CYBER&CLOUD
experience

Proteção de Dados Pessoais: Como Proteger Nossos Dados Pessoais em Um Mundo Cada Vez Mais Conectado

Bem-vindo(a)

A nova era digital trouxe uma infinidade de possibilidades para facilitar nosso dia a dia pessoal e profissional. É muito difícil encontrar, hoje, quem não está conectado a uma rede social, por exemplo. Não podemos negar: há muita coisa boa no ambiente digital, mas, em contrapartida, uma infinidade de ameaças cibernéticas que usuários de todo o mundo estão propensos a serem vítimas.

Proteger nossos dados pessoais tornou-se uma tarefa difícil, pois compartilhamos informações pessoais diariamente, seja fazendo uma compra online ou aceitando os termos de uso de um aplicativo.

E se você quer saber como manter a segurança dos seus dados, esse material é para você!

Aqui você vai entender mais sobre privacidade e proteção de dados e como se prevenir de ciberataques. Vamos trazer 15 dicas valiosas para aumentar a segurança das suas informações.

Aqui você aprende com quem faz.

Vem com a gente mergulhar nessa temática!

Sumário

Introdução

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020 e, desde então, a segurança dos dados pessoais tornou-se um assunto sério e muito falado por todo o país.

As empresas precisaram correr contra o tempo para se adequar às novas regras e instalar mecanismos de proteção de informações de clientes, fornecedores e colaboradores.

Muito além da sua aplicação no ambiente corporativo, qualquer usuário ativo da internet também deve tomar cuidados extras com os seus dados, sejam eles pessoais, financeiros, de saúde, entre outros. Além disso, conhecer os direitos enquanto detentor dessas informações, que foram, introduzidos pela LGPD também é essencial.

Neste material, você vai ficar por dentro de tudo isso e vai aprender a manter seus dados seguros em um mundo cada vez mais conectado.

Boa leitura!

O que são dados pessoais e qual a sua importância no mundo digital?

Dados pessoais são todas as informações que podem identificar ou tornar identificável uma pessoa física, como nome, CPF, endereço, e-mail, telefone, foto, etc.

Esses são coletados, armazenados e tratados por diversas entidades públicas e privadas, com diferentes finalidades e interesses.

No mundo digital, os dados pessoais ganharam uma importância ainda maior, pois são usados para diversas atividades, como:

- Acesso a serviços online
- Personalização de conteúdo
- Publicidade direcionada
- Análise de comportamento
- Reconhecimento facial

Esses usos podem trazer benefícios para os usuários, mas também podem representar riscos à sua privacidade e aos seus direitos fundamentais.

Por isso, é importante que os usuários estejam cientes dos seus direitos e deveres em relação aos seus dados pessoais, bem como das boas práticas para protegê-los no ambiente digital.

Pensando em criar regras para definir a forma como são tratados e protegidos, o Governo brasileiro criou a Lei Geral de Proteção de Dados (LGPD), dando um importante passo para estabelecer os princípios, direitos e deveres para o tratamento de dados pessoais no país, bem como as sanções para os casos de violação.

Com isso, ter suas informações preservadas tornou-se um direito constitucional dos brasileiros, incorporado como cláusula pétrea à nossa Constituição.

A seguir, vamos conhecer melhor a legislação brasileira, de uma forma simples.

A Lei Geral de Proteção de Dados (LGPD)

A LGPD, como é popularmente conhecida a lei 13.709/2018, foi criada em 2018 e entrou em vigor no dia 18 de setembro de 2020.

Ela é a principal legislação do Brasil no que se refere ao tratamento de informações pessoais, nos meios físicos e digitais, por parte de pessoa física ou pessoa jurídica de direito público ou privado.

A lei proíbe o uso indevido dos dados pessoais de pessoas físicas e determina que empresas, públicas e privadas, cumpram uma série de medidas em relação à coleta, armazenamento, compartilhamento e tratamento para garantir a privacidade e a liberdade dos clientes e usuários do seu negócio.

Assim, a LGPD visa garantir que os dados pessoais sejam tratados de forma lícita, transparente e segura, respeitando a autodeterminação informativa dos usuários titulares.

