NetSupport

LGPD e TI

Como adequar sua empresa na prática?

SUMÁRIO

Você em algum momento já se questionou sobre a necessidade de preencher certos dados pessoais em um formulário online? Já se perguntou o motivo de receber tantos e-mails de spam ou receber chamadas de números para os quais você nunca deu seu telefone?

As empresas modernas têm uma tendência cada vez maior a solicitarem dados de seu consumidor. Isso porque, com o Big Data, é possível utilizar essas informações para traçar um perfil de público e, consequentemente, estratégias de venda de produtos e serviços.

O problema é que a situação tem fugido do controle e nem todo mundo está satisfeito com a forma como esses dados estão sendo utilizados.

A **Lei de Proteção de Dados** entrou em vigor neste ano e reflete um cuidado extra que as empresas deverão ter para não acabarem em prejuízo.

Essa nova lei também impacta na forma como os profissionais de TI e gestores deverão atuar daqui para frente, se especializando cada vez mais nas exigências da nova regulamentação e inovando em suas práticas estratégicas, garantindo que a organização esteja em conformidade com a lei.

Por isso, neste conteúdo você encontrará um guia com tudo que você precisa saber sobre esse tema, que inclui:

- A importância da lei e como ela surgiu;
- O que são dados pessoais e sensíveis;
- O que a lei diz e quando entrou em vigor;
- O que as empresas devem fazer para se enquadrar nos critérios estabelecidos;
- Como a LGPD impacta o setor de TI;
- Princípios para colocar em prática nos projetos de TI;
- Checklist do passo a passo para adequar a empresa.

Boa leitura!

Importância e surgimento da LGPD

A Lei Geral de Proteção de Dados, ou Lei nº 13.709, foi sancionada no Brasil em agosto de 2018 pelo então presidente Michel Temer. A proposta demorou oito anos para ser aprovada no país, mas enfim seguindo o exemplo de países como Estados Unidos, Colômbia, Argentina, Uruguai, entre outros.

As discussões tiveram origem em um projeto da Câmara dos Deputados aprovado por unanimidade e em regime de urgência pelo Senado em julho do mesmo ano, em vista do vazamento de dados dos usuários do Facebook, coletados pela empresa Cambrigde Analytica e usados nas últimas eleições nos Estados Unidos.

Ainda que esse escândalo tenha levantado a necessidade de uma medida imediata, **não é de hoje que o uso de dados pessoais gera discussão e questionamento**. As reclamações de usuários por conta dessa situação são uma questão comum e mais recorrente do que se imagina.

Segundo uma pesquisa realizada pelo Instituto Brasileiro do Consumidor (Idec), o número de problemas com transparência e uso inadequado de informações pessoais teve um aumento de 137% entre 2016 e 2017.

Isso acontece porque, muitas vezes, não nos damos conta de que nossos dados estão sendo compartilhados. Na web há uma sensação comum de que tudo está disponível sem precisarmos fazer muito para ter acesso ao que quer que seja.

Mas **o problema é que tudo que fazemos é computado e utilizado por terceiros**, e muitas vezes nossos dados são pedidos em troca de alguma ação, por mais simples que ela seja.

Por conta da forma como toda essa troca de dados e seu uso por parte de empresas se naturalizou e até mesmo fugiu do controle, surgiu a necessidade de uma lei que atuasse regulamentando e punindo violações de direitos para estes casos específicos.

2

O que são dados pessoais e dados sensíveis?

A LGPD está ligada ao uso de dados pessoais e sensíveis de terceiros. Mas que dados são esses, afinal?

Dados pessoais são definidos como uma informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Os números do CPF e RG, por exemplo, são dados que podem levar à identificação de alguém e, portanto, são dados pessoais.

Outras informações, como etnia, religião e outras, **são consideradas dados sensíveis por também poderem ser usadas de forma discriminatória por pessoas mal-intencionadas**.

Por outro lado, dados que tenham sido descaracterizados, codificados ou colocados de forma pseudônima, mas que possam ser utilizados para identificar uma pessoa, continuam a ser dados pessoais.

