O serviço que você entrega agrega privacidade?

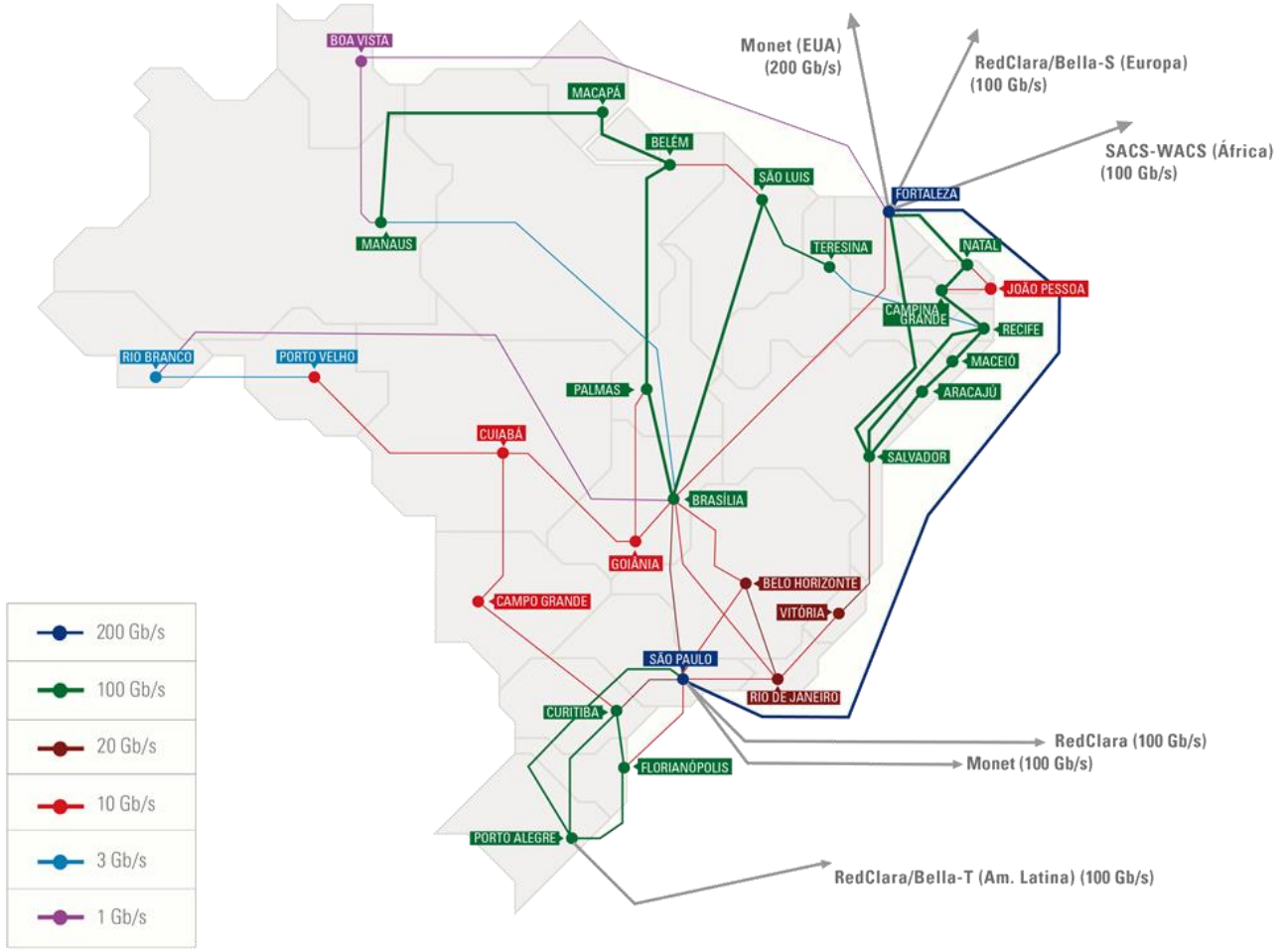
Yuri Alexandro

RNP – Rede Nacional de Ensino e Pesquisa

IX FÓRUM REGIONAL
Incentivando o diálogo sobre os Pontos de Troca de Tráfego Internet

Belo Horizonte/MG
26 de agosto de 2022

RNP


BOA VISTA
MACAPÁ
BELÉM
SÃO LUIS
FORTALEZA
MANAUS
TERESINA
NATAL
JOÃO PESSOA
CAMPINA GRANDE
RECIFE
MACEIÓ
ARACAJU
SALVADOR
RIO BRANCO
PORTO VELHO
PALMAS
CUIABÁ
BRASÍLIA
GOIÂNIA
BELO HORIZONTE
VITÓRIA
CAMPO GRANDE
SÃO PAULO
RIO DE JANEIRO
CURITIBA
FLORIANÓPOLIS
PORTO ALEGRE
Monet (EUA) (200 Gb/s)
RedClara/Bella-S (Europa) (100 Gb/s)
SACS-WACS (África) (100 Gb/s)
RedClara (100 Gb/s)
Monet (100 Gb/s)
RedClara/Bella-T (Am. Latina) (100 Gb/s)
200 Gb/s
100 Gb/s
20 Gb/s
10 Gb/s
3 Gb/s
1 Gb/s

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

#whoami

Yuri Alexandro

Analista de Sistemas

Especialista em Gestão de Segurança da Informação

Encarregado pelo Tratamento de Dados Pessoais na RNP

+20 anos na área de Tecnologia da Informação

+12 anos na área de Segurança da Informação

Privacidade

MICHAELIS | Português | Inglês | Espanhol | Alemão | Italiano | Francês

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*.

Não é só um diferencial competitivo

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)

Não é só um diferencial competitivo...

