2022

Proteção de dados

MANUAL DE BOAS PRÁTICAS

Parceiro e Fornecedor

Sumário

Sumário

Sumário

1 - Objetivo

Status geral 9%

O Senac Alagoas busca constantemente estar em conformidade com a LGPD e faz parcerias com empresas que detêm esse interesse. Deste modo, este manual objetiva demonstrar os principais conceitos referente a LGPD e esclarecer o papel do fornecedor e dos parceiros mediante a Lei para que seja possível entender quais são as boas práticas que pode ser utilizada para proteger os direitos fundamentais de liberdade e de privacidade do titular dos dados, afinal, o respeito à privacidade é o primeiro fundamento da lei 13.709/2018.

2 - Introdução

Status geral 11%

O tema proteção de dados vinha sendo tratado há muito tempo no Brasil, de forma esparsa, através de regulamentos como o Código Civil e o Código de Defesa do Consumidor. Em julho de 2018, a Lei Federal nº 13.709/2018, mais conhecida como LGPD, foi aprovada por unanimidade pelo Senado e criou um importante marco legal para a proteção de dados no Brasil. A LGPD tem grande influência do regulamento europeu sobre a matéria, o GDPR, e mudou completamente a forma como os dados pessoais são manipulados.

A importância da LGPD está baseada na garantia dos direitos à privacidade e proteção de dados pessoais dos cidadãos, que a cada dia passa a ser mais violado em função das necessidades estratégicas do mercado varejista e dos conglomerados políticos em busca de votos. Dois grandes exemplos dessa violação podem ser vistos no grande número de propagandas indesejadas que recebemos, através da definição de um suposto perfil de consumo e no episódio da Cambridge Analytica nas eleições dos EUA. A lei visa especificamente a proteção dos dados pessoais, que são definidos como qualquer informação que possa levar à identificação de uma pessoa, de maneira direta ou indireta.

2 - Introdução

Status geral 13%

É de extrema importância o completo entendimento do ciclo de vida da informação dentro da empresa, visando a implantação de todos os controles jurídicos e de segurança da informação para adequação à lei. A Figura 1 descreve as fases desse ciclo de acordo com a LGPD.

O que poucos líderes de TI e negócios já perceberam é que seguir as novas condições não é apenas uma questão de se evitar sanções. Na verdade, a LGPD é uma grande oportunidade para que as empresas brasileiras entrem de vez na transformação digital, obtendo grandes vantagens comerciais.

