TRANSFEERA + VANZIN & PENTEADO

E-book

Guia completo sobre LGPD e fintechs

aspectos jurídicos e práticos da legislação

A Lei Geral de Proteção de Dados, com previsão de vigência a partir de agosto de 2020, vai mudar a forma como as empresas coletam, tratam, armazenam e utilizam os dados de seus clientes. A proposta é proporcionar maior autonomia para os usuários e aumentar a responsabilidade das empresas com relação aos dados que armazenam.

Há anos, uma legislação específica sobre o tema se fazia necessária para que as empresas passassem a ser responsabilizadas e evitar que informações pessoais fossem expostas. Afinal, nos últimos anos, de acordo com o Avast, diversas empresas sofreram com vulnerabilidades que causaram o vazamento de dados de seus clientes e usuários.

Quando falamos em fintechs, o impacto da nova lei será grande. Isso porque os dados dos clientes são fundamentais para a operação dos negócios. Quando a legislação entrar em vigor, os dados das pessoas deverão ser utilizados para finalidades específicas e as empresas devem deixar claro para onde vão os dados coletados e como eles serão utilizados.

Neste guia completo, resultado de uma parceria entre a Transfeera e a VP Advocacia, reunimos as principais informações que você precisa ter para se adequar à nova lei e ficar por dentro das implicações jurídicas e tecnológicas para o seu negócio.

O que você vai ver neste guia:

Boa leitura!

01

O que é LGPD?

Contextualização do cenário que motivou a LGPD

Com o avanço e o acesso a novas tecnologias por um maior número de pessoas, um grande volume de dados passou a circular na rede, os quais são fornecidos por usuários para acesso a serviços e produtos.

Consequentemente, estão à disposição na rede e, sem controle, podem ser utilizados de forma indiscriminada.

Diante desse novo cenário, passou-se a discutir a necessidade de criação de uma legislação específica, dada essa sociedade marcada por relações cada vez mais complexas e abertas, situação que gera novos desafios jurídicos relacionados à proteção de dados.

O grande marco de uma regulação específica ocorreu na União Europeia em 2018, quando foi aprovado o Regulamento Geral sobre Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR).

A GDPR disciplina a forma como se dará o tratamento de dados pessoais, por pessoas, empresas ou organizações que se encontram no território da União Europeia, gerando efeitos extraterritoriais também a todos aqueles que possuem relação com entes integrantes da União Europeia.

Assim, no Brasil, por influência da GDPR, foi aprovada a Lei nº. 13.709/2018, também chamada de Lei Geral de Proteção de Dados (LGPD), com previsão de entrar em vigor em agosto de 2020.

O que é e qual o objetivo da legislação

A LGPD tem como objetivo central a proteção de dados, assegurando também garantia aos direitos fundamentais de liberdade e privacidade. Sendo assim, conforme regulamenta o seu artigo 1º, a Lei dispõe sobre o tratamento de dados pessoais, inclusive aqueles fornecidos em meios digitais.

Aplicação da legislação (a que/a quem)

A aplicação da LGPD abrange a proteção de dados pessoais de pessoas físicas ou jurídicas, sejam elas de direito privado ou público.

Deve atentar-se às regulamentações da LGPD toda pessoa física ou jurídica, de direito privado ou público, que desenvolva operação de tratamento em território nacional, ou que inclua indivíduos ou dados coletados também em território brasileiro.

A lei não se aplica a dados pessoais que sejam coletados por pessoa física para fins particulares e não econômicos, ou que tenham a finalidade vinculada a propósito jornalístico, artístico, acadêmico, de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais.

02

Quais dados são protegidos?

A LGPD protege o tratamento de dados pessoais, mas também menciona os dados sensíveis e os dados anonimizados.
Compreenda a seguir as diferenças entre essas três classificações:

Dados pessoais

Dados pessoais, de acordo com o artigo 5º, inciso I da LGPD, são aquelas informações relacionadas à pessoa física natural e que podem levar à sua identificação. Compreendem, portanto, nome, RG, CPF, data e local de nascimento, cookies, endereço de IP, dentre outros.

Dados sensíveis

Em seu inciso II, o artigo 5º da LGPD dispõe que dados sensíveis são aqueles de 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 física.

Dados anonimizados

O inciso III do artigo 5º da LGPD aborda os dados anonimizados que são compreendidos como aqueles que são vinculados a titular que não pode ser identificado, considerando o modo de sua utilização e os meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

03

Destaques no tratamento de dados

O tratamento de dados é iniciado com o consentimento do titular. Somente após o consentimento, é realizada a coleta de dados, que pode ocorrer por meio digital ou manual.

Assim, na sequência, os dados são convertidos para um formato mais legível, como planilhas, gráficos e documentos para, então, adquirir forma dentro do contexto necessário para serem interpretados por computadores utilizados pelos interessados no tratamento.

Trata-se de um processo complexo e que abrange uma ampla gama de elementos, incluindo a observância de princípios previstos na LGPD (art. 6º), os players envolvidos, as hipóteses em que o tratamento pode ser realizado, as etapas que devem ser observadas e as responsabilidades inerentes à atividade de tratamento.