Fonte
serpro.gov.br/lgpd/menu/arquivos/infografico-lgpd-em-um-giro

Apesar de ser uma grande evolução do ponto de vista jurídico e ter sido bem avaliada por especialistas, a norma brasileira não é tão rígida como outras leis mundo afora.

A LGPD foi inspirada na GDPR (General Data Protection Regulation), a legislação europeia sobre o tema. O Regulamento Geral sobre a Proteção de Dados da União Europeia foi aprovado em 2016 e é tido como a referência mundial quando o assunto é proteger as informações dos cidadãos.

Quais os tipos de dados considerados na LGPD?

Segundo a lei brasileira, existem três tipos de dados:

Dado pessoal:

Qualquer informação relacionada à pessoa física, seja ela identificada ou identificável;

Dado pessoal sensível:

Dados vinculados a pessoa que se referem a questões pessoais, como etnia ou raça, religião, opinião política, vida sexual, saúde, etc;

Dado anonimizado:

Dados onde o titular não pode ser identificado no momento do tratamento dos dados, por razões técnicas. Por exemplo, crianças ou adolescentes por serem menores de idade.

Com essa definição, a LGPD proíbe o uso ou o tratamento indiscriminado dessas informações para práticas ilícitas ou abusivas.

Em atenção ao princípio da transparência, a lei estabelece o direito do titular à informação, isto é, o direito de ser informado sobre como o tratamento de dados ocorrerá.

Trouxemos exemplos para clarificar algumas situações em que é vedado o tratamento ou compartilhamento de dados pessoais:

- Mediante vício de consentimento;
- Com objetivo de obter vantagem econômica;
- Entre controladores de dados pessoais sensíveis ligados à saúde com objetivo de obter vantagem econômica;
- Entre operadores de planos de saúde para a prática de seleção de riscos, de modo a dificultar a contratação de qualquer modalidade do plano;
- Transferência de dados dos órgãos públicos para instituições privadas, com exceção de casos que exigem a transferência para fins específicos.

Para além desses pontos, a lei tornou estritamente proibido o compartilhamento sem o consentimento do titular visando lucro ou vantagem econômica. Ou seja, as empresas não podem vender os dados de seus clientes.

Quais são os seus direitos?

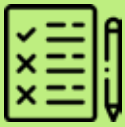
Esse é um ponto bastante importante. Você deve conhecer seus direitos para poder exercê-los quando julgar necessário.

Confira abaixo os direitos dos titulares dos dados, conforme o artigo 18 da LGPD:

Confirmação de que existe um ou mais tratamento de dados sendo realizado

Acesso aos dados pessoais conservados que lhe digam respeito

Correção de dados pessoais incompletos, inexados ou desatualizados



Eliminação de dados pessoais desnecessários, excessivos ou caso o seu tratamento seja ilícito

Portabilidade de dados a outro fornecedor de serviço ou produto, obervados os segredos comercial e industrial

Eliminação de dados (exceto quando o tratamento é legal, mesmo que sem o consetimento do titular)

Informação sobre compartilhamento de seusdados com entes públicos e privados, caso isso exista

Informação sobre o não consentimento, ou seja, sobre a opção de não autorizar o tratamento e as consequências da negativa

Revogação do consentimento, nos termons da lei

Reclamação contra o controlador dos dados junto à autoridade nacional

Oposição, caso discorde de um tratamento feito semseu consentimento e o considere irregular

Com o que você deve ficar atento?

Com a vida moderna e conectada que nos habituamos, informar nossos dados pessoais em plataformas online tornou-se algo corriqueiro. Assim, essas informações circulam nas mãos de diferentes pessoas e com as mais variadas finalidades. Por isso, é importante entendermos as ameaças e possíveis violações que estamos sujeitos.

Quando falamos em segurança da informação, temos que pensar em três cenários.

1. Tratamento de dados pelas empresas

Aqui a atenção deve se voltar à idoneidade das empresas e a forma como cumprem a legislação e protegem seus dados pessoais. A Governança de Dados tornou-se uma área muito importante para as companhias, atendendo às regras de Compliance e da LGPD.

