

LGPD na Prática

Manual de Boas Práticas e Principais conceitos sobre a Lei Geral de Proteção de Dados para entidades do Terceiro Setor



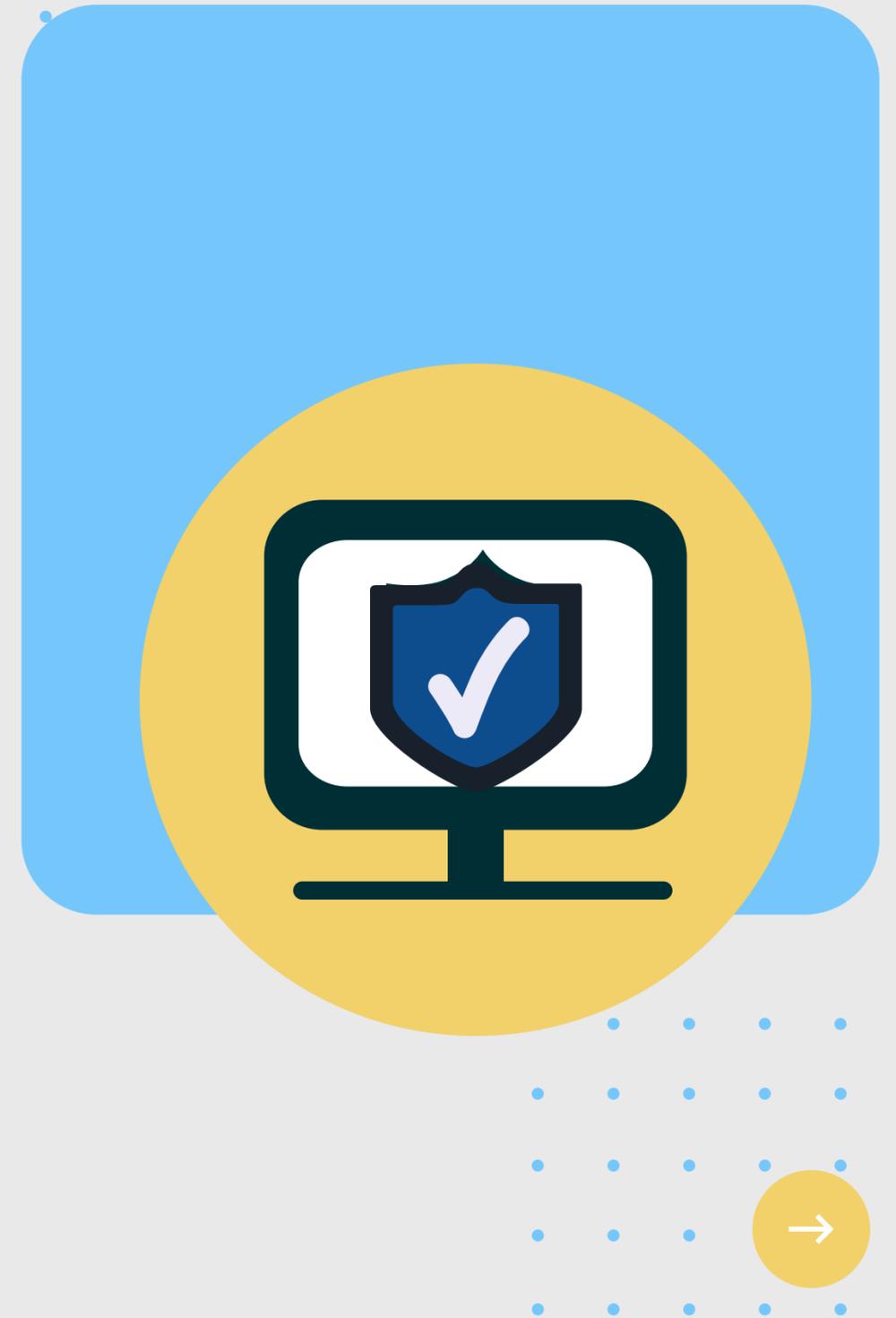
O QUE É A LGPD?

Em uma época em que o alcance das nossas informações aumentou muito por causa das ferramentas digitais, se tornou também importante aumentar a proteção a estas informações de cada um de nós, que também chamamos de **dados pessoais**.

