Photo by ckturistando on Unsplash

BRASIL

Lei de Proteção de Dados Pessoais

Resumo Conceitual

Prof. Ms. Edison Fontes, CISM, CISA, CRISC

Controles de informação exigidos para a conformidade da organização com a Lei de Proteção de Dados Pessoais – Lei No. 13.709, de 14 de Agosto de 2018, Publicada no Diário Oficial da União, Brasil, em 15 de Agosto de 2018.

DOC ELGF.0104.01.1

São Paulo, setembro, 2018 - Brasil

Licença para uso deste documento

Este documento

Este documento tem por objetivo descrever de maneira objetiva, simples e resumida os principais controles que uma organização precisa implementar e garantir o seu funcionamento, para estar em conformidade com a Lei de Proteção de Dados Pessoais – Lei No. 13.709, de 14 de Agosto de 2018, Publicada no Diário Oficial da União, Brasil, em 15 de Agosto de 2018.

É dado ênfase aos controles relacionados às organizações privadas. Não destacamos as diversas situações de exceções descritas nesta lei.

Este documento expõe a opinião pessoal do autor, considerando as informações disponíveis neste momento.

Este documento não é suficiente para a implementação de todos os controles para a Proteção de Dados Pessoais exigidos pela legislação brasileira. Para a implementação destes controles o leitor deve ler por completo o texto da Lei de Proteção de Dados Pessoais Brasil e das demais leis brasileiras relacionadas a informação, Internet, direito do consumidor e similares.

Técnica e muito cuidado foram utilizados na elaboração deste documento. Porém erros podem acontecer, tipo digitação ou versão original incorreta. Qualquer erro encontrado, qualquer dúvida de interpretação, solicitamos que seja enviada uma mensagem para edison@pobox.com para a devida verificação e resposta. O autor não assume qualquer responsabilidade por eventuais danos ou perdas a pessoas, organizações ou bens, originados do uso deste documento. Este documento é conceitual e didático sobre os temas apresentados.

O Autor

Edison Fontes é Mestre em Tecnologia, certificado internacional CISA, CISM, CRISC e profissional de segurança da informação. É professor de MBAs, autor de livros e desenvolve atividades de:

Estrategista, Gestor, Consultor em Segurança Informação, Proteção de Dados Pessoais, Continuidade de Negócio, Risco Operacional, Conformidade *(Compliance)* da Informação e Combate à Fraude de Informação.

Como profissional já desenvolveu trabalhos para várias organizações privadas e organizações públicas, dos mais diversos portes e tipos de negócio. Desenvolveu normativos que foram transformados em lei em Estado membro da Comunidade de Países de Língua Portuguesa.

Participa das entidades ou grupos profissionais:

ABSEG – Associação Brasileira de Profissionais de Segurança.

ACFE - Association of Certified Fraud Examiners.

FIESP – Grupo de Estudo Direito Digital e Compliance.

ISACA – Information Systems Audit and Control Association.

OAB – Comissão de Direito Digital e Compliance.

É sócio consultor da Núcleo Consultoria em Segurança

Contato: edison@pobox.com, ef@nucleoconsult.com.br

A Lei de Proteção de Dados Pessoais do Brasil foi aprovada pelo Congresso Nacional no mês de julho e sancionada pelo Presidente da República em 14 de agosto de 2018. Foi publicada no Diário Oficial da União em 15 de agosto de 2018. Os controles exigidos por esta lei entrarão em vigor decorridos 18 (dezoito) meses de sua publicação oficial.

Esta lei dispõe sobre o tratamento de dados pessoais de pessoa natural. Este tratamento pode ser realizado por outra pessoa natural ou por pessoa jurídica de direito público ou privado.

Seu objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

(Apresentação, Art. 1)

Photo by Rafaela Biazi on Unsplash

INTRODUÇÃO

Com esta lei o Brasil se posiciona como um Estado que deseja proteger os dados pessoais das pessoas naturais localizadas no seu território nacional.