Dados que tenham sido tornados anônimos, de modo que a pessoa não seja mais identificável, deixam de ser considerados dados pessoais. Importante ressaltar que, para que os dados sejam verdadeiramente colocados em anonimato, essa ação precisa ser irreversível.

Os dados pessoais são considerados em todas as formas de armazenamento, ou seja, em um sistema informático, através de videovigilância, ou em papel; em todos estes casos, **os dados pessoais estão sujeitos aos requisitos de proteção**.

O que diz a Lei Geral de Proteção de Dados?

A Lei Geral de Proteção de Dados passou por diversas alterações e quase foi adiada para 2022. Porém, ela entrou oficialmente em vigor no dia **18 de setembro de 2020**.

Ela foi criada basicamente com o objetivo de fornecer mais ferramentas de **controle aos usuários sobre como seus dados estão sendo usados por empresas digitais**. Regulamentando o uso, a proteção e a transferência de dados pessoais nos âmbitos privado e público.

A LGPD tem como objetivo criar um cenário de segurança jurídica mais eficiente a partir da padronização de normas e práticas, que buscam garantir a proteção, no país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil.

O texto da lei é baseado em uma regulamentação europeia semelhante ao Regulamento Geral de Proteção de Dados (GDPR, em inglês), que entrou em vigor em maio de 2018.

A nova lei, que altera o Marco Civil da Internet, de 2014, insere o Brasil em um círculo que, como comentamos anteriormente, compreende vários países comprometidos em proteger a privacidade e o uso de dados de seus usuários.

Ela se baseia nos direitos fundamentais da constituição de liberdade e de privacidade, como a livre iniciativa e o desenvolvimento econômico e tecnológico do país.

Um ponto importante da lei é que ela estabelece ainda, de modo claro, quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil, que podem chegar a uma **multa de milhões de reais** por incidente.

Podemos resumir os principais aspectos da lei nos seguintes pilares:

Consentimento e interesse legítimo

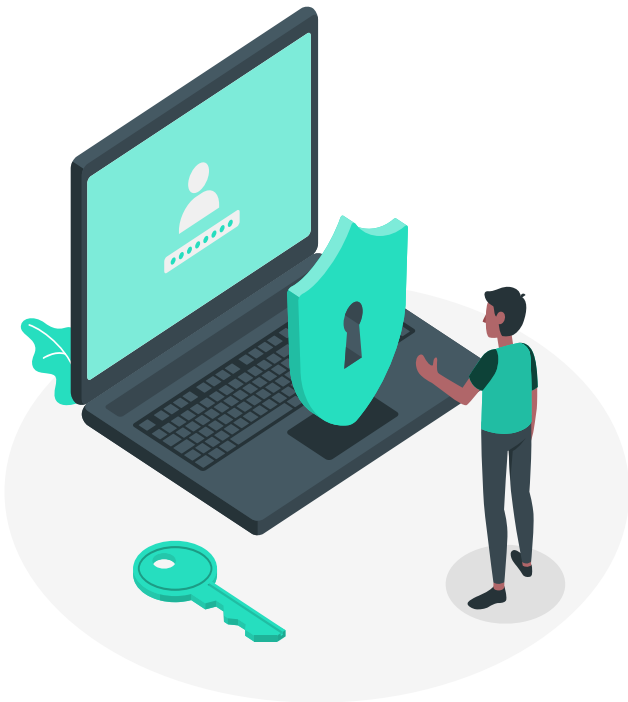
O consentimento é a base da criação da lei, no caso, o consentimento do cidadão que pode disponibilizar seus dados. **O motivo da coleta deve ser informado e o interesse de ambas as partes precisa ser claro e estar em sintonia**, daí a necessidade de assegurar essa relação.

