FORTE

e-Book

Introdução à Lei Geral de Proteção de Dados

Forte Privacy

A FORTE

A **Forte Security** nasceu com o objetivo de entregar maior produtividade operacional e elevar o nível de inteligência tecnológica das organizações. Garantindo uma infraestrutura completa para **proteger e potencializar** os seus negócios, através da Segurança da informação.

É assim que estamos há 3 anos entregando **soluções inteligentes e seguras para as empresas**, com qualificação, e qualidade técnica.

Forte Security

Forte IT 360

Forte Privacy

O que é a Lei Geral de Proteção de Dados?

FORTE

A LGPD

O Brasil já possuía uma série de normas setoriais relacionadas à proteção de dados, espalhados na Constituição Federal, Código de Defesa do Consumidor, Código Civil, Lei de Acesso à Informação, Lei do Cadastro Positivo e Marco Civil da Internet. Porém, inspirada no Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation) da União Européia, nasceu em agosto de 2018, a primeira lei geral brasileira sobre o tema, chamada Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709.

A LGPD

Art. 1°

"Esta Lei dispõe sobre o tratamento de dados pessoais inclusive nos meios digitais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

A LGPD aplica-se a todas as pessoas físicas e jurídicas, sejam elas públicas ou privadas, de qualquer porte, setor ou tipo de tributação, que realizam qualquer operação de tratamento de dados dentro do território nacional, tanto no ambiente online quanto no off-line.

Toda operação de tratamento de dados deve ter uma finalidade legítima e estar associada a uma base legal.

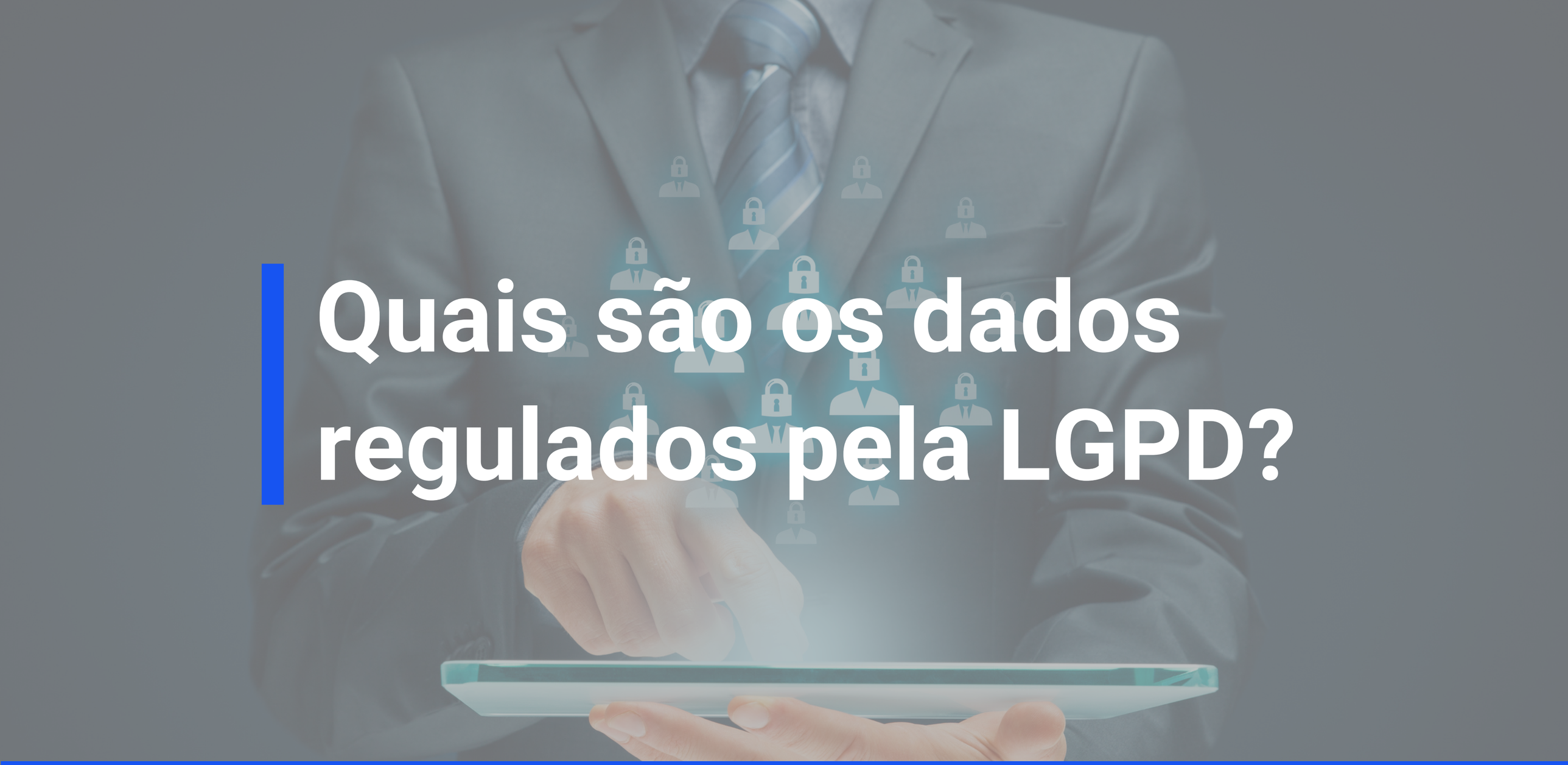
Empresas não sediadas no Brasil também podem vir a ter que observar os termos da LGPD nas seguintes hipóteses:

1. Se elas realizam tratamento de dados pessoais no território nacional;
2. Se o tratamento dos dados pessoais tem como objetivo ofertar bens ou serviços para o mercado nacional;
3. Caso os dados pessoais sejam de indivíduos localizados no território

FORTE

BASES LEGAIS

- Consentimento
- Cumprimento de obrigação legal
- Execução de política pública
- Execução de contrato
- Exercício regular do direito
- Proteção da vida
- Tutela da saúde
- Atividade acadêmica
- Proteção de crédito
- Legítimo interesse



Quais são os dados regulados pela LGPD?

FORTE

TIPOS DE DADOS

1

Dados Pessoais:

Trata-se de toda e qualquer informação relacionada à pessoa natural (física) identificada ou identificável. Ou seja, dados como nome completo, e-mail, telefone, RG, CPF e endereço, e dados indiretos como endereços de IP, geolocalização de dispositivo móvel e demais identificadores eletrônicos.

2

Dados Sensíveis:

É todo 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.

FORTE

TIPOS DE DADOS

3

Dados Anonimizados:

É todo dado relativo ao titular que não permite ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

4

Dados Pseudonimizados:

Processo semelhante ao da anonimização, em que um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. O pseudo anonimato é incentivado pelo próprio regulamento como forma de reduzir os riscos.

FORTE

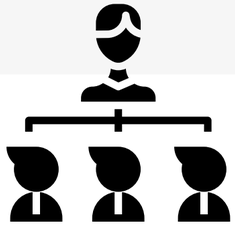
Quem são os atores da LGPD?

FORTE

ATORES DA LGPD

Titular

A pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.



Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes aos tratamentos de dados pessoais.

ATORES DA LGPD

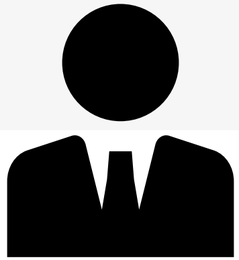
Operador

Pessoa natural ou jurídica, de direito público ou privado que realiza o tratamento de dados em nome do controlador.

ANPD

Agência responsável pela regulação sobre a proteção de dados pessoais. Responsável por zelar, implementar e fiscalizar a LGPD.

ATORES DA LGPD



Encarregado/ Data Protection Officer

É a 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), com base no art. 5º, inciso VIII, da lei.). O DPO é o encarregado pela proteção de dados da organização, podendo ser este, uma pessoa interna ou externa à empresa.