Há muitos anos o Brasil já carecia de uma legislação para este tipo de proteção. Apesar da existência de algumas leis que perifericamente tratam da proteção da informação ou que protegem a informação para alguns segmentos de mercado, não existia um regulamento legal tratando como tema central: proteção de dados pessoais, independentemente do local onde se localizam os dados, do tipo de usuário, do segmento de negócio ou do tipo de organização. Esta lei protege a pessoa natural localizada no Brasil quando a coleta de dados for realizada no território nacional. (Art. 3)

Esta lei, principalmente os controles para o tratamento da informação, se baseia no regulamento da União Europeia, GDPR – General Data Protection Regulation, que entrou em vigor em 25 de maio de 2018.

Este tema, transformado em lei, afeta a todas as organizações que atuam no Brasil, independente do seu porte, do seu tipo de negócio e da sua origem acionista. Todos os gestores de organizações deverão entender os direcionadores desta legislação e exigir que os controles exigidos na mesma, sejam implementados nas suas organizações, tendo a sabedoria profissional de adequar a implementação às características de cada uma.

Para facilitar, apresento neste documento as principais diretrizes que você como executivo, gestor ou profissional de uma organização precisa conhecer e avaliar como a sua organização está tratando este tema.

DIRECIONADOR DOS CONTROLES DE PROTEÇÃO

(Art. 1, Art. 2, Art. 17)

O principal direcionador desta legislação **é a proteção do tratamento de dados pessoais de pessoa natural,** também denominada**, pessoa singular.**

Seu objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural,

> ***Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos de liberdade, de intimidade e de privacidade***.
>
> *(Art. 17.)*

Para esta lei, a proteção de dados pessoais tem como fundamentos:

- o respeito a privacidade;
- a autodeterminação informativa;
- a liberdade de expressão, de informação, de comunicação e de opinião;
- a inviolabilidade de intimidade, da honra e da imagem;
- o desenvolvimento econômico e tecnológico e a inovação;
- a livre iniciativa, a livre concorrência e a defesa do consumidor;
- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Photo by William on Unsplash

Dado Pessoal
é uma informação ou um conjunto de informação relacionada a pessoal natural identificada ou identificável.
(Art. 5º)

Photo by Sara Aho on Unsplash

Pessoa Natural ou Pessoa Singular
é uma pessoa que possa ser especificada, diretamente ou indiretamente, por um dado pessoal.

Exemplo de dado pessoal:
nome, CPF, localização, preferências, perfil comportamental.

Pessoa Natural: é o Titular dos seus dados pessoais. (Art. 17.)

Controlador: realiza o tratamento dos dados pessoais. (Art. 5º.)

Dado Pessoal Sensível: é o dado pessoal referente origem étnica, convicção religiosa, opinião política, religião, filosofia de vida, saúde, genética, biometria, quando vinculado a pessoa natural. (Art. 5º.)

Operador: realiza atividades em nome do Controlador. (Art. 5º.)

Tratamento: qualquer operação realizada com dados pessoais. (Art. 5º)

PRINCIPAIS CONTROLES LEI PROTEÇÃO DADOS PESSOAIS

Descrevo a seguir, de uma maneira estruturada, consolidada e resumida, os princípios (obrigações) que as atividades de tratamento de dados pessoais devem obrigatoriamente seguir.

Lembro que este documento não deve substituir a leitura completa de todo o regulamento.

Photo by Fancycrave on Unsplash

1. Aplicação

(Art.3)

Esta Lei aplica-se a qualquer tratamento realizado em dados pessoais de pessoa natural:

a. Independente se realizado por outra pessoa natural, por pessoa jurídica de direito público ou privado.

b. Independente do país sede da pessoa jurídica.

c. Independente do país onde estejam localizados os dados.

Desde que aconteça uma das condições:

a. O tratamento dos dados pessoais seja realizado no território nacional.

b. O tratamento tenha por objetivo a oferta ou o oferecimento de bens ou serviços para indivíduos localizados no Brasil.

c. Os dados pessoais tenham sido coletados quando o Titular se encontre no território nacional no momento da coleta.

