FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

PATRÍCIA CRISTINA AZEVEDO PARO
VITOR LUIZ SANTIAGO DA SILVA

INÍCIO DE ADEQUAÇÃO À LGPD

Estudo de caso da empresa multinacional alemã de engenharia e eletrônica

Americana, SP
2020

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

PATRÍCIA CRISTINA AZEVEDO PARO
VITOR LUIZ SANTIAGO DA SILVA

INÍCIO DE ADEQUAÇÃO À LGPD

Estudo de caso da empresa multinacional alemã de engenharia e eletrônica

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.(a) Especialista Juliane Borsato Beckedorff Pinto

Área de concentração: Segurança da Informação

Americana, SP
2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

P267i PARO, Patrícia Cristina Azevedo

Início de adequação à LGPD: estudo de caso da empresa multinacional alemã de engenharia e eletrônica. / Patrícia Cristina Azevedo Paro. – Americana, 2020.

60f.

Monografia (Curso de Tecnologia em Segurança da Informação) -- Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Esp. Juliane Borsato Beckedorff Pinto

1 Lei geral de proteção de dados 2. Segurança em sistemas da informação I. PINTO, Juliane Borsato Beckedorff II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 34:681.3
681.518.5

Patrícia Cristina Azevedo Paro
Vitor Luiz Santiago da Silva

INÍCIO DE ADEQUAÇÃO À LGPD

Estudo de caso da empresa multinacional alemã de engenharia e eletrônica

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 30 de junho de 2020.

Banca Examinadora:

_____
Juliane Borsato Beckedorff Pinto
Especialista
FATEC Americana Ministro Ralph Biasi

_____
Jonas Bodê
Especialista
FATEC Americana Ministro Ralph Biasi

_____
MARIANA GODOY VAZQUEZ MIANO
Doutora
FATEC Americana Ministro Ralph Biasi

AGRADECIMENTOS

Em primeiro lugar agradecemos à toda nossa família que estiveram conosco suportando em todo o período de graduação.

À nossa professora orientadora Juliane Beckedorff, pela troca de conhecimento, ajudando no desenvolvimento e conclusão deste trabalho.

DEDICATÓRIA

Aos nossos familiares, colegas de curso e à Juliane nossa orientadora.

RESUMO

O presente texto tem como objetivo descrever e compreender a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, aprovada em 14 de agosto de 2018 e o início da adequação de uma determinada empresa. Tal lei se mostrou necessária para a manipulação, tratamento e armazenamento de dados pessoais pelas organizações públicas e privadas e também importante para manter relações econômicas e políticas com países que já possuem leis voltadas para a proteção de dados pessoais. Este estudo faz um panorama geral das disposições legislativas presentes no Brasil, apresenta a LGPD, como também aponta documentos relevantes para as empresas se adequarem e fortalecerem a privacidade dos dados pessoais, e como objetivo principal é apresentado o estudo de caso da empresa multinacional alemã que produz principalmente componentes automotivos e qual o plano de ação definido para dar início à conformidade à lei. A abordagem é feita através de pesquisas em livros, artigos, estudos recentes disponíveis na internet sobre a lei em questão. Também é feita uma análise das ferramentas utilizadas pela empresa multinacional alemã, como os questionários respondidos por todos os departamentos e o material de apoio disponibilizado pela consultoria jurídica contratada. Por se tratar de uma lei recém aprovada, estar em conformidade à LGPD requer empenho e pode ser uma tarefa complexa, porém indispensável por ser uma regulamentação taxativa.

Palavras Chave: Lei Geral de Proteção de Dados; Privacidade, Segurança da Informação; Dados Pessoais; Conformidade.

ABSTRACT

This document aims to describe and outline the Law of Protection of Personal Data (LGPD), Law No. 13.709/2018 approved on August 14, 2018 and the initial compliance measures required for a specific company. This law proved necessary for the manipulation, processing and storage of personal data by public and private organizations as well as an important measure to maintain economic and political relations with countries that have existing personal data protection laws. This study gives an overview of the existing Brazilian legislation, presents the LGPD, as well as relevant documents for companies to adapt and strengthen personal data privacy. A case study of the multinational german company, which already has an action plan defined. Books, papers, and recent studies found on the internet were the basis for developing the initial implementation plans set forth in this paper. An analysis was also made from the company tools, such as multi-department questionnaires and third party legal advice materials. This document outlines the newly passed law and suggests compliance measures required to adhere to LGPD, though complex in nature the regulation is now an obligation for all industries that have access to personal data.

Keywords: *Law of Protection of Personal Data; Privacy; Information Security; Personal Data; Compliance.*

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD Autoridade Nacional de Proteção de Dados

BS British Standards

BSI British Standards Institute

CDC Código de Defesa do Consumidor

DPA Data Protection Act

DPO Data Protection Officer

EBIT Earnings Before Interest and Taxes

ECA - Estatuto da Criança e Adolescente

GDPR General Data Protection Regulation

IEC International Electrotechnical Commission

ISO - International Organization For Standardization

LGPD Lei Geral de Proteção de Dados

MCI Marco Civil da Internet

MP Medida Provisória

NCC National Computing Centre

SGSI Sistema de Gestão de Segurança da Informação

PDCA Plan Do Check Act

PME Pequenas e Médias Empresas

UE União Européia

SUMÁRIO

INTRODUÇÃO

Com o avanço da tecnologia no mundo atual, a internet tornou-se essencial na vida das pessoas e com isso a utilização de dados pessoais como compras online e transações eletrônicas vem se fazendo mais presentes no dia a dia. O manejo de dados pessoais é uma nova forma de exercer poder pelas empresas, e há uma vulnerabilidade por parte do consumidor, que disponibiliza os dados sem receber uma proteção específica, até é possível fazer algumas ações que ajudam a na segurança de dados pessoais, como criptografar seu computador e aparelho móvel, utilizar senhas fortes e não repeti-las em sites diferentes, estes são alguns exemplos que auxiliam, porém neste contexto de recentes violações de dados, fez se necessário ter uma legislação mais representativa para a segurança desses dados e como armazená-los, sem que haja um perigo para os usuários que os forneceram.

Com isso surgiu a necessidade da criação da Lei n. 13.709/2018, chamada de Lei Geral de Proteção de Dados, que regulamenta o tratamento e armazenamento de dados pessoais pelas empresas públicas e privadas, trazendo transparências e consistência para o motivo e necessidade de deter destes dados, sendo passível de sansões legais e multas, pois as leis existentes até o momento, que citavam algo relacionado à privacidade, não se faziam suficientes para atender a demanda de assegurar a proteção dos dados pessoais, que é visto como o recurso mais visado do século XXI.

A Lei Geral de Proteção de dados, conhecida como LGPD, foi promulgada no dia 14 de agosto de 2018 pelo então presidente Michel Temer. Esta lei foi inspirada na versão europeia GDPR – *General Data Protection Regulation*. Conforme citado por Patrícia Peck Pinheiro, no livro Proteção de Dados Pessoais:

> [...] no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda,

> manuseio e descarte dentro dos padrões mínimos de segurança condizentes. (PINHEIRO, 2019).

A LGPD é uma lei que diferente da GDPR, ainda não entrou em vigência. O brasileiro está enfrentando diversas dúvidas em relação ao prazo, pois existem vários cenários que podem prorrogar a vigência da lei por até mais um ano. E também existem dúvidas em relação à como será feito o controle do atendimento das regras impostas pela lei. Já que a lei prevê a criação de um órgão fiscalizador que ainda não foi criado pelo governo. Até a entrega deste trabalho, em junho de 2020, algumas medidas provisórias ainda estavam sendo discutidas para postergar a vigência da lei que está prevista para agosto de 2020.

Esse trabalho irá fazer um breve levantamento histórico das regulamentações vigentes no Brasil, referentes à proteção de dados pessoais, apresentar a nova Lei Geral de Proteção de Dados, chamada de LGPD, expor algumas alterações no modo de tratamento de dados pessoais que irão acontecer com a sanção desta lei no país e também como ela pode favorecer as relações econômicas e políticas com países que possuem legislação similar. Será mostrado documentos considerados relevantes para uma empresa se adequar a esta nova legislação, como estas instituições públicas e privadas serão fiscalizadas e de que maneira elas e clientes lidam com a mudança que foi imposta devido a lei no processo de armazenamento, compartilhamento dos dados pessoais e os direitos dos titulares destes dados. O objetivo principal deste trabalho é fazer um estudo de caso sobre o início de adequação à LGPD da empresa multinacional alemã, uma organização multinacional do ramo automotivo, apresentando os primeiros passos tomados por ela, o plano de ação iniciado e as ferramentas que estão sendo utilizadas para entrar em conformidade com a Lei Geral de Proteção de Dados que pretende entrar em vigor brevemente e serão aplicadas multas altas para àquelas que não estarem de acordo com a lei.

A metodologia utilizada será pesquisas através de livros, artigos, sites especializados na constituição brasileira, noticiários disponíveis na internet, podcasts, webinars, jornais e revistas para estruturar o levantamento histórico das leis e a apresentação mais detalhada da LGPD. O estudo de caso será feito através da análise das ferramentas utilizadas pela empresa, como os questionários

respondidos pelos departamentos e o material disponibilizado consultoria contratada.

1 BREVE PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS

É inegável que a internet tenha se tornado essencial na vida cotidiana. Com ela podemos conversar com pessoas do outro lado do continente ou em qualquer lugar do mundo simultaneamente. Somos capazes de fazer compras do conforto de nosso lar, pesquisar sobre múltiplas coisas, utilizando *smartphones*, *laptops* e *notebooks*, estamos conectados 24 horas por dia. As opções de atividades e entretenimento que a Internet nos proporciona são incontáveis, mas apesar dessas inúmeras atividades, a Internet também é usada para finalidades ilegais. O autor Peter T. Knight comentou em seu livro: A Internet no Brasil (2014, p.99), alguns exemplos de como a internet pode ser utilizada para fins ruins, e que pode ser uma ameaça à economia, política e sociedade:

> Enquanto os benefícios da Internet para o desenvolvimento econômico, social e político são inegáveis, ela, como qualquer tecnologia, pode ser usada para o bem, ou para fins questionáveis, ilegais ou militares. Spam, phishing, abuso infantil, tráfico de drogas, pirataria da propriedade intelectual, invasões de privacidade, terrorismo, espionagem econômico e política e guerra cibernética são ameaças reais.

A internet mudou o mundo, com ela as fronteiras desapareceram e a comunicação obteve uma configuração quase instantânea, de forma difundida. E a cada dia surgem avanços em velocidade tão grande que nem os profissionais conseguem mais acompanhá-la. Em menos de vinte anos de uso comercial, a internet alterou diversas perspectivas da convivência humana. Com toda a facilidade do acesso em qualquer hora e lugar, a velocidade do alastramento de informações é quase imensurável. A descentralização das informações é uma característica da internet. Essa liberdade e agilidade de difusão de informações, conteúdos e opiniões, trouxe problemas à sociedade, é inviável conferir a veracidade das informações, ter a certeza da transparência dos conteúdos, não sabemos o que é feito com o armazenamento dos nossos dados e histórico de acesso. Assim, iniciou-se debates referentes à necessidade de uma questão legal ligada à Internet, mais específica à dados pessoais.