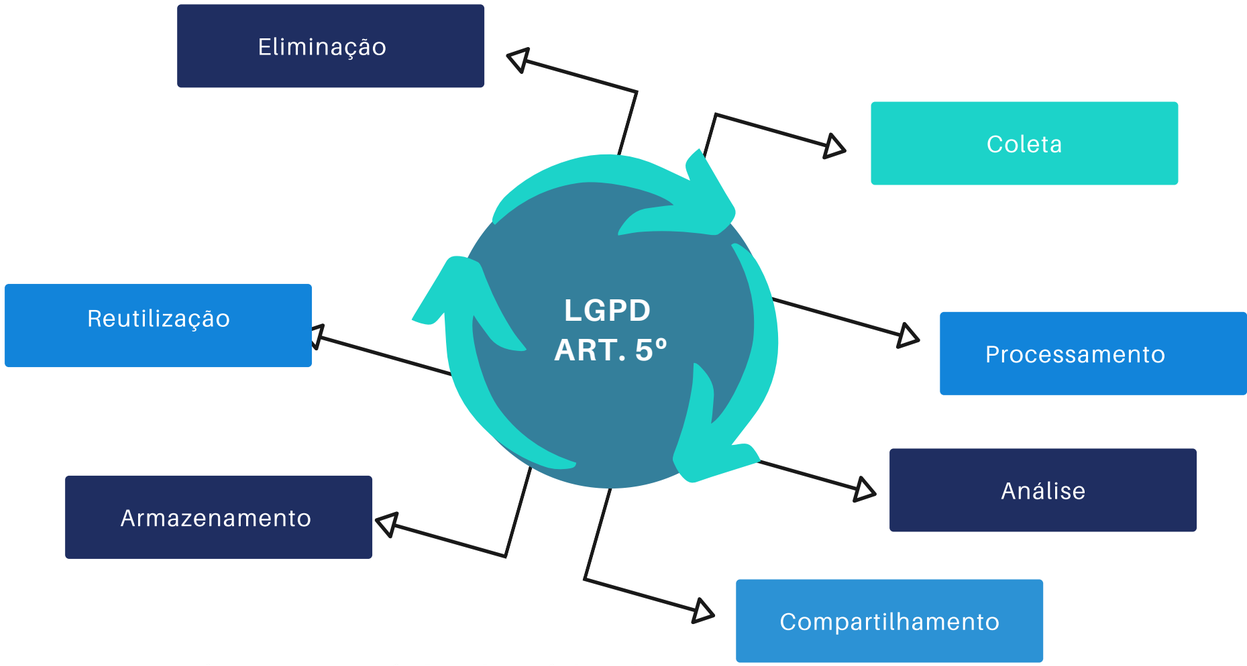


Figura 1 - Ciclo de Vida da Informação

2 - Introdução

Status geral 15%

Como as informações transitam pelos setores da empresa assim como o nosso sangue transita pelos nossos órgãos, é necessário analisar as diversas fontes de dados existentes. A Figura 2 mostra um exemplo do ciclo de vida das informações sob responsabilidade de uma empresa.

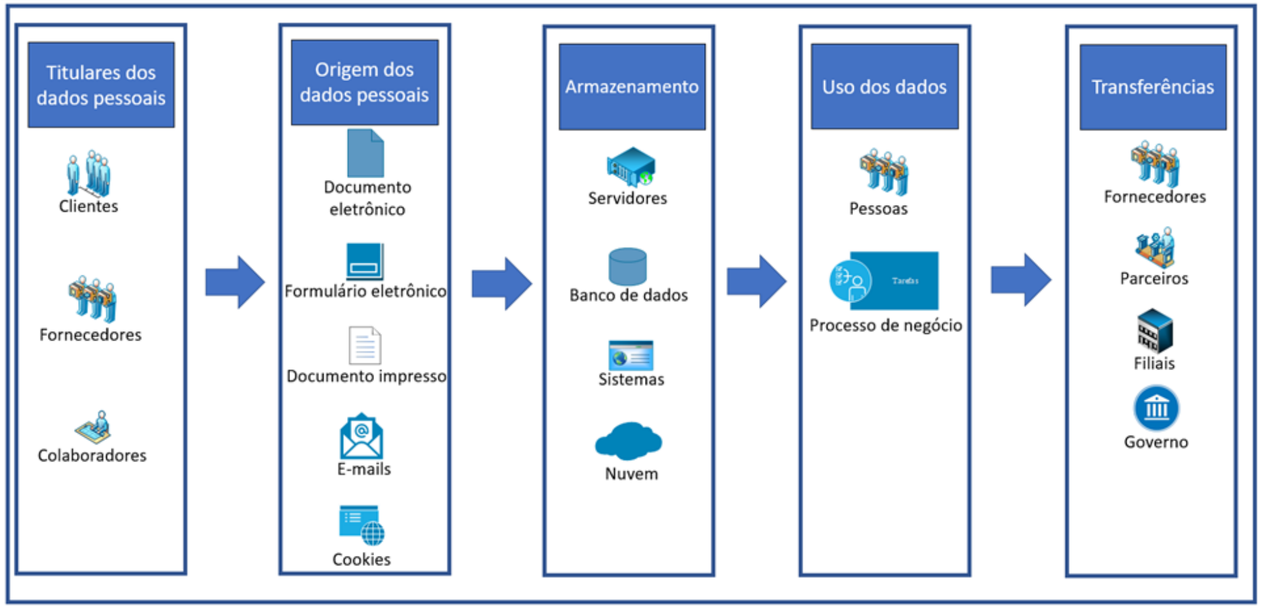


Figura 2 - Ciclo de Vida da Informação

3 – Conceitos gerais LGPD

- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- Dado pessoal sensível: 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;

Definições importantes

3 - Conceitos gerais LGPD

- Titular: 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 ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: 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);
- Agentes de tratamento: o controlador e o operador

Definições importantes

3.1 - Dados Pessoais Sensíveis

Status geral 21%

Um dado sensível contém informações que ninguém gostaria que fossem compartilhadas e que podem causar uma grande exposição tanto na vida social quanto profissional do cidadão.

Essa preocupação com os dados sensíveis advém do fenômeno da publicidade comportamental, utilizada para formação de perfis das pessoas. Os dados sensíveis possibilitam conclusões a respeito de um indivíduo, como por exemplo, a sua orientação sexual, sua religião, alguma doença que possa ter e com essas informações, torna-se muito perigoso que as pessoas venham a ser classificadas de forma preconceituosa, interferindo diretamente em seus direitos e liberdades individuais.

