

Lei Geral de Proteção de Dados e os Impactos na sua Empresa

Por Roberto Crespo

<http://e-qr.me/362a5a>



CENÁRIO DE CRIAÇÃO DA LEI

- Aumento de Valor dos dados;
- Desenvolvimento de Tecnologias com potencial aumento de conectividade (5G, IoT, entre outras);
- Utilização abusiva de dados (Facebook/Cambridge Analytics, registros e cadastros pessoais sendo utilizados em contextos estranhos à relação);
- Aumento dos Cyberataques no mundo (WannaCry, Banco Inter, Estante Virtual);

OBJETIVOS DA LEI

- A LGPD possui 2 objetivos principais, um expresso na lei, outro “oculto”;
- 1 – proteger dados pessoais, protegendo os direitos fundamentais dos usuários;
- 2 – prevenir e reduzir o impacto de Cyberataques.

OBJETIVOS

Menos dados



banco de dados mais enxuto



proteção mais eficaz

TRIPÉ PRINCIPAL DO CONCEITO DE PROTEÇÃO DE DADOS

Confidencialidade

a informação só deve ser
acessada por quem de Direito

Integralidade

evitar que os dados sejam
apagados ou alterados sem a
devida autorização do titular

Disponibilidade

as informações devem sempre
estar disponíveis para acesso

BASES LEGAIS

- Constituição Federal
- Lei 13.709/2018
- Medida Provisória 869/2018
- Projeto de Conversão em lei 7/2019 (Parecer e Relatório Comissão Mista do Congresso Nacional – 08/05/2019)
- Outras legislações (Marco Civil da Internet, Código de defesa do Consumidor, Lei 12.414/2011 – Cadastro Positivo, Lei complementar 105/2011 – operação inst. Financeiras)
- Regras Importantes
ISO 27001 e 27002. International Standardization Office.

ESCOPO DA LEI

O que?

Proteção no Tratamento de dados pessoais da

PESSOA NATURAL

ESCOPO DA LEI

Por Quem?

Por pessoa natural ou por pessoa jurídica de direito público ou privado

ESCOPO DA LEI

Onde?

independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou ainda os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

VIGÊNCIA

- LEI – 18 meses – fevereiro de 2020.
- Medida Provisória – 24 meses – agosto de 2020.

VIGÊNCIA

IMPORTANTE!!!

se a MP não for convertida em lei em 120 dias, perde a eficácia (e voltaria o prazo para fevereiro de 2020).

VIGÊNCIA

IMPORTANTE!!!

PROJETO DE LEI DE CONVERSÃO Nº 7/2019

Feito com base no relatório de Comissão Mista do CN

Modifica diversos aspectos da Lei.

Deverá ser votado no Congresso Nacional (1 de 3 hipóteses).

PRINCIPAIS CONCEITOS

- **Titular** – Art 5º, inc V – em essência, a **peessoa natural** a quem pertencem os dados pessoais.
- **Dados pessoais** (inc I) – todas as informações relacionadas à **peessoa natural** que podem ser identificadas ou identificáveis (meio razoável – inciso III). A Identificação é a **CHAVE** para a caracterização do dado como pessoal.

PRINCIPAIS CONCEITOS

- **Dados pessoais sensíveis** (inc II) – informações relacionadas à **pessoa natural**, sobre os seguintes temas:
 - 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 (reconhecimento facial, monitoramento cardíaco).
- Obs: gênero??? Apesar do rol da lei ser taxativo (ou seja, não admitir interpretações além dos listados), questões relacionadas à gênero devem ser tratadas como sensíveis por equiparação.

PRINCIPAIS CONCEITOS

- **Dados anonimizados** (inc III) também devem ser protegidos. Anonimização, para ser efetiva, não deve ser revertida por meios “razoáveis” (ou seja, por atividade regular dentro do próprio tratamento).
- **Dados de menores** devem ser dados com o consentimento dos pais e/ou responsáveis legais (pelo menos 1).

PRINCIPAIS CONCEITOS

Consentimento – (inc XII)

Tripé – Consentimento DEVERÁ ser **LIVRE**, **INFORMADO** e **INEQUÍVOCO**.