A LGPD ou Lei Geral de Proteção de Dados (lei 13.709/18) entrou em vigor em 18 de setembro de 2020 e cria novas obrigações para proteção de dados pessoais, sejam eles digitais ou não, estabelecendo mais direitos aos indivíduos e mais obrigações às organizações públicas ou privadas que usam dados pessoais no Brasil.

Além disso, ela cria regras claras sobre os processos de coleta, armazenamento e compartilhamento dessas informações para que elas não sejam usadas de maneira errada ou diferente do que foi informado para o titular. Isso ajuda a promover o desenvolvimento tecnológico ao mesmo tempo que procura garantir a segurança dos indivíduos.

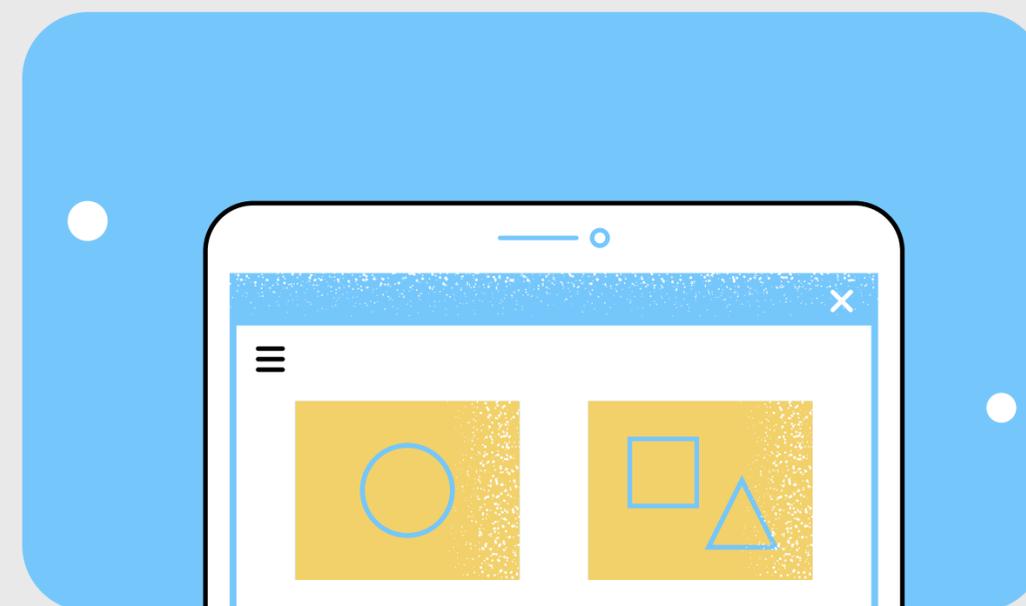
Com esta lei, o Brasil passará a integrar um grupo de 134 países implementando leis de proteção de dados pelo mundo.



PERSONAGENS E TERMOS DA LEI

A LGPD traz nomes e conceitos novos que podem parecer um pouco de "juridiquês", mas é importante conhecê-los.

Vamos dar uma olhada neles?



Titular

Pessoa física que é a proprietária dos dados pessoais.

Todos nós somos titulares de dados e compartilhamos nossos dados diariamente com empresas, entidades e o Poder Público.

Encarregado

Responsável da instituição, para acompanhar o tratamento de dados dos titulares, e ser o canal de comunicação com titulares, Autoridade Nacional e parceiros. Pode ser pessoa física ou jurídica.

Dados Pessoais

É a informação relacionada a uma pessoa identificada ou identificável. Ele pode ser o seu CPF isoladamente, o seu endereço, um login de e-mail ou mesmo uma foto, que pode ser reconhecida em um aplicativo que vai relacionar esta foto a você.

Controlador

A pessoa física ou jurídica que decide a respeito do tratamento dos dados pessoais.

Exemplo: uma empresa que coleta dados para empregar funcionários, uma escola que coleta dados de alunos.

Operador

Pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Exemplo: uma assessoria contábil que processa pagamentos de funcionários de várias empresas, uma solução em nuvem que hospeda dados.

Bases Legais

Uma base legal é uma finalidade prevista em lei para que empresas, entidades e o poder público possam tratar dados pessoais.