Mas, como toda regra, há exceções também. Há a possibilidade de utilizar dados de terceiros sem seu consentimento se isso for indispensável para as seguintes situações:

- Cumprir uma obrigação legal;
- Executar política pública prevista em lei;
- Realizar estudos via órgão de pesquisa;
- Executar contratos;
- Defender direitos em processo;
- Preservar a vida e a integridade física de uma pessoa;
- Tutelar ações feitas por profissionais das áreas da saúde ou sanitária;
- Prevenir fraudes contra o titular;
- Proteger o crédito;
- Atender a um interesse legítimo, desde que não prejudique os direitos fundamentais do cidadão.

Autorização de revogação

Outro direito que a LGPD confere como garantia é a **solicitação para que dados fornecidos sejam deletados, revogando um consentimento prévio, além de proibir a transferência das informações para qualquer outro fornecedor de serviços**.



Ou seja, a lei estabelece um controle total do cidadão sobre o seus dados, podendo inclusive mudar de ideia após compartilhá-los.

É importante citar também que o tratamento dos dados deve ser feito levando em conta alguns quesitos específicos, como finalidade e a real necessidade de seu uso. Estes devem ser previamente definidos e informados ao cidadão, para que ele possa decidir se disponibiliza seus dados ou não.

Ainda que o processo em questão seja totalmente automatizado para a construção de um perfil de consumidor, por exemplo, o cidadão deve também estar ciente dessa manipulação de dados por meio de máquina.

Criação da ANPD

Um dos destaques da lei é a criação de um órgão responsável por fiscalizar seu cumprimento.

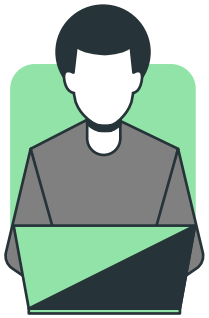
A **Autoridade Nacional de Proteção de Dados Pessoais (ANPD)**, órgão que ainda não foi instituído, será responsável por monitorar os processos relativos à LGPD, assim como ficará encarregado de tarefas específicas de orientação preventiva, repassando instruções sobre como aplicar a lei. Nesse sentido, cidadãos e organizações poderão colaborar conjuntamente.

Dentro dessa medida também está a criação dos chamados agentes de tratamento, classificados como controlador, operador e encarregado. Assim, para contextualizar melhor o papel de cada um dentro do processo de proteção de dados, podemos dizer que quatro personagens estarão envolvidos:

TITULAR
O proprietário dos dados - no caso, as pessoas físicas;

CONTROLADOR
Tomador dos dados - ou seja, as pessoas jurídicas (empresas);

OPERADOR
Empresa efetivamente responsável pela coleta de dados e sua segurança através de soluções inovadoras e automatizadas;



ENCARREGADO
Profissional que pode ou não ser exigido (dependendo do porte da empresa ou do volume de dados tratados) e responde pela proteção dos dados - ou seja, que fará ponte com a ANPD e os cidadãos quando necessário, podendo até ser responsabilizado junto à pessoa jurídica por mal uso ou vazamento de informações.

Reforço da gestão de segurança

A ANPD e os indivíduos afetados devem ser imediatamente avisados em caso de vazamento de dados. A lei é clara sobre os custos que falhas de segurança poderão acarretar. As multas podem chegar a até 2% do faturamento anual da organização no Brasil, com um limite de 50 milhões de reais por infração.

A ANPD avaliará os níveis de penalidade segundo a gravidade da falha em questão, enviando alertas e orientações antes de aplicar sanções às organizações. As penalidades se aplicam a todas as empresas envolvidas no tratamento de dados.

A comunicação em caso de falha também deverá ser feita em tempo razoável, contendo a descrição da natureza dos dados pessoais afetados e as informações sobre os titulares envolvidos.

Além disso, deverá conter também a indicação das medidas técnicas e de segurança utilizadas, os riscos relacionados ao incidente, eventuais motivos da demora (se for o caso) e ainda as medidas que foram ou que serão adotadas para reverter ou diminuir os efeitos do prejuízo.

Transferência internacional

Outro ponto importante da lei é em relação a como será a regulamentação do fluxo de dados para outros países, ação conhecida como transferência internacional de dados.