DIREITOS DOS TITULARES

Art. 18°

"O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; [...]"

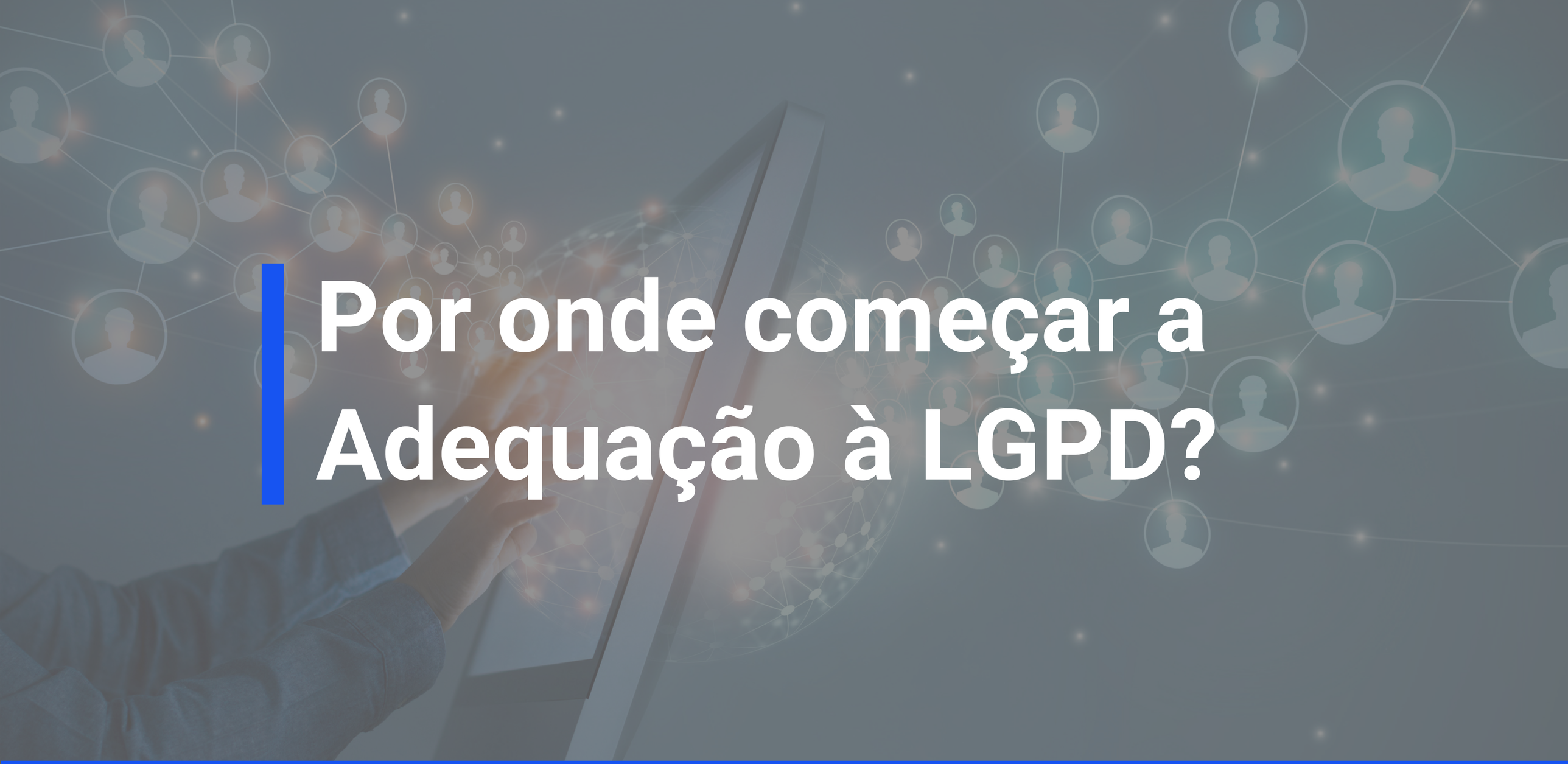
FORTE

DIREITOS DOS TITULARES

Art. 18°

"[...] V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei."

