quem são os titulares?** exemplos: regulados – pilotos, mecânicos; servidores, colaboradores, pessoas sem vínculo com a ANAC (familiar de servidor)	**Quais os direitos assegurados aos titulares?** exemplos: solicitar correção, solicitar informações sobre compartilhamento	**Qual o canal de comunicação com os titulares?** (informar como os titulares podem solicitar seus direitos)	**Quais as medidas técnicas e administrativas de segurança?** exemplos: controle lógico de acesso, criptografia, registro de eventos, rastreabilidade, entre outros)

Anexo II

A tabela a seguir apresenta um exemplo de identificação e avaliação de riscos:

Risco referente ao tratamento de dados pessoais	Causa	P	I	Nível de Risco (P x I)	Medidas de Mitigação
Acesso não autorizado	• controles de gerenciamento de acesso insuficientes	10	15	150	• exigência de senha de autenticação forte; • autenticação em dois fatores (2FA); • login único; • criação de diferentes perfis de acesso; • adoção do princípio do privilégio mínimo
Vazamento de dados	• controles de gerenciamento de acesso insuficientes; • armazenamento inseguro; • falta de treinamento da equipe; • falta de rastreabilidade	10	15	150	• criptografia; • treinamento dos usuários; • redes privadas virtuais (VPNs); • anonimização ou pseudoaninimização; • adoção do princípio do privilégio mínimo
Roubo de identidade	• controles de gerenciamento de acesso insuficientes; • falta de treinamento da equipe; • falta de rastreabilidade; • falha em aplicar encerramento da sessão	10	15	150	• encerramento automático de sessão; • implementação de logs e trilhas de auditoria; • conscientização dos usuários; • autenticação em dois fatores (2FA)
Coleta de dados desnecessários	• falta de treinamento e conscientização; • falta de transparência ou informação suficiente para o titular	5	15	75	• minimização de dados: limitar a coleta e o uso de dados pessoais ao mínimo necessário; • elaboração ou revisão e detalhamento da Política de Privacidade
Retenção prolongada de dados pessoais sem necessidade	• erro na arquitetura do sistema (ex.: não permitir eliminação do dado)	5	15	75	• definição de prazos de retenção dos dados; • implementação de rotina de descarte; • revisão da arquitetura para permitir a eliminação dos dados
Informação insuficiente sobre a finalidade do tratamento	• Política de Privacidade incompleta ou ausente	5	10	50	• elaboração ou revisão e detalhamento da Política de Privacidade
Modelo de estrutura de dados insuficiente para atender os direitos do titular	• erro na arquitetura do sistema (ex.: não permitir eliminação do dado)	5	15	75	• revisão da arquitetura para permitir a eliminação, alteração e bloqueio dos dados
Impossibilidade dos titulares de acessar e modificar dados	• falta de clareza sobre os canais de comunicação com o titular	5	15	75	• elaboração ou revisão e detalhamento da Política de Privacidade
Falha na notificação e resposta a incidentes	• falta de testes de segurança; • falta de treinamento	5	15	75	• elaboração de plano de resposta a incidentes; • realização de simulações periódicas
Compartilhamento de dados pessoais em desconformidade com a LGPD	• liberação de acesso direto à base de dados; • compartilhamento de dados em excesso; • finalidade do compartilhamento incompatível	5	15	75	• controle e formalização por meio de Termo de Compartilhamento; • compartilhamento por meio de API (*Application Programming Interface*)

Matriz Impacto x Probabilidade para avaliação de riscos

Probabilidade (P)			
15	75	150	225
10	50	100	150
5	25	50	75
	5	10	15

Impacto (I)

Anexo III

A tabela abaixo apresenta um check list para verificar se o sistema ou processo atende aos princípios de proteção de dados pessoais:

Princípio da LGPD	Pergunta de Verificação	Status	Observações
Finalidade	O sistema trata dados pessoais para finalidades legítimas, específicas, explícitas e informadas ao titular?		
Adequação	O tratamento de dados está compatível com as finalidades informadas e com a atividade da organização?		
Necessidade	O sistema coleta apenas os dados pessoais estritamente necessários para atingir a finalidade declarada?		
Livre Acesso	O sistema permite que os titulares acessem facilmente informações sobre seus dados tratados?		
Qualidade dos Dados	Os dados pessoais tratados são exatos, claros, relevantes e atualizados conforme necessário?		
Transparência	O sistema apresenta de forma clara e acessível as políticas de privacidade e informações sobre o tratamento de dados?		
Segurança	Existem medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, vazamentos ou alterações indevidas?		
Prevenção	Há controles para prevenir danos aos titulares, como falhas de segurança, tratamento excessivo ou indevido de dados?		
Não Discriminação	O sistema evita tratamento de dados pessoais com fins discriminatórios, ilícitos ou abusivos?		
Responsabilização e Prestação de Contas	O sistema mantém registros, relatórios e mecanismos de governança que comprovem a conformidade com a LGPD?		