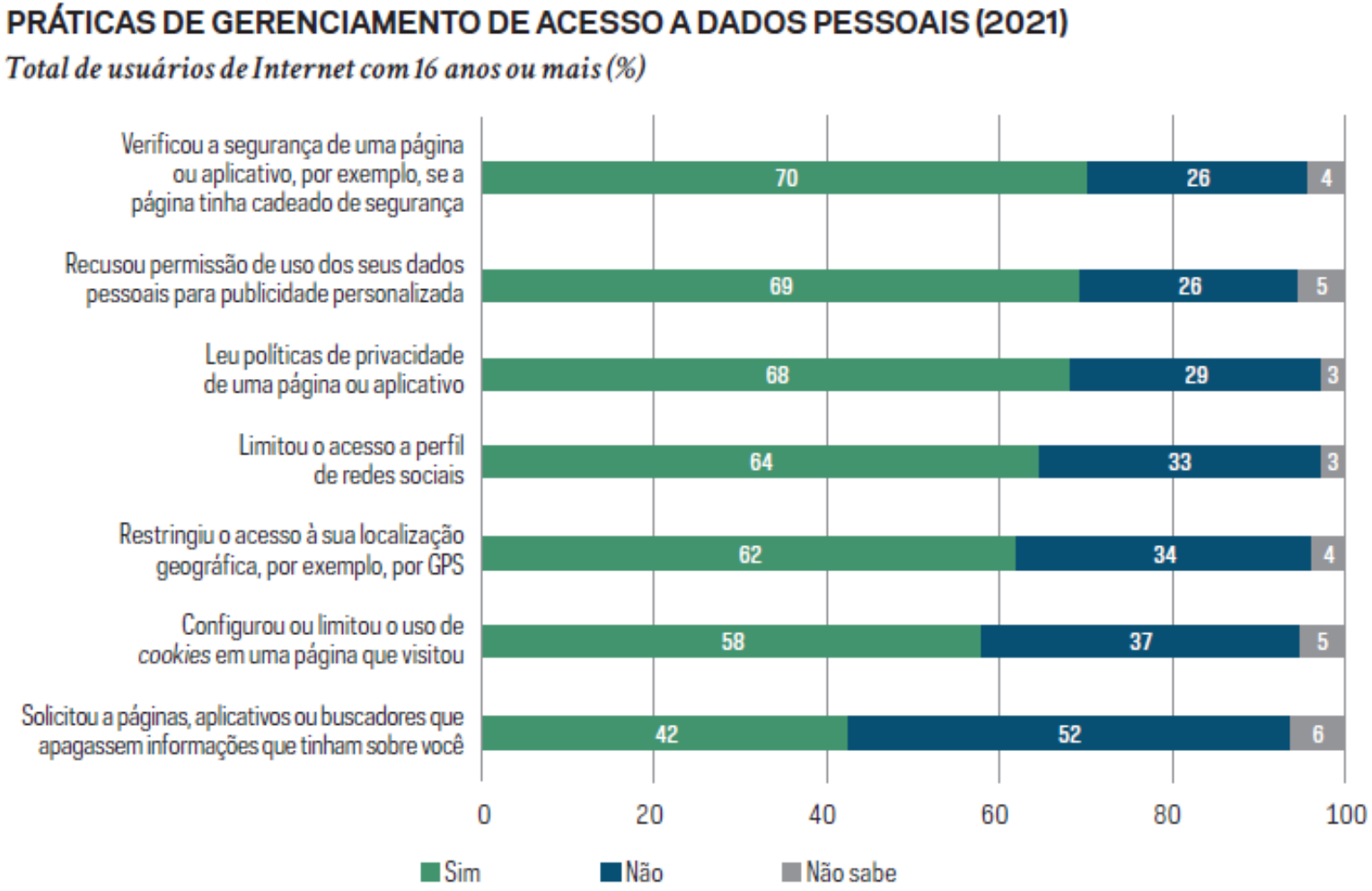
LGPD

Lei Geral de Proteção de Dados Pessoais

Não é só um diferencial competitivo...

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2021
Usuários de Internet

Não é só um diferencial competitivo...