FORTE



Por onde começar a Adequação à LGPD?

FORTE

Diagnóstico de Dados

O Diagnóstico de Dados trata-se do preenchimento de um questionário de Operações de Tratamento de Dados (OTD’s), por cada setor da empresa, para que seja possível entender o funcionamento do tratamento de dados dentro da empresa.

Vale ressaltar que nesta etapa, serão identificados todos os documentos da empresa, sejam eles contratos, normativas internas, políticas e termos que podem ser impactados pela LGPD, como também serão identificados os lugares, ou seja, os locais onde o dado é coletado, armazenado, tratado ou processado, seja em meio físico ou digital.

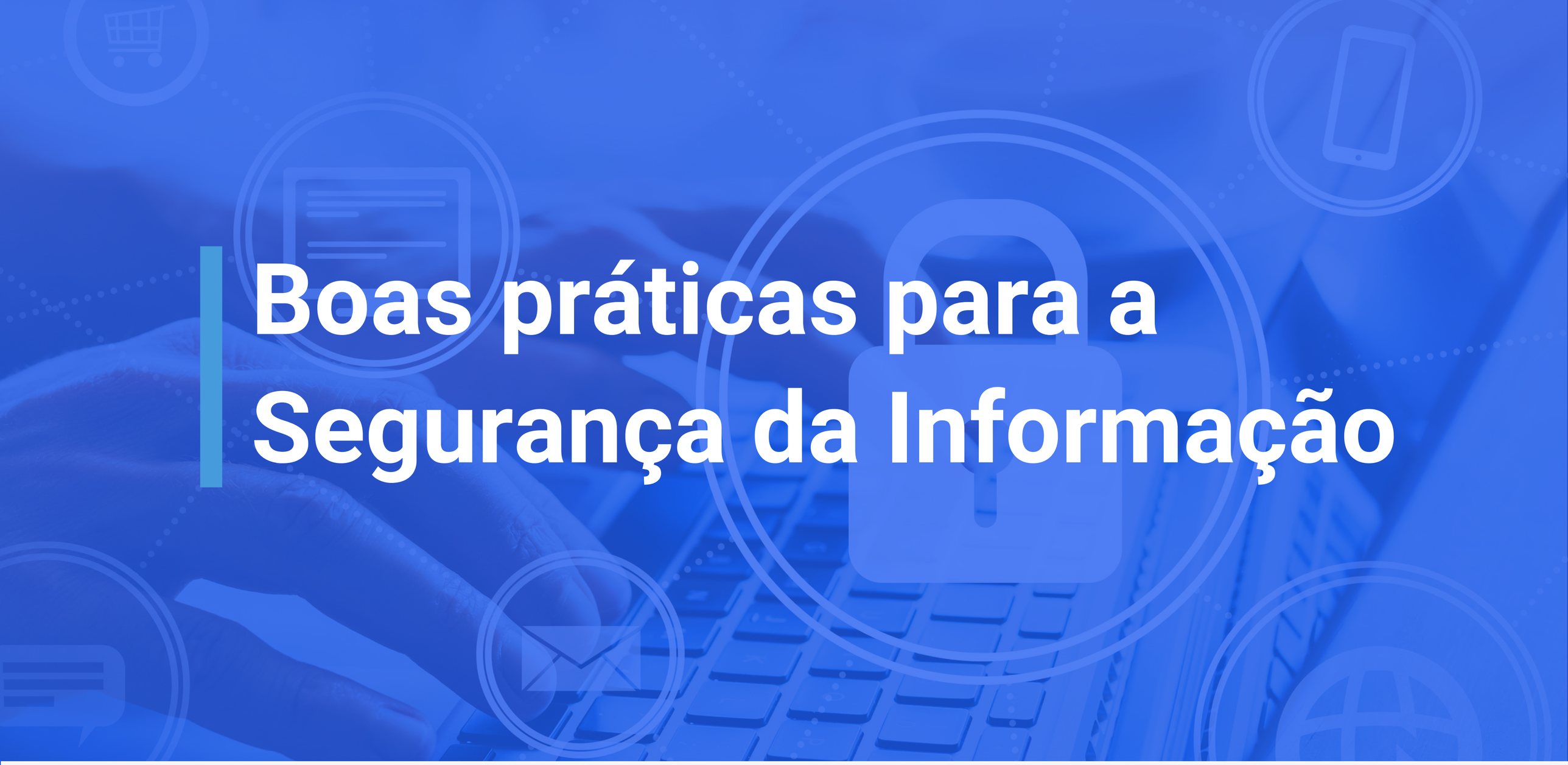
Mapeamento de Dados

O mapeamento de dados, refere-se a um documento essencial quando estamos no processo de adequação às normas de proteção de dados. O documento - ou planilha - de mapeamento de dados devem refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita, pois este documento que nos dará um panorama geral de como a empresa está lidando com a questão da privacidade e segurança da informação.

Segurança da Informação

Segundo a Lei Geral de Proteção de Dados (LGPD), dentre os princípios a serem seguidos ao tratar quaisquer dados pessoais, está a segurança, por meio da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, assim como, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado.