A legislação brasileira possui leis que são ligadas diretamente e indiretamente à utilização da internet, como comenta os autores Bezerra e Waltz, que a privacidade e a intimidade que são direitos essenciais e estão presentes na Declaração Universal de Direitos Humanos, que delineia os direitos humanos

básicos e na Constituição Federal de 1988, que é a lei fundamental e suprema do Brasil:

> A privacidade e a intimidade são direitos fundamentais presentes na Declaração Universal dos Direitos Humanos e na Constituição da República de 1988. A privacidade refere-se a tudo o que o indivíduo não pretende que seja de conhecimento público, reservado apenas aos integrantes de seu círculo de convivência particular, enquanto a intimidade diz respeito única e exclusivamente ao indivíduo. Esses direitos se estendem ao domicílio, à correspondência, às comunicações e aos dados pessoais. (2014, p.15)

Apesar desses direitos fundamentais estarem disponíveis, o Brasil não estava amparado por uma legislação específica, como comentado no e-book Social Miner: “A verdade é que até 2018, o Brasil ainda não contava com uma legislação específica que garantisse os direitos de privacidade de dados dos seus consumidores, tendo disposições sobre a matéria apenas em leis esparsas.” Com o desenvolvimento muito grande na humanidade que a internet trouxe, foi necessário discutir a respeito de novas legislações. Dentro desse cenário é evidente e inegável que o direito não poderia ficar impermeável às mudanças trazidas pela internet. A autora Patrícia Peck Pinheiro, também comenta eu seu livro Proteção de Dados Pessoais, que o surgimento de regulamentações, começou no início dos anos 90, com o desenvolvimento dos negócios digitais (2019, p.17):

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente relacionados à pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Antes disso, na Europa, o assunto referente à processamento de dados já era debatido, pois as pessoas começaram a ter consciência da importância dos dados pessoais, além da idéia de que estes dados são de posse de cada indivíduo. Essa compreensão surgiu a partir de uma legislação feita na UE, como menciona a Social Miner (2020, p.09):

> Desde que o processamento de dados se tornou algo relevante na União Européia, lá pela década de 1980, os estados membros do grupo começaram a discutir o assunto, com frequência. Neste mesmo período, uma importante legislação, conhecida como Data Protection Act (DPA), foi aprovada no Reino Unido. O ato trouxe para o público a noção de que os dados são uma propriedade de cada indivíduo e que as pessoas têm poder de decisão sobre eles.

Diante de todo esse contexto e discussões em torno da privacidade e proteção de dados, o Brasil aprovou a Lei Geral de Proteção de Dados, a LGPD. Baseada na GDPR -General Data Protection Regulation, regulamentação da União Europeia, para proteger os cidadãos brasileiros da exposição de dados pessoais e para inibir o uso indevido e sem autorização dessas informações.

Como dito anteriormente, o Brasil possui leis e decretos voltados para a proteção de dados pessoais, mas nenhuma tão específica quanto a LGPD. O país já dispunha de mais de 40 normas que direta ou indiretamente tratam da proteção à privacidade e aos dados pessoais. No *e-book*, A Nova Lei de Proteção de Dados, é dado um breve panorama histórico (2020, p.10):

> [...] no Brasil, vez ou outra eram criadas leis voltadas para proteção de dados. O Código de Defesa do Consumidor, por exemplo, cita a possibilidade de obtenção de dados por parte das empresas. Já a Lei Carolina Dieckmann penaliza a invasão de dispositivos. Por sua vez, o Marco Civil, de 2014, pontua alguns dos direitos que são mais bem elaborados na nova lei. Mas o fato é que, antes da LGPD, o Brasil nunca contou com um documento que contemplasse todos os aspectos desses sistema, desde a manipulação de dados e as questões de privacidade, até alternativas eficientes para fiscalização desses processos.

Ou seja, o país não estava alheio à legislações que lidava com dados pessoais. A Lei Nº 12.737/2012, conhecida como Lei Carolina Dieckmann, inseriu três tipos penais específicos envolvendo crimes informáticos, que são:

- Invasão de dispositivo informático alheio;
- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública;
- Falsificação de cartão de crédito ou débito. Artigos 154, 266 e 298 do Código Penal, respectivamente.

O Decreto Nº 7.962/2013, que regulamenta o Código de Defesa do Consumidor, para dispor sobre a contratação no comércio eletrônico. Traz diversos esclarecimentos sobre atendimento ao consumidor em relação às compras realizadas pela internet, direito de arrependimento em comércio eletrônico.

E também a Lei Nº 12.965/2014, Marco Civil da Internet conhecida popularmente também como “Constituição da Internet”, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, tanto para provedores

de conexão, provedores de aplicação e usuários da Internet. Foi sancionada pela presidente Dilma Roussef, a Lei 12.965 de 23 de junho de 2014. É uma referência na regulação da internet e tem a privacidade como um de seus pilares. Como dito numa publicação por Nathalie Fragoso: “Trata-se de um instrumento regulatório específico, que lida com questões também no campo da privacidade para as quais a jurisprudência e a legislação anteriores ofereciam respostas contingentes e frequentemente contraditórias.” O Marco Civil impactou sobre a proteção de dados no Brasil, mas esta lei não garante a privacidade e a proteção de dados de forma abrangente, completa e estruturada. A lei garante a privacidade dos usuários, evitando que as informações pessoais sejam vendidas ou ofertadas para empresas terceiras, nacionais ou internacionais, sem a prévia autorização do usuário. Apesar das leis existentes no Brasil, elas não estavam sendo suficientes para o tratamento de dados pessoais, pois o avanço da tecnologia está aumentando consideravelmente o risco potencial da utilização abusiva de informações, e acentua a vulnerabilidade do direito à privacidade. E os meios digitais facilitaram a comunicação e o troca de informações pessoais.

O debate acerca do tema de uma legislação específica para o tratamento de dados pessoais de forma transparente e à livre circulação desses dados, surgiu na União Europeia. Em 27 de abril de 2016 foi aprovado a lei do Regulamento Geral de Proteção de Dados Europeu n.679 (GDPR), com previsão de dois anos de prazo de adequação. Em 25 de abril de 2018 foi iniciada a aplicação de penalidades. Esta aprovação acarretou com que outros países também buscassem regulamentações de mesmo nível para a abordagem correta dos dados pessoais, pois poderiam ter danos com questões econômicas e ter objeções para fazer negócios com países da União Europeia. Como comenta Peck (2019, p.18):

> [...] ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que a GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE.

E também, neste trecho do *e-book* publicado pela Social Miner (2020, p.11), fica claro a necessidade de uma legislação mais específica para tratamento de dados pessoais para além da questão jurídica, como também questões econômicas

e políticas, trazendo mais confiança nas relações com países que dispõem deste tipo de lei:

> Porém, com a chegada da GDPR e diante de tantos escândalos envolvendo o vazamento de dados, a verdade é que o Brasil se viu obrigado a criar uma legislação para proteção de dados, entrando para a seleta lista de 100 países que conta com uma norma adequada. Essa é, aliás, uma estratégia política, uma vez que nosso país busca conquistar uma cadeira na Organização para Cooperação e Desenvolvimento Econômico.

A Lei Geral de Proteção de Dados, Lei N. 13.709/2018 foi promulgada em 14 de agosto em 2018, pelo presidente Michel Temer, mas anos antes, em 2010, houve a abertura de uma consulta pública sobre o tema, disposta pelo Ministério da Justiça, dando início ao processo público e legislativo. Brandão (2019) explica: “Ainda que a LGPD ofereça inovações, o Marco Civil da Internet ainda deve ser compreendido como complementar a ela. Isso porque as duas leis estão centradas na perspectiva do titular dos dados pessoais ou, no caso do MCI, dos usuários da internet.”

2 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados, conhecida como LGDP será a ferramenta do governo para regulamentar como os dados brasileiros são tratados, armazenados e protegidos, prevendo punições para o descumprimento em casos de vazamentos, ou outras irregularidades. Ela normatiza a forma como serão tratados os dados pessoais no Brasil. As empresas dos setores público e privado deverão alinhar as práticas de coleta, utilização, tratamento e armazenamento dos dados pessoais de seus empregados e é aplicável a qualquer empresa, isto é, seja pessoa jurídica de Direito público ou privado, que realize o tratamento de dados pessoais, empresas de vários segmentos e abrangência. Para Renato Leite Monteiro, a LGPD é ampla, transversal e multissetorial. Ela se aplica a qualquer processamento de dados pessoais, independente do setor:

> A LGPD tem aplicação transversal e multissetorial, tanto no âmbito público e privado, on-line e off-line. Versa a norma sobre o conceito de dados pessoais, lista as bases legais que autorizam o seu uso – e o consentimento é apenas uma delas, dando destaque para permissão do uso de dados com base no legítimo interesse do controlador dos dados - , além de tratar de princípios gerais, direitos básicos do titular – como acesso, exclusão dos dados e explicação sobre uso – obrigações e limites que devem ser aplicados a toda entidade que se vale do uso de dados pessoais, seja como insumo do seu modelo de negócio, seja para a atividade de seus colaboradores.

A nova legislação regulamentou para que houvesse de forma objetiva critérios considerados adequados para guarda, manuseio e descarte dos dados pessoais. Peck disse (2019, p.19) “Foi nisso que a nova legislação inovou, ou seja, padronizou, ou melhor, normalizou, quase como uma norma ISO, o que seriam os atributos qualitativos da proteção dos dados pessoais sem a presença dos quais haveria penalidades.” A Social Miner menciona no E-book (2020, p.14), alguns objetivos gerais que a LGPD pretende trazer para os usuários:

> A regulamentação oferece mais liberdade e transparência para que usuários saibam quais dados estão sendo coletados, como e para que finalidade, permitindo até mesmo que essas pessoas suspendam o compartilhamento e a autorização para o uso dessas informações, a qualquer momento. Além disso, a lei traz flexibilidade, uma vez que pode ser adaptada de acordo com os avanços tecnológicos e, melhor: abre, também, o mercado para parcerias internacionais, uma vez que países que seguem leis similares restringem suas relações comerciais à empresas de países que garantam a segurança de dados.