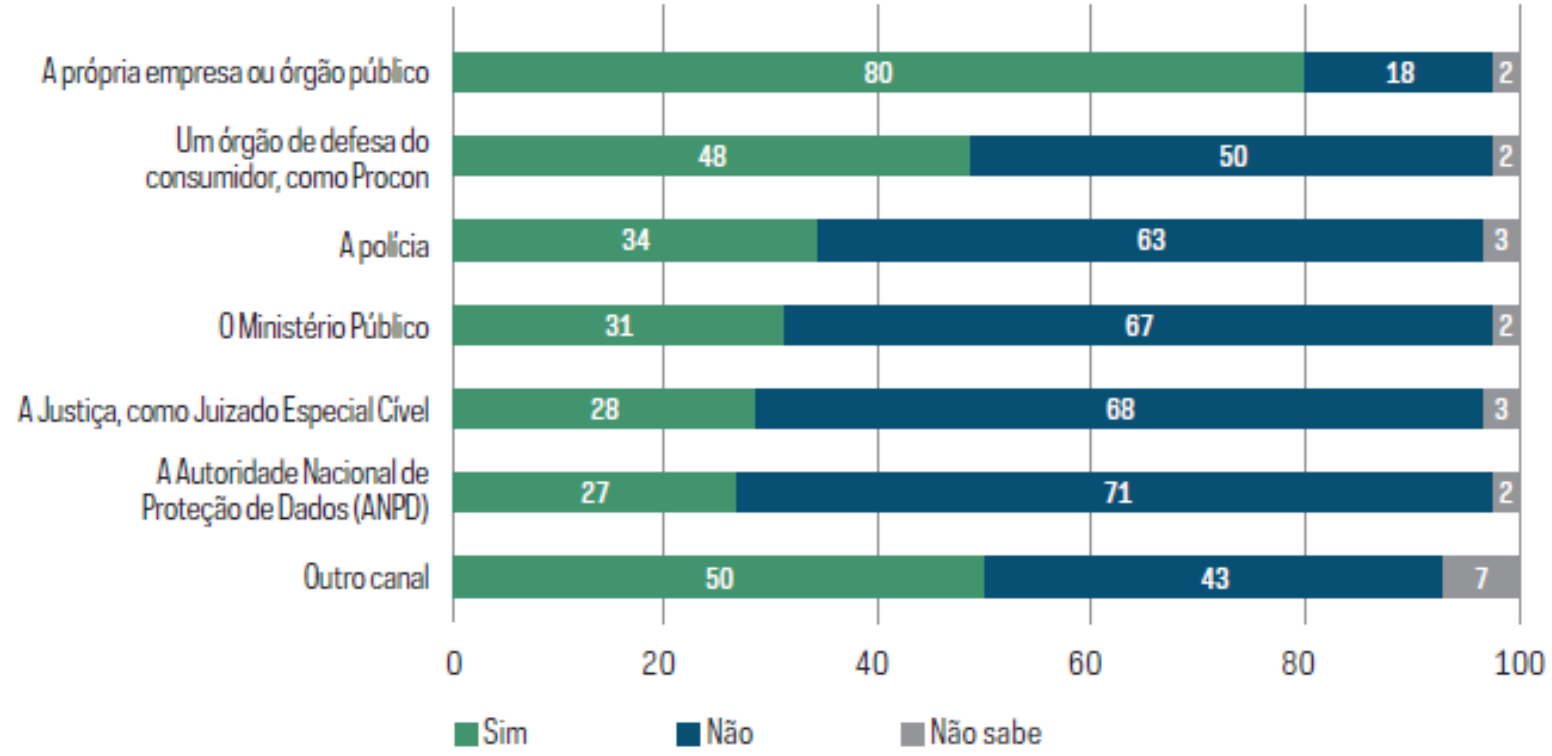


Fonte: Pesquisa Privacidade e Proteção de Dados Pessoais, 2021 – CETIC.br

Não é só um diferencial competitivo...

CANAL DE ATENDIMENTO QUE BUSCARAM SOBRE SEUS DADOS PESSOAIS (2021)

Total de usuários de Internet com 16 anos ou mais que buscaram algum canal de atendimento sobre seus dados pessoais (%)

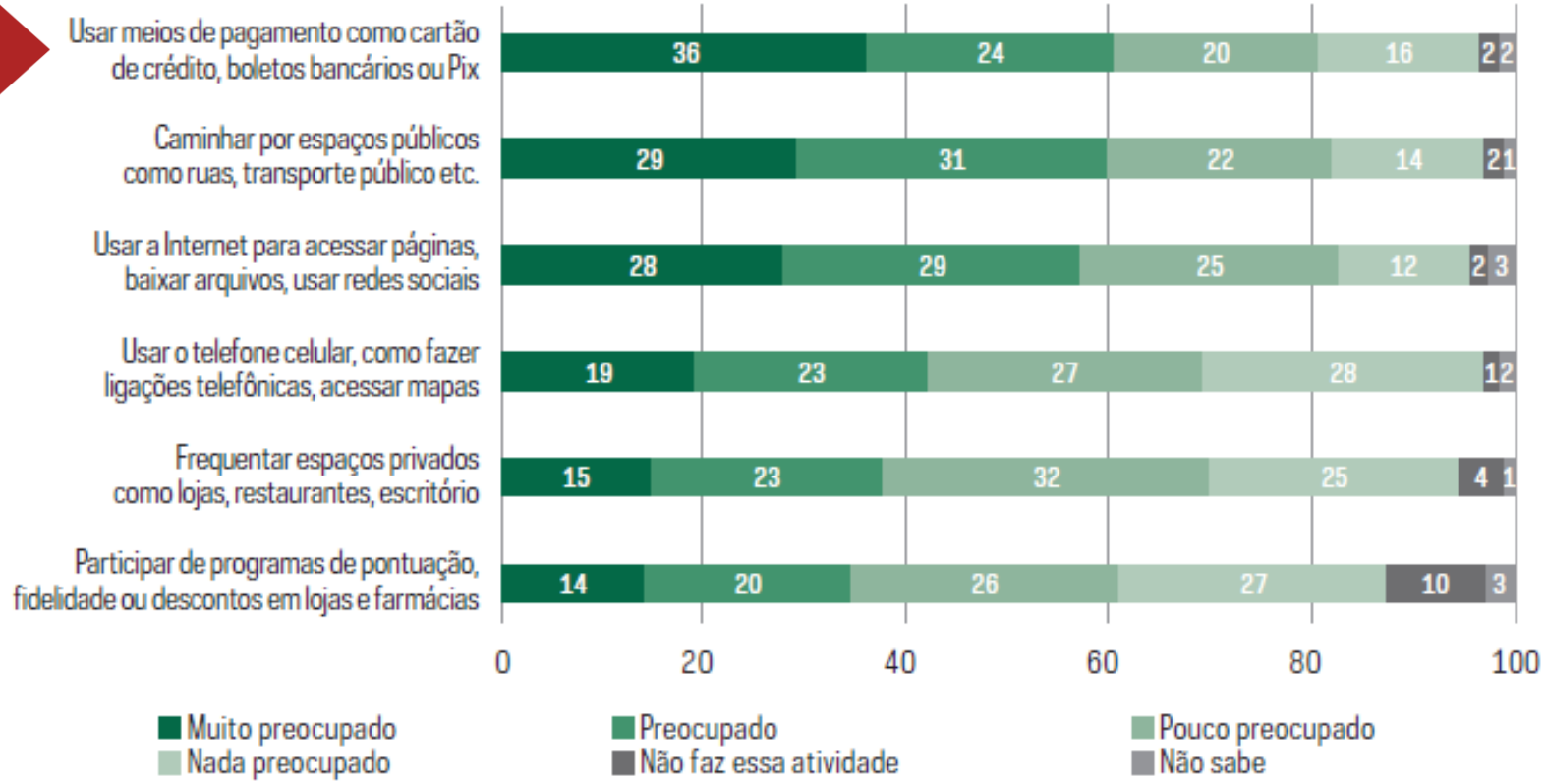


Fonte: Pesquisa Privacidade e Proteção de Dados Pessoais, 2021 – CETIC.br

Não é só um diferencial competitivo...