Lei determina que a manifestação seja livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Responsabilidade do Controlador de comprovar o consentimento.

Art 8º § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

CONSENTIMENTO

- NECESSÁRIO para dados sensíveis, exceto nos casos em que for INDISPENSÁVEL para:
 - a) cumprimento de obrigação legal ou regulatória pelo controlador;
 - b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
 - e) proteção da vida ou da incolumidade física do titular ou de terceiro;
 - f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; *ou
 - g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

CONSENTIMENTO

- Consentimento do empregado?

Por causa do vínculo de emprego, o consentimento **nunca** é livre.

Recomendável que as informações sejam requeridas com outra base legal.

PRINCÍPIOS PARA O TRATAMENTO

- Boa fé – artigo 6º caput
- Finalidade – tratamento para propósitos legítimos, específicos e explícitos informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação – compatibilidade do tratamento com as finalidades informadas ao titular;
- Necessidade – limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

PRINCÍPIOS PARA O TRATAMENTO

- Livre acesso – garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e duração do tratamento dos dados pessoais;
- Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
 - I - finalidade específica do tratamento;
 - II - forma e duração do tratamento, observados os segredos comercial e industrial;
 - III - identificação do controlador;
 - IV - informações de contato do controlador;
 - V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
 - VI - responsabilidades dos agentes que realizarão o tratamento; e
 - VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.)

PRINCÍPIOS PARA O TRATAMENTO

- Qualidade dos dados - garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento de finalidade de seu tratamento;
- Transparência - garantia, aos titulares, de informações claras, precisas e de fácil acesso sobre a realização do tratamento e respectivos agentes de tratamento (possível resguardar segredos comerciais e industriais).
- Segurança – utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PRINCÍPIOS PARA O TRATAMENTO

- Prevenção – adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Não discriminação – impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
- Responsabilização e prestação de contas – Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

REQUISITOS PARA O TRATAMENTO – Art 7º

- I – mediante o fornecimento de **consentimento** pelo titular;
- II – para o **cumprimento de obrigação legal ou regulatória** pelo controlador;
- III – **pela administração pública**, para o tratamento e uso compartilhado de **dados necessários à execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV – para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

REQUISITOS PARA O TRATAMENTO – Art 7º

- V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; ex instalação de NET.
- VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII – para a tutela da saúde, em procedimento realizado por profissionais da saúde, serviços de saúde ou por entidades sanitárias*;

REQUISITOS PARA O TRATAMENTO – Art 7º

- IX – quando necessário para atender aos **interesses legítimos** do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Com o legítimo interesse, somente pode tratar os dados “estritamente necessários” para a atividade. ANPD pode requerer a elaboração de Relatório de Impacto)

IMPORTANTE FAZER 3 PERGUNTAS:

1 – a PJ tem, de fato, interesse nesses dados/conhecimento?;

2 – só posso alcançar esse interesse legítimo se eu tratar esses dados?;

3 – qual o balanceamento que a empresa vai fazer entre a proteção de dados e o interesse legítimo?

REQUISITOS PARA O TRATAMENTO – Art 7º

- X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. GDPR não trouxe limite de atuação.
- **Cadastro Positivo?** A súmula 550 do STJ – Score de Crédito não é considerado banco de dados – acredito que pode ser revisto o entendimento, pois o entendimento entra em conflito com a nova lei.
- **Súmula 550 STJ** – A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. (Súmula 550, SEGUNDA SEÇÃO, julgado em 14/10/2015, DJe 19/10/2015)

CADASTRO POSITIVO

- Lei Complementar 166/2019 modificou diversos artigos da lei 105/2011 e 12.414/2011, permitindo o tratamento e transferência de dados para a “proteção” do crédito, com o cadastro positivo.