Anexo IV

A Secretaria de Governo Digital - SGD, em seu guia sobre Privacidade desde a Concepção e por Padrão, apresenta as metas, objetivos e requisitos recomendados para o desenvolvimento de projetos seguros, além de técnicas e tecnologias voltadas à mitigação de riscos e à proteção de dados pessoais.

Metas de proteção à privacidade

As metas de proteção à privacidade representam os objetivos e diretrizes fundamentais para garantir o tratamento adequado dos dados pessoais em sistemas e serviços. Projetos considerados seguros e confiáveis devem basear-se em análise de riscos e respostas a ameaças, alinhando-se tanto a metas de segurança da informação quanto a objetivos específicos voltados à privacidade.

Metas de segurança da informação aplicadas à privacidade:

- **confidencialidade:** prevenir acessos não autorizados a sistemas, serviços e dados pessoais;
- **integridade:** proteger sistemas, serviços e dados contra alterações indevidas ou não autorizadas; e
- **disponibilidade:** assegurar que sistemas, serviços e dados estejam acessíveis sempre que necessário.

Objetivos específicos de proteção à privacidade:

• **desvinculação:** garantir que os dados pessoais não possam ser facilmente associados a outras fontes de dados. Para isso, recomenda-se o tratamento de dados de forma segregada, em ambientes distintos;

• **transparência:** assegurar aos titulares o direito de acesso a informações claras, precisas e acessíveis sobre o tratamento de seus dados e os responsáveis por esse tratamento, respeitando o sigilo comercial e industrial; e

• **possibilidade de intervenção:** permitir que os titulares de dados ou partes interessadas, possam intervir no processo de tratamento, inclusive para solicitar correções, alterações, ou exclusões, sempre que necessário.

Estratégias de privacidade

As estratégias de privacidade são requisitos essenciais para a proteção de dados pessoais e servem como suporte para o cumprimento das metas e objetivos definidos em projetos que envolvem tratamento de dados. O guia da SGD propõe oito estratégias, organizadas em duas categorias: orientadas a dados e orientadas a processos.

Estratégias orientadas a dados

Essas estratégias apoiam principalmente os objetivos de **intervenção** e **desvinculação**, além de reforçarem os princípios da **necessidade** e **qualidade dos dados** (art. 6º da LGPD):

- **minimizar:** limitar a coleta e o uso de dados pessoais ao mínimo necessário, reduzindo o volume tratado e, consequentemente, o risco de impactos à privacidade;
- **ocultar:** proteger a confidencialidade dos dados pessoais e suas inter-relações, tornando-os visíveis apenas a quem realmente necessita;
- **separar:** manter os dados pessoais desvinculados e distribuídos, evitando correlações que possibilitem a criação de perfis completos dos titulares; e
- **agregar:** tratar os dados no mais alto nível possível de agregação e com o menor detalhamento necessário, reduzindo sua sensibilidade.

Estratégias orientadas a processos

Voltadas ao fortalecimento dos objetivos de transparência e possibilidade de intervenção, essas estratégias se relacionam com os princípios da transparência, da responsabilização e da prestação de contas:

- **informar:** garantir que os titulares tenham acesso a informações claras, precisas e acessíveis sobre o tratamento de seus dados;
- **controlar:** assegurar que os titulares possam exercer controle efetivo sobre o uso de seus dados;
- **impor:** implementar e manter uma política de privacidade compatível com os requisitos legais e normativos aplicáveis; e
- **demonstrar:** comprovar, de forma documentada e transparente, a conformidade com as políticas de privacidade e as obrigações legais.