A seguir - As categorias dos dados sensíveis

3.1 - Dados Pessoais Sensíveis

Os dados pessoais sensíveis são regulados pelos artigos 11 a 13 da LGPD. A lei os define no art. 5º, inciso II (1). É o dado pessoal sobre:

Origem racial ou étnica	Convicção religiosa	Opinião política	Dado genético ou biométrico, quando vinculado a uma pessoa natural
Filiação a sindicato ou a organização de caráter religioso	Filosófico ou político	Dado referente à saúde ou à vida sexual	

3.1 - Dados Pessoais Sensíveis

Estas sete categorias de informação são especialmente protegidas pela lei, em busca do atendimento, principalmente, do Princípio da Não-Discriminação. O art. 11 da LGPD define as hipóteses exclusivas que permitem o tratamento desse tipo de dado.

A primeira hipótese é dada pelo consentimento do titular. Esse consentimento, além de seguir as regras gerais do art. 8º, exige forma destacada a respeito dos dados sensíveis, além de mencionar a finalidade específica. Seguem valendo as regras de Boa-fé, Finalidade, vícios de consentimento, entre outras.

No entanto, o processamento de dados sensíveis poderá ser feito sem o consentimento do titular em sete hipóteses:

Em 7 hipóteses:

3.1 - Dados Pessoais Sensíveis

1. Cumprimento de obrigação legal ou regulatória pelo controlador.

2. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.

3. Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

4. 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).

5. Proteção da vida ou da incolumidade física do titular ou de terceiros.

6. Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

7. Garantia da prevenção à fraude e à segurança do titular.

3.2 - Bases legais para tratamento de dados pessoais

Status geral 28%

1. Consentimento
2. Cumprimento de Obrigação Legal
3. Execução de políticas públicas
4. Estudo por Órgão de pesquisa
5. Execução de contrato/ Diligências Pŕe contratuais

A LGPD definiu dez bases legais para tratamento de dados pessoais. Isso significa que todos os dados pessoais manipulados pela empresa devem pertencer a pelo menos uma dessas categorias. Se não for possível o enquadramento, o dado não deve ser tratado e deve ser excluído, caso esteja armazenado em poder da empresa

3.2 - Bases legais para tratamento de dados pessoais

Status geral 30%

6 Exercício Regular de Direitos

7 Proteção da Vida

8 Tutela da Vida

9 Interesses Legítimos do Controlador/ Terceiro

10 Proteção ao crédito

3.3 - Atendimento aos direitos dos titulares dos dados

A LGPD assegurou 11 direitos aos titulares dos dados pessoais e os controladores desses dados precisam estar prontos para cumprimento dessa obrigação. Como esse requisito não existia, novos processos de negócio precisarão ser criados para garantir o perfeito funcionamento dessa solicitação, livrando a empresa de futuras sanções. Para o melhor controle dos processos, será necessário usar alguma ferramenta para apoio tecnológico como interface para os titulares de dados.

11 direitos:

3.3 - Atendimento aos direitos dos titulares dos dados

11 direitos

Informação sobre a possibilidade de não fornecer o consentimento	Revogação do consentimento	Reclamação à autoridade nacional	Oposição ao tratamento, se irregular
Confirmação da existência do tratamento	Acesso aos dados	Correção de dados incompletos	Portabilidade dos dados a outro fornecedor de serviço ou produto
Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados licitantes	Eliminação dos dados pessoais	Informação das entidades com as quais o controlador realizou uso compartilhado de dados	

3.4 - Transferência internacional de dados

A LGPD trouxe uma redação específica para a transferência internacional de dados pessoais. Na mesma linha das previsões sobre tratamentos de dados pessoais e dados pessoais sensíveis, conforme artigos 7º e 11, respectivamente, a LGPD listou as bases legais da transferência internacional de dados pessoais no artigo 33, a saber:

Bases legais da transferência internacional de dados:

3.4 - Transferência internacional de dados

- Países ou organismos internacionais destinatários com grau de proteção de dados pessoais adequado ao previsto na LGPD (a ser avaliado pela autoridade nacional);

- Mediante o oferecimento e a comprovação de garantias, pelo controlador, de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (na forma de cláusulas contratuais específicas e padrão; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos – cuja análise será realizada pela autoridade nacional);

- Se necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

- Se necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;

3.4 - Transferência internacional de dados

- Mediante autorização pela autoridade nacional;
- Se resultante de compromisso assumido em acordo de cooperação internacional;
- Se necessária para a execução de política pública ou atribuição legal do serviço público (assegurada a publicidade nos termos do artigo 23, inciso I da LGPD);
- Mediante consentimento específico e destacado do titular do dado pessoal, com informação prévia sobre o caráter internacional da operação e com finalidade distinta de qualquer outra eventualmente existente;
- Se necessária para cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de contrato ou de procedimentos preliminares contratuais, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral (vide artigo 7º, incisos II, V e VI da LGPD).