Players do tratamento de dados

A LGPD indica quem são players do tratamento de dados:

01.

Titular dos dados

É qualquer pessoa física **cujos dados pessoais são coletados, mantidos ou processados**. Tem o poder de conceder e revogar o consentimento do uso dos seus dados, para as finalidades que lhe forem convenientes.

Em última análise, são aqueles para quem a LGPD foi escrita para proteger.

02.

Controlador

É a pessoa física ou jurídica que toma decisões sobre as atividades de processamento de dados, exerce o controle geral dos dados pessoais, determina a finalidade (porquê) e os meios (como) pelos quais o processamento de dados pessoais será realizado e, em última análise, **são os responsáveis pelo tratamento**.

O controlador é o responsável por obter e comprovar o consentimento do titular dos dados.

03.
Operador

É a pessoa física ou jurídica **que age em nome do controlador e sob sua autoridade**, devendo processar apenas dados pessoais, de acordo com as instruções do controlador (art. 39 da LGPD).

Desse modo, se, eventualmente, o operador agir sem as instruções do controlador, de forma a determinar o objetivo e os meios de processamento, inclusive para cumprir uma obrigação estatutária, nessa situação, ele será um controlador em relação ao processamento e terá a responsabilidade correlata a esse agente.

04.
Encarregado

Há ainda a figura do encarregado, que, embora não seja um agente para fins de tratamento de dados, desempenha papel relevante no processo de tratamento de dados.

Ou seja, é a pessoa física ou jurídica indicada pelo controlador e operador, divulgada publicamente – costumeiramente no website do controlador, na Política de Privacidade – para **atuar como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)**.

O encarregado deve ser especialista em proteção de dados e reportar ao mais alto nível de gerenciamento.

A fiscalização de todo o processo envolvendo o tratamento de dados ficará ao encargo da Autoridade Nacional de Proteção de Dados (ANPD), devendo as empresas participantes dessa operação observarem todas as especificações trazidas pela LGPD.

É possível que, na prática, surjam dúvidas acerca da figura assumida pela empresa no processo de tratamento de dados.

Dessa forma, importante é que se avalie as atividades efetivamente desenvolvidas, o que definirá a posição de controladora ou operadora, gerando efeitos práticos bem diferentes para a empresa, especialmente em relação às obrigações, conforme demonstrado.

Etapas do tratamento de dados

O processo de tratamento de dados deve seguir regulamentação específica e as etapas dispostas na LGPD, que são:

Coleta dos dados mediante consentimento

O primeiro passo é obter do titular o consentimento para coletar e utilizar os dados. Nesta primeira etapa, a empresa deverá informar ao titular de dados, no momento da coleta:

- Quais dados serão coletados, listando-os um a um;
- A finalidade para a qual os dados serão utilizados;
- Se haverá compartilhamento dos dados com terceiros;
- Por quanto tempo estes dados serão armazenados.

Também será exigida a manifestação expressa do titular dos dados, ou seja, não há margem para obter consentimento de forma tácita.

O usuário deve ter, de fato, o poder de decisão, bem como exercê-lo formalmente via assinatura de contrato ou aceite de termo de uso.

Tratamento e utilização

Após o consentimento do titular e a coleta dos dados, a informação será classificada ou preparada para o efetivo tratamento. Essa atividade poderá ser desempenhada pela própria empresa ou por meio de terceiros e softwares.

Os dados são padronizados e categorizados para posterior uso na prestação de serviços propriamente dita.

Compartilhamento

O compartilhamento pode ocorrer desde o início do processo de tratamento de dados, devendo a empresa observar o modo adequado e compatível com o que dispõe a LGPD.

Para compartilhar dados, a empresa deverá obter consentimento específico do titular para este fim, fazendo valer o princípio da transparência com o usuário, de modo que informa sobre o compartilhamento com terceiros, dispondo sobre a finalidade deste procedimento.

Término do tratamento de dados

Ao final do tratamento de dados, a empresa deverá eliminar a base de dados e de armazenamento. As hipóteses de término da operação se constituem quando:

- A finalidade do tratamento tiver sido alcançada e, portanto, os dados deixam de ser necessários ou pertinentes;

- O período estipulado para o tratamento dos dados se encerra. Normalmente, este período consta no contrato ou termos de uso;

- O titular dos dados, ou usuário dos serviços prestados pela fintech, deseja revogar o consentimento por vontade própria;

- Houver determinações de órgãos reguladores, em decorrência de violações à Legislação.

Responsabilidades por descumprimento

Diante de todo o processo de tratamento de dados, é claro que as empresas que desenvolvem essa atividade possuem responsabilidades não apenas contratuais, mas também legais e decorrentes da LGPD.

No desenvolvimento da operação, terão responsabilidade direta o controlador, em virtude das decisões que lhe serão inerentes no tratamento, mas também o operador, que responderá solidariamente pelos danos causados em caso de descumprimento das obrigações previstas na LGPD.