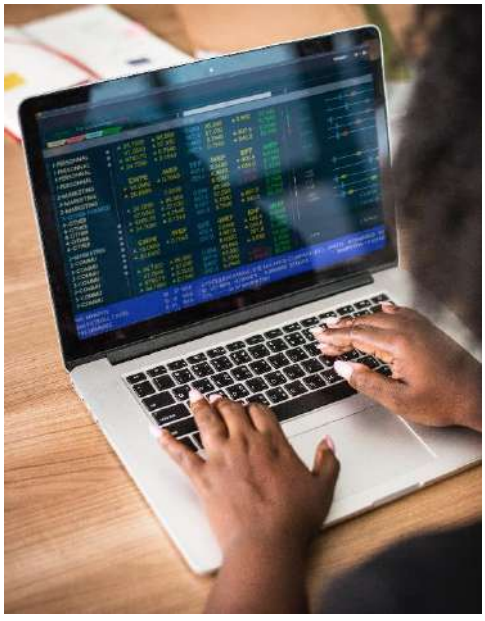


Photo by rawpixel on Unsplash

2. Requisitos para Tratamento de Dados Pessoais

(Art.7)

Para tratamento de dados pessoais é necessário a existência de pelo menos uma das situações descritas abaixo:

a. Fornecimento de consentimento pelo Titular.

b. Obrigação legal ou regulatória pelo Controlador.

c. Execução de políticas públicas previstas em lei ou respaldados em contratos.

d. Estudos por Órgãos de Pesquisas

e. Execução de Contrato ou Diligências pré-contratuais

f. Exercício Regular de Direitos

g. Proteção da vida

h. Tutela da saúde.

i. Interesses legítimos do controlador.

j. Proteção ao crédito

Photo by Florian Pérennès on Unsplash

3. Direitos do Titular

(Art.18, Art. 20, Art. 9, Art. 42)

O Titular tem o direito de obter em relação aos seus dados pessoais:

a. Confirmação da existência de tratamento.

b. Acesso aos dados.

c. Correção de dados incompletos, inexatos ou desatualizados.

d. Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos.

e. Portabilidade dos dados para outro fornecedor de serviço ou produto.

f. Eliminação dos dados pessoais tratados com o consentimento do titular, considerando as exceções descritas nesta Lei.

g. Informações das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados.

h. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

i. Revogação do consentimento, considerando os casos previstos nesta lei.

j. Opor-se ao tratamento realizado, em caso de descumprimento desta Lei.

k. Solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais que afetem seus interesses, inclusive na definição de seu perfil pessoal.

l. Ter acesso facilitado às informações sobre o tratamento de seus dados que deverão ser disponibilizados de forma clara e adequada, respeitando o princípio do livre acesso:
- finalidade específica do tratamento;
- forma e duração do tratamento;
- identificação e informações de contato do Controlador;
- informações acerca de compartilhamento de dados;
- responsabilidades dos agentes que realizarão o tratamento.

m. Receber do juiz a inversão do ônus da prova a seu favor, quando houver hipossuficiência para fins de produção de prova ou quando a produção de prova lhe for excessivamente onerosa.

4. Consentimento do Titular

(Art. 8)

O consentimento do Titular deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do Titular.

Cabe ao Controlador o ônus da prova de que o consentimento foi obtido em conformidade com esta Lei.

O consentimento não pode ter vício, deve se referir a finalidades determinadas e não podem haver autorizações genéricas.

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do Titular, por procedimento gratuito e de fácil uso.

Podemos simplificar afirmando de maneira simples: “Vai coletar dados pessoais de uma pessoa singular? Tem que ter base legal e no pedido de consentimento deve-se pedir formalmente de maneira correta!”

Photo by Cytonn Photography on Unsplash

5. Uso com finalidade específica

(Art.6.)

A coleta de dado pessoal obrigatoriamente tem que indicar qual será o uso que o Controlador fará com esta informação. Não se pode coletar dados pessoais para futuros usos. É obrigatório que o objetivo da coleta dos dados seja informado explicitamente ao Titular. O uso dos dados somente pode acontecer para o objetivo pré-definido.

A informação coletada deve ter uso específico, legítimo, explícito, informada ao titular, sem incompatibilidade com a finalidade.

Photo Valentin on Unsplash

6. Tempo de tratamento

(Art. 16)

Os dados pessoais devem ser eliminados após o término de seu tratamento, isto é, quando a finalidade do tratamento foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

A Lei prevê situações específicas para a continuidade dos dados pessoais, como por exemplo:

- cumprimento de obrigação legal;

- estudo por órgão de pesquisa garantida, sempre que possível, a anonimização;

- uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

7. A Coleta deve ser mínima e adequada (Necessidade)

(Art.6)

A coleta dos dados pessoais deve conter exclusivamente os dados necessários para atender a finalidade específica. Não é permitido coletar dados excessivos em relação às finalidades do tratamento para a finalidade definida.

