

O serviço que você entrega agrega privacidade?

Yuri Alexandro

RNP – Rede Nacional de Ensino e Pesquisa

Yuri Alexandro

Analista de Sistemas

Especialista em Gestão de Segurança da Informação

IFBA, TJBA, UNEB, UFBA, CERT.Bahia e CAIS

Atualmente Coordenador de Privacidade – RNP

+20 anos na área de Tecnologia da Informação

+12 anos na área de Segurança da Informação



AGRADECIMIENTOS



Dicionário Brasileiro da Língua Portuguesa

[Sobre o dicionário](#) [Como consultar](#) [Noções gramaticais](#) [Créditos](#)

 Português Brasileiro ▾

Digite o termo desejado



privacidade

pri·va·ci·da·de

sf

Vida privada; intimidade, privatividade

ETIMOLOGIA

der do ingl privacy+dade, como esp privacidad.



Presidência da República Casa Civil Subchefia para Assuntos Jurídicos

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

PREÂMBULO

Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.

TÍTULO II DOS DIREITOS E GARANTIAS FUNDAMENTAIS CAPÍTULO I DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. [\(Incluído pela Emenda Constitucional nº 115, de 2022\)](#)

LGPD

Lei Geral de Proteção
de Dados Pessoais





The screenshot shows the top of a Terra News article. At the top left is the Terra logo with a rainbow flag icon. Below it is a navigation bar with 'Capa > Notícias'. A secondary navigation bar contains links for 'BRASIL', 'CORONAVÍRUS', 'LOTÉRIAS', 'MUNDO', 'PODCAST', 'POLÍTICA', and 'PREVISÃO DO TEMPO'. The main headline is 'Apenas 16% das empresas aderiram à LGPD'. Below the headline is a sub-headline: 'Em vigor desde 2020, a Lei Geral de Proteção de Dados foi implementada pela minoria das companhias, mesmo a ANPD flexibilizando as normas para pequenas e microempresas'. The article date is '18 abr 2022 15h11 | atualizado em 28/4/2022 às 17h41' and there is a link for 'ver comentários'. At the bottom of the article preview is an audio player with the text 'Ouvir texto' and a progress bar at 0:00.



Desde 2020 está em vigor a Lei Geral de Proteção de Dados - LGPD - que estabelece a regulamentação para que empresas que armazenam informações de clientes, seja por meio físico ou digital. Tal lei tem como objetivo impedir que informações pessoais diversas sejam compartilhadas ou comercializadas sem o devido consentimento do cliente e que isso também não ocorra à mercê da vontade da empresa. Ou seja, a LGPD visa proteger tanto a integridade do cliente, quanto a integridade da empresa que detém os dados.



#Privacidade

Privacidade - Camiseta

3.409.478 visualizações 8 de abr. de 2021 Não deixe seus dados circularem mais que esse vídeo. O Itaú respeita e cuida da sua privacidade. 🗝️

👍 1 mil 🗨️ Não gostei ➦ Compartilhar ➦ Salvar ...

Quer saber mais? Acesse: <https://feitopara.vc/privacidade>

#Privacidade

Em relacionamento com clientes



Banco de dados de clientes



Formulários preenchidos pelos clientes



E-mails de marketing enviados/recebidos



Registros de conexão

LGPD – Art. 7º, inc. I – Consentimento do titular

LGPD – Art. 7º, inc. II – Cumprimento de obrigação legal ou regulatória

LGPD – Art. 7º, inc. V – Execução de contratos

LGPD – Art. 7º, inc. X – Para proteção do crédito

Resolução nº 738, de 21 de dezembro de 2020

Publicado: Quinta, 24 Dezembro 2020 09:42 | Última atualização: Quinta, 21 Janeiro 2021 10:52 | Acessos: 10962

Altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública, e dá outras providências.