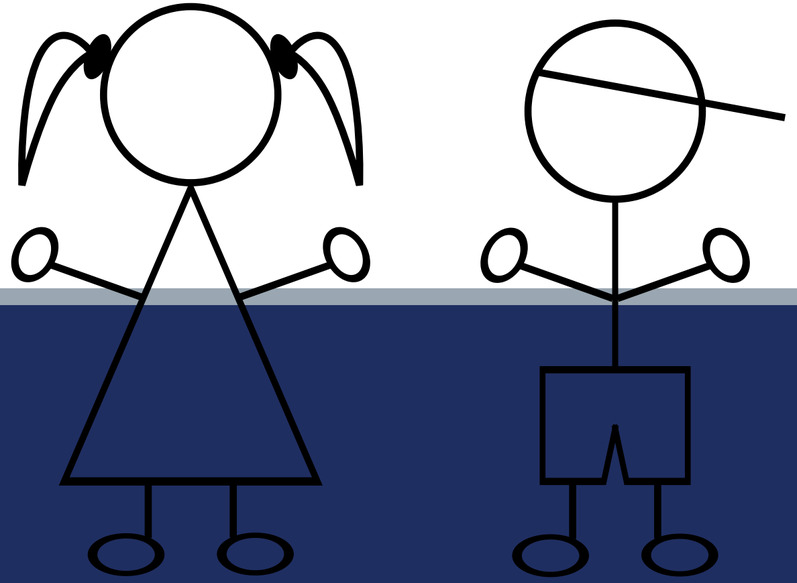
3.4 - Transferência internacional de dados

Principais casos em que é possível a transferência internacional de dados

País de destino com grau de proteção à LGPD

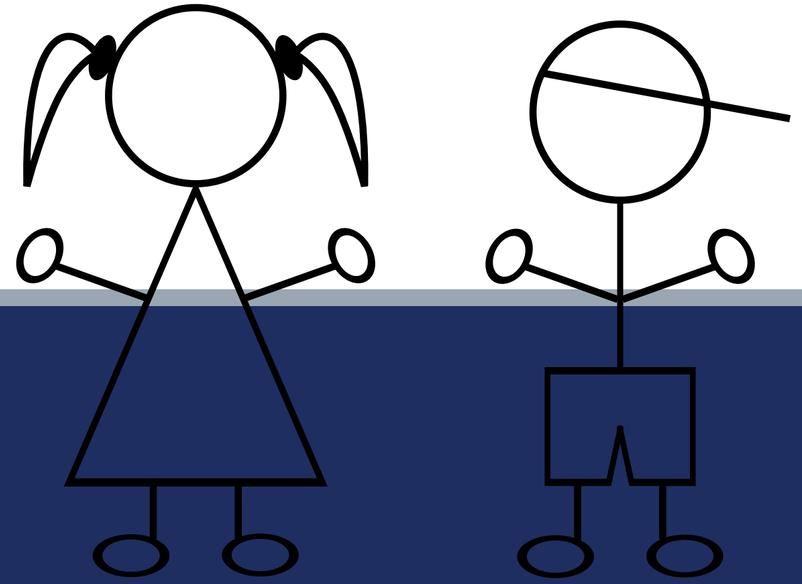
Mediante consentimento específico e em destaque do titular	Relativa à cooperação jurídica internacional para fins de investigação	Para a proteção da vida ou incolumidade física do titular ou do terceiro	Quando autorizada pela autoridade Nacional de proteção de dados
Mediante acordo de cooperação internacional	Mediante garantias oferecidas pelo controlador:	- cláusulas contratuais específicas - normas corporativas globais - cláusuas - padrão contratuais -selos, certificados e códigos de conduta	

3.5 – Tratamento de dados de crianças e adolescentes



O tratamento de dados de crianças e adolescentes deverá ser realizado (i) no melhor interesse da criança ou adolescente (art. 14, caput), (ii) mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, §1º) e (iii) de acordo com a obrigação que os controladores têm de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos Ciente da importância cada vez maior da internet na vida das crianças e dos adolescentes. O § 5º prevê que "O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis." Trata-se de mais um dispositivo em que a LGPD impõe aos controladores o devido dever de cuidado, a ser analisado no contexto das tecnologias disponíveis e dos meios razoáveis para tal. direitos do titular (art. 14, § 2º).

3.5 – Tratamento de dados de crianças e adolescentes



As únicas exceções ao consentimento são (i) quando a coleta dos dados for necessária para contatar os pais ou o responsável legal e, mesmo nessa hipótese, os dados devem ser utilizados uma única vez e sem armazenamento, e (ii) para a proteção da criança ou adolescente, sendo que, em qualquer caso, os dados não podem ser repassados a terceiros sem o consentimento de pelo menos um dos pais ou do responsável legal (art. 14, § 3º, LGPD).