A Lei Geral de Proteção de Dados, tem por finalidade dispor sobre:

> [...] o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Os principais objetivos da Lei Geral de Proteção de Dados são: direito à privacidade, regras claras para empresas, promover desenvolvimento, direito do consumidor, fortalecer confiança e segurança Jurídica. Para o autor e advogado Pigatti, cada um desses objetivos principais, tem uma intenção como explicado:

> Direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais. Regras claras para empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para empresas. Promover desenvolvimento: fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados. Direito do consumidor: garantir a livre iniciativa, a livre concorrência e a defesa do consumidor. Fortalecer confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais. Segurança Jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

A LGPD está baseada no entendimento fundamental de que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações, principalmente daquelas que as identificam, que são os dados pessoais, permitindo a limitação desse processamento, conforme a boa-fé, que deve pautar todas as relações jurídicas. Como a LGPD foi baseada na lei europeia, apresenta basicamente os mesmos princípios e eles funcionam de forma complementar. Isto é, cada princípio traz implicações para os outros. Os princípios devem conduzir a operação da coleta de dados e de seu tratamento Conforme afirmam Blum e Schuch, “nos procedimentos de tratamento de dados, devem ser respeitados os direitos constitucionais e fundamentais dos titulares dos dados, preservando a sua intimidade, vida privada, honra e imagem”. No artigo A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica, de Klee e Neto, os autores comentam como a LGPD deverá ser interpretada, conciliando com as demais regulamentações brasileiras existentes:

> A LGPD deverá ser interpretada e aplicada à luz dos princípios garantidos pela Constituição da República de 1988, tais como a dignidade da pessoa humana, a privacidade, o sigilo de dados e a proteção do consumidor, de maneira a dialogar com as demais fontes normativas do ordenamento jurídico brasileiro. Essas fontes normativas são o Código Civil, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet no Brasil, a Lei do Cadastro Positivo e a Lei do Acesso à Informação, pois todas elas

> asseguram direitos relacionados à proteção de dados e à privacidade, no seu campo de aplicação.

No que diz respeito aos princípios, a regulamentação de proteção de dados pessoais é uma legislação principiológica, a autora Patrícia Peck analisa: “A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido”. Em resumo os princípios são: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação e a responsabilização e prestação de contas.Peck (2019. p.42) destaca oito princípios com mais detalhes que devem ser observados, além da boa-fé no tratamento de dados:

> I. finalidade do tratamento;
> II. compatibilidade do tratamento com finalidades informadas ao titular;
> III. limitação do tratamento ao mínimo necessário para a realização de suas finalidades;
> IV. garantia, aos titulares, de consulta facilitada e gratuita sobre a forma do tratamento;
> V. garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de tratamento;
> VI. transparência aos titulares;
> VII. utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais;
> VIII. prestação de contas, pelo agente da adoção de medidas capazes de comprovar a proteção de dados pessoais.

A orientação principal para o tratamento de dados pessoais é o consentimento pelo titular, que não poderá ser realizado sem que haja uma base normativa, este consentimento deve ser declarado pelo mesmo. Mas existem hipóteses específicas as quais não há a necessidade de um consentimento expresso por parte do titular, que são:

> - para o cumprimeto de obrigação legal ou regulatória pelo controlador;
> - quando necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
> - para proteção da vida do titular ou de terceiro;
> - quando necessário para atender aos interesses legítimos do controlador ou de terceiro;
> - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (PECK. 2019. p.44)

Fora seus princípios, A LGPD garante também alguns direitos aos titulares dessas informações. Os usuários que acessam um site e têm seus dados coletados e processados tem o direito de, como enumerou a Social Miner:

> Serem informados que a empresa está realizado tratamento de seus dados; ter acesso aos dados que são coletados; corrigir dados incompletos ou desatualizados; solicitar anonimização, bloqueio ou eliminação de dados desnecessários a qualquer momento; solicitar a portabilidade dos dados. O usuário pode ter os seus dados transferidos para outra organização, se desejar; pedir a eliminação dos seus dados da base de uma empresa, com garantia de que isso aconteça; ser informado sobre o compartilhamento de seus dados com outras entidades, públicas ou privadas; ser informado sobre a possibilidade de não consentir com o compartilhamento dos seus dados com um site, dando ciência das consequências do não consentimento; informar a empresa que trata seus dados que não quer mais estar na base, revogando o seu consentimento e solicitar a revisão de decisões tomadas por computadores com base em tratamento automatizado de dados pessoais, solicitando informações claras sobre como aquela decisão foi tomada, observados os segredos comercial e industrial, hipótese em que a autoridade nacional poderá ser acionada para verificar tais questões.

A lei N. 13.709/2018 define alguns conceitos que guiarão a sua interpretação e aplicação. Entre os conceitos abordados no texto legal, a ênfase deve ser dado às elucidações de dado pessoal, de dado pessoal sensível, dado anonimizado, tratamento e consentimento. O conceito de dados pessoais é fundamental, sobretudo porque delimita o escopo de aplicação da lei. Dessa forma, o presente regulamento conceitua dados pessoais como toda informação relacionada à pessoa identificada ou identificável (artigo 5º, inciso I, da 13.709/2018). Mas a LGPD não se restringe a apenas esses conceitos, trazendo outros. Os conceitos definidos pela lei como os autores Klee e Neto (2019, p.18) apresentam, estão descritos no Quadro 1:

Quadro 1 - Conceitos definidos pela LGPD

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
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
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
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
Tratamento	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
Transferência internacional de dados	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
Uso compartilhado de dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados
Relatório de impacto à proteção de dados pessoais	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, bem como medidas, salvaguardas e mecanismos de mitigação de risco
Órgão de pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. A importância na definição desses conceitos no texto legal está no fato de servirá de guia para a correta interpretação e aplicação da lei, bem como da fiscalização com relação ao seu fiel cumprimento

Fonte: Klee e Neto (2019)

Além dos conceitos serem alguns dos pontos relevantes da nova lei, também é pertinente outros tópicos da LGPD, como elucida o Pigatti, referente à aplicação extraterritorial, essa transferência internacional de dados pessoais é possível com: adequação; consentimento; autorização; cláusulas corporativas globais e cláusulas padrão.

> Aplicação extraterritorial – em moldes similares à regulamentação europeia, a GDPR, a Lei Geral terá aplicação extraterritorial, ou seja, o dever de conformidade ultrapassará os limites geográficos do país. Toda empresa estrangeira que, pelo menos, tiver filial no Brasil, ou oferecer serviços ao mercado nacional e coletar e tratar dados de pessoas naturais localizadas no país estará sujeita à nova Lei (base do princípio universal da territorialidade).

Esses efeitos internacionais, quando dados são tratados fora do Brasil, são aplicados, e uma empresa deverá cumprir as condições da LGPD, se estes dados foram coletados em território nacional. Patricia Peck comenta em seu livro (2019. p.40):

> A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Desse modo, o dado pessoal tratado por uma empresa de serviço de cloud computing que armazene o dado fora do país terá que cumprir as exigências da LGPD.

No que tange às penalidades previstas pela LGPD, ressalta-se que algumas sanções tiveram veto presidencial, para atender a necessidade e realidade do Brasil. Para Peck: “(...) o critério de aplicação deverá observar alguns requisitos, especialmente o da proporcionalidade”. As seguintes penalidades foram expostas por Klee e Neto (2019):

> Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: advertência, com indicação de prazo para adoção de medidas corretivas; 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; multa diária, observado o limite total referido acima; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração.

Ademais, a LGPD não substitui o cumprimento de sanções administrativas, civis ou penais definidas no CDC (Código de Defesa do Consumidor) e em outra legislação específica. Klee e Neto (2019) também comentam que:

> As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé, a condição econômica e a cooperação do infrator; a vantagem auferida ou pretendida pelo infrator; a reincidência; o grau do dano; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A fiscalização e a regulação da LGPD ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais, chamada de ANPD. Ela foi definitivamente criada após a sanção da MP 869/2018, convertida na Lei 13.853/2019, é uma autoridade pública autônoma e independente para sua supervisão na aplicação da lei. Para Patrícia Peck Pinheiro (2019, p.49) “Pode-se afirmar que a ANPD foi criada para trazer mais segurança e estabilidade para a aplicação da Lei Geral de Proteção de Dados.”

> A LGPD, com a redação dada pela Lei nº 13.853/2019, passou a dispor sobre a criação, sem aumento de despesa, da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. A avaliação quanto à transformação deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (KLEE e NETO, 2019)

De acordo com conceito disposto no art. 5º, XIX, da LGPD, a Autoridade Nacional é o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Além disso “(...) tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras (...)” (PINHEIRO, 2019. p. 49). A ANPD será composta por 6 elementos: Conselho Diretor, Conselho Nacional de Proteção de Dados, Corregedoria, Ouvidoria, Órgão de Assessoramento Jurídico Próprio e Unidades Administrativas e Unidades Especializadas.

> Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; sugerir ações a serem realizadas pela ANPD; elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.(KLEE, NETO. 2019)

2.1 *Privacy by Design* - Sete princípios básicos

A GDPR previu dois princípios importantes: o Privacy by design e Privacy by default. Apesar de a LGPD ter se inspirado na lei europeia, o Brasil, ainda não aderiu a esses princípios taxativamente. Todavia, a legislação já faz uso de ideias parecidas, indicando que as empresas devem utilizar medidas técnicas aptas a proteger os dados contra acessos não autorizados, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Devido a instauração da nova lei LGPD, as empresas precisam se voltar para o tratamento dos dados pessoais e sensíveis que estão incorporados nas bases de seu domínio. Com o prazo para a vigência da lei se aproximando, todos os projetos poderão utilizar os princípios de *Privacy by Design,* podendo os novos serem implementados com essas ideias e os projetos já existentes serem adaptados. A intenção é que as empresas incluam esse conceito em toda elaboração de produto ou serviço, colocando a proteção da privacidade no centro de todo o desenvolvimento, incluindo essa ideia entre seus valores e destacando sua conduta ética.

Privacy by Design é uma metodologia que foi criada pela Dra. Ann Cavoukian, na década de 90 em Ontário, Canadá. Ela já imaginava que seria necessário a criação de meios para prevenção de compartilhamento e armazenamento não necessários de dados pessoais, por causa do avanço da tecnologia e a facilidade de comunicação. Essa metodologia possui como ideia, incorporar em empresas, a privacidade de todos os envolvidos em seus produtos e serviços, a fim de proteger os dados pessoais, fazendo isso como parte de seus valores e de uma conduta ética. *Privac*y by Design possui 7 princípios básicos segundo sua criadora Dra. Ann Cavoukian. Seguindo esses princípios uma empresa está bem encaminhada na sua adequação às novas normas de privacidade.