Deve haver compatibilidade do tratamento dos dados pessoais com as finalidades informadas ao Titular.

8. Livre acesso pelos Titulares

(Art. 6)

Os Titulares de dados pessoais devem ter garantidos os seguintes direitos:

a. A consulta facilitada e gratuita sobre a forma e a duração do tratamento.

b. A exatidão, a clareza, a relevância, e a atualização dos dados para o cumprimento da finalidade de tratamento.

c. Informações claras, precisas e facilmente acessíveis sobre a realização do tratamento os respectivos agentes de tratamento.

9. Adequação

(Art. 6)

Deve haver compatibilidade do tratamento realizado no dado pessoal com as finalidades informadas ao titular.

(Foto: unsplash.com, sem reservas)

10. Gestão de segurança pelo Controlador e Operador

(Art. 37, Art. 43, Art. 46)

O Controlador e o Operador de dados pessoais devem garantir a existência dos seguintes controles:

a. Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e de eventos acidentais ou eventos ilícitos de destruição, perda, alteração, comunicação ou difusão.

b. Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

c. Não realização do tratamento para fins discriminatórios ilícitos e abusivos.

d. Demonstração de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e eficácia dessas medidas.

e. Manter registro das operações de tratamento de dados pessoais que realizarem.

f. Estar apto a elaborar o relatório de impacto à proteção de dados pessoais referente às suas operações de tratamento de dados.

g. Observar e cumprir a legislação.

h. Fornecer a segurança adequada que o titular dos dados pode esperar, considerando:
- o modo pelo qual o tratamento é realizado;
- o resultado e os riscos que razoavelmente se esperam do tratamento;
- as técnicas de tratamento disponíveis à época que foi realizado.

i. Responder pelos danos decorrentes da violação de segurança dos dados pessoais, ao deixarem de adotar as medidas de segurança previstos nesta lei.

j. Adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de eventos acidentais ou ilícitos de destruição, preda alteração, comunicação ou difusão ou qualquer outra ocorrência decorrente de tratamento inadequado ou ilícito.

11. Estruturação da segurança dos dados pessoais

(Art. 49, Art. 50)

Para o adequado cumprimento dos controles exigidos nesta Lei e nos demais normativos de segurança da informação:

a. Os dados pessoais devem ter uma estruturação técnica de maneira a facilitar a sua proteção e sua rastreabilidade

b. As medidas de segurança devem ser consideradas pelo Controlador ou pelo Operador desde a fase de concepção do produto ou serviço até a sua execução.

c. A segurança da informação prevista na legislação referente à dados pessoais, deve ser garantida mesmo após o término do tratamento.

d. Os sistemas devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas, às diretrizes de governança e aos controles exigidos nesta Lei ou outra legislação ou regulamento relacionado a dados pessoais.

Photo by Dawn Armfield on Unsplash

12. Comunicação de incidentes de dados

(Art. 48º.)

A organização deverá comunicar à Autoridade Nacional e ao Titular a ocorrência de incidentes de segurança que possa acarretar risco ou dano relevante aos Titular.

A comunicação deverá acontecer em prazo razoável e deverá mencionar no mínimo:

a. a descrição dos dados pessoais afetados;

b. as informações sobre os titulares envolvidos;

c. as medidas técnicas e de segurança utilizadas para a proteção dos dados, considerando os segredos comercial e industrial;

d. os riscos relacionados ao incidente;

e. os motivos da demora caso o comunicado não seja imediato;

f. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente;

g. Considerar a necessidade da divulgação do fato em meios de comunicação. A Autoridade Nacional poderá exigir esta comunicação.

(Foto: unsplash.com, sem reservas)

13. Anonimização dos dados

(Art. 12)

Sempre que for possível e coerente com os objetivos do negócio, a organização deve Anonimizar os dados pessoais coletados e desta maneira diminuir seu risco no tratamento a ser realizado.