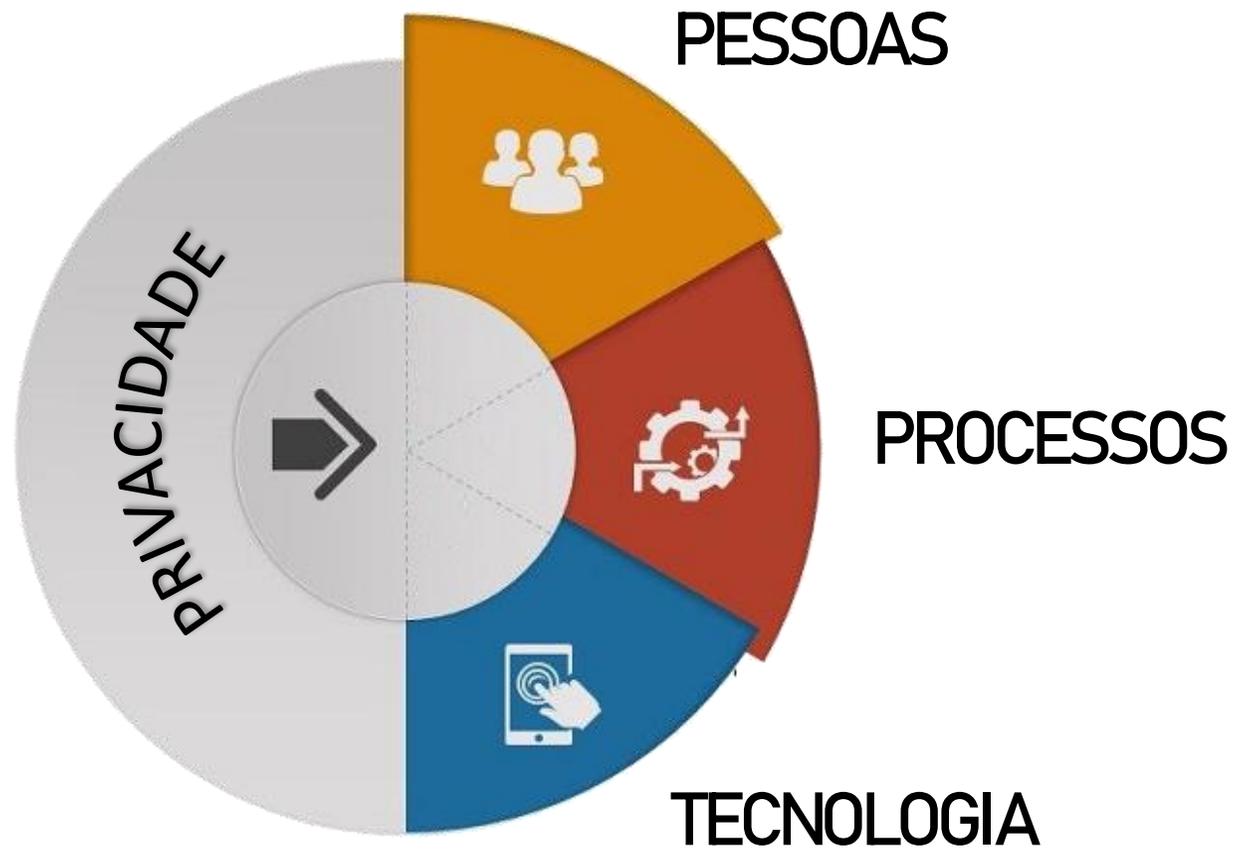
Art. 65-J. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:

I - documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico; e,

II - registros de conexão à Internet pelo prazo mínimo de 1 (um) ano nos serviços que permitam a conexão à Internet.

Parágrafo único. Para fins do disposto neste artigo, considera-se registro de conexão à Internet o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados.

Onde podem estar os dados pessoais



Qual a dimensão da demanda para atender a LGPD?





APLICANDO PRIVACY BY DESIGN



EM SISTEMAS EM PRODUÇÃO



01 Princípio

Proativo e não reativo; preventivo e não corretivo

O Privacy by Design, também referido por meio de sua sigla "PbD", tem por objetivo antecipar as situações que podem ferir a privacidade das pessoas antes mesmo de elas ocorrerem. O PbD não espera que os riscos à privacidade se materializem, ao contrário: visa impedir que eles ocorram. Isso pode ser feito por meio de medidas técnicas e organizacionais, conforme os exemplos a seguir:

Medida organizacional

Garantir que os diretores e acionistas da sua organização estejam comprometidos em adotar os mais altos padrões de privacidade. Isso significa não apenas

buscar a conformidade com as regulamentações em matéria de proteção de dados, mas também proativamente prevenir qualquer prática ou decisão de negócio que possa gerar impactos negativos na privacidade dos usuários de seus produtos e serviços.