Vamos ver dois exemplos:

1. Se você se cadastrou em uma newsletter de um site de notícias, o seu e-mail só pode ser usado com essa finalidade, que foi para a qual você deu seu consentimento. A empresa não pode usar seu e-mail para outros fins ou mesmo vender o seu endereço eletrônico para uma empresa de publicidade, por exemplo. Por isso, você deve sempre ficar atento ao realizar cadastros online e ler as Políticas de Privacidade para saber como a empresa vai usar e tratar suas informações.

2. Quando uma farmácia pede o seu CPF para atribuir descontos em medicamentos, em tese você deu seu consentimento para esse uso, assim a empresa não pode usá-los para outros fins, como, por exemplo, realizar uma análise da sua vida financeira ou compartilhar com outras empresas. A autoridade de proteção de dados vai fiscalizar as farmácias por uso excessivo de CPF e outras informações de clientes. Assim, caso queiram dar outro uso ao dado, com a LGPD, a farmácia precisa pedir o seu consentimento. Com base na lei, você pode autorizar a nova finalidade ou revogar o acesso ao seu dado pessoal.

Esses são dois pontos muito importantes da LGPD: o titular dos dados deve dar seu consentimento para uso específico e a sua finalidade deve ser respeitada.

2. Vazamento de dados

Com a sofisticação dos crimes cibernéticos, uma das modalidades que mais cresce é o ataque para acessar bancos de dados com informações de usuários. E, nesse cenário, nosso país aparece com destaque negativo. Um levantamento recente apontou que o Brasil é o país mais propenso a sofrer vazamentos de dados em todo o mundo.

Essa prática ilegal tornou-se um mercado lucrativo, já que os criminosos vendem as informações roubadas. Recentemente, houveram diversos casos no país. O mais chamativo com certeza foi o vazamento de CPFs, fotos e até salários de 223 milhões de brasileiros (incluindo até pessoas falecidas). Só nesse caso, estima-se que os dados vazados poderiam render 80 milhões de reais ao criminoso que colocou o banco de dados à venda na deep web.

A maior preocupação com esses vazamentos é que, com a posse de dados pessoais, criminosos podem contratar empréstimos e cometer outras fraudes em nome de terceiros.

A atenção se volta para a segurança das infraestruturas das empresas, que devem investir cada vez mais em Políticas de Segurança da Informação. O ideal é ser criterioso com as empresas que você fornece seus dados pessoais – o que mesmo assim torna a tarefa difícil, já que as maiores empresas do mundo já foram vítimas de vazamentos.

Como saber se seus dados foram expostos? Conheça aqui algumas maneiras de monitorar.

3. Roubo de dados pessoais

Com o crescimento de fraudes e golpes digitais durante a pandemia, o roubo de dados pessoais tornou-se uma preocupação muito forte em território nacional. Uma pesquisa da Federação Brasileira de Bancos (Febraban) mostra que 86% dos brasileiros têm medo de ser vítimas de violação de dados pessoais.

E a preocupação não é pra menos. Os golpes bancários dispararam no Brasil e podem ter gerado prejuízos de 2,5 bilhões de reais em 2022. A maior parte (1,8 bilhão) está relacionada com o Pix.

Aqui a orientação é ficar atento com sites fraudulentos, e-mails suspeitos ou ligações que pedem confirmações de dados. E lembre-se: nunca forneça nada de primeira.

Como não ser vítima de golpes? Conheça os principais tipos praticados no Brasil e como se prevenir.

15 dicas valiosas de como manter seus dados seguros

Agora que você entendeu como funciona a LGPD e como seus dados pessoais são importantes – para você, para as empresas e também para os criminosos – vamos ver algumas dicas para torná-los mais seguros no universo digital.

1. Leia as Políticas de Privacidades dos sites e aplicativos que usa:

Veja quais dados são coletados e qual a finalidade de uso. Se perceber algo muito fora do padrão, desconfie e não aceite os termos. Com a LGPD, uma das obrigações das empresas é ter tudo de forma clara e explícita para o usuário dar o seu consentimento, também de forma clara.