Os dados anonimizados não serão considerados dados pessoais. Exceto quando o processo de anonimização ao qual foram submetidos permita ser revertido, utilizando meios próprios ou com esforços razoáveis, considerando esforço, tempo e complexidade técnica.

(Foto: unsplash.com, sem reservas)

14. Governança de Privacidade para Dados Pessoais

(Art. 50º.)

A organização deve definir regras de boas práticas e de governança que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e outras medidas relacionadas ao tratamento de dados pessoais.

Ao definir a Governança da Privacidade para Dados Pessoais, a organização deve considerar para a sua estrutura:

a. A natureza, o escopo, a finalidade do tratamento.

b. Os riscos de situações que comprometam a proteção dos dados.

c. A efetividade das contramedidas implementadas.

d. A estrutura, escala e volume das operações de tratamento.

e. A sensibilidade dos dados.

f. A gravidade dos danos para os titulares dos dados tratados.

A Governança da Privacidade para Dados Pessoais deve contemplar na sua abrangência e deve ser implementada de maneira que no mínimo:

a. Demonstre o comprometimento da organização em adotar processos e políticas internas que assegurem o cumprimento dos controles relativos à proteção de dados pessoais.

b. Seja aplicável em todo o conjunto de dados pessoais que estejam sob sua responsabilidade.

c. Estabeleça um processo de avaliação sistemática de impactos e riscos à privacidade.

d. Construa uma relação de confiança com o titular por meio de uma atuação transparente que lhe assegure mecanismos de participação.

e. Esteja integrado à governança corporativa e possua mecanismos de supervisão internos e externos.

f. Conte com plano de resposta de incidentes e de remediação;

g. Seja atualizado constantemente em função monitoramento contínuo e avaliações periódicas.

A Governança da Privacidade para Dados Pessoais pode ser questionada pela Autoridade Nacional ou de outras entidades que sejam responsáveis por promover o cumprimento desta Lei.

As regras de governança deverão ser publicadas e atualizadas periodicamente e poderão verificadas pela Autoridade Nacional.

Photo by Patrick Tomasso on Unsplash

15. Transferência internacional de dados

(Art. 33)

A transferência internacional de dados pessoais somente é permitida:

a. Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei.

b. 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.

c. Quando necessária à cooperação jurídica internacional entre órgãos públicos de inteligência ou similar, em cumprimento ao direito internacional.

d. Quando necessário à proteção da vida ou salvaguarda física do Titular ou de terceiros.

e. Quando autorizada pela Autoridade Nacional.

f. Quando de acordo de cooperação internacional.

g. Para a execução de política pública.

h. Quando o Titular tiver fornecido consentimento específico.

Photo by kazuend on Unsplash

16. Tratamento Dados Pessoais Crianças e Adolescentes

(Art. 14)

O tratamento de dados pessoais de crianças e adolescentes somente poderá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

O Controlador deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e a garantia de cumprimento da Lei.

Poderão ser coletados dados pessoais de crianças sem o consentimento exigido neste artigo, quando a coleta for necessária para contatar os pais ou responsável legal.

As informações deverão ser fornecidas de maneira simples, clara e acessível.

Photo by Kelly Sikkema on Unsplash

17. Encarregado pelo Tratamento de Dados Pessoais

(Art. 41)

A empresa deve ter um profissional para exercer as funções de Encarregado pelo Tratamento de Dados Pessoais. A identidade e informações para contato deste encarregado deverão ser divulgadas publicamente e de maneira clara e objetiva.

Este profissional tem as seguintes principais responsabilidades:

a. Orientar os funcionários e os contratados da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

b. Receber reclamações e comunicações de titulares, prestar esclarecimento e adotar providencias.

c. Receber comunicações da Autoridade Nacional e adotar providências.

A Autoridade Nacional definirá regras complementares sobre este encarregado, inclusive sua definição, suas atribuições, e hipótese de dispensa de sua indicação.

A Lei não define, porém recomendamos, seguindo o GDPR da União Europeia que este profissional deve ter posição hierárquica adequada e sem gerar conflito de interesse.