Esse fluxo internacional somente será permitido para países ou órgãos internacionais que proporcionem grau de proteção de dados pessoais compatível com a lei brasileira ou mediante oferecimento de garantias do regime de proteção de dados local.

O que muda para as empresas?

O que podemos perceber é que, com a Lei Geral de Proteção de Dados entrando em vigor no Brasil, **todas as empresas de pequeno, médio e grande porte terão que investir em cibersegurança**.

Será obrigatório implementar sistemas que sejam efetivos em prevenir, detectar e remediar violações de dados pessoais. Isso porque a lei indica que a adoção de políticas de boas práticas será considerada como critério atenuante das penas, que, como dissemos, podem ter valores muito altos.

Da mesma forma, **usuários que tiverem seus dados de rede usados de forma indevida, podem acionar a justiça, pois a ação será caracterizada como crime cibernético**.

Esse processo de adequação não é simples e, logicamente, não acontece de um dia para o outro. Portanto, é ideal é que as empresas comecem desde já a tomar ações que preparem melhor o terreno para quando a lei já estiver valendo. Algumas dessas medidas são:

Criação de um comitê de segurança interno

O primeiro passo para se adequar às normas da LGPD é formar um comitê de segurança dentro da empresa. **Essa equipe deverá fazer uma varredura por todos os processos internos e avaliar potenciais falhas**.

Será necessário reavaliar informações solicitadas ao público, considerando que quanto menos dados pessoais forem retidos pela organização, menor o risco.

Da mesma forma, o comitê deverá estabelecer procedimentos para inventário de dados pessoais, controle e armazenamento dessas informações, bem como indicar os responsáveis pelas atualizações das mesmas, uma vez que as punições legais podem ser bem severas.

Toda a governança de TI deverá ser reformulada.

Proteção de dados

As medidas preventivas de segurança deverão ser parte das operações internas da empresa. Elas deverão conter, por exemplo, planos de contingência, auditorias frequentes e testes de vulnerabilidade no sistema de segurança para evitar ataques virtuais.

A segurança da informação será uma obrigatoriedade e prioridade no novo modelo de gestão de TI regido pela Lei Geral de Proteção de Dados.

O compliance com a lei é baseado na garantia de que os controles certos de segurança estarão preparados para proteger as informações. A criptografia, nesse contexto, é apenas uma medida, mas não a única.

A equipe de TI deve ter consciência da importância de um monitoramento rígido e constante, que esteja acompanhando de ações rápidas para o caso de uma invasão de sistema e violação de dados.

A tecnologia, sem dúvidas, tem um papel mais do que importante para essa tarefa, mas não se engane pensando que ela poderá resolver tudo sozinha. Mais do que as melhores ferramentas, máquinas e softwares, é preciso ter uma combinação forte de técnicas e operações.

Padronização dos fluxos de trabalho

A padronização dos fluxos de trabalho deve ser uma das medidas estabelecidas na governança de TI adaptada à LGPD. Todos os membros da equipe devem saber o que fazer e como fazer, principalmente em uma situação de vulnerabilidade.

Educar os profissionais quanto à lei e quanto ao regulamento interno é uma forma de garantir o cumprimento dessa estratégia.

Controle de acesso

O controle de acesso visa criar um limite para os dados recolhidos pela empresa. Essa medida evita que as informações transitem entre muitas pessoas ou sistemas, ficando mais vulneráveis.

Restrinja o acesso apenas para quem realmente utilizará os dados para as necessidades consentidas pelo público. Quanto menos essas informações circularem, menores são as chances de caírem em mãos erradas.

Atualizações constantes

As equipes de TI deverão estar ainda mais comprometidas com as boas práticas de gestão e com as atualizações do mercado. **Certificações que garantam a qualidade e segurança serão exigência** para a conformidade da lei.

Uma dessas certificações é, por exemplo, a Privacy and Data Protection Essentials (PDPE). Parte do programa de certificações da EXIN, uma das referências no mercado de TI, essa certificação certamente será um grande diferencial para o currículo dos profissionais da área.