Outro ponto importante é o § 4º, segundo o qual "Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade."

4 – Relatório de impacto à proteção de dados pessoais

Status geral 47%

O relatório de impacto à proteção de dados pessoais (RIPD), também conhecido como DPIA (Data Protection Impact Assessment) é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Ele também apresenta as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme o artigo 5º, inciso XVII da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

5 - Processo de tratamento de incidentes de segurança e privacidade de dados

A LGPD exige que as empresas gerenciem de forma completa os incidentes de segurança e privacidade ocorridos para prestação de contas aos titulares e para a ANPD. Um incidente é sempre gerado pela exploração de alguma vulnerabilidade existente nos ativos organizacionais. A Figura 3 ao lado descreve esse fluxo.

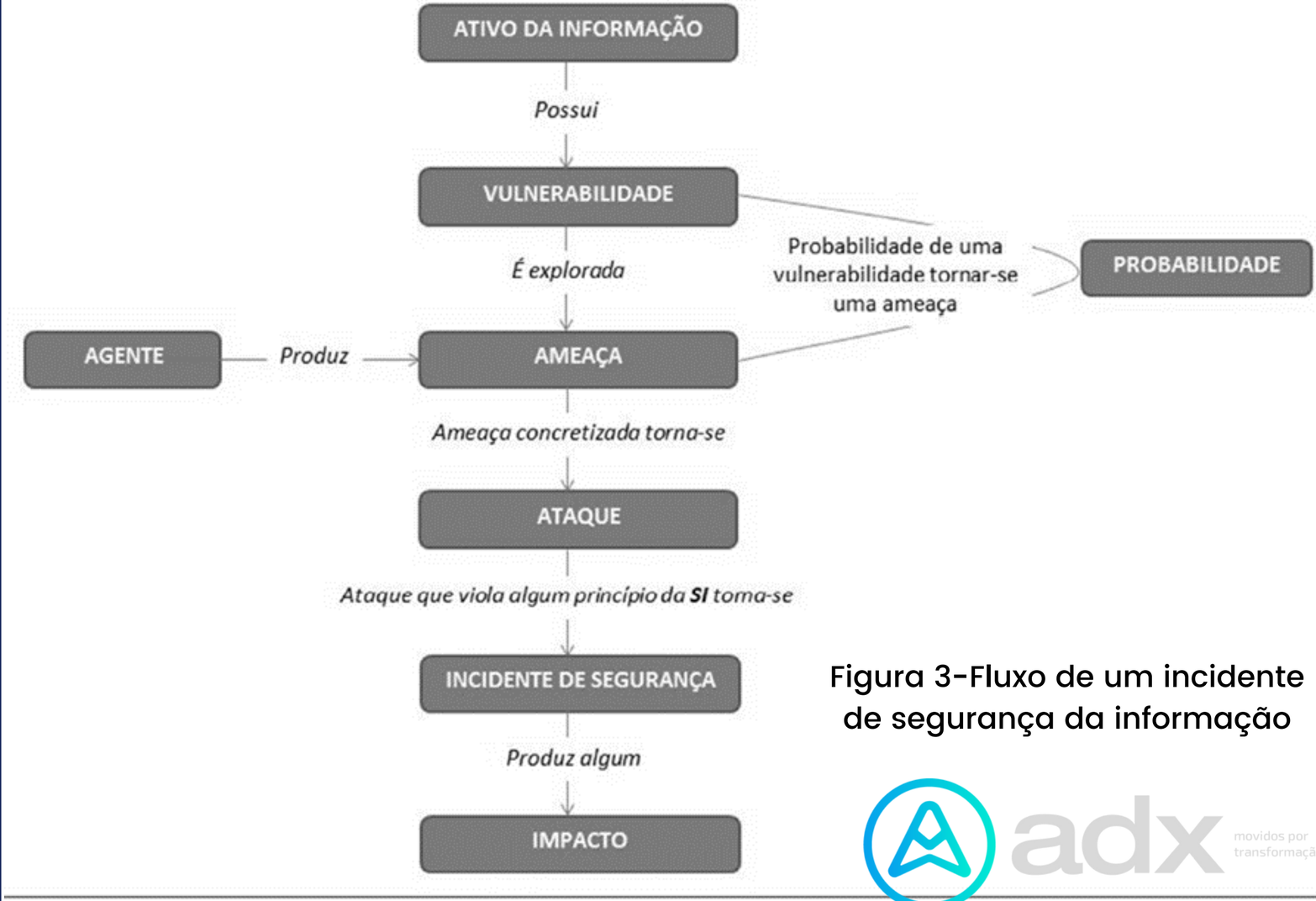


Figura 3-Fluxo de um incidente de segurança da informação

5 - Processo de tratamento de incidentes de segurança e privacidade de dados

É importante diferenciar uma violação de segurança de uma violação de privacidade. A violação de dados pode ou não acontecer quando uma violação de segurança ocorre. Como exemplo, se um pen drive ou laptop perdido tiver os dados criptografados, não será categorizada uma violação de dados.
No texto da lei, a previsão legal para a resposta a incidentes de segurança vem no capítulo VII, justamente o que trata da segurança da informação e das boas práticas a serem adotadas para tanto. Em seu artigo 48, consta:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

- 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.