Photo by Form on Unsplash

18. Documento Impacto à Proteção de Dados Pessoais

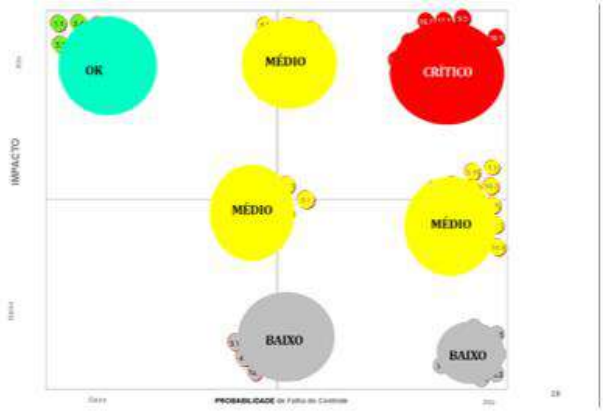
(Art. 10, Art. 38)

A empresa deve ter no seu conjunto de Controles Corporativos, a Avaliação de Impacto à Proteção de Dados Pessoais. Este mapeamento deve ser apresentado para o corpo diretivo da organização para que os executivos tomem conhecimento dos possíveis impactos para a empresa, em função de vulnerabilidades e tratamento não adequado dos dados pessoais.

Este documento deve conter no mínimo a descrição dos processos de tratamento de dados pessoais (coleta, armazenamento, processamento, compartilhamento) que podem gerar riscos às liberdades civis e aos direitos fundamentais.

Esta avaliação e documentação também serão utilizados como evidências de uma gestão adequada de proteção de dados pessoais pela organização, para a Autoridade Nacional.

Photo by rawpixel on Unsplash



19. Penalidades

(Art. 42 e Art. 52.)

O Controlador ou Operador que, em razão do exercício da atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado à repará-lo.

Os agentes de tratamento de dados pessoais estão sujeitos as seguintes principais penalidades:

a. Advertência.

b. Multa por infração de até 2% (dois por cento) do faturamento no seu último exercício da pessoa jurídica de direito privado, grupo ou conglomerado excluídos os tributos, limitada, no total a R$ 50.000.000,00 (cinquenta milhões de reais).

c. Multa diária.

d. Publicização da infração.

e. Suspensão parcial ou total do funcionamento do banco de dados pelo período máximo de seis meses, renovável.

f. Suspensão por período de seis meses, renováveis, do exercício da atividade de tratamento dos dados pessoais.

g. Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais.

A penalização será proporcional à gravidade e à natureza das infrações e dos direitos pessoais afetados, considerando as ações da organização, em especial a existência de mecanismos e procedimentos internos para o tratamento seguro de dados e controles para a minimização do dano.

(Foto: unsplash.com, sem reservas)

20. Autoridade Nacional de Proteção de Dados e o Conselho de Proteção de Dados Pessoais e da Privacidade

Vetado pelo Presidente da república em função de que o Congresso Nacional não pode criar órgão no Poder Executivo.

Photo by Sanwal Deen on Unsplash

21. Política de Dados Pessoais

(Art. 50)

Considerando a importância da proteção de dados pessoais, é recomendável que a empresa possua uma política específica para este tema. No nosso entendimento este documento deve ser assinado pela presidência da organização ou aprovado pelo conselho de administração.

Esta política deve:

a. Demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento da proteção de dados pessoais.
b. Ser aplicável a todo o conjunto de dados pessoais sob o controle da organização.
c. Ser adaptável à estrutura, à escala e volume de suas operações.
d. Garantir a avaliação sistemática de impactos e riscos à privacidade.
e. Estabelecer uma relação de confiança com o titular.
f. Estar integrado à estrutura de governança.
g. Contar com planos de resposta de incidentes e remediação.
h. Ser atualizada constantemente.

(Foto: unsplash.com, sem reservas)

22. Direito ao esquecimento

(Art. 15, Art.16)

Os dados pessoais serão eliminados após o término de seu tratamento, exceto quando de cumprimento de obrigação legal/regulatória e outras situações específicas descritas nesta lei.

A pessoa singular tem o direito de solicitar que seus dados sejam apagados, quando não forem relevantes para as motivações que coletaram estes dados inicialmente. Porém é definido que o interesse público na disponibilidade dos dados deverá ser considerado para o atendimento destas solicitações.