Ela é voltada especificamente para validar e comprovar os conhecimentos específicos da LGPD, sendo especialmente relevante para o profissional que ficará encarregado da gestão de dados dentro desse novo cenário.

Estabelecimento da transparência com o público

Lembre-se de que o consentimento é um aspecto essencial da LGPD. Por isso, **trabalhe na comunicação com o público**, mantendo-o, desde já, ciente das razões pelas quais seus dados são solicitados e que uso será feito deles, além de reforçar que a autorização pode ser revogada.

Contratação de uma assessoria jurídica

Outro ponto que sem dúvidas ajuda muito no processo de adaptação à lei é contar com a ajuda de uma assessoria jurídica. **Trabalhando de forma conjunta, a parte jurídica e a de TI poderão estabelecer normas de governança** que atendam corretamente à legislação.

Contratação de bons profissionais de TI

Como está sua equipe de TI hoje? Ela conta com profissionais experientes e devidamente qualificados? Com a entrada da LGPD em vigor, o departamento de TI passará a ocupar um nível de importância ainda mais alto dentro das empresas.

De fato, já há algum tempo ele não é apenas um setor operacional, mas que elabora estratégias para produzir resultados ainda melhores para o negócio. A partir deste ano, porém, **a TI será um dos setores mais importantes do negócio, garantindo a segurança dos dados e, consequentemente, a conformidade com a lei**.

Portanto, gestores não devem hesitar em formar uma equipe com excelentes profissionais. Seja uma equipe interna ou terceirizada.

5

Como a LGPD impacta o setor de TI?

Como você já deve ter notado aqui, o impacto da LGPD para o setor de TI e seus profissionais é direto. O cuidado com os dados de clientes, bem como com todas as informações da empresa, precisa ser ainda maior agora.

Muitas das empresas precisarão **reformular totalmente suas medidas de segurança da informação**, ou seja, é uma mudança estrutural.

A preocupação com a proteção de dados agora também se estende à transparência com o cliente, que precisa estar ciente de como suas informações estão sendo utilizadas.

Consequentemente, a LGPD traz diversos desafios para a TI, tanto no sentido operacional, quanto na forma de encarar a proteção de dados. Para gestores e colaboradores, surgem demandas como:

- Configurar a privacidade como padrão em qualquer tecnologia utilizada pela empresa;
- Implementar uma visão geral dos dados capturados e tornar os canais de captura mais transparentes;
- Certificar-se de escolher e gerir tecnologias confiáveis para o armazenamento dos dados, evitando seu vazamento ou interceptação;
- Gerir os dados coletados e os acessos a eles;
- Interpretar as diretrizes da lei e trazê-las para a realidade do negócio;
- Orientar uma mudança na cultura interna;
- Estabelecer novos processos e definir os responsáveis por cada um deles;
- Conscientizar os profissionais do setor e supervisionar o cumprimento de suas responsabilidades.

6

Quais princípios colocar em prática nos projetos de TI?

Dentro das áreas de TI e compliance das empresas, o conceito de privacidade de dados tem grande importância. Dentro desse contexto, existe uma metodologia conhecida como **Privacy by Design**, que nada mais é do que a segurança da informação pensada desde o desenvolvimento de sistemas.

Considerando a LGPD e as consequências negativas que o descuido para com os dados pessoais de terceiros pode trazer para as empresas, os princípios dessa metodologia se mostram como boas práticas. São eles:

1. Ser proativo e não reativo

O primeiro princípio é o de prevenir situações de invasão de privacidade antes que elas ocorram, ou seja, **prevenir e não remediar**. Isso vale para todas as atividades da empresa, desde a aplicação de novas tecnologias até as práticas organizacionais.

Para que dê certo, é preciso ter um comprometimento por parte dos níveis mais altos da empresa, assim como estabelecer métodos para o reconhecimento de falhas, criando uma cultura dentro da equipe.