A LGPD prevê que, em caso de infrações, ficarão os agentes sujeitos a multas administrativas, que podem chegar até a 2% (dois por cento) do faturamento do último exercício, limitado a R$ 50 milhões por infração.

Além disso, há a possibilidade de, além do desembolso de valores decorrentes de multas, a empresa também sofrer outras penalidades. Entre elas estão:

- A suspensão parcial do funcionamento do banco de dados;
- A proibição parcial ou total do exercício das atividades relacionadas ao tratamento de dados;
- Outras punições, que variam de acordo com a gravidade, a reincidência, o grau do dano, a cooperação do infrator etc.

Dessa forma, é de extrema relevância, para qualquer empresa que faça o tratamento de dados, implementar as medidas necessárias de monitoramento, controle e atendimento à legislação de proteção de dados.

Isso deve incluir a implementação de uma política de privacidade, de segurança e demais medidas técnicas, como softwares e hardwares para fortalecer e blindar sua operação.

04

Proteção de dados para fintechs

Os novos serviços oferecidos pelas fintechs representam um avanço significativo no setor financeiro. Isso porque entregam uma experiência aberta, honesta e sem os longos processos de aprovação que normalmente as instituições financeiras mais tradicionais impõem.

Para entregar essa experiência, geralmente são utilizados algoritmos complexos, não humanos, que coletam e processam dados do cliente e os convertem em requisitos e decisões, como empréstimos, pagamentos e transferências.

O tradeoff desta operação é o risco decorrente do uso massivo de dados – Big Data – coletados via smartphones, tablets e computadores, e do compartilhamento de informações com terceiros.

Para mitigar esse risco, uma gama de elementos deve ser avaliada para, com estratégia e robustez, implementar medidas concretas relativas à proteção de dados.

Cyber security

Com o altíssimo volume de dados pessoais, principalmente dados bancários, que serão trafegados pela interface das fintechs, o cenário torna-se extremamente atrativo para hackers.

Um dos maiores vilões das empresas, no que diz respeito às vulnerabilidades de sistema, é o ransomware. São os “softwares maliciosos” criados com o intuito de restringir ou bloquear o acesso a arquivos ou sistema infectado, cobrando resgate para que o acesso possa ser restabelecido. Além, é claro, de eventuais vazamentos de dados que podem ocorrer dentro da própria empresa.

Portanto, é evidente a relevância do trabalho aprofundado de especialistas em infraestrutura de rede, que devem cuidar de todas as ferramentas de firewall, configurações dos servidores e métodos para tornar a segurança digital mais robusta.

Regulamentação específica para fintechs

Além da Lei Geral de Proteção de Dados, para as fintechs que atuam em soluções para o mercado financeiro, é importante também estar atento às regulamentações específicas que abordam a coleta e a proteção de informações.

Destacamos a seguir algumas delas:

Lei do sigilo bancário

Lei Complementar 105/2001: dispõe sobre o sigilo das operações de instituições financeiras e dos serviços prestados.

Política de segurança cibernética

Resolução CMN 4.658/18 e Circular BACEN 3.909/18: dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras, de pagamentos e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Proteção a base de dados de risco operacional

Circular BACEN 3.979/20: dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil de informações relativas a eventos de risco operacional.

Open banking

Resolução Conjunta BACEN n.1: dispõe sobre a implementação do sistema financeiro aberto, também chamado de open banking, e que prevê o compartilhamento padronizado de dados por meio de abertura e integração de sistemas.

Prevenção à lavagem de dinheiro

Circular BACEN 3.461/09: dispõe sobre as práticas necessárias para prevenção à lavagem de dinheiro, incluindo as informações cadastrais mínimas e o prazo de manutenção de informações e registros.

Lei do cadastro positivo

Lei 12.414/11: dispõe sobre como instituições podem gerenciar dados de pessoas naturais ou jurídicas em bancos de dados para formação de “perfil” de crédito.

Vale também atenção especial às disposições contidas na lei de crimes contra o sistema financeiro nacional (Lei 7.492/86) e à lei de prevenção à lavagem de dinheiro (Lei 9.613/98).

Instrumentalização da proteção de dados

Destaca-se a relevância de instrumentalização jurídica adequada dos documentos que regulam a relação da instituição com clientes, parceiros, funcionários ou prestadores de serviços, os quais devem estar em compliance com as normas relativas à proteção de dados.

Uma construção jurídica adequada, por profissionais especializados, garante a mitigação de riscos decorrentes da operação centrada em dados. Alguns exemplos são:

- Política de privacidade;
- Política de segurança de dados;
- Política de cookies;
- Termos do desenvolvedor (para implementar APIs);
- Termos de confidencialidade.

Tais documentos permitem que as empresas estejam resguardadas em situações de adversidade, perante seus clientes, perante o regulador, bem como os futuros fiscalizadores que serão instituídos de acordo com a LGPD.

Implementação da política de proteção de dados

A LGPD em breve entrará em vigor e, em pouco tempo, produzirá efeitos, sendo fundamental para quem quer prosperar e fazer parte do mercado.