NÍVEL DE PREOCUPAÇÃO COM REGISTROS DE ATIVIDADES SEGUNDO TIPO DE REGISTRO (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Fonte: Pesquisa Privacidade e Proteção de Dados Pessoais, 2021 – CETIC.br

Não é só um diferencial competitivo...

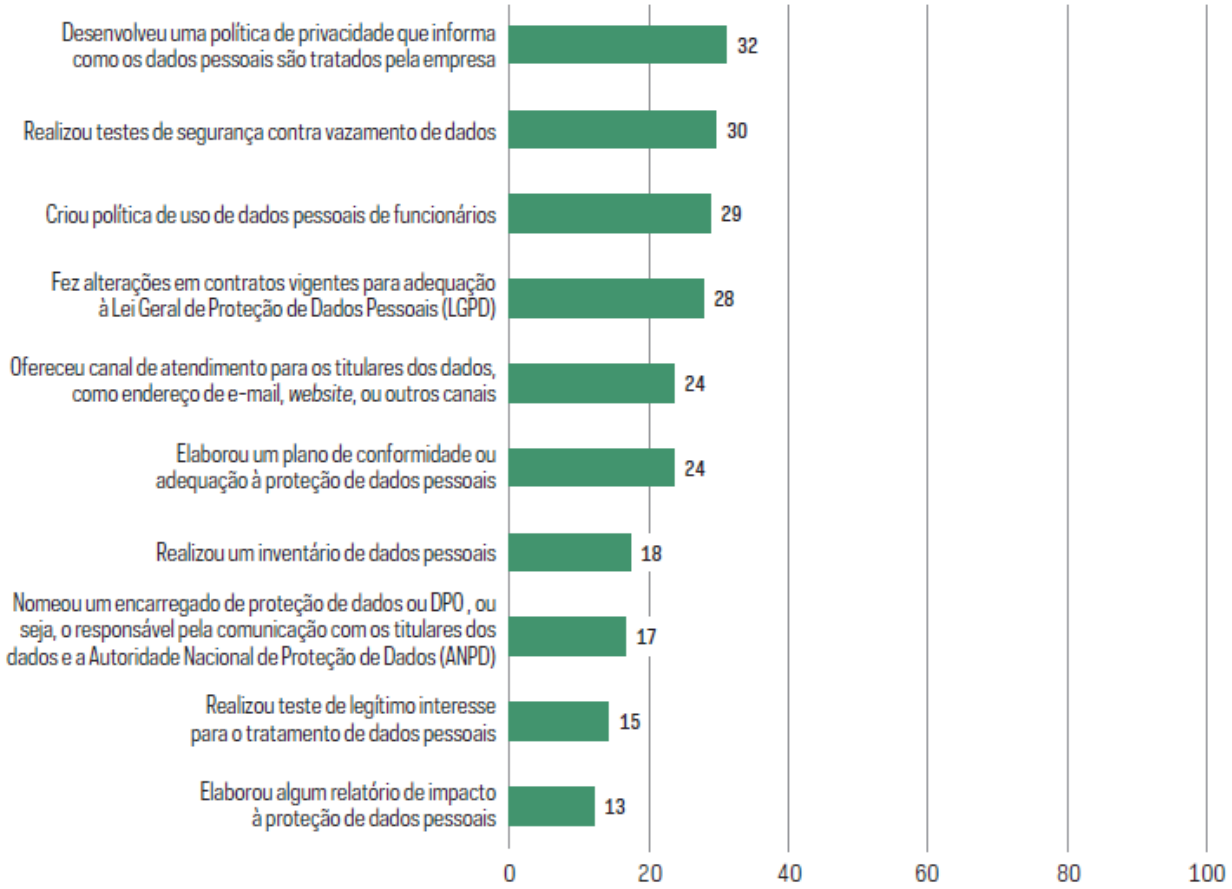
Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2021
Empresas

Não é só um diferencial competitivo...

GRÁFICO 10

EMPRESAS, POR TIPO DE AÇÃO DE ADEQUAÇÃO À LGPD (2021)

Total de empresas que mantêm dados de pessoas físicas (%)