2. Privacidade como padrão

Aqui estamos falando das configurações referentes à privacidade. Elas devem estar **presentes desde a concepção até o lançamento do projeto**, de modo "padrão", sem que o usuário precise fazer nada para que sua privacidade permaneça intacta.

Trata-se também de assegurar que todo serviço, produto ou sistema desenvolvido pela empresa seja ajustado desde o início para preservar a privacidade do usuário, mesmo que de forma mais restritiva. Cabe ao usuário aceitar a configuração padrão ou desativar uma ou mais configurações adicionais.

3. Privacidade incorporada ao design

Aqui a privacidade é encarada como o **core do negócio**, sendo uma parte indissociável do projeto, independentemente da etapa em que ele se encontra. Tecnologias, operações e arquiteturas, tudo deve ser pensado de maneira integrada e criativa, reinventando os moldes sempre que necessário.

4. Funcionalidade total

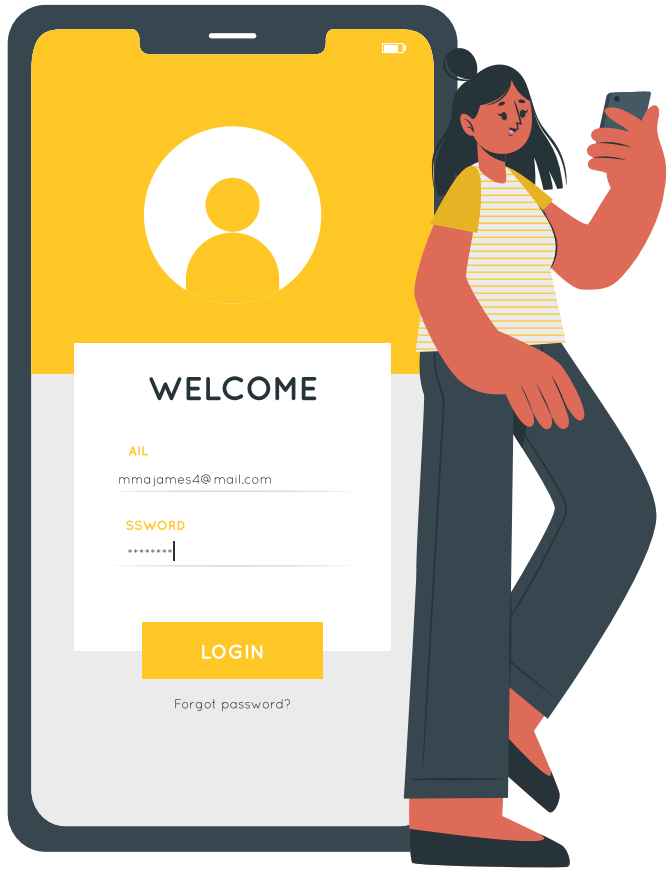
O princípio de funcionalidade total coloca a privacidade dos dados em consonância com os interesses legítimos daqueles que fazem uso das informações.

Ou seja, mantém o produto ou serviço **utilizável independentemente das configurações de privacidade do usuário**.

É necessário prezar pela segurança e pela privacidade sem afetar a performance.

5. Segurança de ponta a ponta

Pensando no ciclo de vida dos dados, a **segurança deve estar presente do início ao fim**. Isto é, a proteção da privacidade deve existir desde a coleta dos dados até a sua eventual destruição.



6. Visibilidade e transparência

A visibilidade e transparência são essenciais para se estabelecer uma relação de confiança com os usuários. Nessa perspectiva, a empresa precisa **comprovar que coloca sua política de privacidade em prática**.

Essa verificação não se restringe apenas ao titular dos dados, mas também a todo o processo de compliance e auditoria, responsável por monitorar, avaliar e verificar se as políticas estão realmente sendo cumpridas.

7. Respeito pela privacidade do usuário

As empresas devem **priorizar o interesse do indivíduo**. Ou seja, é preciso garantir que os dados sejam tratados com confidencialidade e integridade.