Ambientar-se e implementar as novas regras para proteção de dados permitirá que o seu negócio já esteja à frente e em conformidade com a nova regulação, que é realidade.

Mas não somente em razão do que dispõe a lei, mas com o propósito de oferecer um serviço de qualidade aos clientes, com máxima segurança, segue uma ideia de roteiro para a criação de uma política de proteção de dados:

01 Estruturar equipe estratégica para entender a LGPD e demais leis que regulamentam as atividades da empresa;

02 Mapear todos os dados de usuários tratados pela empresa, seja por e-mail, plataforma virtual, aplicativo etc;

03 Verificar se todos estes dados são de fato necessários para execução do serviço prestado;

04 Mapear a jornada dos dados de seus clientes dentro da sua empresa, desde a coleta até a eliminação;

05 Avaliar tecnicamente a infraestrutura de segurança e os riscos de cyber security que permeiam o negócio;

06 Estruturar política de proteção de dados e players para operacionalizar o plano;

07 Atualizar em tempo real os instrumentos contratuais da empresa, com colaboradores, terceiros e clientes;

08 Divulgar amplamente, bem como solicitar consentimento do cliente.

05

Os desafios das fintechs para se adaptar à LGPD

Impactos no mercado financeiro

Segundo o State Of The Internet/Segurança 2019, um dos principais alvos de ações para roubo e venda de dados são instituições financeiras.

Um outro estudo da indústria de fintechs realizado pela Infiniti Research apontou que a disponibilidade dos dados em formatos digitais, embora facilite a análise e a geração de insights, torna-os mais suscetíveis a violações de segurança.

Além disso, cerca de 56% das fintechs não possuem políticas de segurança de dados, de acordo com estudo de 2019 da PwC e da Associação Brasileira de Fintechs (ABFintechs).

Muitas vezes, as fintechs não se preparam para lidar com as ameaças de cyber security, focando apenas no investimento em tecnologias para melhorar o desempenho e expandir as possibilidades de negócios.

A segurança das informações deve ser um pilar estratégico e prioritário para todas as instituições financeiras, principalmente as que oferecerem serviços digitais.

Para garantir a segurança dos usuários e da própria empresa, alguns investimentos são necessários, como criptografia, equipe e cultura de segurança, compliance com padrões mundiais e selo de segurança que ateste compromisso com a proteção de dados.

Vale lembrar que as instituições financeiras, dentre elas as fintechs, sofrerão um grande impacto com a nova lei de proteção de dados. Isso porque os dados dos clientes são fundamentais para a operação dos negócios.

Com a LGPD, o consentimento do usuário poderá ser revogado a qualquer momento, caso não exista clara finalidade ou outra base legal vigente que obrigue o armazenamento dos dados.

Aqui, cabe ressaltar que alguns dados, no que diz respeito ao sistema financeiro, não podem ser apagados, pois existem bases legais que se sobrepõem à LGPD, como regulamentações específicas do setor promovidas pelo Banco Central do Brasil.

Sendo assim, o mercado financeiro já possui uma arquitetura de segurança maior, por tratar de dados sensíveis, mas a nova legislação deve alavancar o nível de proteção.

A recomendação é que as fintechs trabalhem em duas frentes: jurídica e tecnológica, visando conscientizar os usuários e trazer clareza sobre as mudanças que podem ocorrer e quais são as responsabilidades das partes envolvidas.

Por onde começar?

Uma das maiores dificuldades para se adequar à LGPD é a barreira cultural nas empresas. É difícil mensurar valor para investimento em ferramentas de segurança digital.

Esse valor normalmente é percebido quando as empresas sofrem com incidentes de segurança, como vazamento e/ou sequestro de dados ou danos a imagem.

Para começar, é importante que a empresa tenha um mapeamento dos dados pessoais que são processados na organização. Quem tem acesso aos dados pessoais precisa garantir logs de auditoria e backup dessas informações.

É preciso fazer revisão dos acessos aos dados pessoais com base no need to know para verificar se quem tem acesso realmente precisa desse acesso para desempenhar seu trabalho. Com o mapeamento em mãos, será possível compreender suas necessidades e avaliar que tipo de ferramenta pode atender o cenário para cada gap.

Dentre as adequações técnicas, é importante ter uma ótica out of the box relacionada à segurança da informação e à cyber security. O foco deve ser estar em compliance com padrões mundiais, como CIS (Center for Internet Security), NIST(CSF) e ISO 27001.

Ao se adequar aos padrões internacionais, além de estar preparada para a LGPD, a fintech também facilita o processo de internacionalização.

Estar em compliance com padrões mundiais, como CIS, eleva a cyber security, tanto a nível de hardware quanto a nível de software.

Outro ponto muito importante é garantir que os serviços contratados pelas empresas também estejam de acordo com as leis de proteção de dados e assegurem a confidencialidade das informações armazenadas.

Isso é de suma importância para a segurança da fintech e dos seus clientes. Ter respaldo jurídico nesse quesito é essencial, contratar consultorias e ter advogados especialistas em segurança digital à disposição pode ser uma boa saída.