1. O primeiro fala sobre proatividade, ser proativo e não reativo, ou seja, sempre será necessário o monitoramento constante de análises para que assim que houver algum evento que possa comprometer a privacidade do usuário, ou alguma falha seja encontrada, deverá ser tomada as precauções devidas para evitar que ocorra algum problema (CAVOUKIAN, 2011).
2. O segundo princípio é a privacidade por padrão, o usuário precisará se sentir seguro, a privacidade por padrão deve lhe proporcionar o máximo de proteção possível, o mesmo não precisa ajustar nenhuma configuração existente para que se torne protegido (CAVOUKIAN, 2011).
3. O terceiro é a privacidade incorporada ao projeto (embutida no design), esta deve ser parte integrante do sistema, a proteção tem que ser automática, a própria empresa tem que incluí-la sem o usuário precisar garanti-la (CAVOUKIAN, 2011).
4. O quarto é a funcionalidade total, soma positiva e não soma zero, em um jogo de soma positiva, todos ganham, já a soma zero, para um ganhar o outro tem que perder. A proteção de dados tem que estar de acordo com os interesses e objetivos dos usuários, todas as funcionalidades têm que estar protegidas sem o usuário precisar escolher entre segurança ou privacidade, como a soma zero (CAVOUKIAN, 2011).
5. O quinto é a segurança de ponta a ponta é a proteção dos dados desde quando é coletada até ser destruída, ou compartilhada com terceiros, esses dados necessitam de uma ampla proteção durante todo o seu ciclo (CAVOUKIAN, 2011).
6. O sexto é a visibilidade e transparência, o titular dos dados sempre terá de saber com clareza, para qual finalidade que estão coletando suas informações, e quem tem acesso a elas, para o mesmo ter a certeza se seus dados estão protegidos (CAVOUKIAN, 2011).
7. O sétimo é o respeito pela privacidade do usuário, ou seja, a solução centrada no usuário, sendo este capaz de gerenciar seus próprios dados, visando garantir que este tome suas próprias decisões e, portanto, tenha um consentimento destas (CAVOUKIAN, 2011).

2.2 *Privacy by Default*

Privacy by Default (privacidade por padrão) é uma decorrência do Privacy by Design, conforme informado por Henrique Dantas no blog Advogatech (2019), significa que ao ser lançado no mercado, um produto ou serviço, deve vir por padrão, com as configurações de privacidade no modo mais restrito possível, ou seja, todas as medidas de proteção da privacidade que foram formadas desde o início do projeto, considerando o princípio do Privacy by Design. A privacidade mais restritiva possível é formada desde do momento zero, são coletados apenas os dados essenciais para entregar produto ou prestar um serviço, mesmo assim o usuário ainda deve saber para qual finalidade está sendo utilizada, para quem estão sendo compartilhadas as suas informações e com qual propósito. Caso deseje, o próprio usuário poderá desativar essas salvaguardas. As empresas sempre devem fornecer seus produtos ou serviços com essa opção ativa, nunca desativadas.Muitas empresas de tecnologias fazem totalmente o oposto disto, coletam o máximo de dados possíveis, ainda sim permitindo que os mesmos desativem essa coleta. Se o Privacy by Default fosse aplicado, os aplicativos iriam coletar somente as informações necessárias e iriam permitir, caso achasse benéfico, que o próprio usuário ativasse a coleta de dados extras.

3 ADEQUAÇÃO DE UMA EMPRESA À LGPD

A LGPD é uma lei taxativa, ou seja, não permite que dados pessoais sejam tratados de qualquer outra maneira, diferente do que foi definido no texto legal. Sendo assim, todas as empresas que lidam com dados pessoais deverão estar em conformidade com a nova lei, de acordo com o prazo determinado após sua regulamentação. Cotidianamente, milhares de empresas lidam com dados pessoais, e em muitas delas, esses dados são vitais para o funcionamento do próprio negócio, e todas deverão se adaptar à regulamentação aprovada. Em suma, não se trata de uma opção, mas de uma obrigação das empresas em se adequarem às normas brasileiras de proteção de dados pessoais. E está previsto sanções no caso de descumprimento da LGPD, as empresas poderão ser multadas em até 2% do faturamento anual, podendo chegar até R$50 milhões. No artigo 7º estão dispostas as condições para o tratamento de dados pessoais que devem ser seguidos. Que são os seguintes:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> 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;
>
> 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;
>
> 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, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> 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; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018)

Há vários tipos de processos de adequação que uma empresa pode seguir, ele pode variar de acordo com tamanho, maturidade de processos já existentes, ramo de atividade da empresa entre outros fatores. Como as empresas podem se adequar a LGPD segundo consta no artigo publicado no site Delphos - Lei Geral de Proteção de Dados (LGPD), como se adequar?:

> 1. Nomeando um encarregado: Podem ser pessoas físicas ou jurídicas, de direito privado ou público. São dois agentes, um operador e o controlador. O controlador é responsável pelas decisões do tratamento dos dados pessoais, já o operador é o responsável por efetuar o tratamento desses dados sob o comando do primeiro. As empresas devem nomear 2 nomes que ficarão responsáveis desses cargos.
> 2. Realizar uma auditoria de dados: Os auditores são responsáveis por examinar o sistema, essa auditoria serve para não ficar nada para trás, serve também para verificar a segurança de dados dos sistemas quanto ao controle de acesso, plano de recuperação e backup.
> 3. Revisar as políticas de segurança de dados : Existem ameaças de softwares mal intencionados, quase sempre, por isso é importante rever as políticas de segurança de dados da empresa. É uma boa estratégia, fortalecer a segurança desses sistemas e orientar todos os colaboradores sobre os procedimentos da segurança a serem adquiridos.
> 4. Revise os contratos: Um dos itens mais importantes da LGPD, o contrato tem que deixar claro para quais finalidades os dados estão sendo utilizados, os documentos deve prever a retirada e a portabilidade de dados para outros servidores.

3.1 Documentos Essenciais

Para estar em conformidade com a LGPD, será necessária uma avaliação de maturidade dos processos e impactos de riscos na sua empresa e redução dessa exposição ao risco, ou seja, avaliar todo o cenário empresarial e até onde esses dados são necessários para que os processos ocorram sem impacto. Conforme informado por Davis Alves, Ph.D. presidente da ANPD (Associação Nacional dos Profissionais de Privacidade de Dados) no Webinar - “LGPD - Como as PMEs devem enxergar a adequação?” (ALVES, 2020). Existem 9 documentos essenciais que uma empresa precisa para estar em conformidade com a nova lei LGPD, esses documentos norteiam a adequação da instituição:

1) Política de proteção de dados: como a empresa vai proteger os dados pessoais. Presente nos incisos §§ 1º e 2º do artigo 46 da LGPD:

> 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.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (BRASIL, 2018, Art. 46).

2) Aviso de Privacidade: como a empresa garante a privacidade de dados. Presente nos incisos 1º, 2º, 3º ou 5º do artigo 9º da LGPD.

3) Aviso de Privacidade para funcionários: como a empresa cuida dos dados pessoais de funcionários. Presente no artigo 9º da LGPD.

> 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;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (BRASIL, 2018, Art. 9º).

4) Política de retenção de dados: por quanto tempo a empresa guarda os dados pessoais. Presente nos artigos 5º - X, XIV, XV, 18º - § 1º, 19º - §1 e 9º de forma indireta. Seção II e Seção III - § 3º da LGPD. Conforme consta no artigo 5º da LGPD:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado

> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; (BRASIL, 2018, Art 5°).

5) Cronograma de retenção de dados: quando os dados serão apagados quando não mais necessário. Presente na Seção – II, e Artigos 40 º e 9º de forma indireta da LGPD.

> A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência. (BRASIL, 2018, Art. 40).

6) Formulário de consentimento do titular: quais dados é utilizado consentimento. Presente na seção I – artigo 7(I, § 4º, § 5º) e artigo 8º (§1º ao § 6º), seção II (II, § 2º), da LGPD.

> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. (BRASIL, 2018, Art. 7º).

7) Formulário de consentimento dos pais: alinhado com ECA: estatuto da criança e do adolescente, assinado pelos pais. Presente na seção III – artigo 14 (§ 1 º, § 3º, §3º) da LGPD.

> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. (BRASIL, 2018, Art. 14º).

8) DPO: Nomeação e descrição de cargo do DPO, se for exigido um: colocar no site da empresa. Presente no artigo 41 da LGPD.

> O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 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.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. (BRASIL, 2018, Art. 41).

9) Registro (inventário) de todas as atividades de um processamento, se a empresa tiver mais de 250 funcionários: como é manipulado, pode ser demonstrado por logs de acesso. Presente no artigo 37 º da LGPD. “O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.” (BRASIL, 2018, Art. 37).

3.2 ISO

ISO é a sigla de *International Organization for Standardization*, ou Organização Internacional para Padronização, em português. Tem como objetivo fomentar o desenvolvimento de normas, testes e certificação, com o propósito de impulsionar o comércio de bens e serviços. No site Significados, descrevem a ISO como: “A ISO tem como objetivo principal aprovar normas internacionais em todos os campos técnicos, como normas técnicas, classificações de países, normas de procedimentos e processos, e etc.” Ou seja, é um modo de promover a normalização de produtos e serviços, utilizando determinadas normas para que a qualidade seja melhorada. Muitas empresas adotam as normas da ISO e as utilizam como boas práticas, mesmo sem obter a certificação, e é uma norma reconhecida e vista com bons olhos no mundo inteiro.

3.2.1 ISO 27000

Do ponto de vista da LGPD, a ISO 27000 significa um diferencial complementar, pois a maioria das empresas lidam com algum nível de informação pessoal. Como comentado no site da OSTEC, é uma vantagem a empresa ter a certificação ISO 27000: “Aos olhos dos clientes, agrada a ideia de haver uma chancela dessa magnitude voltada exclusivamente à segurança das informações

que ele fornece – principalmente em tempos de vazamentos de dados, noticiados em uma frequência quase diária nos grandes meios de comunicação.” OSTEC também pontua que:

> ISO 27000: oferece uma visão geral do conceito. Atua como uma norma introdutória, que traz consigo um glossário de termos que prepara para as certificações seguintes.
> ISO 27001: trata dos requisitos para que exista um Sistema de Gestão da Segurança da Informação (SGSI). O SGSI é parte essencial da gestão da empresa, e é baseado em abordagens de risco do negócio com o intuito de estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. Dessa maneira, age como a principal norma que o empreendimento deve utilizar para obter a certificação empresarial em gestão da segurança da informação.
> ISO 27002: trata-se de um documento de práticas no qual consta um conjunto de controles que dá apoio à aplicação do Sistema de Gestão da Segurança da Informação na empresa. Assim, existem certificações profissionais para esta ISO, onde os critérios para avaliar se uma pessoa é ou não qualificada para receber esse certificado são inspecionados com uma prova.