Ele deve poder compreender com clareza as configurações referentes à sua privacidade, recebendo avisos apropriados e tendo acesso a opções amigáveis, visando o seu empoderamento.

7

Como adequar minha empresa?

Sem dúvidas, a adequação à LGPD é um processo complexo, que exige um esforço conjunto de toda a empresa. São diversas etapas que exigem planejamento, disciplina e muito conhecimento sobre os pontos-chave da lei.

Pensando nisso, elaboramos um checklist didático do passo a passo que você precisa seguir na sua empresa para ficar em conformidade com tudo que foi dito até aqui. Veja:

- [ ] **1. Analise os riscos:** conheça os dados pessoais que a empresa possui e identifique os potenciais riscos que eles representam. Identifique as vulnerabilidades de alto e baixo risco, priorizando aquelas que podem causar danos maiores.

- [ ] **2. Defina responsáveis:** o processo de implementação da LGPD precisa muito contar com um comitê de segurança interno, formado por pessoas que ficarão à frente das alterações, supervisionando tudo e garantindo que nenhuma brecha passe despercebida.

- [ ] **3. Adapte documentos:** todos os contratos e documentos da empresa devem atender às diretrizes legais, sejam eles impressos ou digitais. Acione o departamento jurídico para atualizar toda essa documentação.

- [ ] **4. Crie uma política de proteção de dados:** a adequação à LGPD é uma mudança na cultura da empresa. Estabeleça uma política clara e forte, que será repassada a todas as equipes. Todos os profissionais precisam estar conscientes de seus deveres dentro de todo esse processo.

- [ ] **5. Exija a proteção de dados de fornecedores e parceiros:** é preciso que todos os envolvidos com a empresa também estejam de acordo com a lei. Certifique-se de verificar se as diretrizes também estão sendo cumpridas pelas empresas com quem você se relaciona.

- [ ] **6. Adote princípios de proteção de dados em seus projetos:** após fazer da LGPD uma realidade da empresa, é o momento de pensar no que está por vir. Seja na concepção de novas ideias, seja no desenvolvimento de produtos e serviços, é essencial seguir os princípios do Privacy by Design.

- [ ] **7. Contrate profissionais especializados:** a especialização será fundamental para que as empresas consigam elaborar estratégias que se adequem não só às exigências da lei, mas também à realidade do negócio.

Conclusão

Agora você já conhece os principais pontos da nova Lei de Proteção de Dados Pessoais e também sabe o que muda nas empresas por conta da LGPD.

A necessidade de se **investir em segurança da informação** é cada vez maior e as empresas não podem mais negligenciar esse compromisso. Desse momento em diante, além de perder mercado, elas estão sujeitas a rígidas punições.

Estamos vivendo um momento de disrupção, em que a privacidade do usuário conquistou o patamar de prioridade. Isso exige uma mudança que deverá ser **incorporada a todos os projetos** que as empresas desenvolverem daqui para frente.

Por fim, a figura dos **profissionais e gestores de TI** assume uma importância ainda mais central dentro das empresas. Além de buscarem se atualizar o quanto antes sobre o que diz a lei, é preciso que estejam cientes dos novos desafios nas rotinas de trabalho e de que a capacitação e o preparo para atuar nesse cenário são fundamentais.

Sobre a NetSupport

Somos uma plataforma digital de suporte técnico de TIC, operada pela **maior comunidade de tecnologia do Brasil**.

Com técnicos e profissionais especializados, presentes em mais de **3.200 cidades em todo o Brasil**, temos o preparo, a expertise e a disponibilidade de que seu negócio precisa para alcançar a alta performance dentro das diretrizes da LGPD.

Com valores flexíveis e um trabalho rápido e eficiente, levamos inovação para sua empresa através de projetos de suporte em TI, Telecom e IoT. Tudo isso sem burocracia, que fica por nossa conta.

Se a sua empresa quer contar com a melhor equipe e um suporte de excelência nesse momento de adequação, conte conosco!

CONHEÇA A NETSUPPORT

NetSupport®