Portanto, o tratamento de dados pessoais se torna irregular caso deixe de obedecer a esse princípio, ou quando não fornecer a segurança que o titular dos dados pode esperar dele



Boas práticas para a Segurança da Informação

eBook: Introdução a Lei Geral de Proteção de Dados

FORTE

Mapeie os Riscos à Segurança

Para garantir a correta identificação, gerenciamento, controle e tratamento dos riscos da organização, é imprescindível a enumeração dos agentes de ameaça e o mapeamento das principais vulnerabilidades presentes no negócio.

Proteja sua Rede

A fim de detectar, prevenir e remediar tentativas de ataque, ações e/ou acessos remotos não autorizados à rede da organização, é vital utilizar dispositivos de segurança de rede, como Firewalls, IDSs e IPSs. Assim, criam-se possibilidades para gestão do tráfego de rede e uso de aplicações, tratamento de incidentes e bloqueio de conexões maliciosas ou indesejadas.

Proteja-se contra Malwares

Grande parte dos ataques e incidentes de segurança digitais, atualmente, envolvem a instalação de malwares no computador dos usuários, entre eles principalmente o ransomware. Por esse motivo, é essencial ter um software antimalware instalado em todos os dispositivos e na rede, como antivírus e EDRs, de forma a prevenir eventuais incidentes, ameaças e ataques.