TRATAMENTO

Tratamento (art 5º inc X) – 20 verbos

- coleta,
- produção,
- recepção,
- classificação,
- utilização,
- acesso,
- reprodução,
- transmissão,
- distribuição,
- processamento,
- arquivamento,
- armazenamento,
- eliminação,
- avaliação ou controle da informação,
- modificação,
- comunicação,
- transferência,
- difusão
- extração

em essência, qualquer forma de trabalho com informações identificadas ou identificáveis é considerado como Tratamento.

PARTICULARIDADES NO TRATAMENTO

- Menores – consentimento deverá ser dado em destaque e em específico de, pelo menos, um pai ou responsável
- IMPORTANTE - § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

TERMINO DO TRATAMENTO

- Ocorre nas seguintes hipóteses:
- I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- II – fim do período de tratamento;
- III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
- IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

- Depois de terminado o tratamento, os dados deverão ser eliminados, salvo se forem necessários para:
- I – cumprimento de obrigação legal ou regulatória pelo controlador;
- II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

DIREITOS DOS TITULARES

- a pessoa titular dos direitos é, **SEMPRE** titular, independentemente de autorização para tratamento.
- *Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.*

DIREITOS DOS TITULARES

- Art 18 – os titulares tem direito de requerer dos controladores:
- I - confirmação da existência de tratamento (**simples – imediatamente;**
declaração completa – 15 dias);
- 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;
- V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
- 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.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

- Permitida, via de regra, para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

TRANSFERÊNCIA INTERNACIONAL DE DADOS

- Quando não for o caso, nos seguintes casos (mesma lógica dos princípios):
- II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei;
- III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
- IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- V - quando a autoridade nacional autorizar a transferência;
- VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
- VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;
- IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

AGENTES

- Controlador (art 5º, VI) – define quais serão as políticas e elabora relatório conforme requerimento pela ANPD. Pessoa Física ou Jurídica.
- Operador (art 5º, VII) – realiza atividades de tratamento de acordo com as diretrizes determinadas pelo Controlador. Pessoa Física ou Jurídica.

AGENTES

- Encarregado/**DPO – Data Protection Officer** (art 5º, VIII) – atua como canal de comunicação entre o controlador, titulares de dados e a ANPD. Indicado pelo Controlador. PJ e PF. Precisa de certificação.
- Atribuições do encarregado:
 - I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
 - II - receber comunicações da autoridade nacional e adotar providências;
 - III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
 - IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

RESPONSABILIDADE

- Somente será caracterizado dano responsabilizável se o vazamento trouxer riscos ou prejuízos aos titulares.
- A responsabilidade de controlador e operador envolvido é, via de regra, solidária (ou seja, todos respondem). O ressarcimento pelo dano **NÃO ISENTA** a empresa do pagamento da multa pela(s) infração(ões).
- O tema ainda será regulado pela ANPD.

FISCALIZAÇÃO E CRIAÇÃO DA ANPD

- Agência Nacional de Proteção de Dados, por enquanto, foi criada apenas na Medida Provisória 869/18 (ainda não convertida em lei)*.
- Ela será vinculada, diretamente, à Presidência da República (não vinculada a qualquer Ministério), e terá autonomia técnica.

ATRIBUIÇÕES DA ANPD – **16 NO TOTAL**

- I - zelar pela proteção dos dados pessoais;
- **II - editar normas e procedimentos sobre a proteção de dados pessoais;**
- III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos;
- **IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais;**
- V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei;
- **VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;**

ATRIBUIÇÕES DA ANPD

- VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
- VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal;
- IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança;
- X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores;
- XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

ATRIBUIÇÕES DA ANPD

- XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD;
- XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; (Incluído pela Medida
- XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
- XVI - elaborar relatórios de gestão anuais acerca de suas atividades.

SEGURANÇA

- Caso haja algum problema, é dever da empresa, na pessoa do Controlador, informar o órgão competente quanto ao vazamento, apresentando relatório com as seguintes informações:
- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
- A ANPD pode requerer, ainda, que a empresa proceda com a divulgação de forma ampla do evento, bem como a adoção de medidas necessárias para mitigar os danos.