É imprescindível a utilização de um cofre para armazenar as credenciais de acesso aos serviços externos e internos. Sem dúvida, também é crucial ter logs a nível de rede e de aplicação de tudo o que está acontecendo na empresa.

Além de ter os logs, é preciso centralizá-los, analisá-los e organizá-los de maneira que seja viável identificar possíveis ameaças. Isso pode ser facilmente monitorado com a implementação de um SIEM (Software de Gerenciamento de Informações e Eventos de Segurança).

Assim, é possível ter essas informações categorizadas, prevenindo um vazamento de dados por meio da implementação de um DLP (Data Loss Protection). O uso de firewall também é indispensável.

O roadmap para compliance com a LGPD é vasto. O que precisa estar claro para todos é a preocupação de estar evoluindo e implementando melhorias constantes em relação à segurança da informação e à cyber security. É importante ter a segurança como base de sustentação da empresa, ainda mais quando se trata do mercado financeiro.

06

Muito além da LGPD: boas práticas de cyber security

Frameworks internacionais de segurança digital

Existem hoje no mercado diversos frameworks internacionais de segurança digital, como CIS, NIST(CSF) e ISO 27001.
A adoção e a implementação desses frameworks eleva a maturidade de segurança da fintech e, com isso, os dados serão mantidos seguindo boas práticas internacionais.

Os frameworks não dizem a tecnologia utilizada para conformidade nem como será feito, porém diz o que é preciso ser feito. Por isso, é importante ter um especialista em segurança da informação para avaliar a melhor forma de adequação para cada cenário.

Treinamento e cultura interna

As fintechs precisam se lembrar da importância do treinamento e da cultura interna para a segurança dos dados.

Uma pesquisa feita pela ISACA com 1,5 mil gerentes e profissionais de segurança, sobre os principais vetores de incidentes, teve o seguinte resultado:

1º
cibercriminosos em busca de ganho financeiro (32%);

2º
hackers com intuito de prejudicar o funcionamento da empresa ou danificar a imagem (23%);

3º
erros humanos não intencionais realizados por funcionários da empresa (15%).

Em sua maioria, esses incidentes se dão ao clicar em um link malicioso ou efetuar downloads de softwares infectados. Por isso, o treinamento aos funcionários se torna bastante eficaz.

Tecnologicamente falando, algumas ações e tecnologias são de simples implementação e podem elevar a maturidade de segurança da organização:

- Utilizar senhas fortes ou cofres de senhas;
- Manter os computadores atualizados e com antivírus sempre ativado;
- Ter atenção aos e-mails falsos, como spam ou phishing.

O mercado de fraudes envolvendo phishing, smishing (“SMS” + “Phishing”) ou mesmo usando engenharia social (alguém se passando por funcionário da instituição solicitando informações) tem evoluído muito rápido.

Esses ataques são muito dinâmicos e, mesmo sendo detectados, um hacker pode facilmente criar outra página falsa em outro domínio.

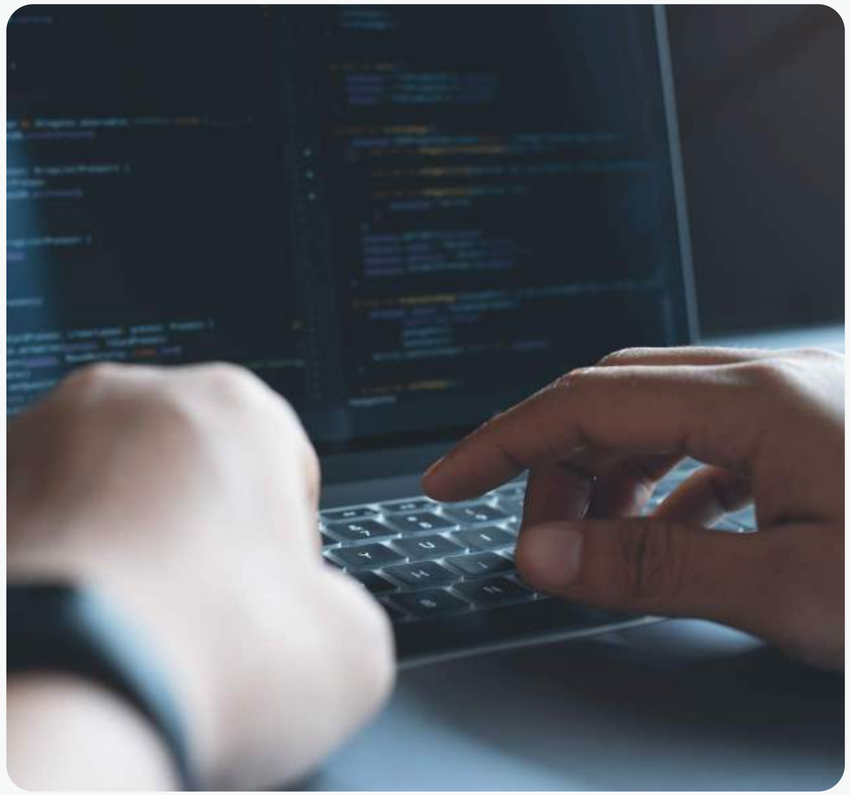
Essas boas práticas precisam estar na cultura de todos usuários de instituições financeiras que fazem transações online.