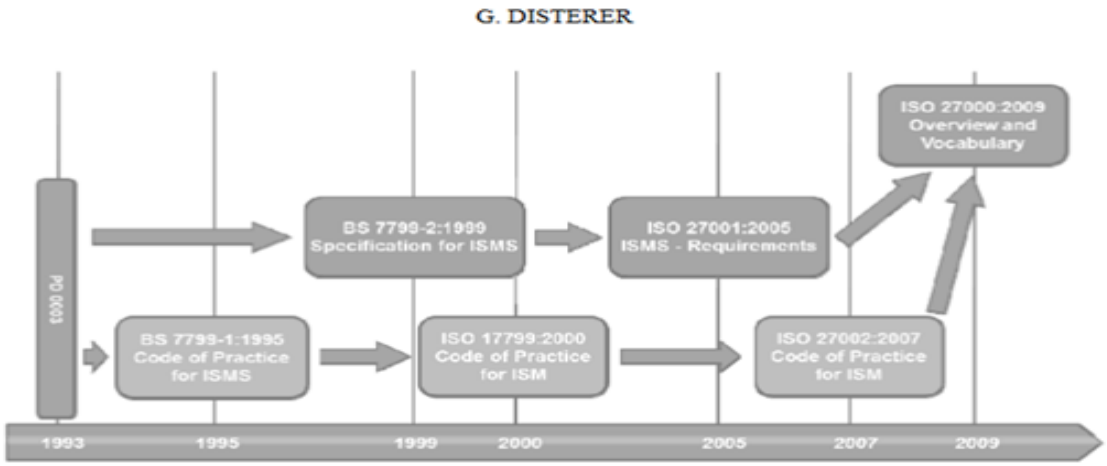
3.2.2 ISO 27001

A ISO 27001 é uma norma internacional certificável para a segurança da informação, que atesta que sua empresa cumpre os requisitos da ISO para gestão da segurança da informação. Ela se apresenta como uma ótima ferramenta para adequação às leis de privacidade de dados como a LGPD e GDPR , vem sendo melhorada com o passar dos anos, seu objetivo é fazer com que as empresas acolham essa norma a fim de garantir a segurança das informações. Conforme consta no artigo científico ISO/IEC 27000, 27001 and 27002 for Information Security Management, escrito pelo alemão Georg Disterer:

> A existência das normas ISO 27000 a ISO 27002 pode ser traçada desde 1993 (Figura 1), pela qual uma associação profissional britânica, o National Computing Centre (NCC), publicou um documento intitulado "PD 0003 Um Código de Prática para Gestão de Segurança da Informação". O British Standards Institute (BSI) adotou isso e emitiu o "BS 7799-1 IT —Técnicas de segurança — Código de prática para gerenciamento de segurança da informação" como padrão nacional em 1995. A parte complementar "BS 7799-2 Information security management systems — Especificação com orientação para uso" permite que as empresas certifiquem seus processos. A ISO harmonizou esse padrão com outras como a ISO 9001 e desenvolveu a ISO 27001 em outubro de 2005. Desde então, as empresas podem certificar seus processos a partir desse padrão internacional. A ISO 27001 formou a base para a família de padrões ISO 27 K, que englobam vários padrões de segurança da informação. Em 2007, a antiga norma ISO 17799 foi atribuída à família ISO 27 K como ISO 27002. Em 2009, a ISO 27000 foi emitida para fornecer uma visão geral, introdução e explicação da terminologia com o título "TI técnicas de segurança –

Sistemas de gerenciamento de segurança de informações. Visão geral e vocabulário"(Tradução Livre).[1]

Figura 01 - G. Disterer



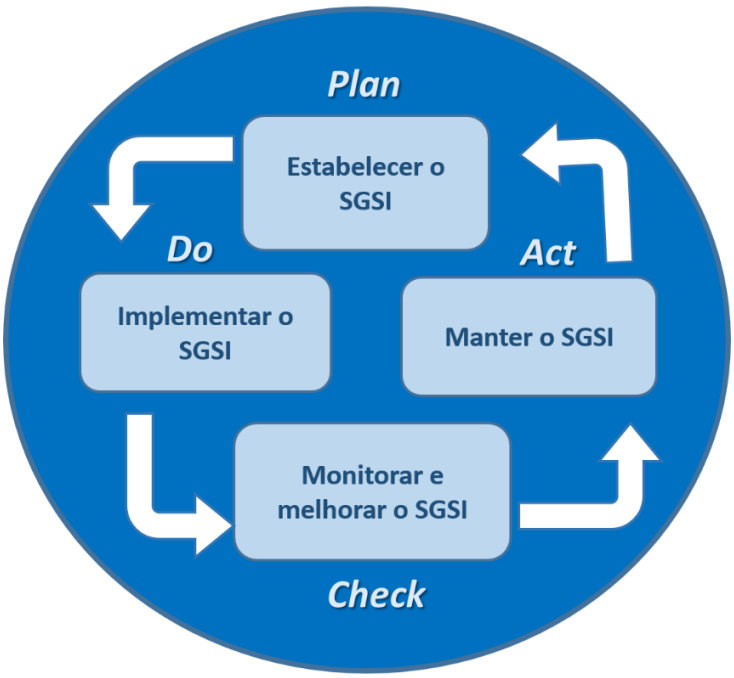
Fonte:DISTERER, Georg. ISO/IEC 27000, 27001 and 27002 for information security management. 2013.[2]

ISO 27001 define os preceitos para um Sistema de Gestão da Segurança da Informação (SGSI), que é um sistema de gestão voltado para a Segurança da Informação, a fim de adotar medidas de proteção à confidencialidade, integridade e disponibilidade das informações. Estes são os principais pilares da Segurança da Informação e inclui toda uma abordagem organizacional que protege a informação empresarial. Para explicar o SGSI, a ISO 270001 adere o modelo do ciclo PDCA, como consta na imagem a seguir encontrada no site Portal GSTI:

[1] The existence of the ISO 27000 to ISO 27002 standards can be traced back to 1993 (Figure 1), whereby a British professional association, the National Computing Centre (NCC), published a document titled “PD 0003 A Code of Practice for Information Security Management”. The British Standards Institute (BSI) adopted this and issued “BS 7799-1 IT—Security techniques—Code of practice for information security management” as national standard in 1995. The complementary part “BS 7799-2 Information security management systems—Specification with guidance for use” enables companies to certificate their processes. ISO harmonized this standard with others like ISO 9001 and developed the ISO 27001 in October 2005. Since then, companies can certify their processes according to this international standard. ISO 27001 formed the foundation for the ISO 27 K family of standards, which encompass various standards for information security. In 2007 the old ISO 17799 standard was assigned to the ISO 27 K family as ISO 27002. In 2009 ISO 27000 was issued to provide an overview, introduction and explanation of terminology with the title “IT—Security techniques—Information security management systems—Overview and Vocabulary”

[2] Dísponível em:
<https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf>

Figura 2 - PDCA



Fonte: Site Portal GSTI (2016)[3]

Para explicar esse ciclo PDCA, temos quatro ações que tem o objetivo de promover a melhoria contínua do processos: Planejar (Plan), Fazer (Do), Checar (Check) e Agir (Act).

As quatros ações do PDCA em SGSI é

1. Planejar: Nesta etapa se estabelece o SGSI
2. Fazer: Após estabelecido o SGSI é o momento de implementar o mesmo.
3. Checar: Após feito os dois primeiros processos são necessários monitorar e melhorar o SGSI
4. Agir: Por fim após melhoria é necessário manter o SGSI, sempre voltando ao início e criando o ciclo, para melhorias e novas informações.

Esta norma pode ser implementada por qualquer organização, não importa se é publico ou privada, grande, médio ou pequeno porte. A maioria dessas organizações obrigam que seus parceiros e fornecedores tenham a certificação da

[3] Disponível em : <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>Acesso em 13, Jun.2020.

ISO 27001 para que seus clientes se sintam confortáveis, quanto a posse de suas informações.

As empresas para protegerem a segurança da informação, devem ter mecanismos, processos e controles para os diversos tipos de segurança, como segurança física, segurança técnica e segurança organizacional. A ISO 27001 apresenta um checklist com os requisitos necessários para a adequação da empresa. Para que esta norma seja implementada nas empresas, estas precisam seguir fatores internos e externos. São 5 etapas para a implementação da ISO 27001:

1- Entender o contexto da organização: Precisa-se entender em sua organização quais são as características e necessidades para assim conseguir estabelecer as políticas e objetivos para a segurança dos dados.

2- Avaliação de riscos: Avaliação dos riscos à segurança dos dados e os processos internos das organizações e criar para todos os itens identificados, uma classificação de risco.

3- Controles operacionais: A fim de Eliminar, diminuir, controlar a classificação dos riscos são implementados controles operacionais nos processos.

4- Análise de eficácia: Auditoria interna. Para garantir a segurança de todas as informações concedidas às empresas, são feitas análises e fiscalizações do desempenho dos controles realizados.

5- Melhoria: Nesta última etapa encontra-se a partir do estabelecimento de certificação um estágio de melhoria contínua, que garante que os processos estão em avaliação constante e riscos monitorados e possíveis novos controles operacionais.

Levando em consideração que um dos maiores recursos empresariais na atualidade é a posse de informações, é primordial que as empresas tenham um sistema para gerenciar e proteger essas informações.

3.2.3 ISO 27002

A ISO 27002 é uma norma internacional que determina códigos de melhores práticas para apoio a implantação o sistema de gestão de segurança nas empresas (SGSI), ela descreve como os controles podem ser estabelecidos, estes por sua vez, devem ser escolhidos com base em uma avaliação de risco dos ativos da empresa. Pode ser implementada igualmente como ISO 27001, não apenas para uma empresa tecnológica, mas sim em qualquer tipo de organização, não importa se é pública ou privada, pequena ou grande porte, com ou sem fins lucrativos. É importante frisar que a ISO 27002 não é uma certificação, mas sim uma norma com dicas e recomendações que devem ser seguidas para que as empresas estejam de acordo com as normas de segurança e assim serem auditadas para conseguirem uma certificação da ISO 27001.

O principal objetivo do ISO 27002 é estabelecer critérios e princípios para iniciar, manter, melhorar e implementar a gestão de segurança da informação em uma organização. Após implementar essa norma, as empresas possuem alguns benefícios, por exemplo: um melhor controle da segurança, oportunidade de identificar e corrigir os pontos fracos, diferencial competitivo para conquistar clientes, promove redução de custos, etc.

3.2.4 ISO 27701

A ISO 27701 é um padrão internacional para proteção de dados e tem um ótimo alcance em relação a adaptação das empresas com as normas de privacidade, como a GDPR e a LGPD. E com a obtenção dessa certificação a empresa estará pronta para atender vários requisitos necessários para essa adequação. Essa norma possui um foco adicional em privacidade de dados em relação às outras normas, como a 27001 que era voltada aos requisitos e a 27002 aos controles. Ela atinge a privacidade através de técnicas para proteção de dados e aplica-se a Controladores e Operadores. Assim dados pessoais, críticos e sensíveis são gerenciados com maior controle e cuidados.

Necessário ressaltar que essa certificação é uma extensão da ISO 27001 e poderá ser obtida apenas após o recebimento do certificado dessa. Ela é aplicável a todos os tipos de organizações e não somente a área de T.I, ela sempre se

relaciona com as normas de segurança da informação, ampliando diretrizes e requisitos, criando novas e específicas, até mesmo mantendo as características já criadas nas normas de segurança da informação.

3.3 A Empresa Alemã de Engenharia e Eletrônica

A empresa alemã que iremos observar quanto ao início do processo de adequação à LGPD foi mantida em sigilo devido a termos de privacidade. Esta empresa, é uma multinacional, conta com aproximadamente 400 mil funcionários pelo mundo. Em 2019 obteve 2,9 milhões de euros de EBIT. Suas plantas localizadas nos países da União Européia já estão em conformidade com a GDPR, isto contribuiu para um melhor entendimento da lei brasileira, sobre sua importância para manter seus negócios com clientes internacionais e locais, e também deu consciência para funcionários em relação à adequação dos processos com tratamento de dados pessoais.