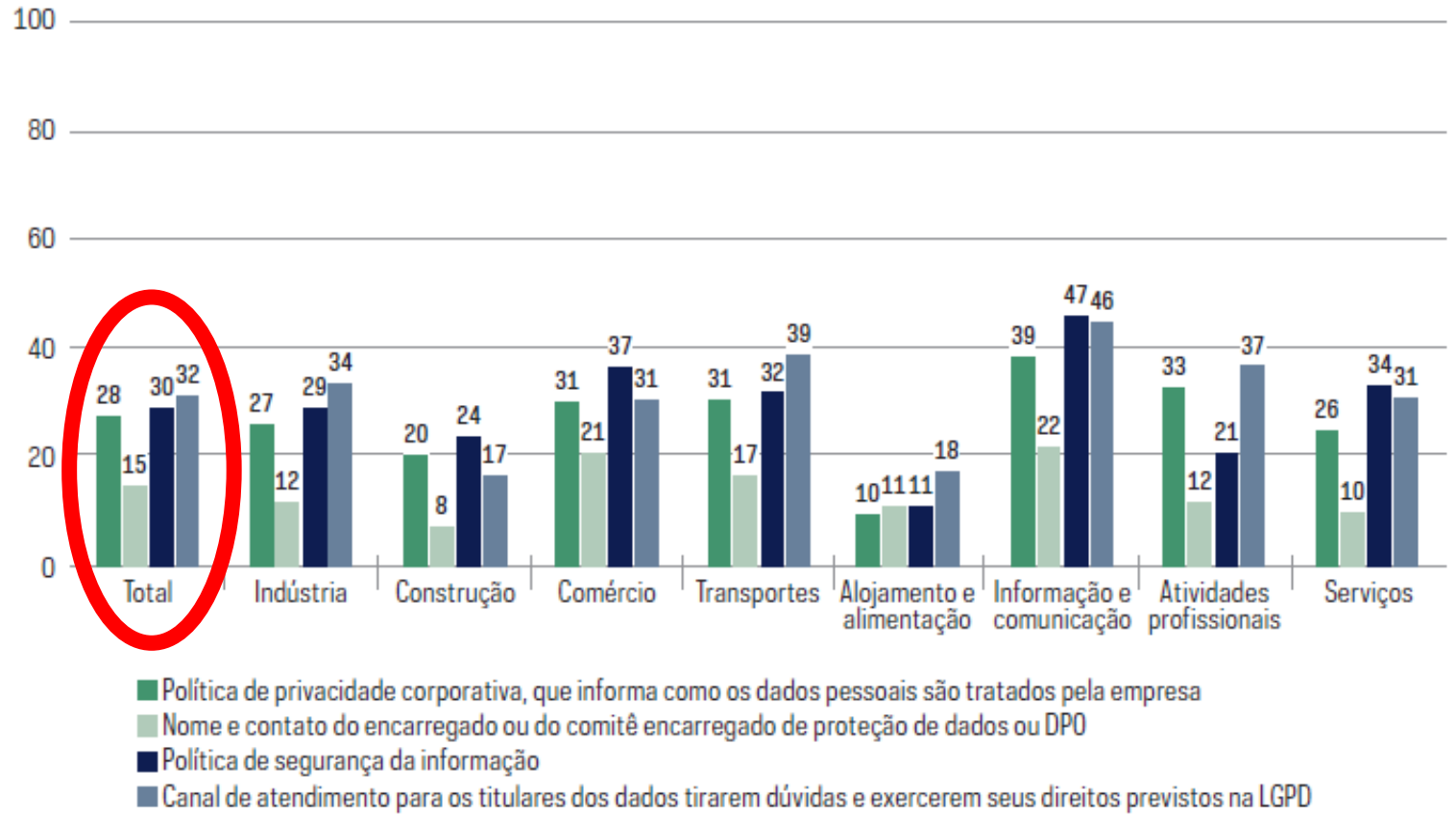
Fonte: Pesquisa Privacidade e Proteção de Dados Pessoais, 2021 – CETIC.br

Não é só um diferencial competitivo...

GRÁFICO 13

EMPRESAS, POR RECURSOS OFERECIDOS NO *WEBSITE* (2021)

Total de empresas que possuem website (%)



Fonte: Pesquisa Privacidade e Proteção de Dados Pessoais, 2021 – CETIC.br

...mas também é um diferencial competitivo

YouTube BR

#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

...mas também é um diferencial competitivo

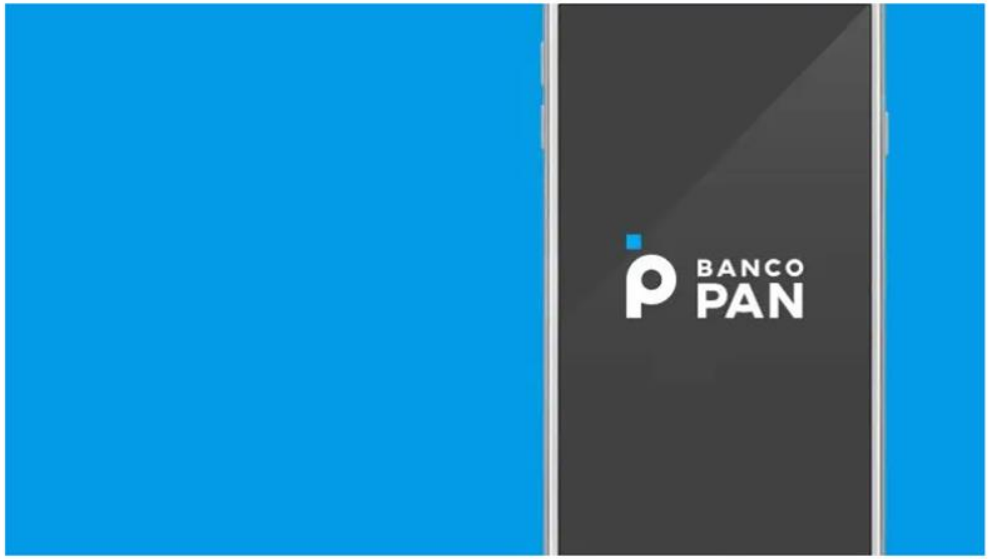
InfoMoney

Cartão de crédito

Banco Pan (BPAN4) confirma vazamento de dados de clientes

Empresa, que tem 17 milhões de clientes, não diz quantos foram afetados e culpou 'fragilidade na plataforma de um fornecedor de tecnologia'

Por Equipe InfoMoney 18 abr 2022 11h11-Atualizado 4 meses atrás



O Banco Pan (BPAN4) confirmou o vazamento de dados de clientes, como dados cadastrais, limite disponível do cartão de crédito e do saldo devedor de fatura, mas não informou quantos clientes foram afetados.

Onde podem estar os dados pessoais

Em relacionamento com clientes

Banco de dados de clientes

Formulários preenchidos pelos clientes

E-mails de marketing enviados/recebidos

Registros de conexão

Hipóteses de tratamento de dados pessoais

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

Hipóteses de tratamento de dados pessoais

Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Vigência

Regulamento

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.**

§ 3º Na hipótese do § 2º , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput.**

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

Hipóteses de tratamento de dados pessoais

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.