Técnicas de privacidade

As técnicas de privacidade são medidas práticas aplicadas para proteger as informações pessoais. Elas podem ser utilizadas como suporte direto à implementação das estratégias descritas no tópico anterior, contribuindo para a mitigação de riscos e o fortalecimento da proteção de dados.

A tabela a seguir apresenta exemplos técnicas aplicáveis à proteção da privacidade:

Técnica	Descrição	Exemplo
Autenticação	Verificação da identidade do usuário antes de permitir o acesso a áreas restritas de sistemas ou serviços	· Senhas · Tokens de hardware e software · Perguntas de segurança · Códigos PIN · Impressão digital
Credenciais baseadas em atributos	Autenticação flexível com base em atributos como função, cargo ou unidade organizacional, permitindo controle seletivo de acesso	Servidores de uma área tem acesso apenas a determinados tipos de informação ou com permissão apenas de leitura
Comunicações privadas seguras	Proteção das comunicações dos usuários por meio de criptografia, evitando vazamentos de dados ou ataques cibernéticos.	· protocolos criptográficos (por exemplo, SSL/TLS para comunicações web); · redes privadas virtuais (VPNs); · assinaturas digitais; · autenticação forte; e · boas práticas de segurança da informação
Anonimato e pseudonimato em comunicações	Redução da exposição de metadados durante comunicações, protegendo a identidade e localização do usuário	· proxies e VPNs únicos; · roteamento em camada; · redes mistas; e · esquemas de transmissão broadcast
Privacidade em banco de dados	Restrições de acesso e técnicas para proteger dados armazenados, evitando exposição indevida e garantindo uso apropriado	· supressão de célula; · perturbação ou restrição de consultas; e · mascaramento ou síntese de dados

Padrões de privacidade

Padrões de projeto de privacidade são diretrizes específicas que visam tratar desafios relacionados à proteção de dados e privacidade que aparecem repetidamente em um contexto específico durante o desenvolvimento de sistemas ou serviços.

A tabela a seguir apresenta exemplos de padrões de privacidade:

Nome do Padrão	Objetivo	Estratégias de Privacidade Suportadas
Ofuscação com Ruído Adicionado	Adiciona ruído a dados (como medidas de uso) para mascarar informações reais e evitar identificação de padrões	Agregar, Minimizar, Ocultar
Agregação no Tempo	Coleta dados de diferentes momentos e os trata de forma agregada para dificultar a reidentificação dos titulares	Agregar
Obtendo Consentimento Explícito	O responsável deve obter o consentimento informado do titular para certos processos	Controlar
Controle de Acesso	Estabelece mecanismos para controlar o acesso à informação com base na "necessidade de saber"	Impor
Auditoria	Realiza auditorias periódicas	Demonstrar
Padrão de Confinamento de Dados do Usuário	Evita o tratamento centralizado de dados, transferindo o controle para ambientes de confiança do titular	Separar

Tecnologia de privacidade

As tecnologias de privacidade são soluções de tecnologia da informação desenvolvidas para reduzir os riscos à privacidade por meio de aplicação práticas de estratégias e padrões previamente definidos. Essas tecnologias possibilitam a proteção de dados sem comprometer as funcionalidades dos sistemas de informação, conciliando segurança, desempenho e usabilidade.

A tabela a seguir apresenta as principais categorias de tecnologias de privacidade:

CATEGORIA	SUBCATEGORIA	DESCRIÇÃO
Proteção de Privacidade	Ferramentas de pseudonimização	Permitem transações sem pedir informações pessoais
	Produtos e serviços de anonimização	Oferecem acesso a serviços sem exigir a identificação do titular dos dados
	Ferramentas de criptografia	Protegem documentos e transações contra acessos não autorizados por terceiros
	Filtros e bloqueadores	Bloqueiam conteúdos indesejados, como spam, rastreadores ou publicidade invasiva
	Anti-rastreadores	Impedem o rastreamento digital de usuários durante a navegação e uso de serviços online
Gerenciamento de Privacidade	Ferramentas de informação	Criam e verificam políticas de privacidade e políticas proteção de dados pessoais
	Ferramentas administrativas	Gerenciam identidades e permissões dos usuários em sistemas

ANAC

AGÊNCIA NACIONAL
DE AVIAÇÃO CIVIL

ACOMPANHE A ANAC NAS REDES SOCIAIS

/oficial**anac** /**company**/oficial-**anac** /oficial**anac** /oficial**anac**br