A história da empresa no Brasil iniciou-se em 1954. Atualmente emprega no país cerca de 8 mil trabalhadores e registrou, em 2018, um faturamento líquido de R$ 5.3 bilhões esta informação é relevante para termos uma percepção do valor que pode ter uma sanção sofrida por esta instituição em caso de não conformidade à Lei Geral de Proteção de Dados, como comentamos anteriormente, a multa da não concordância à regulamentação, pode chegar a 2% de seu faturamento, limitada a 50 milhões de reais. Este faturamento está diluído com a oferta de produtos e serviços automotivos para montadoras e para o mercado de reposição, bem como ferramentas elétricas, entre outros. A empresa tem uma maturidade alta em relação à segurança da informação em seus processos, conta com uma política de privacidade sólida, fundamentada na ISO 27001, além de possuir a certificação ISO 27001, e funcionários certificados para realizar auditoria interna. Possui documentação de acessos, regras para arquivamento de documentos, respeitando a confidencialidade, integridade e disponibilidade dos dados e demais requisitos que tange a manutenção da certificação ISO. Todo departamento dispõe de um documento intitulado *Data Concept,* que é um “Conceito de Dados”, onde os dados armazenados pelo departamento são classificados de acordo com sua confidencialidade, integridade e disponibilidade, a partir daí cumpre um prazo de retenção deste dado, que pode ir de 1 a 35 anos. A ideia do *privacy by design* já é incorporada na empresa, que utiliza essa metodologia em toda concepção de

produto e/ou serviço, colocando a proteção da privacidade no centro de todo o desenvolvimento.

Após a promulgação da LGPD pelo então presidente Michel Temer em agosto de 2018, com o prazo inicial estabelecido para adaptação às novas regras de 18 meses, tanto para iniciativa pública como para a privada, e apesar deste prazo inicial já ter sido alterado por medidas provisórias, a empresa alemã observada, iniciou o movimento de adequação à Lei Geral de Proteção de Dados através levantamento de todos os processos com tratamento de dados pessoais dentro de suas atividades. Seguindo a linha que a autora Patrícia Peck elucidada em seu livro Proteção de Dados Pessoais (2019, p.64):

> Para iniciar a implementação dos requisitos de conformidade à LGPD, o primeiro passo é a realização de um levantamento. Ou seja, deve-se fazer uma análise de diagnóstico para identificar como a instituição está no tocando aos indicadores de conformidade e o que falta para atender aos controles exigidos. Para tanto, a primeira atividade é fazer o inventário dos dados pessoais (quais são e onde estão).

Para tal início de implementação e realizar o levantamento dos processos com dados pessoais, foi contratada uma consultoria jurídica, o escritório Opice Blum, capacitado em fraudes cibernéticas, compliance digital, proteção e gerenciamento de dados, a equipe admitida é composta por especialistas da nova legislação, para poder guiar e auxiliar na adequação, tornando-a mais eficiente e ágil. Toda a condição já formada quanto à Segurança da Informação pela empresa alemã como: política de privacidade, certificação ISO 27001, treinamentos periódicos com funcionários, também a questão das demais unidades de negócio da empresa já estar de acordo com a GDPR, foram relevantes para o começo da adequação à LGPD porém não suficiente para deixar a empresa em conformidade, por isso foi elaborado um plano de ação associado à consultoria contratada.

3.4 Plano Adequação Jurídica à LGPD

O plano de adequação à Lei Geral de Proteção de Dados foi criado em conjunto com uma consultoria contratada e o responsável pelo tema de Segurança da Informação na empresa alemã. Além deles, o projeto contou com o apoio dos analistas de segurança da informação da empresa. O planejamento iniciou-se em setembro de 2019, com previsão para ser finalizado a primeira fase em janeiro de

2020. A Opice Blum com intuito de dar um entendimento mais aprofundado sobre a LGPD, realizou um Workshop de conscientização onde houve a oportunidade de expor e debater sobre alguns conceitos importantes acerca da legislação. A proposta contou com a participação de 13 analistas de segurança da informação da empresa alemã. A ideia destes analistas participarem deste Workshop foi deixá-los com o papel de suporte nesta primeira etapa. Depois do treinamento, deu-se início à primeira fase prática de adequação da empresa. Foi elaborado um questionário como parte do primeiro passo para a adequação de conformidade à lei, para ser respondido por todos os departamentos que tem processos com tratamentos de dados pessoais na empresa.

De modo a garantir maior assertividade no preenchimento, foi criado um material com o objetivo de facilitar o preenchimento do “Questionário de Mapeamento de Dados Pessoais”. Foi recomendado sempre verificar as instruções e exemplos dos campos de respostas, no momento do preenchimento em caso de dúvida. Primeiro foi disponibilizado um quadro com alguns conceitos importantes e que podem aparecer no “Questionário de Mapeamento”, apresentado abaixo, no Quadro 2, com termos e definições presentes comumente quando se é falado em LGPD. Apresentamos anteriormente um quadro (Quadro 1) com ideias definidas pela LGPD, de acordo com os autores Klee e Neto. Os conceitos expostos pela Opice Blum estão mais sucintos para atender as demandas específicas pertinentes a empresa do estudo. O material oferecido pela Opice Blum como apoio para o preenchimento dos questionários, nas instruções gerais, destaca uma observação de que deveria ser preenchido um questionário para cada atividade (Quadro 3), ou seja, dentro de um departamento, pode haver diversas atividades distintas que têm tratamento de dados pessoais, não tendo um limite de quantidade de questionários que possam ser preenchidos por cada área.

Então este questionário criado foi o plano de ação à adequação jurídica da empresa com intuito de fazer um levantamento detalhado dos processos de tratamento de dados pessoais, para posteriormente ser feito uma análise do que deverá ser alterado ou já está em conformidade à lei.

Quadro 2 - Conceitos importantes para preenchimento do Questionário de Mapeamento de Dados Pessoais

Termo	Definição
Dados Pessoais	Qualquer informação obtida em razão do presente contrato, relacionada a pessoa natural identificada ou identificável, como por exemplo: nome, CPF, RG, endereço residencial ou comercial, número de telefone fixo ou móvel, endereço de e-mail, informações de geolocalização, entre outros.
Dados Pessoais Sensíveis	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.
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.
Titular dos dados	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Tratamento	Qualquer operação ou conjunto de operações efetuadas com dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição.
Controlador	A quem competem as decisões referentes ao tratamento de dados pessoais, especialmente relativas às finalidades e os meios de tratamento de dados pessoais.
Operador	Parte que trata dados pessoais de acordo com as instruções do Controlador
Autoridade Nacional de Proteção de Dados	Órgão responsável pela fiscalização do cumprimento das disposições da Lei Geral de Proteção de Dados, Lei Federal nº 13.709/2018 no território nacional.
Incidentes	Qualquer acesso, aquisição, uso, modificação, divulgação, perda, destruição ou dano acidental, ilegal ou não autorizado que envolva dados pessoais.

Fonte: Arquivo Pessoal (2019)

O Quadro 3, traz instruções gerais de preenchimento, como: as áreas devem preencher somente dados pertencentes à elas mesmas, não devem utilizar de dados de outras áreas. E também ressalta que cada atividade que faz tratamento de dados pessoais, deve ser preenchido em um questionário distinto do outro.

Quadro 3: Instruções de preenchimento

Objetivo	Mapear as atividades de tratamento de dados pessoais, com base em cada processo da companhia.
Instruções Gerais	- Preencher apenas dados relacionados à sua área. - Preencher um formulário para **cada atividade** de tratamento.

Fonte: Arquivo Pessoal (2019)

Ao total o questionário contém 25 campos a serem preenchidos, dentre eles espaços para identificação, como o nome de quem respondeu, a área e/ou departamento e o nome da atividade relativa ao questionário. Estes campos servem para facilitar assimilação dos processos posteriormente pela Opice Blum. De outro modo também contém campos mais específicos e significativos à LGPD, como por exemplo se há a coleta do consentimento do titular do dado, quais são os dados pessoais coletados no processo e qual é a base do legal do tratamento desses dados, essas questões são importantes para estar de acordo com a regulamentação. Todas as perguntas contidas no questionário elaborado pela Opice Blum estão no Quadro 4:

Quadro 4: Campos a serem preenchidos (continua)

Nome do respondente ***Aviso: É necessário preencher um formulário para cada atividade de tratamento de dados***
Nome da sua Área/Departamento
RH Financeiro Atendimento ao Cliente Auditoria Interna Juridico Marketing Compliance/Ética Tecnologia da informação Outras: -Engenharia -Qualidade -Manutenção -Logística -Manufatura -Controladoria -Vendas -Compras,-Meio Ambiente, Segurança Patrimonial e Saúde -Inovação -Ambulatório
Qual o nome de sua área?
Processo/Atividade
Já possuo relacionamento direto com o titular dos dados? (Exemplo: SIM - o titular já é seu cliente ou cadastrou-se em seu site. NÃO - Recebeu os dados de uma base terceira para prospecção de novos clientes.)
Sim Não Sim, mas não para a totalidade dos dados
Ponto de Coleta **Onde o dado foi coletado? Assinale quantas opções forem necessárias.*
Site Aplictivo Mobile Serviço Atendicemento ao Cliente Central Telefônica Processo RH Ponto de venda Fisico Outros
Origem do Dado(Quem forneceu o dado? Titular: o próprio titular do dado a informação; Responsável: responsável da criança ou adolescente; Terceiro: o dado foi coletado por meio de terceiro.)
Titular Responsavel(criança ou adolescente) Terceiro ou Titular+terceiro

Quadro 4: Campos a serem preenchidos (continua)

Terceiro de Origem(Caso um terceiro tenha provido o(s) dado(s) pessoal(is), informar quem é este terceiro. Por exemplo: Serasa Experian.)
Esta atividade envolve tomada de decisões automatizadas? **(Decisões automatizadas: aquelas tomadas de maneira automática com base nos dados pessoais (por exemplo, pelo uso de inteligência artifical ou regras pré-determinadas).*
Sim Não
Volume estimado de dados
Numero de campos de dados pessoais x numero de pessoas
Natureza dos dados
Dados financeiros Dados cadastrais Dados comportamentais Outros
Possui dados de algumas dessas categorias? *
De menores de 12 anos de idade De maiores de 12 e menores de 18 anos de idade Saúde ou vida sexual Origem racial/étnica, religião, opinião ou filiação política ou filiação sindical Genético ou biométrico Não possuo nenhum dos dados mencionados acima
Dados pessoais envolvidos (Detalhe quais os dados pessoais que estão envolvidos neste processo. Por exemplo: nome, CPF, perfil de consumo, renda anual, etc.)
Nível de criticidade dos dados (1 - Baixa; 2 - Média; 3 - Alta) O nível de criticidade é de acordo com a política interna da organização ou a interpretação da área de negócio. Quanto maior o volume de dados e mais sensíveis as informações, maior a criticidade.)
Finalidade ****(Descrever para qual finalidade o dado é tratado.)***
Base legal para tratamento(Informar a base legal, nos termos da LGPD, que permite o tratamento destes dados.)
Obrigação legal ou regulatória Proteção da vida de titular ou terceiro Prevenção à fraude e segurança Legítimo interesse Proteção ao Crédito Tutela da saúde por profissional de saúde Exercício Regular de Direito Consentimento Execução de Contrato Não sabe informar

Quadro 4: Campos a serem preenchidos (conclusão)

Como o consentimento é obtido? *(Informar como é obtido o consentimento do titular do dado pessoal.)Exemplo: Por meio de cláusula contratual específica e destacada, em contrato assinado à mão pelo titular do dado.*
Compartilhamento de dados *
Não é compartilhado Terceiro Área Interna Empresa do mesmo grupo
Com quem os dados são compartilhados? *Ex.: Departamento de Marketing e XYZ Processamento de Folhas de Pagamento Ltda.*
O dado é compartilhado para o exterior? *
Não, somente dentro do território brasileiro. Sim e também é compartilhado dentro do território brasileiro. Sim, apenas para o exterior.
Países envolvidos *
Qual o prazo de retenção dos dados? *Indicar por quanto tempo os dados são armazenados/retidos após cessado seu uso.*
Transcorrido o período de retenção, o dado é descartado ou destruído? *
Sim Não
Alguma observação adicional em relação a este processo/atividade?