Medida técnica

Empregar os melhores esforços preventivos para que os problemas relacionados à privacidade sejam identificados e corrigidos na fase do design (planejamento), antes do desenvolvimento e lançamento de um produto, por exemplo, mediante avaliação sistemática e adoção de alternativas inovadoras e mais protetivas à privacidade.

Aplicando a provedores

Identificação prévia das bases legais aplicáveis para tratamento de dados pessoais (incluindo consentimento).

Acesso facilitado dos clientes às próprias informações pessoais.

Segurança do cliente no acesso da interface de serviço (MFA).

Processos bem definidos para identificação positiva do cliente.



02 Princípio

Privacidade como padrão (by default)

Os dados pessoais devem ser automaticamente protegidos em qualquer sistema de tecnologia da informação (TI) ou prática de negócio de modo que as pessoas não precisem fazer esforços para ter a sua privacidade garantida. Assim, nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - ela é embutida no sistema, por padrão. Isso pode ser feito por meio de medidas

técnicas e organizacionais, conforme os exemplos a seguir:

Medida organizacional

Especificar a finalidade para a coleta, uso, armazenamento e compartilhamento dos dados pessoais antes mesmo de coletá-los. Esse princípio de PbD tem, portanto, estrita relação com o princípio da finalidade, previsto no artigo 6º, inciso I, da LGPD. Se não há propósito legítimo para o tratamento do dado, por padrão deve-se evitar coletá-lo.

Medidas técnicas

(i) Limitar a coleta apenas àquelas informações estritamente necessárias para as finalidades específicas e relacionadas ao serviço ou produto utilizado pelo usuário. Essa medida está relacionada com princípio da necessidade,

consagrado pelo artigo 6º, inciso III, da LGPD.

(ii)

Coletar o mínimo de informação possível e fazer o máximo esforço para não identificar individualmente o titular de dados, coletando apenas os dados relevantes e essenciais ao cumprimento das suas finalidades legítimas. Essa prática tem ligação direta como princípio da minimização previsto no artigo 5, 1, c, do GDPR.

(iii)

Limitar o uso, retenção e divulgação de informações pessoais aos propósitos relevantes identificados e para os quais o indivíduo prévia e expressamente consentiu, quando necessária sua autorização para esses tipos de operações.

Aplicando a provedores

Compartilhamento dos dados
deve ser os mais restritivos possíveis

Definir limitações no uso,
retenção e divulgação dos dados pessoais.

Ajustar configurações de opção
de opt-in para desabilitadas por padrão.

Aplicar controles de minimização/ocultação
dos dados pessoais no serviço/sistema





03 Princípio

Privacidade incorporada ao Design

A privacidade deve ser um componente essencial da funcionalidade de um produto ou serviço disponibilizado para a sociedade e deve ser incorporada nas tecnologias de maneira holística, segura e criativa. Isso pode ser feito da seguinte forma:

Medida organizacional

Adotar uma abordagem sistemática de Privacy by Design baseada em padrões

e frameworks reconhecidos, passíveis de revisões e auditorias externas. É importante realizar, sempre que possível, avaliações detalhadas de impacto e risco à privacidade com documentação clara das técnicas de PbD empregadas, medidas tomadas para mitigação de riscos, utilizando métricas objetivas para avaliar o impacto e risco à privacidade.

Medida técnica

Incorporar privacidade ao design dos produtos e serviços, minimizando o impacto da tecnologia na privacidade das pessoas, de forma que as configurações de privacidade não sejam facilmente degradadas por meio de uso, configuração indevida ou erro dos sistemas.

Aplicando a provedores

Privacidade deve fazer parte desde a análise de requisitos do sistema.

Regras de negócio devem prever o uso mínimo de informações pessoais.