5 - Processo de tratamento de incidentes de segurança e privacidade de dados

E Dessa forma, será extremamente importante a criação de um processo para gerenciamento de todos os incidentes, bem como para o registro das deliberações realizadas pelo comitê de privacidade e pelo DPO. Para potencializar esse processo, recomenda-se que seja usado um software especialista nessa função. Esse software deve catalogar cada registro de incidentes ocorridos dentro da empresa. O registro de incidente normalmente contempla os seguintes dados:

O registro de incidente normalmente contempla os seguintes dados:

- Quando ocorreu o incidente;
- Quais dados foram afetados;
- Quais e quantos titulares foram afetados;
- Quais as causas do incidente;
- Quais seus efeitos e consequências;
- Qual o plano para mitigação desses efeitos e suas respectivas consequências;

5 - Processo de tratamento de incidentes de segurança e privacidade de dados

O registro de incidente normalmente contempla os seguintes dados:

- Uma linha do tempo do incidente, incluindo quando houve o primeiro alerta quanto ao incidente e quando de fato foi determinado que o mesmo ocorreu;
- As decisões relativas à notificação.

Após a análise do incidente pela equipe de segurança, comitê e DPO, as seguintes informações devem ser registradas para determinação do plano ação:

- O tipo do incidente/vazamento;
- O tipo de dados pessoais afetados;
- A sensibilidade dos dados afetados;
- O volume de dados afetados;
- O número de titulares atingidos;
- A natureza do processamento;
- A facilidade ou não de identificação dos titulares (se por exemplo, os dados estavam criptografados ou anonimizados, o risco reduz);

5 - Processo de tratamento de incidentes de segurança e privacidade de dados

Após a análise do incidente pela equipe de segurança, comitê e DPO, as seguintes informações devem ser registradas para determinação do plano ação:

- A gravidade das consequências para os titulares;
- A extensão das consequências para os titulares;
- Se houve menores entre os titulares;
- Caso haja uma falha de confidencialidade, quais as possíveis intenções de quem perpetrou o ataque que gerou o incidente.

6 - Sanções

Parâmetros e critérios considerados para a aplicação das sanções

Reincidência	Boa - Fé	Condição econômica	
Proporcionalidade	Pronta adoção de medidas correlativas	Mecanismo e procedimentos internos de proteção de dados	Vantagem obtida ou pretendida
Políticas de boas práticas e governança	Cooperação do infrator	Grau do dano, gravidade	

6 – Sanções

São penalidades atribuídas às empresas pelo não cumprimento dos requisitos da LGPD.

Sanções

-Eliminação de dados pessoais

-Bloqueio do tratamento de dados

- Multa de até 2% de faturamento do grupo no Brasil

Teto de R$ 50 milhões /infração

- Multa diária com o teto acima

- Advertência

- Publicização da infração

7 - ANPD (Autoridade Nacional de Proteção de dados)

Competências

Lei 13.709/2018 Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

7 - ANPD (Autoridade Nacional de Proteção de dados)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

7 - ANPD (Autoridade Nacional de Proteção de dados)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

7 - ANPD (Autoridade Nacional de Proteção de dados)

https://anppd.org/

A ANPD possui o site para mais informações em relação a Autoridade Nacional e o site para a realização de comunicações, notificações ou denúncia de algum incidente de segurança.

https://www.gov.br/anpd/pt-br

8 – Encarregado pelo tratamento de dados pessoais o DPO (Data Protection Officer)

Lei 13.709/2018 Art. 41. § 2º As atividades do encarregado consistem em:

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.

No dia 29 de Julho de 2021 foi incluída a ocupação de DPO/ Encarregado pelo tratamento de dados na CBO - Classificação Brasileira de Ocupações iniciando em 2022.

1421-35 - Oficial de Proteçao de Dados Pessoais (DPO)

9 – Processo de adequação

Status geral 72%

O Processo de adequação requer um profundo conhecimento da legislação, de segurança da informação e de gestão de processos de negócio. Essas três áreas estão fortemente ligadas.