Ao consultar buscadores estes dados não apareceriam.

(Foto: unsplash.com, sem reservas)

23. Fora da abrangência – Esta lei não se aplica

(Art. 4)

Esta lei não se aplica ao tratamento de dados pessoais, sempre considerando os controles exigidos nesta lei:

a. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos.

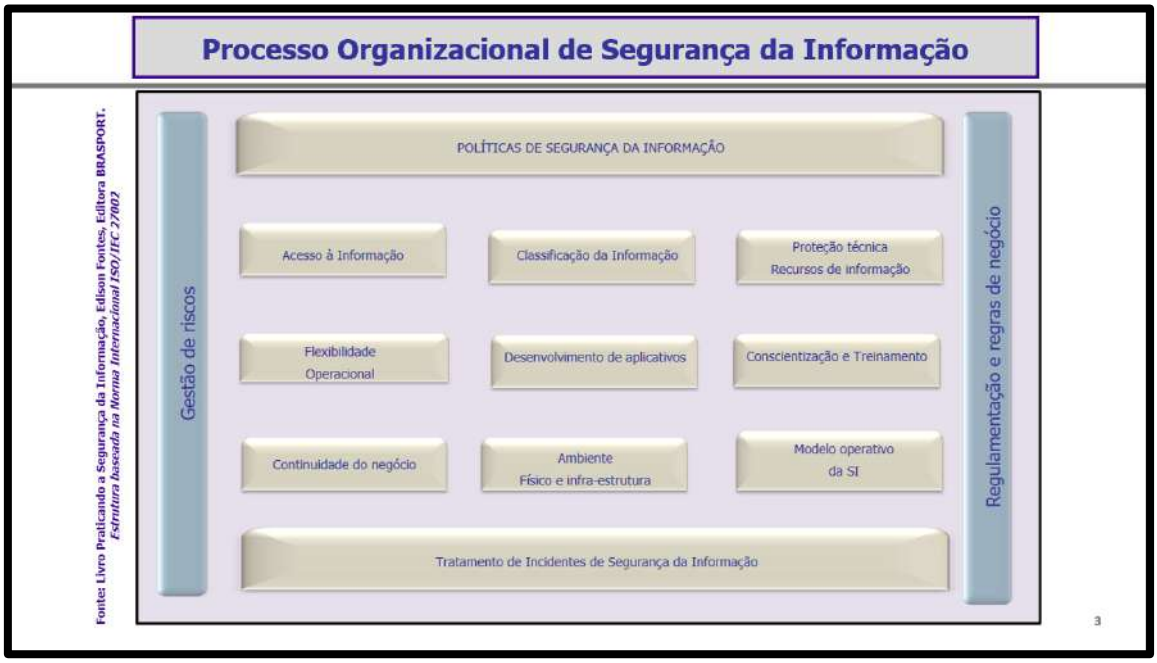
b. Realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos.

c. Realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, provenientes de fora do território nacional que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros.

PROCESSO ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

O Processo Organizacional de Segurança da Informação define em suas dimensões, macrocontroles que possibilitam que os requisitos exigidos pelo GDPR sejam considerados.

Segue abaixo a estrutura do Processo Organizacional de Segurança da Informação, baseado na Norma ISO/IEC 27002:2013, apresentando as suas dimensões.



Fonte: Livro Praticando a Segurança da Informação, Edison Fontes, Editora BRASPORT.
Estrutura baseada na Norma Internacional ISO/IEC 27002

Segue abaixo um quadro controle indicando os requisitos da Lei de Proteção de Dados Pessoais, do Brasil, Lei 13.709, de 14 de agosto de 2018 e as Dimensões de Segurança da Informação, considerando a estrutura deste documento, que devem ter controles definidos para atendimento específicos destes requisitos.