Fonte: Autoria Própria (2020)

As perguntas deveriam ser respondidas por uma pessoa julgada tendo o melhor conhecimento do processo, em que estava sendo respondido dentro do departamento, isto sempre com o auxílio do analista de segurança da informação treinado pelo escritório jurídico Opice Blum. A primeira fase da adequação foi o preenchimento deste questionário por cem por cento dos departamentos que tem coleta, tratamento e armazenamento de dados pessoais. Esta fase iniciou-se em outubro de 2019, com limite para serem finalizados em janeiro 2020, totalizando 4 meses.

4 PRIMEIRA FASE DA ADEQUAÇÃO À LGPD

A advogada Patrícia Peck, comenta em seu livro Proteção de Dados Pessoais, que: “A complexidade da implementação desse tipo de regulamentação se dá pelo fato de que os negócios estão globalizados” (2019, p.64). Há uma necessidade de se aplicar uma abordagem de direito comparado e de direito internacional, ainda mais porque já dispõem leis em diferentes países. Particularidades irão surgir dependendo do ramo de negócio da empresa e de sua maturidade relacionada a administração dos dados pessoais. Por se tratar de uma empresa de grande porte e possuir negócios e processos globalizados, a empresa deste estudo precisa estar conforme a GDPR e a LGPD, e cada lei tem sua singularidade de acordo com seu país de atuação.

4.1 Particularidades do questionário

Alguns campos merecem maior observação, por serem mais relevantes na adequação. A maioria destes campos remetem a fatores essenciais que dita a lei. No quadro 5, o questionamento é sobre a origem do dado. As opções são: dados fornecidos pelo próprio titular, pelo responsável quando se trata de criança ou adolescente, por terceiro e ainda a opção do dado pessoal ter sido fornecido por uma combinação destes. Essa informação é pertinente, pois a LGPD traz os direitos do titular dos dados, como citado anteriormente. Sendo assim, o titular pode recorrer aos seus direitos quando tem seus dados coletados.

Quadro 5: Origem do Dado

Origem do Dado	Indicar quem forneceu o dado. Se: a) Titular: O Titular dos dados é quem forneceu as suas próprias informações; b) Responsável (de criança ou adolescente): o pai, a mãe ou um responsável legal forneceu os dados de uma criança ou adolescente; c) Terceiro: Dados pessoais de um Titular foi fornecido por consultoria terceirizada, parceiros, etc.) d) Titular/Responsável + Terceiro: quando os dados pessoais envolvidos numa operação de tratamento foram fornecidos pelo menos por duas das seguintes pessoas: o titular, o responsável e o terceiro.

Fonte: Arquivo Pessoal (2019)

O quadro 6 faz referência a finalidade da coleta do dado, que também tem sua importância, visto que a finalidade está entre os princípios da Lei Geral de Proteção de Dados para um tratamento considerado legítimo, específico e explícito aos titulares, ou seja, as empresas não podem coletar informações e, depois, usá-las para outros fins. Além disso, a finalidade está bastante vinculada com o consentimento do titular do dado, esse que é a linha principal para o tratamento de dados. Ambos necessitam da consciência do titular, o consentimento precisa ser expresso por ele e a finalidade deve ser apresentada a este.

Quadro 6: Finalidade

Finalidade	Por que a companhia precisa dos dados? Para que são utilizados? Mencionar todos os procedimentos que não poderiam ser feitos sem esse dado. P.ex.: Emissão de Nota Fiscal

Fonte: Arquivo Pessoal (2019)

A base legal para o tratamento de dados pessoais, tem diversas opções, que estão entre: obrigação legal ou regulatória, tutela da saúde por profissional de saúde, proteção da vida de titular ou terceiro, exercício regular de direito, prevenção à fraude e segurança, consentimento, legítimo interesse, execução de contrato e proteção ao crédito. Essas hipóteses taxativas para o tratamento de dados, estão no artigo 7º da LGPD, e significa que o tratamento de dados somente poderá ser legalmente realizado dentro dessas previsões. Vale lembrar que nenhuma das hipóteses legais prepondera sobre as demais, sendo sempre necessário buscar a base legal que seja mais adequada às operações do controlador.

No quadro 7 é possível observar as opções de escolha referente a base legal. No material preparado pela Opice Blum, foram listados exemplos e dado um breve significado para cada um deles, contando que a base legal é categórica, é fundamental que a resposta a essa questão esteja o mais próximo da realidade possível, para caso nos próximos passos seja necessário uma modificação dentro da atividade realizada, seja feita da melhor maneira possível.

No quadro 8, é a questão referente ao prazo de retenção, isto é, indagando por quanto tempo os dados são mantidos pela companhia após o término da finalidade. E também se ocorre o descarte e a destruição do dado quando o prazo é atingido. Esse ponto entra em um dos documentos essenciais indicado por Davis

Alves (ALVES, 2020) para adequação de uma empresa, que foram listados outrora: “ Política de retenção de dados: por quanto tempo a empresa guarda os dados pessoais e cronograma de retenção de dados: quando os dados serão apagados quando não mais necessário.” A empresa alemã conta com uma política de retenção de dados e descarte, conforme informado no documento *Data Concept* de cada departamento.

Quadro 7: Base Legal para tratamento

Base Legal para tratamento	Conforme a Lei Geral de Proteção de Dados, toda atividade de tratamento tem de estar justificada em uma base legal (hipótese da Lei Geral de Proteção de Dados que autoriza o tratamento). Selecionar na lista a base legal que parece mais se encaixar com a atividade: a) Obrigação legal ou regulatória: Quando uma norma, lei, regulamento ou decisão judicial obriga o tratamento dos dados pessoais. O tratamento deve ser uma obrigação, não pode ser opcional. Ex.: Declaração de imposto de renda, cumprimento de acordo judicial. b) Tutela da saúde por profissional de saúde: Para realização de procedimentos visando a proteção da saúde do titular. Somente pode ser usada por profissionais da saúde, autoridade sanitária, ou serviços de saúde. Ex.: consulta médica. c) Proteção da vida de titular ou terceiro: Em situações de vida ou morte, ou para proteger a incolumidade física do titular\ar ou de terceiros. A vida ou incolumidade física de alguém deve estar em risco para justificar o enquadramento. Ex.: Atendimento de emergência. d) Exercício Regular de Direito: Quando o tratamento é necessário para a defesa de direitos em processos administrativos, judiciais ou arbitrais. Ex.: Análise pelo departamento jurídico, arquivamento de recebido de pagamentos e comprovante de entrega. e) Prevenção à fraude e segurança: Quando a informação sensível é utilizada para garantir a segurança do titular ou prevenir fraudes, nos processos de identificação e autenticação de cadastro. Ex.: Biometria para registro de ponto. f) Consentimento: Quando nenhuma outra base legal puder justificar o tratamento, o titular precisa dar seu consentimento. Ex.: Formulário de "fale conosco", com a coleta de consentimento separado para o cadastro em *mailing*. g) Legítimo interesse: Para apoiar as atividades do controlador, ou para o benefício do titular. Ex.: Dados e estatísticas de uso de serviços para melhoria. f) Execução de Contrato: Quando o tratamento é necessário para cumprimento de contrato com o titular, ou para possibilitar o cumprimento futuro. Ex.: Prestação de serviços para o titular, atendimento ao cliente. h) Proteção ao Crédito: Quando o tratamento é necessário para o cumprimento de contrato com o titular, ou para possibilitar o cumprimento futuro. Consulta em órgãos de proteção ao crédito. i) Não sabe informar: Caso não consiga identificar alguma das bases legais acima.

Fonte: Arquivo Pessoal (2019)

Quadro 8: Prazo de Retenção, Descarte

Prazo de Retenção	Por quanto tempo os dados são mantidos pela companhia após o término da finalidade? Ex.: Nome de cliente: 5 anos, a partir do final do atendimento. Se permanente, inserir "Permanentemente". Se não há regra, inserir "Indeterminado".
Transcorrido o período de retenção, o dado é descartado ou destruído?	Há o descarte do dado após a finalidade é atingida? Ou o dado é mantido para outros fins?

Fonte: Arquivo Pessoal (2019)

Por fim, vale ressaltar a questão: Como o consentimento é obtido? Devendo informar como é obtido o consentimento do titular do dado pessoal. Como mencionado, o consentimento é o primeiro requisito que as empresas precisam cumprir para lidar com dados. Caso esta exigência não seja cumprida pela empresa, seja necessária uma modificação no processo de coleta do dado pessoal, adicionando alguma forma do titular consentir a coleta, por exemplo: por meio de cláusula contratual específica e destacada, em contrato assinado à mão pelo titular do dado.

4.2 Questionários coletados

O levantamento das atividades que possuem coleta, tratamento e armazenamento de dados pessoais, foi o primeiro passo dado pela empresa, após os quatro meses de prazo estipulado inicialmente para o preenchimento dos questionários de mapeamento de dados pessoais por todos os departamentos desta e foram coletados um total de 556 questionários respondidos.

Dentre estes mais de 500 questionários respondidos, todas as áreas da empresa tiveram algum processo com coleta de dados pessoais preenchido. As áreas: Recursos Humanos, jurídico, *compliance*, ambulatório, áreas estas que lidam mais com pessoas, foram as que tiveram maior número de coleta de processos. Estes questionários foram para análise do escritório jurídico Opice Blum, que fará uma análise mais aprofundada e com uma noção mais especializado na LGPD, para apresentar quais desses processos precisarão de algum ajuste ou não para estar de acordo à nova lei. Na tabela 1 é possível visualizar a quantidade de questionários

respondidos por todas as áreas na empresa, totalizando os 556 questionários coletados.