Utilize a Criptografia como Aliada

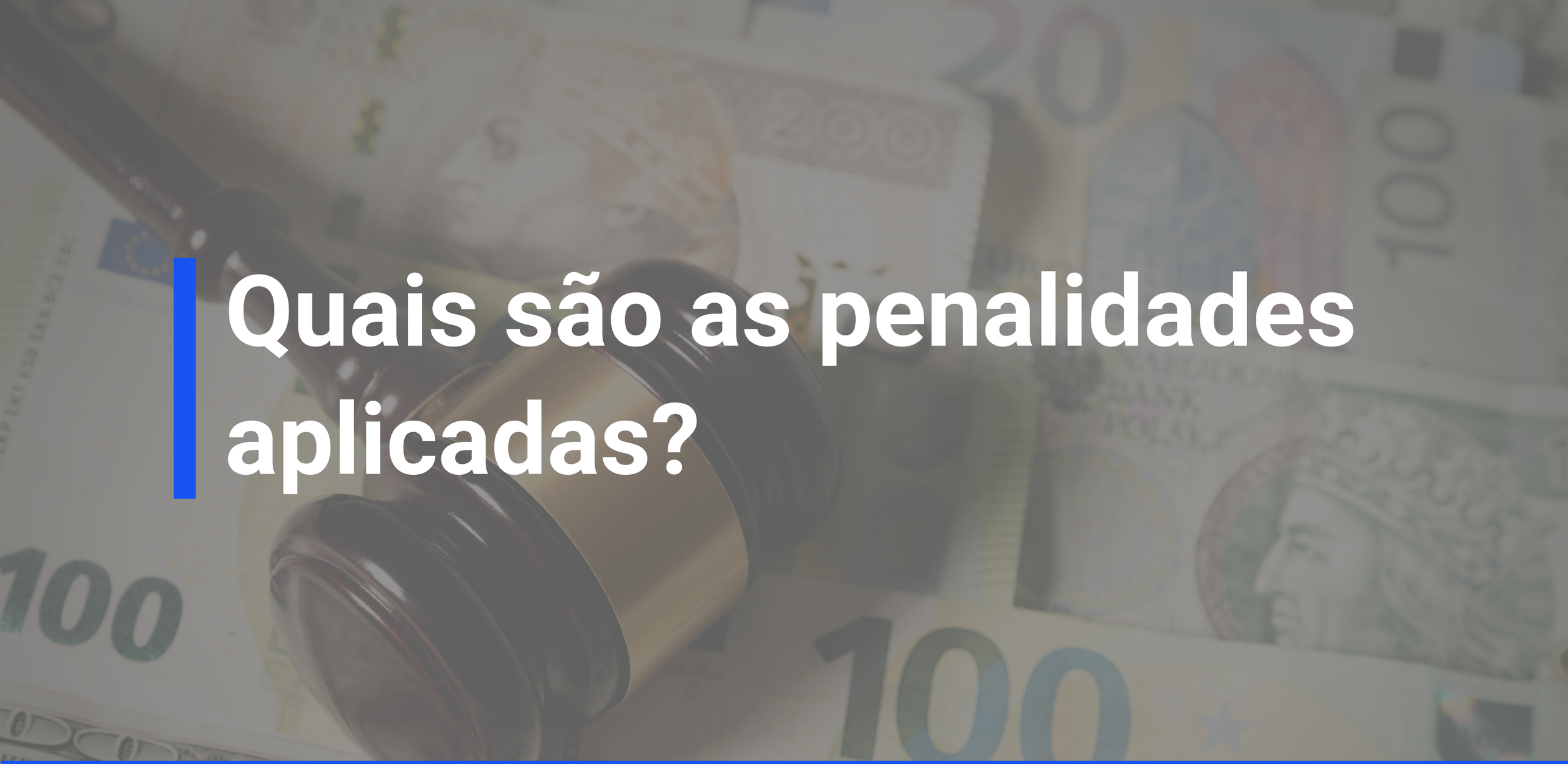
A criptografia não somente objetiva proteger as informações, mas também fazer com que elas sejam veiculadas de forma segura. Mesmo que seja utilizado um canal inseguro, ela busca preservar a integridade, a confidencialidade e a disponibilidade dos conteúdos.

Controle o Acesso

Realize um controle de acesso apropriado, distribuindo privilégios, autorizações e permissões somente quando necessárias para o cumprimento das responsabilidades do usuário. Para isso, sempre que possível, opte pela utilização de múltiplos fatores de autenticação, junto de uma forte política para gestão de senhas, com o uso de credenciais seguras e trocas periódicas.

Treine os Usuários

É essencial termos ciência de que todos os controles que implementarmos ainda estão sujeitos a falhar, pois a última linha de defesa sempre será caracterizada pelo cliente ou usuário. Por isso, promova treinamentos!



Quais são as penalidades aplicadas?

FORTE

1

Advertência

Com indicação de prazo para adoção de medidas corretivas

2

Multa Simples

De até 2% (dois por cento) do faturamento da pessoa jurídica

3

Multa Diária

Observado o limite total de R$50.000.000,00 por infração

4

Publicização

Após devidamente apurada e confirmada a sua ocorrência

5

Bloqueio dos dados pessoais

A que se referem a infração até a sua regularização.

6

Eliminação dos dados pessoais

A que se referem a infração

7

Suspensão parcial do funcionamento do banco de dados

8

Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados

FORTE

(55) 3347-1831

Rua Alameda Santiago do Chile, 185.
Sala 101. Nossa Sra. das Dores
Santa Maria - RS

www.fortesecurity.com.br