Exemplo: a **execução de um contrato** de trabalho é uma finalidade prevista para coletar dados necessários de funcionários. O **consentimento** pode ser uma base legal para mandar e-mail marketing. O **cumprimento de obrigação legal** pode requerer que você guarde alguns dados coletados por um período de tempo. Existem 10 bases legais dando permissões diferentes para o uso de dados pessoais.

Tratamento

É qualquer tipo de operação realizada com o uso de dados pessoais.

Alguns exemplos são a coleta, acesso, armazenamento, distribuição, avaliação, modificação, processamento, transferência recepção e mesmo a eliminação destes dados.

Dados Pessoais Sensíveis

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Têm hipóteses mais restritas de tratamento.

Dado Anonimizado

É o dado relativo a um titular que não pode ser mais identificado, considerando a utilização de meios técnicos razoáveis na ocasião de seu tratamento.

Exemplo: quando, em uma pesquisa, apenas dados genéricos são coletados que identifiquem a pessoa a um grupo (homem, 60 anos, aposentado) e não tenha capacidade de identificá-lo individualmente. No entanto, se houver qualquer dado que identifique a pessoa (endereço, por exemplo), ele deixa de ser anonimizado.

COMO TRATAR DADOS PESSOAIS

Nós usamos dados pessoais para tudo. Damos nosso CPF para comprar produtos, fazemos login para acessar nosso e-mail, registramos pessoas em fotos, que depois são marcadas por ferramentas de reconhecimento facial, que as identifica.

Mas com a chegada da LGPD, existem regras para o que podemos ou não podemos fazer com os dados pessoais dos outros, como empresa, entidade ou Poder Público. Vamos ver aqui um pouquinho o que são e como usar as **BASES LEGAIS** que mencionamos antes e outros requisitos especiais, como o tratamento de dados pessoais de menores.



Consentimento

Autorização para tratamento de dados. As informações sobre o tratamento devem ser claras e acessíveis. O uso deve ser específico apenas para aquela finalidade solicitada. O consentimento deve ser registrado. Lembre-se que o consentimento não é a única forma de usar dados pessoais. Existem todas as outras opções abaixo.

Execução de Contrato

Quando os dados são necessários para que um contrato possa ser assinado. Ex: verificação da situação cadastral de um fornecedor junto à Receita Federal, endereço de entrega de itens adquiridos pela internet, contratação de funcionário.

Cumprimento de obrigação legal

Quando uma lei obriga que dados pessoais sejam guardados por um certo período de tempo, a entidade deve cumprir o que pede a lei e guardar os dados pelo tempo necessário (ex: dados de ex-funcionários, colaboradores, ex-alunos, dados médicos em entidades que trabalhem na área da saúde).

Exercício regular de direito

O exercício regular de direitos permite o uso de dados pessoais em contrato e em processo judicial, administrativo e arbitral. Por exemplo, para apresentar um documento em juízo, para fazer prova em processo judicial, mesmo apresentando dados sensíveis, como dados de saúde.

Proteção da vida

A proteção da vida tem escopo de aplicação mais limitado. Seu uso pode ser levantado durante o monitoramento de epidemias, para garantir ajuda humanitária, para tratar paciente inconsciente, para internação de urgência ou campanhas de vacinação em empresas ou instituições.

Tutela da saúde

O tratamento de dados com base na tutela da saúde é aplicável exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Estes dados também *não podem* ser compartilhados para obter vantagem econômica.



Execução de Políticas Públicas

Dados pessoais também poderão ser usados para a execução de políticas públicas, para o atendimento de necessidades e solução de problemas da coletividade. Ex: cadastro de bolsa família, auxílios emergenciais e política de cotas.

Estudo por órgão de pesquisa

Os estudos por órgãos de pesquisa têm um papel importante no desenvolvimento econômico. São órgãos da administração pública direta ou indireta, sem finalidade lucrativa. Assim, órgãos de pesquisa privada não podem se valer dessa finalidade para uso indiscriminado de dados.

Proteção ao crédito

A base de proteção ao crédito pode ser usada para a criação de cadastros de inadimplentes e também de adimplentes (cadastro positivo) para avaliação de risco de crédito, quando o titular solicita um empréstimo, financiamento ou vai contratar determinados serviços.

Interesse legítimo do Controlador ou terceiros

Quando alguém já tem um relacionamento anterior com uma instituição, seja como doador, voluntário ou colaborador, entende-se que a instituição poderá manter esta pessoa informada de atividades, eventos, relatórios, podendo se valer do legítimo interesse sem a necessidade do consentimento para esta finalidade.