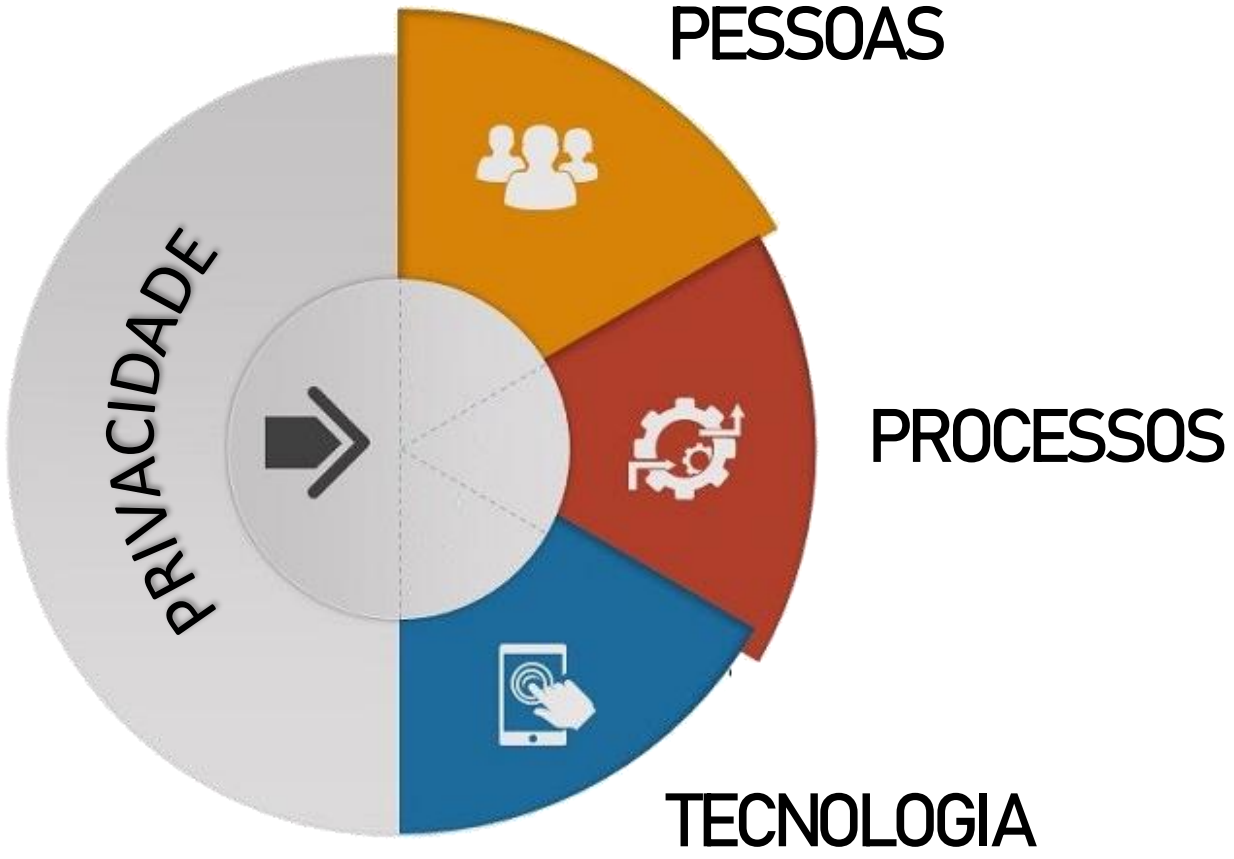
Art. 65-J. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:

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?

Privacy by design

Privacy by design

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, incluindo consentimento.

Pensar em facilitado dos clientes às próprias informações pessoais.

Processos estruturados dos para identificação positiva do cliente.

Privacy by design

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)

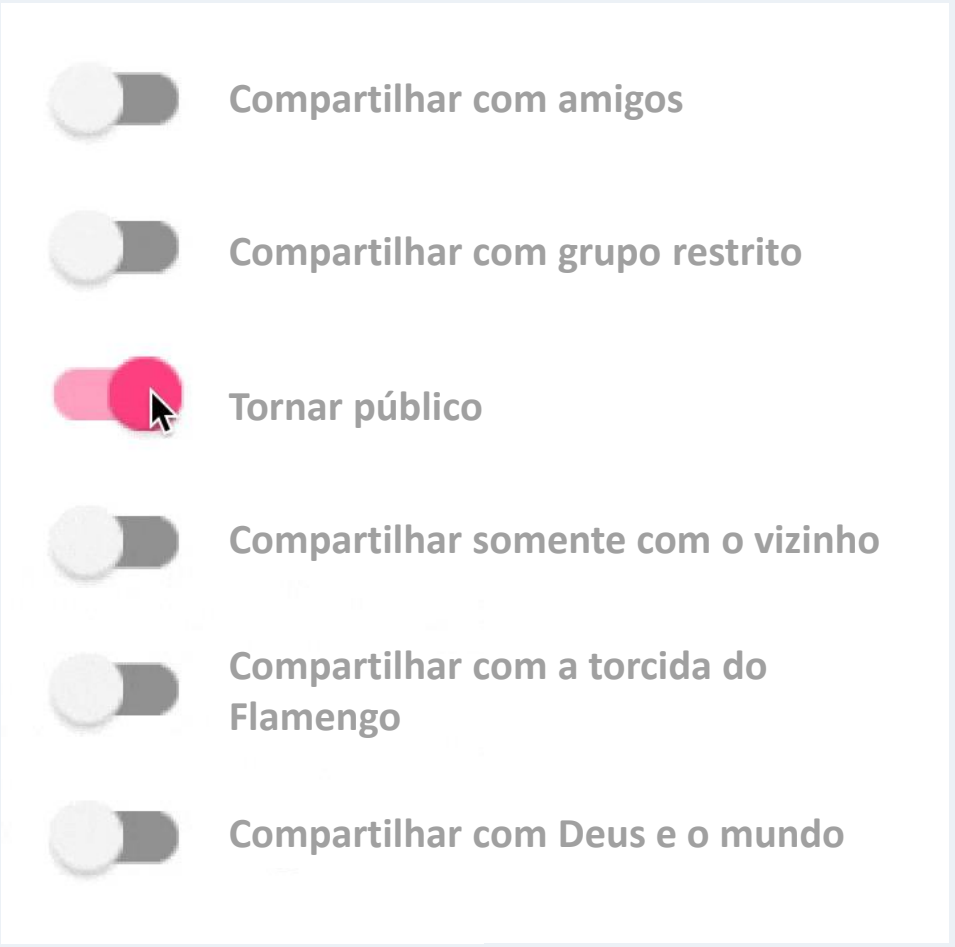
Limitar o uso, retenção e divulgação de informações pessoais aos propósitos relevantes identificados e para os quais o indivíduo prévia e expressamente consentiu, quando necessária sua autorização para esses tipos de operações.