9 – Processo de adequação

Status geral 74%

O processo de adequação deve ser encarado como um projeto e deve ser dividido em duas grandes fases, a saber:

1

Diagnóstico

O processo de adequação requer uma análise detalhada do funcionamento da empresa. Todos os processos que manipulam dados pessoais precisam ser diagnosticados para definição dos riscos de violação e das estratégias de respostas mais adequadas. Será preciso também revisar todas as políticas, procedimentos e contratos com terceiros para garantir a conformidade com a lei.

2

Implantação

Com base no que foi diagnosticado, devem ser definidos planos de ações com responsável, investimento e data de conclusão, deixando claro o esforço necessário para correção de todos os GAPs e oportunidades de melhorias encontrados.

10 – O papel do fornecedor mediante a LGPD

1

Agente de tratamento

O fornecedor e/ou parceiro quando trata dados dos quais o controlador fornece, torna-se o operador desses dados e um agente de tratamento que a partir desse momento, também possui responsabilidades sobre os dados do titular.

2

O operador mediante o controlador

De acordo com a Lei 13.709/2018 Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

3

Adoção de medidas de segurança

De acordo com a Lei 13.709/2018 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

10 - O papel do fornecedor mediante a LGPD

Status geral 77%

Responsabilidades dos agentes de tratamento

Garantir a segurança da informação

De acordo com a Lei 13.709/2018 Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Controlador e operador

De acordo com a Lei 13.709/2018 Art. 42. O controlador ou o operador que, em razão do exercício de 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 a repará-lo

Compartilhamento

De acordo com a Lei 13.709/2018 Art. 18. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

10 - O papel do fornecedor mediante a LGPD

Status geral 79%

Danos causados

Responsabilidade do operador

De acordo com a Lei 13.709/2018 Art. 42. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei.

11 - Como o fornecedor pode contribuir para proteger os direitos fundamentais de liberdade e de privacidade do titular dos dados?

1. Entender e aplicar a LGPD com os dados aos quais possui acesso.

2. Cumprimento do contrato realizado com o controlador.

3. Buscar melhoria contínua para os métodos utilizados para proteção de dados.

12 - Boas práticas para proteção de dados

Após o alinhamento de todos os processos aos quais o controlador compartilha os dados com os fornecedores e parceiros, faz-se necessário o alinhamento dos agentes de tratamento de dados para que esses dados sejam tratados da melhor maneira possível e, os titulares estarem cientes deste tratamento.

12 - Boas práticas para proteção de dados

De acordo com a Lei 13.709/2018 Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

A seguir - Boas práticas a serem adotadas

movidos por transformação

1 Manter resgistro das operações realizadas com o Senac Alagoas;

2 Manter resgistro dos dados compartilhados pelo Senac Alagoas;

3 Definir periodicidade para revisão desses registros e realizar a revisão dos mesmos.

Pausa para a Lei

Lei 13.709/2018 Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

4 Definir um comitê ou responsável pelo tratamento de dados para facilitar a comunicação entre controlador e operador;

5 Definir um canal de comunicação para assuntos referentes a LGPD;

6 Manter uma boa comunicação e contribuir para o alinhamento de estratégias e para a resolução de problemas;

7 Cumprimento do contrato, onde estão presentes as claúsulas referentes a LGPD;

8 Evitar a impressão de dados presentes em meio digital;

9 Criar processo ou procedimento para o descarte dos dados compartilhados pelo Senac Alagoas esteja de acordo com a Lei 13.709;

10 Ao tratar os dados pessoais e dados pessoais sensíveis observar a boa-fé e os prinípios citados na Lei 13.709.

Pausa para a Lei

Lei 13.709/2018 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - 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.

11 Ter conhecimento sobre os dados tratados, a natureza, escopo, finalidade, probabilidade e a gravidade dos riscos e benefícios levando em consideração estes aspectos para a definição de como os dados serão tratados;

12 Comunicar o Senac Alagoas qualquer risco de vazamento de dados;

13 Informar, através de um relatório de tratamento de dados, os dados que o Senac Alagoas compartilhou que estão sendo tratados.