Por isso, é indispensável investir em campanhas de conscientização para os usuários finais sobre:

- Como reconhecer páginas suspeitas;
- Nunca enviar dados sensíveis por e-mail, chat, WhatsApp;
- Como proceder em caso de ter clicado em algum link suspeito;
- Evitar acessar a conta por links disponibilizados em sites de pesquisa ou encaminhados por aplicativos de mensagens, procurando sempre digitar a URL da instituição começando por https:// ou acessar pelo aplicativo oficial da instituição.

07

Experiência e dicas Transfeera para fintechs de meios de pagamento



Como a Transfeera adaptou suas rotinas internas?

Para proteger os dados dos nossos clientes, nós, da Transfeera, estamos rodando 100% na AWS, nosso provedor de cloud. Com isso, conseguimos implementar score de standards, como o CIS Basic, e garantir que nossa infraestrutura esteja segura de acordo com os melhores padrões do mercado.

Também usamos um firewall de aplicação web na frente de todos os serviços expostos para a internet. Assim, conseguimos monitorar e prevenir ataques que possam prejudicar nosso sistema, como DDOS, top 10 da lista de vulnerabilidades reportada pela OWASP e regras customizadas, como Bruteforce.

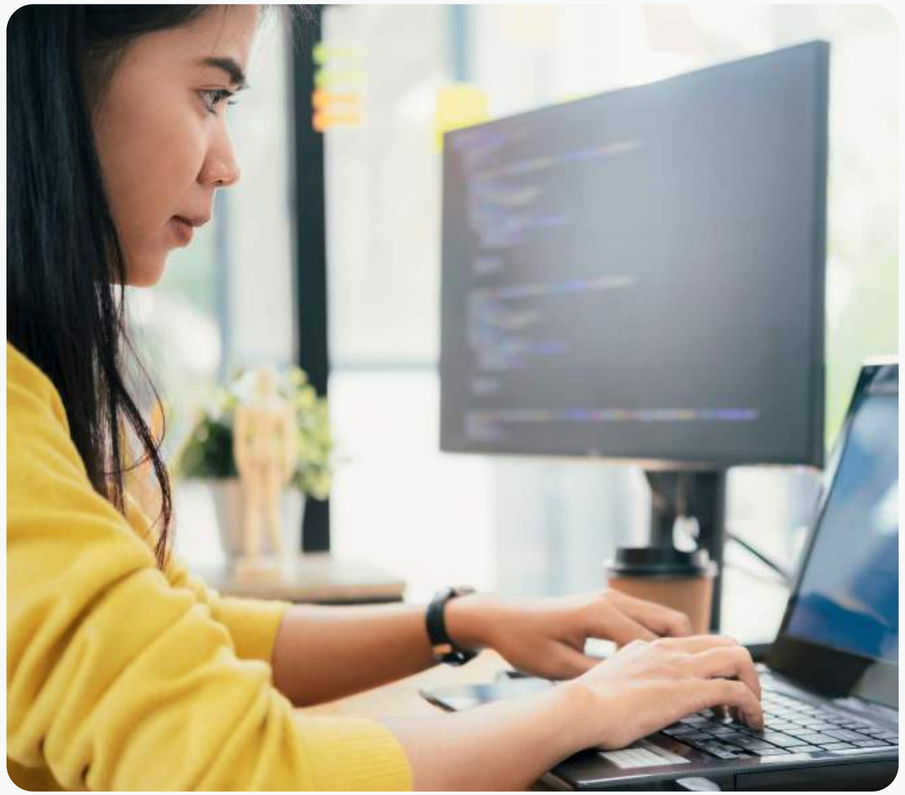
Tivemos ainda uma consultoria técnica com um especialista em segurança da informação e cyber security e também uma consultoria jurídica para adequar os termos e os contratos, como por exemplo: termos de uso, termos de privacidade, política de segurança da informação, política de segurança cibernética, política de cookies, dentre outros documentos.

Checklist dos principais pontos para cumprir a LGPD e manter a segurança dos dados

O start para adequação de fintechs de meios de pagamentos à LGPD é o mapeamento dos dados. É a partir do entendimento de quais dados cada área manipula e cada ferramenta utiliza que é possível entender onde trafegam os dados sensíveis e pessoais e, com isso, poder traçar estratégias para controles específicos de acordo com a criticidade dos dados.

Para que tudo ocorra da melhor forma possível, é preciso que os líderes de cada área estejam dispostos a participar e/ou indicar as melhores pessoas do seu time para a “entrevista” de mapeamento.

A partir dessa etapa, é preciso gerar um plano de ações, que deve incluir as adequações de controle de acesso, a exclusão de determinadas informações que não são necessárias para o seu negócio, a criptografia de informações sensíveis pela ótica de legislação vigente ou da própria LGPD, dentre outros pontos inerentes ao negócio.