Tabela 1 - Quantidade de questionários respondidos por área/departamento

ÁREA/DEPARTAMENTO	QTD QUESTIONÁRIOS
Recursos Humanos	76
Financeiro	31
Atendimento ao Cliente	28
Auditoria Interna	12
Juridico	70
Marketing	17
Compliance/Ética	52
Tecnologia da informação	18
Engenharia	19
Qualidade	16
Manutenção	5
Logística	25
Manufatura	7
Controladoria	20
Vendas	31
Compras	32
Meio Ambiente	4
Segurança Patrimonial	11
Inovação	18
Ambulatório/Saúde	64
Total	556

Fonte: autoria própria (2020)

4.3 Próximos passos

O preenchimento dos questionários pelos departamentos com o objetivo de levantar e fazer um inventário de todos os processos com tratamento de dados pessoais da empresa, foi o primeiro passo dado por esta para iniciar a adequação e estar em conformidade com a LGPD. Outros procedimentos ainda serão necessários, pois agora os questionários estão em análise da consultoria jurídica Opice Blum, que fará um julgamento do que precisa ser modificado em cada processo ou não, baseados nas informações obtidas pelo mapeamento. Outro passo importante que até o momento está pendente pela empresa alemã é a

definição do DPO (*Data Protection Officer*), ou seja, o Encarregado de Proteção de Dados. A ideia é que as empresas tenham alguém para cuidar da proteção de dados pessoais que tratam.

5 CONSIDERAÇÕES FINAIS

A aprovação da Lei Geral de Proteção de Dados, Lei nº 13.709/2018, chamada de LGPD no Brasil, em agosto de 2018, foi acelerada após o Regulamento Geral de Proteção de Dados (GDPR) entrar em vigor na Europa, em maio de 2018. O país deu um passo importante para a proteção e privacidade dos dados pessoais, adequando-se às práticas de países desenvolvidos. Esses tipos de leis trazem segurança jurídica para os cidadãos e inibem o descuido por parte das empresas. Além de favorecer relações econômicas, políticas entre países que possuem legislação voltada à proteção de dados pessoais e não podemos negar que uma adequação à LGPD gera a oportunidade de fazer com que as pessoas tenham consciência sobre a importância do tratamento de dados no seu dia-a-dia.

As questões de conformidade à LGPD ainda é um desafio constante de compreender, por se tratar de uma lei recém aprovada e pioneira no quesito dados pessoais, o assunto é atual e passível de alterações, além de ser um tema de constantes estudos em fase de conclusão. Todas as ações a serem tomadas por parte de empresas públicas e privadas ainda tem hesitações.

O trabalho se limitou a estudar o início de uma adequação à conformidade a LGPD pela empresa alemã que apresenta um modelo de empresa multinacional, de grande porte e detém de uma política de privacidade, certificação ISO 27001, política de conceitos de dados, com padrão de tempo de retenção e armazenamentos dos dados pessoais, todas estes requisitos são considerados essenciais, o que colabora com o processo de adequação por parte da empresa, porém impossibilitando generalizações a nível de pequenas e médias empresas possam ser consideradas.

Foi possível analisar através deste estudo, que estar em conformidade à LGPD demanda trabalho e também necessita de conhecimentos básicos dos conceitos referentes à dados pessoais, por isso a empresa optou pelo suporte de uma consultoria jurídica, para tornar esta adequação mais eficiente, visto que as sanções previstas pela lei são consideradas de altíssimos valores, e estar em conformidade não é uma opção, pois a lei é taxativa. Foi disponibilizado um material de apoio com comentários a fim de auxiliar o respondente. Departamentos que usualmente utilizam dados pessoais e dados pessoais sensíveis em suas atividades

rotineiras, como recursos humanos, jurídico e ambulatório, tiveram um maior número de questionários respondidos, o que tomará maior demanda de análise pela consultoria jurídica e possíveis adaptações mais consistente à LGPD.

Ademais, estar de acordo com a nova regulamentação exige um planejamento que vai além do levantamento dos processos com tratamento de dados pessoais, é necessário analisar documentos já utilizados pela empresa, envolver grande número de trabalhadores e é indicado ser feito em etapas, e estar atento ao prazo que a lei passa a entrar em vigor podendo sancionar as multas previstas.

REFERÊNCIAS

ALBUQUERQUE, Daniela. **ISO 27001 - Como Implementar? Tudo o que Você Precisa Saber.** Templum, [s.d.]. Disponivel em: <https://certificacaoiso.com.br/iso-27001/>. Acesso em 11, Jun. 2020.

ALVES, D. LGPD - **Como as PMEs Devem Enxergar a Adequação?** Youtube. Abril. 2020. Disponível em: <https://www.youtube.com/watch?v=mYoD7S0mBGU&t=3518s> Acesso em 15 de junho de 2020.

BEZERRA, A. C.; WALT, I. **Privacidade, Neutralidade e Inimputabilidade da Internet no Brasil: Avanços e Deficiências no Projeto do Marco Civil**

BLUM, Renato Opice; SCHUCH, Samara. **Compartilhamento e comercialização de dados pessoais em ambiente on-line**. Contraponto jurídico. Ed. 2019.

BRANDÃO. L. C. C. **O Marco Civil da Internet e a Proteção de Dados: diálogos com a LGPD**. 2019

BRASIL. **Lei 13. 709, de 14 de agosto de 2018.** Diário Oficial da República Federativa do Brasil. Brasília, DF: 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 01 junho 2019.

Café Jurídico: **Implementação Prática da LGPD e seus Desafios.** Entrevistadores: Aline Carneiro e Tales Calaza. Entrevistado: Marcílio Braz. UberHub LegalTech,15 de maio de 2020. Podcast. Disponível em: https://spoti.fi/2Ao3ok3. Acesso em 23 de maio de 2020.

CAVOUKIAN, Ann. **Information & Privacy:7 Foundational Principles. Internet Architecture Board**. 2011. Disponível em: https://www.iab.org/wp-content/IABuploads/2011/03/fred_carter.pdf. Acesso em 25 maio.2020.

DANTAS, Henrique. **LGPD: O que é Privacy by Design e Privacy by Default**. Advogatech, 2019. Disponivel em: <https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv>. Acesso em 17, Jun. 2020.

DELPHOS. **Lei Geral de Proteção de Dados (LGPD), Como se Adequar?**. Delphos. [s.d.]. Disponível em:<https://www.delphos.com.br/lei-geral-de-protecao-de-dados-lgpd-como-se-adequar> Acesso em 14 de junho de 2020.

DISTERER, Georg. **ISO/IEC 27000, 27001 and 27002 For Information Security Management**, 2013.Disponível em: <https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf> Acesso em 13, Jun. 2020.

FRAGOSO. N. **O impacto do Marco Civil sobre a proteção da privacidade no Brasil**. [s.d.]. Disponível em <https://www.internetlab.org.br/pt/especial/o-impacto-

do-marco-civil-sobre-a-protecao-da-privacidade-no-brasil/> Acesso em 21 de maio de 2020.

INTEGRITY. **Em Que consiste? ISO 27001 Sistema de Gestão de Segurança da Informação**, [s.d.]. Disponivel em: <https://www.27001.pt/iso27001_3.html>. Acesso em 07, Jun. 2020.

INTEGRITY. **O Que é a norma ISO 27001?. ISO 27001 Sistema de Gestão de Segurança da Informação**, [s.d.]. Disponivel em: <https://www.27001.pt/index.html>. Acesso em 07, Jun. 2020.

INTEGRITY. **Para Que Serve? ISO 27001 Sistema de Gestão de Segurança da Informação**, [s.d.]. Disponivel em: <https://www.27001.pt/iso27001_2.html>. Acesso em 07, Jun. 2020.

INTEGRITY. **Quais os Benefícios Para os Clientes, Fornecedores ou Parceiros? ISO 27001 Sistema de Gestão de Segurança da Informação**, [s.d.]. Disponivel em: <https://www.27001.pt/iso27001_5.html>. Acesso em 07, Jun. 2020.

INTEGRITY. **Quais os Benefícios Para Quem a Adopta? ISO 27001 Sistema de Gestão de Segurança da Informação**, [s.d.]. Disponivel em: <https://www.27001.pt/iso27001_4.html>. Acesso em 07, Jun. 2020.

JOSE MILAGRE. **O que é ISO 27701 e Como Entender a Aplicação da Norma Para Gestão da Privacidade da Informação em 5 Passos**. José Milagre & Associados, 2019. Disponivel em: <https://josemilagre.com.br/blog/2019/12/11/o-que-e-iso-27701-e-como-entender-a-aplicacao-da-norma-para-gestao-da-privacidade-da-informacao-em-5-passos/>. Acesso em 13, Jun. 2020.

KLEE. A. E. L., NETO. A. N. P. **A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica.** 2019.

MIDAS SOLUTIONS. **Privacy by Design: Entenda Tudo e Prepare-se Para a LGPD**. Midas Solutions, 2019. Disponivel em: <http://www.midassolutions.com.br/blog/privacy-by-design-privacidade-dados/>: Acesso em 04, Jun. 2020.

MONTEIRO. R. L. **Lei geral de Proteção de Dados do Brasi l - Análise**. 2018

OLIVEIRA, Samanta. **LGPD: as Diferenças Entre o Privacy by Design e o Privacy by Default. Consumidor Moderno**, 2019. Disponivel em: <https://www.consumidormoderno.com.br/2019/05/27/lgpd-diferencas-privacy-design-privacy-default/>. Acesso em 17, Jun. 2020.

OSTEC. **ISO 27000: As Vantagens da Certificação de Segurança da Informação Para o Seu Negócio**. [s.d.]. Disponível em <https://ostec.blog/geral/iso-27000-vantagens-certificacao-seguranca> Acesso em 15 de junho de 2020.

PALMA, Fernando. **Sistema de Gestão de Segurança da Informação (SGSI)**. Portal GSTI, 2016. Disponivel em: <https://www.portalgsti.com.br/2016/12/sistema-

de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em 13 de junho de 2020.

PANDINI, Willian. **30 dez ISO 27002: Boas Práticas Para Gestão de Segurança da Informação**. Ostec Segurança Digital de Resultados, [s.d.].Disponivel em: <https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi>. Acesso em 07 de junho de 2020.

PIGATTI. C. M. R. B. **PROJETO DE LEI Nº 53/2018**. Aprovado em 10 de julho de 2018. Disponível em <https://spcm.com.br/dmkt/Parecer-Projeto-de-Lei-53-2018.pdf> Acesso em 30 maio 2020.

PINHEIRO, P. P. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 2 Ed. São Paulo. Saraiva. 2019.

SOCIAL MINER. **Privacidade de Dados: Tudo que sua empresa precisa saber sobre a LGPD**. [s.d.]. Disponível em: <http://blog.socialminer.com/people-marketing/privacidade-de-dados-e-tudo-sobre-a-lgpd/#E_o_que_sua_empresa_tem_a_ver_com_isso> Acesso em 01 de junho de 2020.

SOCIAL MINER. **A Nova Lei Geral de Proteção de Dados. Cuidados que você precisa tomar pra não ser penalizado pela LGPD**.

Significado de ISO. Significados, 2018. Disponível em: <https://www.significados.com.br/iso/>. Acesso em 20, Jun. 2020.