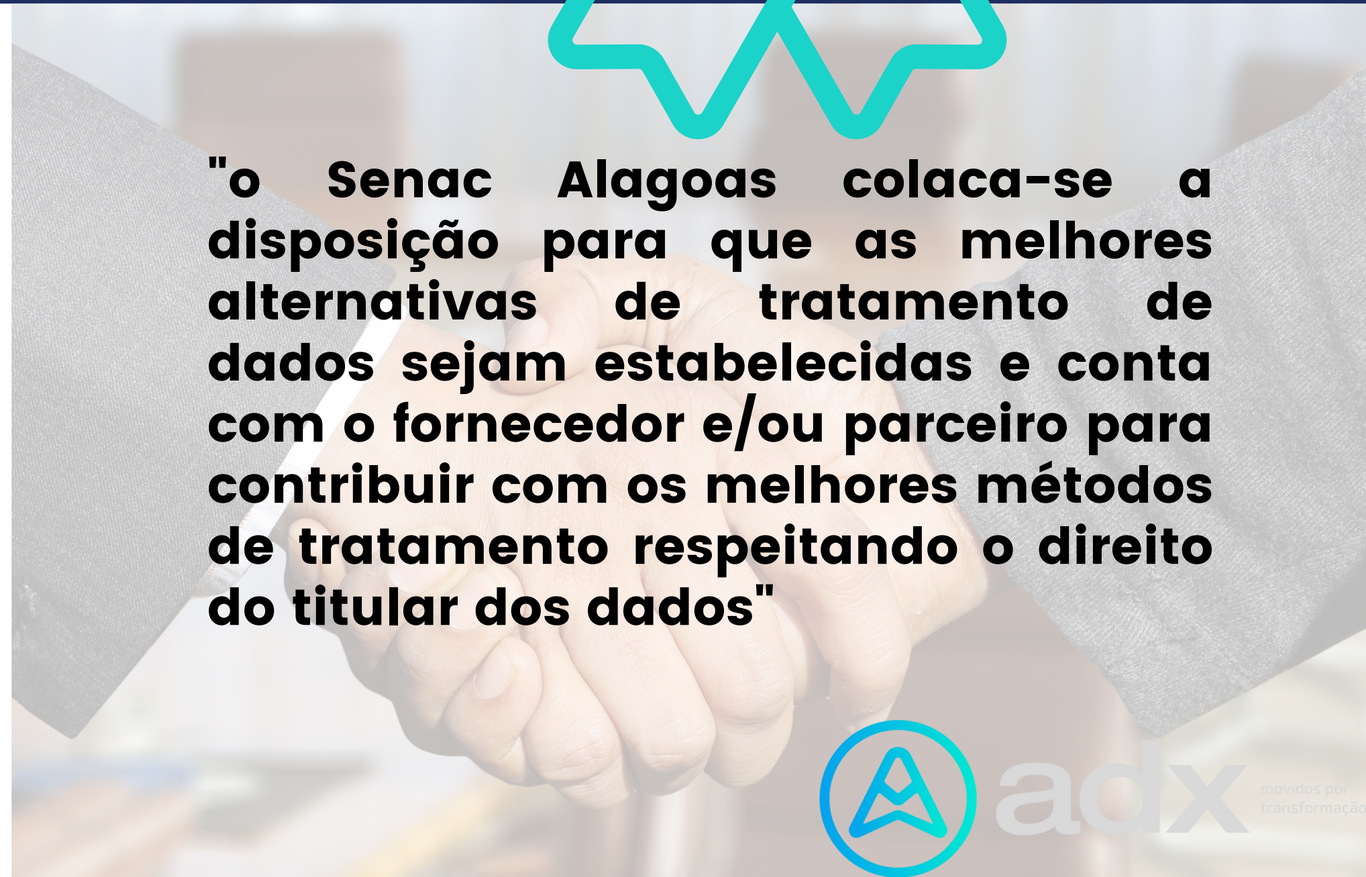
Pausa para a Lei

Lei 13.709/2018 Art. 47.§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

13 - Conclusão

Status geral 96%

O Senac Alagoas por meio deste e-book busca fortalecer as boas práticas e contribuir com as decisões dos seus fornecedores e parceiros referente a LGPD e os dados que são tratados em comum. Assim, é possível notar que a excelente comunicação entre os agentes de tratamento é a melhor alternativa para proteger os direitos fundamentais da liberdade e da privacidade da pessoa natural. Deste modo, o Senac Alagoas colaca-se a disposição para que as melhores alternativas de tratamento de dados sejam estabelecidas e conta com o fornecedor e/ou parceiro para contribuir com os melhores métodos de tratamento respeitando o direito do titular dos dados.



"o Senac Alagoas colaca-se a disposição para que as melhores alternativas de tratamento de dados sejam estabelecidas e conta com o fornecedor e/ou parceiro para contribuir com os melhores métodos de tratamento respeitando o direito do titular dos dados"

SENAC ALAGOAS

AGRADECE!

movidos por transformação

adx

movidos por
transformação

dpo@grupoadx.com.br

Aracaju: (79) 3013-4140

www.grupoadx.com.br

Av. ministro Geraldo Barreto Sobral, 2100 - JFC Trade Center -
Sala 1506 - Jardins - Aracaju - SE