Confira alguns pontos relevantes não apenas para o compliance com a Lei, mas também para a segurança digital da empresa:

NDA com serviços de terceiros

Se a sua empresa, assim como a Transfeera, utiliza alguns serviços complementares para ajudar o seu negócio, é importante ter uma materialização jurídica de proteção de dados e o acordo de confidencialidade oferece isso.

Caso você não consiga para todos os serviços, no mínimo, avalie o termo de uso, de privacidade e de cyber security, se a empresa tiver, para garantir que tenham informações sobre proteção dos seus dados.

Implementar WAF (Web Application Firewall)

Ao configurá-lo na frente de todos os seus serviços expostos para a internet, vai ajudar a identificar e prevenir ataques do tipo de negação de serviço (DOS, DDOS), ataques mais conhecidos pela OWASP, Bruteforce, restrição de versão de TLS, bloqueio geográfico, monitoramento, dentre outras funções que você pode configurar.

Implementar um antivírus corporativo para o gerenciamento remoto das máquinas

Na Transfeera, usamos o Kaspersky em uma versão específica que nos permite atualizar os softwares de forma remota, criptografar os discos, escanear o equipamento, resolver incidentes de segurança, bloquear portas USB e sites e ter controle de wi-fi que o equipamento poderá acessar.

Vale ressaltar que aqui só são monitorados os equipamentos que são de propriedade da empresa e os softwares que são utilizados para o desempenho da função do colaborador e com a conscientização de cada um referente ao gerenciamento remoto dentro da política de segurança cibernética.

Gestão de Logs, a nível de rede e de software

Além de ter tudo isso consolidado, é preciso ter ferramentas para analisá-los, organizá-los e categorizá-los de forma a entender se existe algum vazamento de informação, principalmente PII, incidentes de segurança e para conseguir encontrar a causa raiz de algum possível incidente que venha a ocorrer.

É possível obter isso com a aplicação de SIEM (Security information and event management), DLP (Data Loss Prevention), IDS (Intrusion Detection System) e IPS (Intrusion Prevention System).

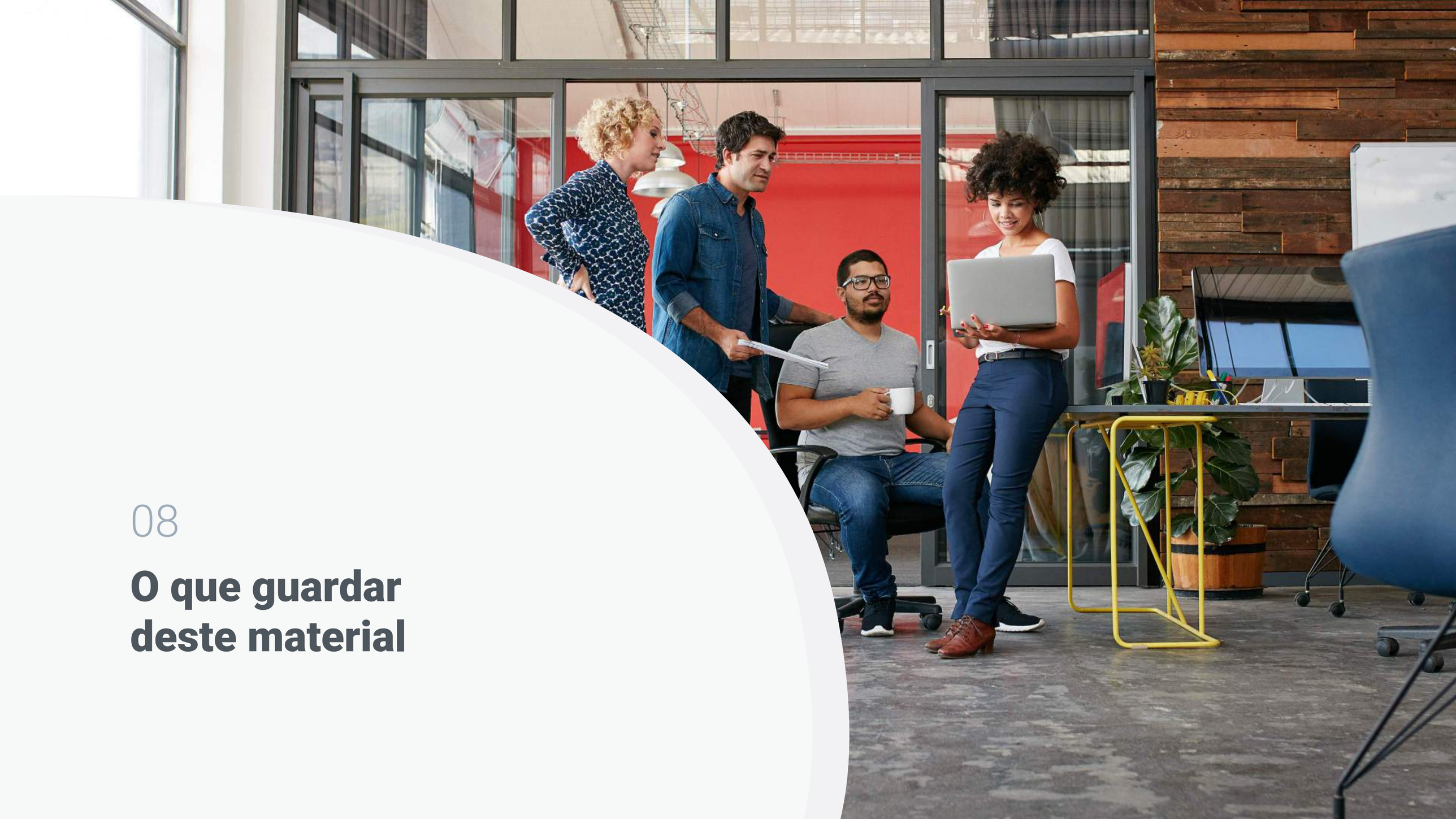
Frameworks de cyber security a nível mundial