2. Verifique as permissões de acesso dos aplicativos instalados no seu celular:

Veja se as permissões fazem sentido para o uso definido pelo app. Por exemplo, um aplicativo de lanterna não precisaria acessar a sua galeria de arquivos para funcionar. Se pede esse acesso, é motivo para desconfiar. O app pode se passar por um outro de uso legítimo para ter acesso a dados sensíveis. Esse tipo de golpe tem aumentado muito. Em 2022, 2,3 milhões de falsos apps foram detectados no Brasil.

3. Use senhas fortes e únicas:

Dê preferência para combinações longas, com letras maiúsculas, minúsculas e números. Para aumentar ainda mais a segurança, use caracteres especiais. Tente não repetir as mesmas senhas em e-mails, redes sociais, logins de sites e outros. Crie o hábito de atualizar suas senhas periodicamente.

4. Ative autenticação de dois fatores (2fa):

Utilize um aplicativo de autenticação, como o Google Authenticator. Evite usar a verificação por SMS, pois esse método não é seguro.

5. Não compartilhe seus dados abertamente em redes sociais:

Tenha atenção inclusive com fotografias que mostrem endereços ou outras informações sensíveis sobre você e seus familiares.

6. Cuidado com redes wi-fi públicas:

Evite digitar senhas dos serviços que usa enquanto estiver conectado em redes públicas. Também não acesse o internet banking.

7. Não use VPNs gratuitos:

Principalmente se for digitar dados sensíveis, como números de cartão de crédito.

8. Não deixe informações importantes na nuvem:

Nada de salvar uma foto do seu cartão de crédito em serviços como o Google Drive ou Dropbox. Se precisar realmente arquivar esse tipo de informação, faça a criptografia dos dados.

9. Ao navegar na internet, fique atento aos protocolos de segurança, como https:

Não coloque suas informações, como dados bancários, em sites que não utilizem o protocolo https. O uso não garante 100% de segurança, mas se o site não utiliza essa camada extra de segurança pode estar mais vulnerável a deixar seus dados expostos.

10. Não clique em links que não tem total confiança:

Tenha atenção redobrada com links recebidos por e-mail, SMS ou WhatsApp sem ter solicitado, as principais formas de espalhar phishing. Passe o mouse sobre o hiperlink (sem clicar) e veja no rodapé o site para o qual será redirecionado. Tenha também atenção à grafia dos nomes dos sites. Os criminosos usam termos muito parecidos que somente um olhar atento consegue perceber.

11. Não deixe cartões de crédito salvos em sites de varejo:

Seus dados ficarão armazenados e poderão ser expostos em um possível vazamento. Cadastre o cartão somente para a compra que está fazendo. Para uma camada extra de segurança, utilize cartões virtuais de compra única.

12. Em ligações, nunca confirme seus dados de primeira:

Somente forneça após o atendente demonstrar que sabe com quem está falando. Se tiver dúvidas sobre a veracidade da ligação, desligue e retorne a ligação para a empresa (entre no site e procure o número oficial).

13. Tome cuidado com quiz e correntes nas redes sociais:

Esses aplicativos podem receber mais dados do que você pensa e o uso não é explícito. Testes e correntes no Facebook podem criar riscos.

14. Atenção com downloads de sites duvidosos e pastas zipadas:

Esses arquivos podem esconder software malicioso com mais facilidade. Só instale se confiar na fonte.

15. Use o bom senso:

Promessas mirabolantes, itens grátis ou prêmios incríveis são iscas fáceis para atrair e fazer novas vítimas de golpes. Por isso, use sempre seu bom senso e desconfie de muitas facilidades, principalmente se o emissor não for uma empresa de renome no mercado.

Com essas dicas, as chances de ter seus dados violados diminuem consideravelmente. Mas, se mesmo assim você for vítima de uma infração da LGPD, você pode procurar ajuda dos órgãos governamentais.

Para garantir a aplicação da lei, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), que tem um canal de denúncias e monitora as boas práticas do setor.