SANÇÕES

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até **2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;**
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - **publicização da infração** após devidamente apurada e confirmada a sua ocorrência (mostrar site do TST como exemplo);
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;

SANÇÕES *

- X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador;
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

SANÇÕES

- Para o cálculo da sanção, serão avaliados os seguintes critérios:
- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
- IX - a adoção de política de boas práticas e governança;
- X - a pronta adoção de medidas corretivas; e
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

SEGURANÇA E BOAS PRÁTICAS

- A empresa, através dos controladores e operadores, deverá desenvolver uma política de governança de proteção de dados, bem como demonstrar sua efetividade perante a ANPD, se assim for requerido.
- Criar a política não é o problema, a lei traz o roteiro do que deve compor a política (art 50, §2º, inc I). No entanto, o cumprimento pode significar problemas.

SEGURANÇA E BOAS PRÁTICAS

Pessoas, de forma até contraditória, são o elo fraco e forte da relação. Elo fraco tendo em vista que o vazamento ocorre por pessoas. Seja uma invasão, seja roubo de informações, seja mesmo uma cópia não autorizada de arquivos. No entanto, um time engajado pode realmente mitigar quaisquer desses problemas, como em todas as áreas da empresa.

Um time engajado não exporá os dados em atividades de risco, não copiará dados, não procederá com vazamento de informações, entre outras questões.

SEGURANÇA E BOAS PRÁTICAS –

Conceitos GDPR – Art. 25

Privacy by design – produto/aplicação/banco de dados criados com o propósito de guardarem o mínimo possível de dados, pelo mínimo possível de tempo, anonimizando ao máximo os dados fornecidos.

Privacy by default – por padrão, dados pessoais não devem ser acessíveis sem a intervenção pessoal do usuário no produto/aplicação.

SEGURANÇA E BOAS PRÁTICAS –

Conceito GDPR – Art. 30

Tracking by design – possibilidade de rastreamento de qualquer ato realizado manipulando dados. Sempre que proceder com o desenvolvimento da solução, é importante pensar na rastreabilidade de acesso, mesmo que seja do próprio algoritmo.

SEGURANÇA E BOAS PRÁTICAS

Além disso, importante permitir uma rota de fuga relativamente fácil, para facilitar o monitoramento de vazamento, já que é mais fácil monitorar uma rota óbvia do que a monitorar possíveis e criativas novas formas de vazamento de informação.

“Arte da Guerra – o inimigo sem saída luta até a morte.”

CONCLUSÃO

notícia ruim...

a depender da estrutura do seu banco de dados atual, pode ser mais fácil construir um novo banco de dados do que adaptar o antigo com as informações não necessárias.

Por isso, a fim de atender a lei, será importante a nova aquisição de informações, sempre requerendo o consentimento.

Isso significa **novos contratos**, **nova estrutura de consentimento**, **novos padrões de segurança e trabalho**, entre tantas outras novas práticas.

CONCLUSÃO

Tratar TODAS as informações como SENSÍVEIS trará confiança ao cliente e aos empregados, bem como a todos os stakeholders da empresa.

Isso gera confiança e valor ao cliente, bem como dos empregados.

DICAS

Dica #1 – tenha somente o necessário, pelo quanto for necessário. Menos dados significa uma base mais enxuta, sendo mais fácil a proteção.

DICAS

Dica #2 – a necessidade de proteção deve ser traduzida para toda a empresa. É necessário envolver todas as áreas necessárias desde o início, de forma legítima e engajada. Não adianta o TI se preocupar em proteger dados se o setor de vendas age de forma imprudente com as informações da empresa.

DICAS

Dica #3 – sempre tenha uma rota óbvia e de fácil de monitoramento, a fim de encontrar vazamentos de forma mais eficiente.

DICAS


Dica #4 – Faça sempre treinamentos e simulações de Cyberataques e vazamentos.

DICAS

Dica #5 – Privacidade e Segurança JÁ SÃO
diferenciais competitivos.

CONTATOS

 Roberto Crespo

 Av. Paulista, 37 – 4º Andar – Ed. Parque Cultural Paulista. São Paulo – SP.

 +55 11 2246-2810

 +55 11 98083-3028

 robertocrespo.adv@gmail.com