Tratamento de dados de menores de idade

O tratamento de dados pessoais de crianças deverá ser realizado com consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

As informações de tratamento devem ser dadas de forma clara e acessível.

Apenas os dados estritamente necessários devem ser coletados.

→ Sem consentimento - apenas em duas situações: para contatar os pais/responsáveis - sem armazenamento, sem passar para terceiros; e quando utilizado para a proteção da criança.



Princípios da LGPD

A LGPD tem dez princípios que precisam ser observados. E só por eles já temos uma boa ajuda do que devemos ou não devemos fazer a respeito de dados pessoais.

Também temos boas dicas sobre o que você pode fazer para colocá-los em prática.



Princípios da LGPD

Nós traduzimos aqui os 10 princípios da LGPD em perguntas que podem te ajudar na decisão sobre o uso dos dados:



- **Necessidade:** é realmente necessário utilizar estes dados para atingir o objetivo desejado pela entidade?
- **Finalidade:** os dados estão sendo coletados para uma finalidade específica e informada ao titular?
- **Adequação:** o tratamento está sendo feito de acordo com o que foi informado para o titular e não para outro fim?
- **Livre acesso:** o titular pode consultar, de forma fácil e gratuita, seus dados, a forma de tratamento e sua duração?
- **Qualidade dos dados:** os dados estão corretos, atualizados e estão de acordo com a necessidade para a finalidade?
- **Transparência:** a pessoa foi informada o motivo do tratamento dos dados de forma clara e transparente?
- **Segurança:** os dados são guardados em lugar seguro, seja física ou digitalmente?
- **Prevenção:** conseguimos prevenir da melhor maneira possível o acesso não autorizado a estes dados?
- **Não discriminação:** os dados não serão usados de maneira alguma para causar qualquer tipo de discriminação?
- **Responsabilização e prestação de contas:** somos capazes de provar que tomamos as medidas necessárias para cumprir as normas de proteção de dados?

LGPD na Prática

Como fazer para colocar todas essas informações na prática em sua instituição? Vamos dar algumas dicas e apresentar boas práticas que podem ser adequadas à realidade de cada local.



CARTA TÉCNICA FEAC



Tratamento de Dados

É preciso entender a) quais dados sua instituição coleta, b) de que forma eles são coletados e c) qual a finalidade de uso destes dados.

Com isso, é possível estabelecer qual a base legal para usar estes dados e ficar de acordo com a lei.

Dados que não são necessários devem ser excluídos.



Site e Cadastro

Se a instituição tem um site, é importante verificar os seguintes itens:

- [Política de Privacidade](#): falamos sobre ela no quadro abaixo.
- [Cookies](#): se a entidade faz uso de cookies para coletar dados do usuário é preciso notificar e pedir o aceite do usuário.
- Se não tem site, mas faz [Cadastro](#) para qualquer finalidade, a coleta de dados para cadastro deve focar nos dados estritamente necessários e apenas para a finalidade informada.

Indicação do Encarregado

O Encarregado é 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).

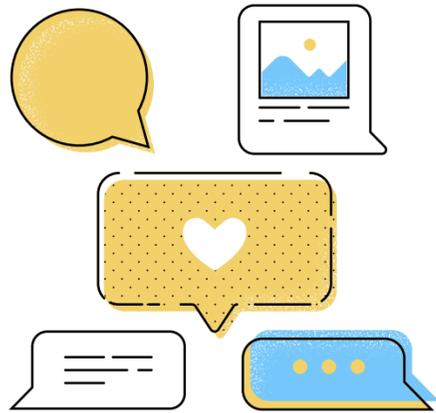
Por enquanto, até a ANPD se manifestar a respeito das exceções, toda instituição que trata dados pessoais deve ter um Encarregado apontado. Esta pessoa pode ser indicada na Política ou Aviso de Privacidade da instituição.



Política e Avisos de Privacidade

- [Política de Privacidade](#): é necessário criar uma política de privacidade de maneira simples, informando pelo menos o seguinte: identificação e informações de contato do Controlador, quais dados são coletados, com que finalidade, se estes dados são compartilhados com terceiros, quais os direitos dos titulares e como fazer para exercê-los.
- [Avisos de Privacidade](#): caso você trabalhe na sua instituição com monitoramento via câmera, monitorea a internet, ou faz qualquer outro tipo de coleta de dados pessoais, é importante informar o usuário, colaborador, ou visitante.