Implementar funções para mascarar dados pessoais na interface do usuário.

Aplicar mecanismos de proteção de dados em repouso e em trânsito.





04 Princípio

Funcionalidade total

O Privacy by Design busca acomodar todos os objetivos e interesses legítimos de uma maneira positiva, com “ganhos em dobro” para os indivíduos e sociedade. Portanto, rejeita abordagens antiquadas que coloquem a privacidade como um cálculo de resultado zero e destaca que, traçando objetivos legítimos, é possível inovar respeitando a privacidade, o que resultará em uma soma positiva. Esse princípio pode ser colocado em prática por meio das seguintes medidas:

Medida organizacional

Acomodar todos os interesses legítimos e positivos, evitando falsas dicotomias, como privacidade x segurança, demonstrando que é possível e muito mais desejável ter ambos. É importante documentar: (i) as decisões e processos que foram rejeitados por ter uma soma zero; (ii) como foi possível atender aos objetivos legítimos que não têm relação com a privacidade, e (iii) quais foram as soluções encontradas para atender esses objetivos com respeito à privacidade.

Medida técnica

Desenvolver tecnologias inovadoras que alcancem resultados reais de soma positiva, onde é possível atender múltiplos interesses além da privacidade. Ann Cavoukian ressalta que as organizações que conseguem superar as escolhas de soma zero, sem comprometer a

Aplicando a provedores

Requisitos complementares
de privacidade e de segurança.

Projetar recursos para executar sem
obrigatoriedade de uso/compartilhamento.

Otimizar uso do sistema quando
necessário aplicar criptografia em dados pessoais.

Minimizar impacto do uso de
dados pessoais em funções de controle de acesso.





05 Princípio

Segurança de ponta-a-ponta e proteção durante todo o ciclo de vida dos dados

O Privacy by Design garante o gerenciamento seguro das informações durante todo o ciclo de vida dos dados. Não deve haver lacuna na proteção dos dados nem na prestação de contas. Isso pode ser garantido com a aplicação das medidas abaixo:

Medida organizacional

Assumir a responsabilidade pela

segurança dos dados pessoais durante todo seu ciclo de vida, adotando uma política robusta de Segurança da Informação, bem como as melhores técnicas disponíveis no mercado e os padrões desenvolvidos por organismos reconhecidos.

Medida técnica

Garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo seu ciclo de vida, observando, dentre outras técnicas, criptografia forte, métodos apropriados de controle de acesso e registro de operações envolvendo dados pessoais, além da destruição segura.