Aplicando a provedores

Aplicar princípio de minimização de coleta e uso dos dados pessoais no serviço/sistema

Configurações de opção de consentimento (Opt-in) desabilitadas por padrão.

Compartilhamento dos dados deve ser os mais restritivo possível



Privacy by design

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

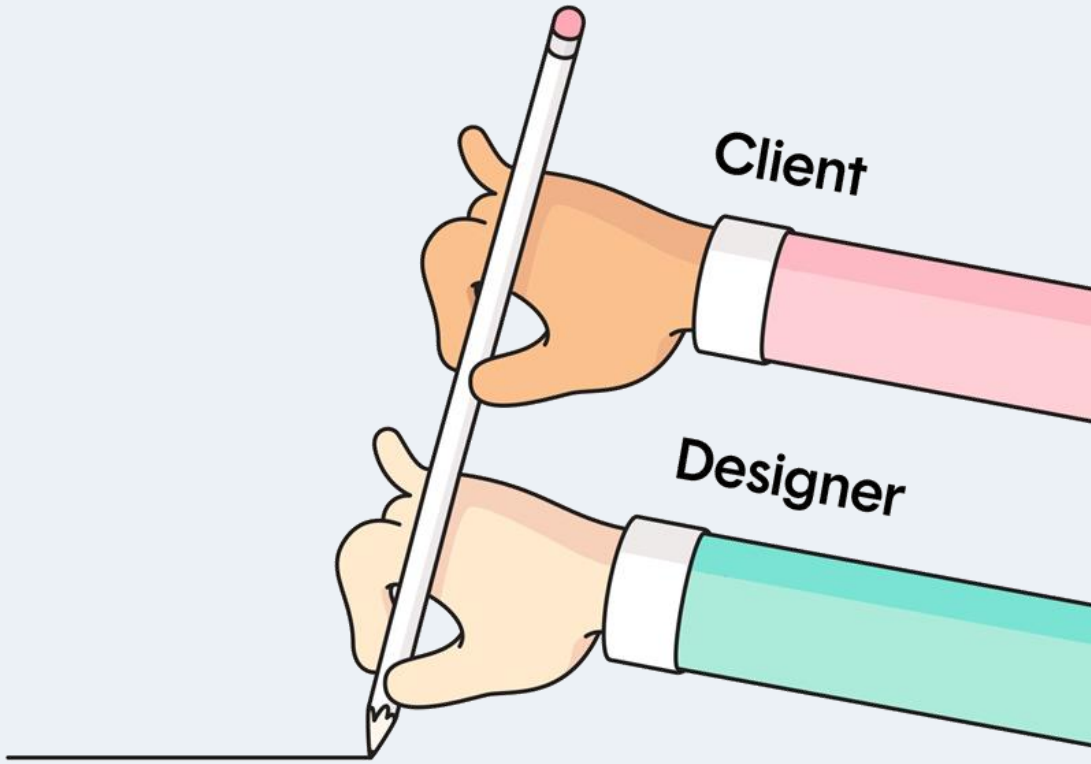
Incorporar privacidade ao design dos produtos e serviços, minimizando o impacto da tecnologia na privacidade das pessoas, de forma que as configurações de privacidade não sejam facilmente degradadas por meio de uso, configuração indevida ou erro dos sistemas.

Aplicando a provedores

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

Implementar funções para mascarar
dados pessoais na interface do usuário.

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



Privacy by design

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.

Otimizar uso do sistema quando
necessário aplicar funções de segurança.

Revisar controles de segurança e controle de acesso
em serviços/interfaces hospedadas em nuvem.

Privacy by design

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.

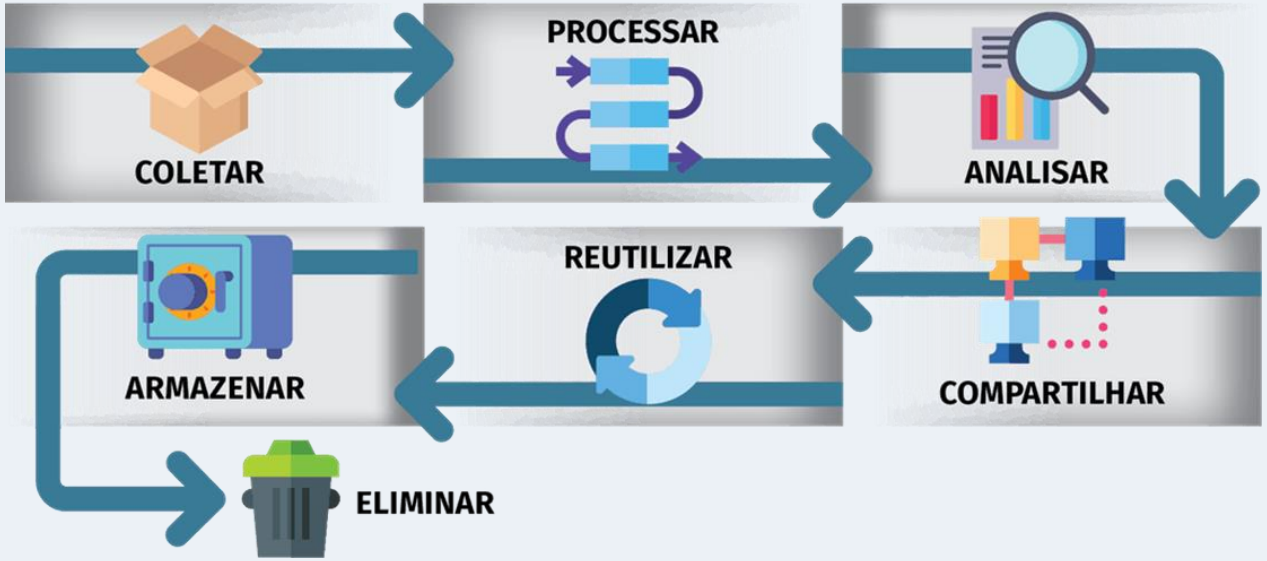
Medida técnica

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.