A agência já está em funcionamento e recentemente aplicou a primeira multa por descumprimento à LGPD no Brasil. Nesse caso, a penalização foi baixa devido ao faturamento da empresa, mas as sanções podem chegar a 50 milhões de reais, de acordo com a lei.

Com multas tão altas, as empresas estão investindo cada vez mais em criar e manter infraestruturas mais protegidas de ciberataques, evitando vazamentos de dados e infrações à LGPD.

Por isso (e outros motivos), a carreira em Segurança Cibernética está em alta. Se você tem interesse nessa área, essa é uma boa hora para aproveitar as oportunidades de mercado e dar uma turbinada na sua carreira.

Você está no lugar certo!

A XP Educação foi criada a partir da integração de duas escolas: o **IGTI,** uma empresa premiada e referência no ensino em tecnologia, e a **Xpeed**. a escola de finanças da XP. Com essa integração, **unimos o ensino ao mercado**, com o objetivo de **transformar o modelo tradicional de ensino.**

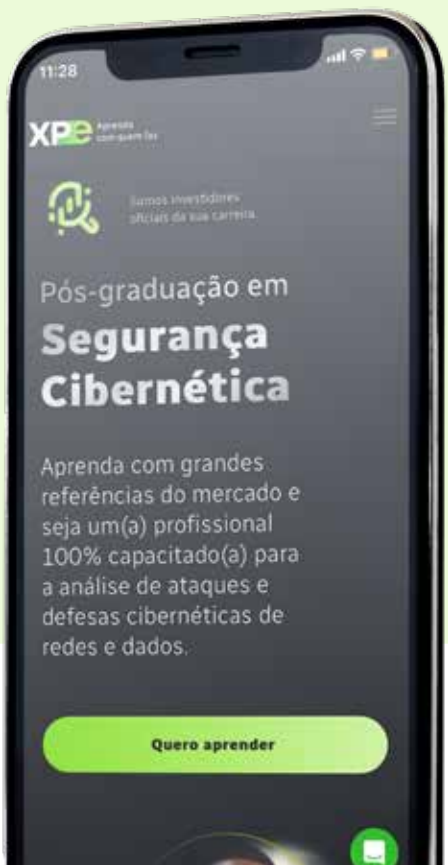
Temos em nosso DNA a inovação e ousadia de quem revolucionou o mercado financeiro com a XP, agora nossa missão é levar a expertise das empresas para as salas de aula. Além disso, nos preocupamos em oferecer uma formação profissional alinhada às necessidades da nova economia digital.

Se você quer ter o seu lugar de destaque nessa profissão altamente valorizada, conheça a nossa pós-graduação em Segurança Cibernética.

Você terá uma formação completa com as melhores práticas do mercado de Cibersegurança e vai ajudar empresas de todos os tamanhos a manter os dados dos clientes seguros, cumprindo com a LGPD.

Torne-se um especialista disputado pelas empresas ao dominar as ferramentas e práticas mais desejadas pelo mercado para trabalhar com cibersegurança e proteção de dados.

Tudo isso em um modelo de ensino inovador e disruptivo em que você pode estudar de qualquer lugar do mundo, com aulas gravadas e ao vivo com professores que são referência no mercado. E agora com novos benefícios para fazer a sua pós:



Carrer Advisor: você terá um aconselhamento de carreira personalizado, com direcionamentos de especialistas para ajudar no desenvolvimento das soft e hard skills que o mercado exige.

Hub de Conexões: vai ajudar você a interagir com os alunos para criar oportunidades de carreira e de negócios – muitos projetos de sucesso surgiram em parcerias de colegas de sala de aula.

MasterClasses: aulas exclusivas com especialistas de referência para você se inspirar e aprender com quem faz o mercado acontecer e tem muita experiência para compartilhar.

Afinal, aqui você aprende com quem faz!

Esperamos que as dicas deste material te ajudem a manter seus dados em segurança e que você tenha total controle sobre as suas informações digitais, agora que você conhece os seus direitos introduzidos pela Lei.

Lembre-se que você pode sempre contar com a gente na sua busca contínua por qualificação.


CYBER&CLOUD
experience
xpeducacao.com.br
blog