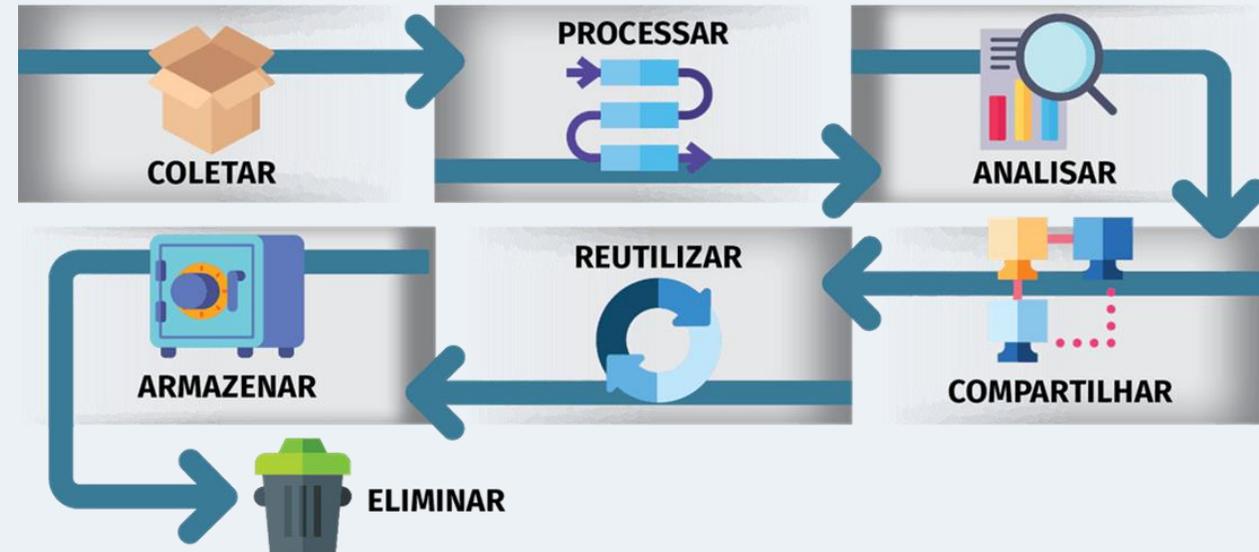
Aplicando a provedores

Dados coletados através de protocolos de comunicação seguros.

Implementar mecanismos robustos de controle de acesso aos dados.

Reavaliar arquitetura dos serviços e identificar se existem controles defasados ou vulneráveis.

Estabelecer processos de resposta à incidentes de segurança envolvendo dados pessoais.





06 Princípio

Visibilidade e transparência

No PbD, a transparência, diligência e o compliance são fundamentais para estabelecer a responsabilidade e confiança, garantindo aos interessados que a organização está operando de acordo com suas declarações e objetivos e que suas promessas são passíveis de verificação. Esse princípio pode ser colocado em prática da seguinte forma:

Medidas organizacionais

Documentar e disponibilizar as políticas

e procedimentos relacionados à privacidade e disponibilizar canal de comunicação para facilitar petições de titulares, parceiros e autoridades públicas. Também é importante estabelecer uma metodologia de auditar terceiros sempre que necessária a transferência de dados pessoais a eles, para verificar se empregam os requisitos de segurança adequados e estabelecer cláusulas contratuais de proteção de dados.

Medidas técnicas

Estabelecer medidas técnicas capazes de monitorar e avaliar continuamente a conformidade com as políticas e procedimentos de proteção de dados.

Aplicando a provedores

Desenvolver Termo de Uso e Aviso de Privacidade, com detalhamento do tratamento de dados pessoais.

Desenvolver interface para permitir ao usuário o acesso e modificação dos seus próprios dados.

Garantir o correto tratamento de dados pessoais por parte de Operadores.

Criar canais de comunicação para atender solicitações de informação dos usuários.





07 Princípio

Respeito pela privacidade do usuário

Acima de tudo, o *Privacy by Design* exige que as organizações prezem ao máximo pelos interesses do indivíduo, mantendo o usuário no controle dos seus dados pessoais. Os melhores resultados de PbD são aqueles projetados para atender as necessidades dos titulares dos dados, colocando-os em primeiro lugar. As medidas abaixo explicam como isso pode ser feito.

Medidas organizacionais

Capacitar os titulares dos dados a gerenciar ativamente os seus dados pessoais, evitando abuso e uso indevido de seus dados.

Medidas técnicas

Estabelecer padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular de dados a exercer, de forma efetiva, todos os seus direitos assegurados por lei, e que lhes deem absoluto controle sobre os seus dados pessoais.