BRASIL LPDP - Lei de Proteção de Dados Pessoais, Lei 13.709, de 14 de agosto de 2018. Edison Fontes, 2018	DIMENSÕES E CONTROLES DE SEGURANÇA DA INFORMAÇÃO													
	Política e regulamentos de S.I.	Acesso/uso informação	Classificação Informação	Proteção Técnica	Flexibilidade Operacional (Inc. Prob. Mud.)	Desenvolv. Aplicativos (Seguro)	Continuidade Negócio	Cópias de Segurança	Gestão de Riscos Informação	Treinamento e Conscientização	Ambiente Físico	Criptografia	Prestadores Serviço	Processo Organizacional S.I.
Diretriz: Titularidade dos dados pessoais	x	x	x						x	x		x	x	
1. Aplicação e abrangência da lei	x		x										x	
2. Requisitos para tratamento dados pessoais	x	x												
3. Direitos do Titular	x	x	x	x		x	x	x	x			x	x	
4. Consentimento do Titular	x	x	x	x		x		x	x			x		
5. Uso com finalidade especifica	x			x		x		x	x					
6. Tempo de tratamento	x			x		x		x	x			x	x	
7. Coleta minima e adequada	x	x						x	x					
8. Livre acesso pelos Titulares	x	x		x		x		x	x				x	
9. Adequação	x	x						x					x	
10. Gestão segurança pelo Controlador	x	x	x	x	x	x	x	x	x	x	x	x	x	x
11. Estruturação da segurança dados pessoais		x		x	x	x	x	x		x			x	
12. Comunicação de incidentes	x			x	x		x		x	x			x	
13. Anonimização de dados	x	x		x		x						x		
14. Governança privacidade de dados pessoais	x	x	x	x		x				x			x	x
15. Transferencia internacional de dados	x	x	x	x	x			x				x	x	
16. Tratadmento dados crianças e adolescentes	x	x	x	x					x	x				
17. Encarregado tratamento de dados pessoais	x									x				x
18. Impacto proteção de dados pessoais	x								x					x
19. Penalidades	x								x	x				x
20. Autoridade Nacional					x				x					x
21. Política de Dados Pessoais	x								x				x	
22. Direito ao esquecimento	x	x		x		x		x	x				x	
Controles de Segurança	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Frequencia	***21***	***14***	***8***	***13***	***5***	***10***	***4***	***11***	***15***	***8***	***1***	***7***	***13***	***6***

Fonte: Autor.

O quadro acima demonstra que a existência de um efetivo Processo Organizacional de Segurança da Informação e a situação de negócio de que a empresa deve seguir a LPDP, possibilita de uma maneira estruturada a implementação dos controles necessários.

O Processo Organizacional de Segurança da Informação facilita o atendimento aos diversos controles exigidos pelo LPDP. Não só facilita como são obrigatórios para uma adequada proteção dos dados pessoais.

O Processo Organizacional de Segurança da Informação é a base para que a empresa tenha condições de cumprir os controles definidos pela LPDP.

Sem Segurança da Informação não existe cumprimento da Lei de Proteção de Dados Pessoais em vigor no Brasil.

O Processo Organizacional de Segurança da Informação é a base para que a empresa tenha condições de cumprir os controles definidos pela Lei de Proteção de Dados Pessoais – LPDP.

Sem Segurança da Informação não existe o cumprimento da LPDP

CONCLUSÃO

A Lei Brasileira de Proteção de Dados Pessoais afeta a todas as organizações, qualquer que seja o porte ou o tipo de negócio. Evidentemente alguns tipos de negócio possuem uma maior exposição aos controles exigidos pela LPDP. O prazo de dezoito meses para que as organizações s adequem e implementem controles para atender esta lei, é um tempo razoável, desde que a organização implante ou aprimore o seu Processo Organizacional de Segurança da Informação.

Outra questão importante é que com esta lei fica explícito a necessidade da área de negócio e o corpo diretivo da organização participarem e se comprometerem com a segurança da informação, que é muito maior e mais abrangente do que a Ciber Segurança.

Recomendo que comece agora a avaliação dos controles de segurança atuais e a sua maturidade para suportar os controles exigidos pela Lei de Proteção de Dados Pessoais.

Fiquem à vontade para contatar e aprimorarmos a segurança da organização e a conformidade com esta lei.

Edison Fontes, CISM, CISA, CRISC

Sócio Núcleo Consultoria
Estrategista, Consultor e Gestor: Segurança da Informação, Riscos, Continuidade e Combate à Fraude, Compliance.
Coordenador do Comitê de Segurança da Informação da ABSEG.

edison@pobox.com
ef@nucleoconsult.com.br

www.nucleoconsult.com.br