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



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

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

Privacy by design

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.

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

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

Privacy by design

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

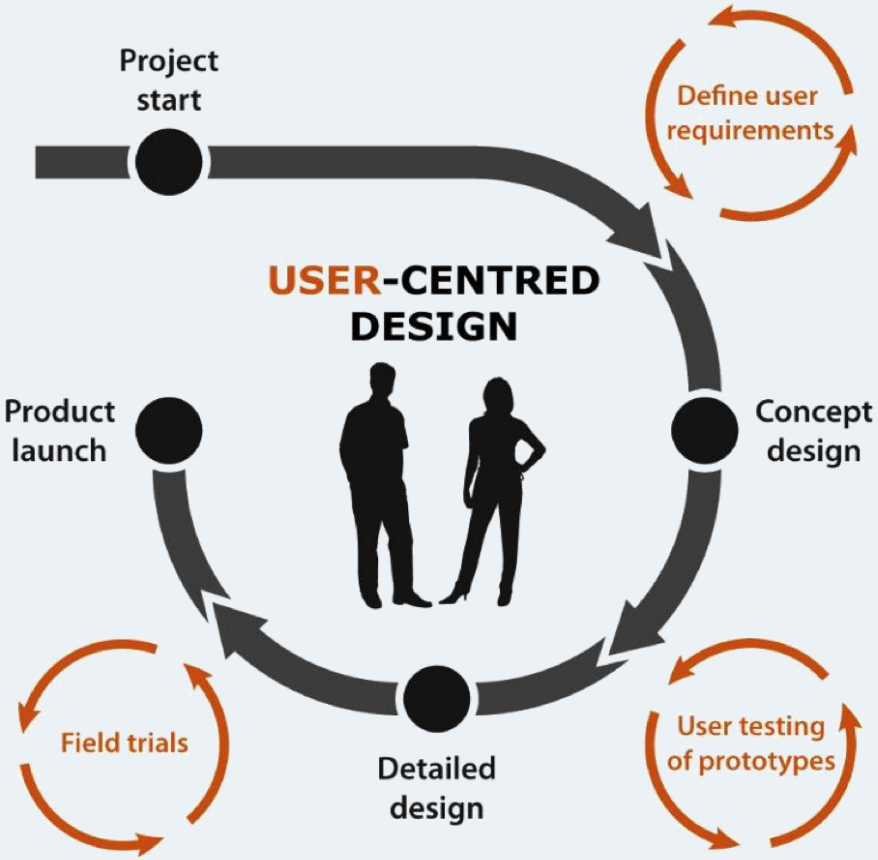
Estabelecer padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular de dados a exercer, de forma efetiva, todos os seus direitos assegurados por lei, e que lhes deem absoluto controle sobre os seus dados pessoais.

Aplicando a provedores

Publicar avisos de privacidade
de fácil entendimento para os clientes.

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

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

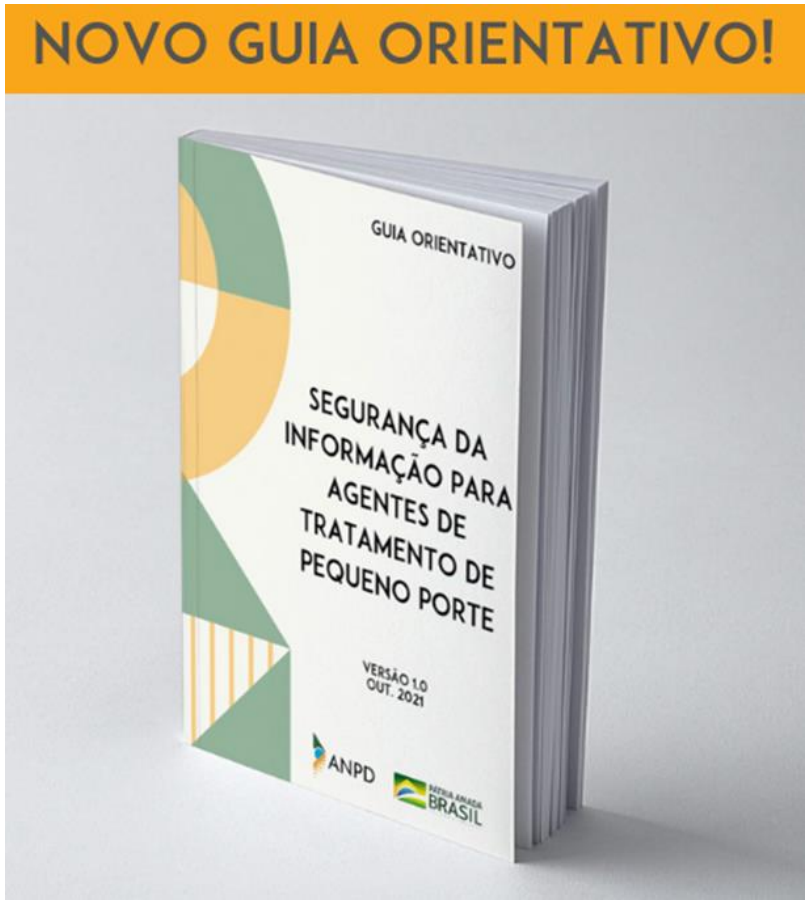


Privacy by design

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



Conclusão

O serviço que você entrega agrega privacidade?

Obrigado!

Yuri Alexandro

yuri.ferreira@rnp.br