Linguagem clara e acessível



Ao explicar para o titular a finalidade do uso de dados, solicitar consentimento, quando for o caso e explicar os direitos, é importante usar uma linguagem clara e acessível.

O uso de recursos visuais é encorajado, para facilitar o entendimento.

As explicações não precisam ser em forma escrita apenas. Desenhos, gráficos podem auxiliar o entendimento.

Softwares e antivírus

Manter softwares e antivírus originais e atualizados que garantam a proteção da instituição contra malwares, ransomwares e outros ataques cibernéticos que podem colocar em risco não só os dados dos titulares, mas a segurança da organização como um todo.



Marketing e Doações

Dentro da LGPD, alguns cuidados são muito importantes quando a entidade fizer campanhas de marketing e solicitar doações.



- Nunca compre listas de e-mail se não tem uma base legal para fundamentar seu uso
- Não inclua contatos automaticamente sem um primeiro contato ou uma relação pré-existente
- Quando fizer um cadastro, não use caixas pré-marcadas obrigando o contato a receber mensagens da instituição



- Sempre solicite ao titular se ele quer receber informações da instituição
- Permita que o titular possa escolher quando não quer mais receber mensagens, e-mails e ligações da instituição, incluindo um botão de descadastro no e-mail ou canais para que o titular possa fazer esta solicitação (por exemplo: um endereço de e-mail)
- O titular tem direito de saber quais dados dele a instituição mantém. Ele pode solicitar a correção, alteração ou mesmo a exclusão destes dados. Forneça na Política de Privacidade da instituição um canal para que ele possa fazer estas solicitações e atenda os pedidos feitos pelo titular

Incidentes de Vazamento

Caso aconteça um vazamento de dados, apesar de todos os cuidados, o Controlador deverá tomar algumas medidas.

Dependendo do grau do vazamento, ele deverá comunicar à Agência Nacional de Proteção de Dados e ao titular a ocorrência de um incidente de segurança.

Este incidente pode ser uma invasão hacker com roubo de dados que possam causar dano real ao titular, por exemplo.

Por isso, atenção! Em que casos isso deve ser feito? Apenas em casos que possam acarretar *risco ou dano relevante* aos titulares. A comunicação deve ser feita em prazo razoável e deve conter a descrição dos dados pessoais afetados, informações sobre os titulares envolvidos, riscos, medidas adotadas.

Se um incidente desses acontecer, procure imediatamente ajuda técnica e jurídica.



Revisão de contratos

Todos os contratos com fornecedores e parceiros que envolvam tratamento de dados pessoais coletados pela organização devem ser revisados e adequados à nova lei.

A ausência de medidas adequadas de segurança e da adequação dos fornecedores à LGPD pode resultar em responsabilidade solidária para o Controlador dos dados.

Inclua no Contrato cláusulas que obriguem os parceiros a proteger os dados compartilhados.

Treinamento de equipe



O envolvimento dos colaboradores no processo garante uma melhor adequação e manutenção das boas práticas de proteção de dados como parte dos valores da entidade.

O treinamento da equipe e esclarecimento com relação às boas práticas permitem que eles possam entender e participar do processo com mais clareza.

Segurança da Informação

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, sejam elas físicas ou digitais, evitando acessos não autorizados. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer de seu uso impróprio. Para sua proteção, sugere-se a criação de uma Política de Segurança da Informação adequada à realidade da instituição. Aqui trazemos algumas práticas que podem ser adotadas dentro desta política:

- Reveja a forma em que dados pessoais são armazenados, utilizando senhas em planilhas sempre que possível e mantendo os dados físicos em locais seguros, com chave;
- Registre a identificação de visitantes em áreas reservadas;
- Use senha nos computadores e usuários diferentes para acessos de pessoas diferentes, mesmo que utilizem o mesmo computador;
- Defina quais pessoas dentro da instituição necessita acessar informações mais críticas;
- Programe o bloqueio do computador quando não estiver em utilização;
- Não deixe senhas acessíveis em post-its, embaixo do computador ou em local de fácil visibilidade;
- Altere as senhas periodicamente;
- Evite deixar documentos com dados pessoais expostos a quem não precisa ter acesso a eles, em especial dados sensíveis;
- Descarte adequadamente os dados que não são mais necessários. CVs devem ser triturados, mídias devem ser destruídas e backups devem ser verificados para eliminar completamente uma informação desnecessária. Dados físicos devem ser rasgados ou triturados. Não reaproveite-os para fazer rascunho.;
- Faça uso de redes de wi-fi confiáveis;
- Se possível, invista no uso de um antivírus para rastrear possíveis ameaças aos computadores da entidade;
- Nos casos em que for possível, anonimize ou criptografe os dados.



Direitos dos titulares

Dentro da LGPD, os titulares, têm direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara e acessível indicando (a) finalidade do tratamento, (b) forma e duração, (c) identificação do Controlador e suas informações de contato, (d) se os dados são compartilhados e qual a finalidade do compartilhamento, (e) as responsabilidades dos agentes de tratamento e os seguintes direitos:

Confirmação	Confirmação da existência de tratamento. Lembrando que tratamento pode ser qualquer ação feita com um dado pessoal: coleta, guarda, compartilhamento, e mesmo a exclusão.
Acesso	Acesso às informações que a informação têm a respeito do titular e como estes dados são tratados. A entidade tem 15 dias para responder a esta solicitação com uma cópia dos dados deste titular.
Correção	O titular tem direito de solicitar a correção dos dados que estiverem incompletos, inexatos ou desatualizados.
Eliminação	Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei. Por exemplo: a manutenção no cadastro de um dado sensível que não é necessário para a finalidade do uso.
Compartilhamento	O titular tem direito de ser informado, quando solicitar, sobre as entidades públicas e privadas com as quais o controlador compartilhou seus dados.
Objecção	Quando o tratamento é baseado em consentimento, o titular tem direito de saber o que acontece se ele negar consentimento. Por exemplo: não ter acesso a certas informações como eventos, festas, etc.
Retirada de consentimento	O titular tem direito de retirar o consentimento dado quando não quiser mais receber comunicações ou contato da entidade, por exemplo. Lembre-se: Isso só vale para dados tratados baseados em consentimento e não com outra base.

Quais as vantagens de se adequar?



Links úteis

Lei Geral de Proteção de Dados Pessoais:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Glossário LGPD - Serpro:

<https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd>

LGPD Acadêmico: Cursos, manuais e outros materiais relevantes na área de proteção de dados pessoais

<https://www.lgpdacademicooficial.com.br/>

Casa Hacker: A Casa Hacker fica baseada em Campinas e é um espaço hacker sem fins lucrativos e 100% dedicada a colocar comunidades locais no controle de suas experiências digitais e a moldarem o futuro da tecnologia da informação e comunicação para o bem público.

<https://casahacker.org/>

NIC.br: Nucleo de Informação e Coordenação do Ponto BR no Brasil. Tem cursos, cartilhas e pesquisas sobre segurança na Internet.

<https://cursoseventos.nic.br/>

Juventude Privada: iniciativa socioeducativa, sem fins lucrativos, que busca promover ensinamentos sobre privacidade, proteção de dados pessoais e cidadania digital, para que os jovens estudantes possam tomar decisões informadas e se protegerem, seja na internet ou fora dela

<https://www.juventudeprivada.org/o-projeto>

Governo Digital: Guias Operacionais do Governo Federal para adequação à LGPD

<https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>

Elaboração e organização



PAES DE MELLO
ADVOCACIA E CONSULTORIA



Elaborado por:

Ana Carolina Mello - Paes de Mello Advocacia

Revisado por:

Nathalia Garcia - FEAC

Os produtos de conhecimento FEAC estão em constante aprimoramento. Colabore enviando sugestões e considerações. Todas as contribuições são bem-vidas.

 feac@feac.org.br

 feac.org.br

 [fundacaofeac](https://www.instagram.com/fundacaofeac)

 [fundacaofeac](https://www.facebook.com/fundacaofeac)

A Fundação FEAC tem como missão a promoção humana, a assistência e o bem-estar social, com prioridade à criança e ao adolescente, em Campinas/SP.



R. Odila Santos de Souza Camargo, 34, Jd. Brandina, Campinas/SP.