Ter como referência CIS, NIST e ISO 27001, que conforme falamos acima são frameworks que ampliam a segurança da fintech. Ao utilizar suas diretrizes como referência, os dados podem ser mantidos seguindo as boas práticas internacionais.

Além dos itens anteriores, recomendamos fortemente:

- Ter um gerenciador de senhas;
- Contar com monitoramento de e-mails;
- Implementar um SAST na sua esteira de desenvolvimento;
- Fazer a gestão de identidade;
- Fazer a separação de redes (VPN, VPC);
- Ter logs centralizados em uma conta para auditoria;
- Contar com um especialista em segurança da informação e cyber security.

Ao lado da sua empresa, crie uma squad com um roadmap bem definido e tenha como pilar principal de sustentação a segurança da informação.



08

O que guardar deste material

Nessa jornada de adequação à Lei Geral de Proteção de Dados, é importante que as fintechs se atentem para a questão da segurança, considerando as frentes jurídica e tecnológica.

Para identificar os dados sensíveis e pessoais, que são o foco da LGPD, comece mapeando todos os dados, levantando quais deles são manipulados por quais áreas e quais são as ferramentas utilizadas.

Assim, é possível verificar onde eles trafegam e traçar estratégias para controles específicos de acordo com a criticidade deles.

Somente com a identificação dos dados críticos, parta para a criação de um plano de ações, que inclua as adequações de controle de acesso, a exclusão de informações que não sejam necessárias para o seu negócio e a criptografia de informações sensíveis.

É imprescindível investir em treinamentos e em uma cultura interna que valorize a segurança da informação. Os colaboradores das fintechs precisam estar cientes das melhores práticas para garantir a cyber security.

Por isso, essas informações devem vir da gestão e ser bastante difundidas na organização para orientar também os usuários.

Também é indispensável ter respaldo jurídico, contratando consultorias e advogados especialistas em segurança digital, além de uma consultoria técnica com um especialista em segurança da informação e cyber security.

Esperamos que este material tenha sido útil e pode ser bastante aproveitado para ajudar sua empresa neste momento de transição. Se tiver alguma dúvida, entre em contato conosco: Transfeera e VP Advocacia!

TRANSFEERA

Nós da Transfeera desenvolvemos uma plataforma para automação das rotinas de pagamentos das empresas, gerando economia a cada transferência realizada entre diferentes bancos e reduzindo os riscos e o esforço operacional deste processo.

Também atuamos com validações bancárias, proporcionando segurança aos nossos clientes ao evitar possíveis fraudes. Em 2019, crescemos 10,5% ao mês e até aqui já movimentamos mais de R$ 1,5 bilhão, realizando mais de 1,2 milhão de pagamentos com sucesso.

Em nosso portfólio, contamos com mais de 150 clientes, entre eles iFood, Rappi, PayGo, Vakinha, Ebanx, Paggue, Unilever, Kimberly-Clark, Whirpool e General Mills.

Solicite uma demonstração

www.transfeera.com.br | 3003-8388

VANZIN & PENTEADO

A VP, escritório de advocacia Vanzin & Penteado, há 23 anos, foi sonhada e idealizada pelos sócios-fundadores Jaime Penteado e Gerson Vanzin, ex-procuradores do Banco Central, que decidiram deixar a carreira pública para darem início a uma nova história marcada pelo empreendedorismo e inovação em serviços jurídicos.

O ritmo de transformação e mudança no mercado exige que as empresas em crescimento necessitem de conhecimentos jurídicos e nós, da VP, estamos sempre a postos para fornecer/oferecer as melhores práticas, métodos e soluções customizadas em matéria societária, contratual, regulatória e digital, acompanhando a inovação, mudança e evolução da economia global.

Dentre os profissionais que integram o time, estão os sócios Kael Moro e Vanessa Naunapper, que contribuíram para a elaboração deste material.

A missão da VP é fornecer aos nossos clientes muito mais do que assistência legal. O foco é apresentar soluções jurídicas inteligentes, modernas, integradas e acessíveis, sempre com transparência, lealdade, competência e ética.

Conheça mais

www.vp.adv.br | (41) 3218-4000