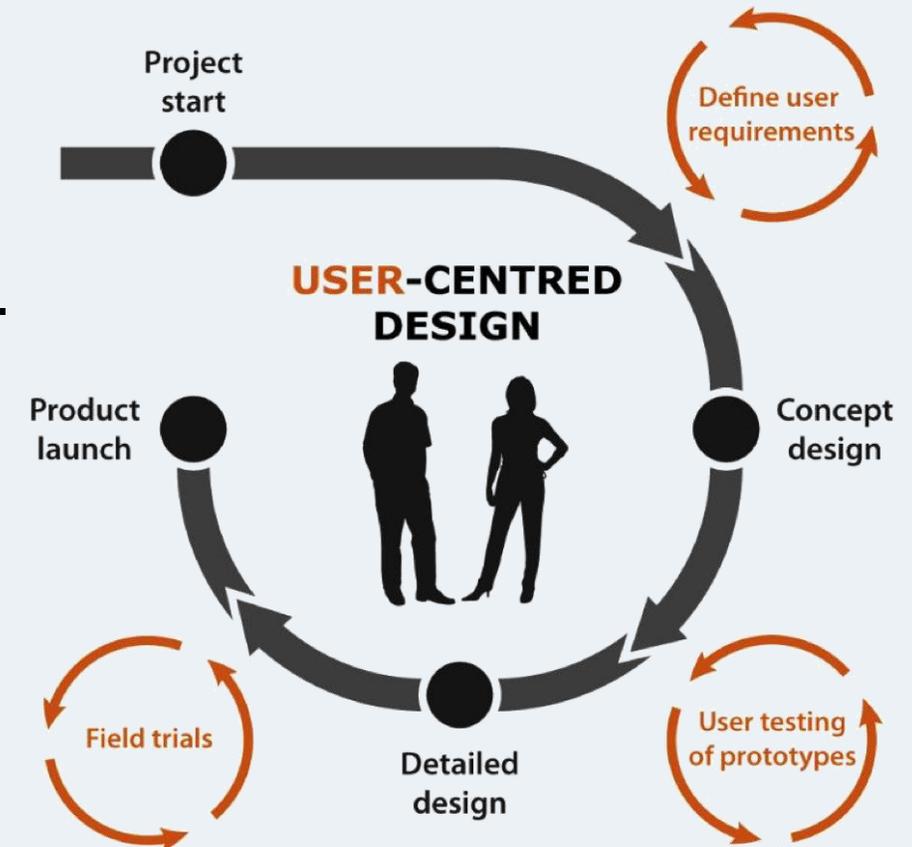
Aplicando a provedores

Publicar avisos de privacidade de fácil entendimento para os clientes.

Permitir ao usuário do sistema controle, acesso e modificação dos seus próprios dados.

Desenvolver interface para coleta de consentimento do cliente. (opt-in)

Permitir, sempre que possível, interface para cliente remover consentimento ou excluir dados. (opt-out)



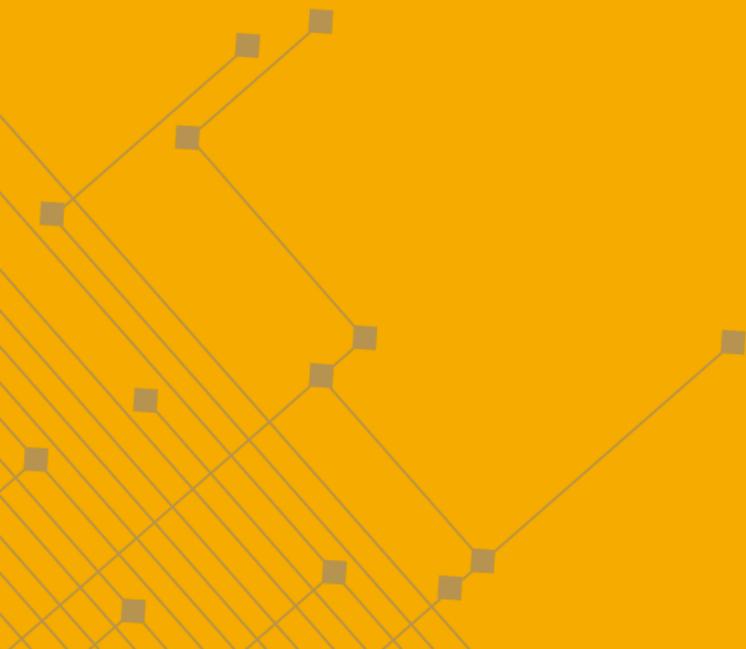
ADEQUAÇÕES DE BASE:

- Ajustes de finalidade de tratamento dos dados pessoais
- Identificação das hipóteses de tratamento
- Desenvolvimento de termos de uso e avisos de privacidade
- Garantir a proteção dos dados pessoais
- Desenvolvimento de Relatório de Impacto de Proteção de Dados (RIPD)
- Estabelecer acordos de processamento de dados com fornecedores
- Análise/Criação/Ajuste dos contratos de serviço (clientes e fornecedores)

Acompanhar as atualizações pela ANPD



Título da divisória de seção em até 2 linhas





MINISTÉRIO DO
TURISMO

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES

