Brazilian Journals of Business

Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso

Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution - A case study

DOI: 10.34140/bjbv2n4-012

Recebimento dos originais: 20/08//2020
Aceitação para publicação: 20/09/2020

Tiago Celidonio
Pós-Graduado em Gestão Estratégica da Tecnologia da Informação pela Faculdade Batista de Minas Gerais – FBMG
Instituição: Faculdade Batista de Minas - FBMG
Endereço: Rua Navio Sálvia, 310 Bl. A apto 56 Jd. Roma Jundiaí-SP
E-mail: tiago_celidonio@outlook.com

Paulo Sergio Neves
MBA em Gerenciamento de Projetos - UNIVEM – Centro Universitário Eurípides de Marília Pós-Graduado em Gerenciamento de Processos de Negócio - UNISC – Universidade de Santa Cruz do Sul
Instituição: Lozinsky Consultoria de Negócios
Endereço: Rua Desembargador Guimarães 92, AP 135, Agua Branca, São Paulo - SP CEP: 05002-050
E-mail: paulo.sergio@lozinskyconsultoria.com.br

Claudio Melim Doná
Mestre em Gestão e Sistemas Produtivos
Instituição: Centro Estadual de Educação Tecnológica Paula Souza
Endereço: Rua Bartholomeu do Canto 248, Vila Palmeiras, São Paulo – SP CEP: 02726-090
E-mail: claudio.dona@lozinskyconsultoria.com.br

RESUMO
No Brasil, tem-se ouvido o relado de muitas empresas a respeito das dificuldades de entendimento sobre como implementar os controles previstos na Lei Geral de Proteção de Dados do Brasil (13.709/18) e se essa adequação é realmente necessária.
Este artigo apresenta o resultado do mapeamento dos requisitos listados na LGPD em uma instituição financeira no Brasil controlado por uma instituição mundial com filiais no mundo inteiro, e que a partir de metodologia própria descrita neste artigo, resultou em um diagnóstico e recomendações de ações necessárias para adequar essa empresa à LGPD.
O método de pesquisa escolhido foi análise bibliográfica do tema junto a sites especializados, publicações como artigos, livros, revistas da área e congressos nacionais e internacionais, pesquisa-ação e estudo de caso.
A combinação de diferentes teorias, métodos e fontes de dados pode ajudar a superar o viés natural que atinge estudos com abordagens singulares (DENZIN, 1970) e oferecer uma resposta mais robusta

Brazilian Journals of Business

à questão proposta, do que aquela que seria produzida por um desenho de pesquisa somente quantitativo ou somente qualitativo (YIN, 2006).
Os resultados mostraram que dos 325 controles determinados pela LGPD e analisados a partir da metodologia proposta, 117 itens de controles (ou 36%) foram atendidos plenamente, 67 itens (ou 21%) atendem atendidos parcialmente e 141 (ou 43%) controles não atendem as necessidades legais. Constatou-se dessa, forma elevado risco de a empresa incorrer em não conformidades quando aplicada a legislação de proteção de dados pessoais, advinda da lei.

Palavras-chave: Metodologia, Mapeamento, Adequação, SGPI, LGPD, GDPR.

ABSTRACT
In Brazil, many companies have heard reports of difficulties in understanding how to implement the controls provided for in the General Data Protection Law of Brazil number 13.709 / 18 and whether this implementation is really necessary.
This article presents the result of mapping the requirements listed in the LGPD in a multinational financial institution with headquarters in Switzerland and branches in Brazil, based on the methodology described in this article and, based on this survey, recommending the necessary actions for the adequacy of that company the law.
The chosen research method was a bibliographic analysis of the topic with specialized websites, publications such as articles, books, magazines in the area and national and international congresses, action research and case study.
The combination of different theories, methods and data sources can help to overcome the natural bias that affects studies with singular approaches (DENZIN, 1970) and offer a more robust answer to the proposed question, than that which would be produced by a research design only quantitative or only qualitative (YIN, 2006).
The results show that of the 325 controls analyzed from the methodology proposed in this work, 117 (or 36%) fully meet the requirements of the law, 67 (or 21%) only partially meet and 141 (or 43%) of the controls do not meet the requirements determined by the LGPD.
In this way, a high risk of the company was found to incur non-conformities when confronted with the law.

Keywords: Methodology, Mapping, Adequacy, SGPI, LGPD, GDPR.

1 INTRODUÇÃO

O Brasil possui mais de quarenta normas federais que, de várias maneiras, lidam com proteção de dados e privacidade, criando uma estrutura legal complexa.

Para reduzir os riscos à privacidade, a pergunta a ser feita para todos os líderes de negócios é se podemos alcançar nossas metas corporativas com métodos menos invasivos à privacidade ou processando dados pessoais com menos riscos a pessoa (WILLEMSEN, 2019).

A LGPD (Lei Geral de Proteção de Dados do Brasil -13.709/18) capacitará os indivíduos e as empresas em um conjunto de direitos e deveres, em vez complexidade e da proteção parcial das leis setoriais em vigor hoje, e é inspirado no Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

O setor público e o privado, assim como o terceiro setor, estão em alta demanda por projetos de adequação à LGPD e esse cenário tem gerado oportunidades de negócios para escritórios jurídicos e consultorias especializadas no tema.

Dessa forma, o desenvolvimento e concepção de uma metodologia madura, assertiva e contendo boas práticas para implantação de projetos que exijam conhecimento sobre essa lei é um fator altamente requerido para propiciar uma agilidade na diagnóstico e a obtenção de êxito nesse novo mercado, fazendo que os clientes que demandem essa atuação, mitiguem os riscos rapidamente.

A forte experiência em infraestrutura, governança de serviços, segurança de TI e especialização em direito digital de uma equipe multidisciplinar de consultores seniores, permitiu a concepção de uma metodologia eficiente, onde foi necessário superar dificuldades e desafios impostos pela regulamentação requerida pela LGPD em um ambiente extremamente complexo e critico como o segmento de investimentos financeiros tratado neste artigo.

Este estudo guiou-se pelo seguinte objetivo geral: Fazer o mapeamento dos requisitos listados na LGPD em uma instituição financeira, a partir de metodologia própria descrita neste artigo e, com base nesse levantamento, recomendar as ações necessárias para a adequação dessa empresa à lei.

2 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa tem como procedimentos metodológicos, análise bibliográfica do tema junto a sites especializados, publicações como artigos, livros, revistas da área e congressos nacionais e internacionais, pesquisa-ação e estudo de caso realizado em uma empresa multinacional do segmento financeiro denominada neste artigo como Empresa Ômega.

A combinação de diferentes teorias, métodos e fontes de dados pode ajudar a superar o viés natural que atinge estudos com abordagens singulares (DENZIN, 1970).

A lógica subjacente da integração de métodos analíticos é oferecer uma resposta mais robusta à questão proposta, do que aquela que seria produzida por um desenho de pesquisa somente quantitativo ou somente qualitativo (YIN, 2006).

Yin (2006), no entanto, afirma que para ser considerado como método misto, o desenho de pesquisa não precisa, necessariamente, combinar técnicas quantitativas e qualitativas.

A pesquisa-ação é um dos vários tipos de investigação-ação, um termo genérico para todo processo no qual estão envolvidas a ação no campo da prática e a investigação a respeito dela.

Trata-se de um método que combina várias técnicas de pesquisa social, utilizando uma estrutura coletiva, participativa e ativa para a captação de informações (THIOLLENT, 1997).

Segundo Lima (2005), essa abordagem é útil como um caminho na busca de elementos teóricos e práticos voltados a resolução de problemas em um contexto social.

Para Oliveira (2000), essa metodologia é de natureza essencialmente qualitativa, ou seja, não mensura o objeto, mas suas categorias e atributos tais como; qualidade, relação, ação, dentre outros.

O estudo de caso não é uma técnica específica. É um meio de organizar dados sociais preservando o caráter unitário do objeto social estudado (GOODE; HATT, 1969).

Para Goode (1969), o método do estudo de caso é considerado um tipo de análise qualitativa com controle possível do investigador sobre o real evento comportamental e o foco na atualidade, em contraste com o caráter do método histórico.

Bonoma (1985) sugere que o estudo de caso é uma descrição de uma situação gerencial. Para este autor os objetivos de um estudo de caso não são a quantificação ou a enumeração, mas sim a descrição, classificação, desenvolvimento teórico e o teste limitado da teoria, buscando a compreensão das informações coletadas.

Considerou-se que, para analisar a perspectiva de processo existente na formulação da estratégia, o método qualitativo oferece subsídios para melhor compreender esses fenômenos, por permitir aprofundar reflexões relevantes e inspirar articulações entre essas temáticas (RICHARDSON, 1999).

Para a análise de dados, foi utilizada a técnica de análise interpretativa de conteúdo. A análise de conteúdo consiste numa técnica de análise de dados que vem sendo utilizada com frequência nas pesquisas qualitativas no campo da administração, assim como na psicologia, na ciência política, na educação, na publicidade e, principalmente, na sociologia.

Segundo Bardin (2009), a análise de conteúdo, enquanto método, torna-se um conjunto de técnicas de análise das comunicações que utiliza procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens.

A análise de conteúdo, além de realizar a interpretação após a coleta dos dados, desenvolve-se por meio de técnicas mais ou menos refinadas com a finalidade de explorar melhor os objetivos do estudo e atingi-los.

2.1 INSTRUMENTO DE COLETA DE DADOS PROPOSTO

A empresa do segmento financeiro objeto deste artigo e aqui denominada como Empresa Ômega, é uma multinacional e deu início às suas operações no Brasil em 2019. Trata-se de uma gestora independente de fundos que garante atuação isenta de conflitos de interesse.

Contando com cerca de 200 colaboradores, consultores e gestores de patrimônio, e com mais de 50 bilhões de reais em ativos sob sua gestão, o objetivo da unidade Brasil é oferecer uma ampla oferta de produtos e acesso aos principais mercados financeiros do mundo.

O método de pesquisa-ação utilizado chama-se Metodologia para a Conformidade com o SGPI – Sistema de Gestão da Privacidade da Informação e foi aplicado ao longo de 07 meses, entre novembro de 2019 e maio de 2020, pela empresa Lozinsky Consultoria de Negócios em todas as áreas da organização, exclusivamente na filial Brasil.

A empresa atua na resolução de problemas complexos, posicionando a TI como pilar estratégico de negócios e eliminando as âncoras que limitam o crescimento das organizações.

Possui uma equipe multidisciplinar, experiente e que reúne habilidades complexas, como amplo conhecimento sobre os processos de negócio em empresas de diversos setores, agindo como extensão da capacidade da TI em planejar e conduzir as ações que aumentarão o valor agregado e entregarão ganhos e resultados para as áreas de negócios.

Os serviços de consultoria da Lozinsky Consultoria de Negócios são personalizados para cada cliente, a partir do entendimento das questões de negócios que precisam ser resolvidas, da cultura empresarial e da capacidade de execução.

Este artigo aponta resultados de mapeamento específicos para todas as áreas da organização, aqui denominada como Empresa Ômega, exclusivamente em sua filial brasileira.

A Metodologia para a Conformidade com o SGPI – Sistema de Gestão da Privacidade da Informação especifica os requisitos relacionados a ISO/IEC 27701/2019 de modo a atender todos os requisitos especificados na LGPD – Lei Geral de Proteção de Dados do Brasil número 13.709/18.

Esta metodologia pode ser utilizada por controladores de dado pessoal (incluindo aqueles que são controladores solidários de dado pessoal) e operadores de dado pessoal (incluindo aqueles que usam operadores de dado pessoal subcontratados e aqueles que tratam dado pessoal ao atuar como subcontratados de operadores de dado pessoal).

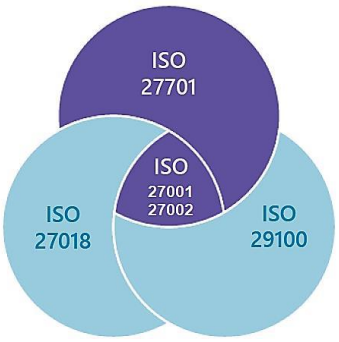
Uma organização que cumpra os requisitos desta metodologia irá gerar evidências documentais de como trata o dado pessoal. Estas evidências podem ser utilizadas para facilitar acordos com parceiros de negócios nos quais o tratamento de dado pessoal é relevante. Estas evidências também podem ajudar no relacionamento com outras partes interessadas, inclusive com a Autoridade Nacional de Proteção de Dados Pessoais.

Esta metodologia é aplicável a todos os tipos e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras e/ou que são operadoras de dado pessoal.

Baseada na ISO/IEC 27701/2019, contém um mapeamento detalhado e orientações específicas para implementar requisitos e controles requeridos na LGPD. Além disso, sugere itens para implementação que mapeiam requisitos de privacidade e controles sugeridos por outros padrões que fazem interface com esta norma:

- ABNT NBR ISO/IEC 27001:2013, Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos.
- ABNT NBR ISO/IEC 27002:2013, Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.
- ISO 27018, Tecnologia da informação – Segurança Técnica - Código de Práticas de Proteção de Informações de Identificação Pessoal (PII) em nuvens públicas atuando como processadores PII.
- ISO 29100, Tecnologia da Informação – Segurança Técnica - Estrutura de Privacidade.

A Figura 1 apresenta as principais interfaces dos padrões que compõe esta metodologia:

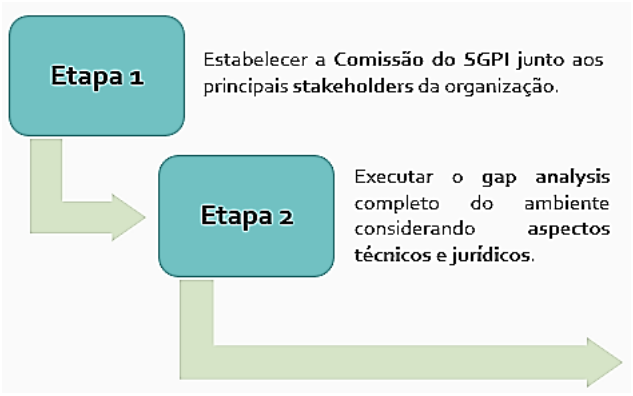


Fonte: Elaborado pelos autores (2019)

A metodologia divide-se em 3 fases e 6 etapas, onde cada fase possui 2 etapas de execução:

- FASE 1: Diagnóstico

Figura 2: Diagnóstico

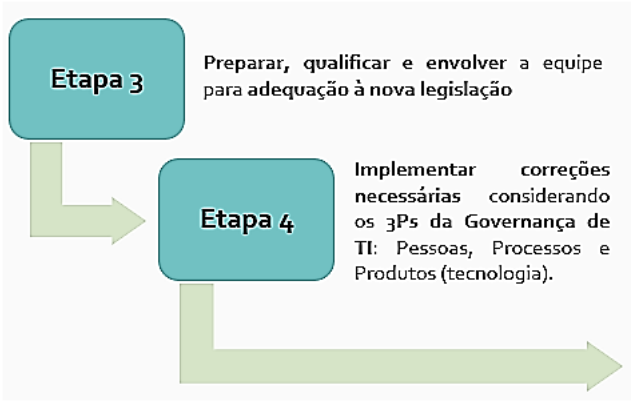


Fonte: Elaborado pelos autores (2019)

Brazilian Journals of Business

- FASE 2: Adequação

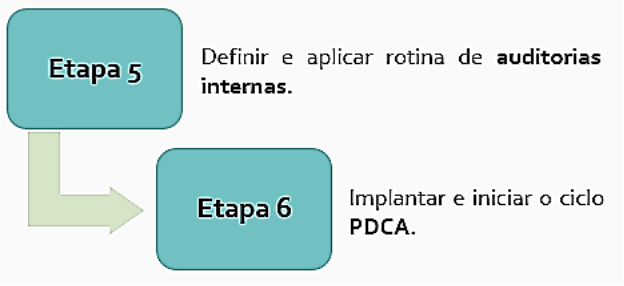
Figura 3: Adequação



Fonte: Elaborado pelos autores (2019)

- FASE 3: Conformidade

Figura 4: Conformidade



Fonte: Elaborado pelos autores (2019)

Esta metodologia recomenda a estrutura desenvolvida pela ISO para melhorar o alinhamento entre as suas normas de sistemas de gestão e permite que uma organização alinhe ou integre seu SGPI aos requisitos de outras normas de sistemas de gestão.

3 FUNDAMENTAÇÃO TEÓRICA

O Brasil possui mais de quarenta normas legais em nível federal que, de várias maneiras, lidam com proteção de dados e privacidade, criando uma estrutura legal cruzada. Estas leis, no entanto, são de natureza setorial, o que significa que se relacionam separadamente, especificando normas e regulamentos para bancos, imóveis, proteção ao consumidor, dentre outros.

A nova Lei Geral de Proteção de Dados do Brasil 13.709/18 (LGPD) visa substituir esse cenário legal complexo por um quadro regulatório abrangente e integrado.

Seu objetivo é capacitar os indivíduos com um conjunto simplificado de direitos, em vez da proteção parcial das leis setoriais em vigor hoje e é inspirado no Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

Brazilian Journals of Business

Para Ferreira (2020), CTO e sócio consultor da Lozinsky Consultoria de Negócios, o aspecto crucial nesse momento é fornecer a transparência necessária para que o titular do dado saiba com qual finalidade e qual os usos são feitos em seus dados pessoais. Essa clareza e transparência no uso da informação e na comunicação exige a adequação de sistemas, possibilitando, por exemplo, a exclusão das informações (se cabível) quando solicitado pelo titular dos dados pessoais, prevista em lei.

Mas é preciso ir além e promover a revisão de todos os mecanismos de segurança da informação que envolvam dados pessoais, garantindo a rastreabilidade no caso de vazamentos e incidentes. Esse cuidado, inclusive, será levado em consideração pela ANPD em caso de ocorrências e pode diminuir as penalidades para a empresa que comprovar que tem governança e políticas claras para atender a proteção exigida pela LGPD (FERREIRA, 2020).

3.1 DIREITOS DOS TITULARES DOS DADOS

A LGPD define um titular de dados como pessoa natural a quem os dados pessoais que são objeto de processamento se referem, indivíduo cujos dados estão sendo coletados e/ou processados.

A lei cria nove direitos para os titulares dos dados descritos no artigo 18 e conferem aos indivíduos o direito de: 1. Confirmação da existência do tratamento dos seus dados. 2. Acessar seus dados. 3. Corrigir dados incompletos, imprecisos ou desatualizados. 4. Anonimizar, bloquear ou excluir dados ou dados desnecessários ou excessivos que não estão sendo processados em conformidade com a LGPD. 5. Seus dados sejam portáveis, ou seja, entregues a outro serviço ou processador, se solicitado. 6. Ter seus dados excluídos. 7. Informações sobre entidades públicas e privadas com as quais o controlador compartilhou dados. 8. Informações sobre a possibilidade de negar o consentimento e as consequências disso. 9. Revogar o consentimento.

3.2 CONSENTIMENTO E BASES LEGAIS

Das dez bases legais para o processamento legal que a LGPD estabelece, o consentimento é o primeiro. Isso é muito importante para o campo de privacidade porque traz implicações diretas na maneira como sites podem definir *cookies*, processar dados de usuários e compartilhá-los com terceiros.

As dez bases legais da LGPD para o processamento de dados pessoais são: 1. Com o consentimento do titular dos dados. 2. Para cumprir uma obrigação legal ou regulamentar o controlador. 3. Para executar políticas públicas previstas em leis ou regulamentos ou com base em contratos, acordos ou instrumentos similares. 4. Realizar estudos de entidades de pesquisa que garantam, sempre que possível, o anonimato dos dados pessoais. 5. Para executar um contrato ou

procedimentos preliminares relacionados a um contrato do qual o titular dos dados é parte. 6. Para exercer direitos, procedimentos judiciais, administrativos ou de arbitragem. 7. Para proteger a vida ou a segurança física do titular dos dados ou de terceiros. 8. Para proteger a saúde, em procedimento realizado por profissionais de saúde ou por entidades de saúde. 9. Para cumprir os interesses legítimos do responsável pelo tratamento ou de terceiros, exceto quando prevalecerem os direitos e liberdades fundamentais do titular dos dados que exigem proteção de dados pessoais. 10. Para proteger o crédito.

Sites, empresas e organizações devem primeiro obter o consentimento específico e inequívoco do titular dos dados antes que qualquer processamento de dados pessoais seja permitido. Haverá exceção a essa regra quando a solicitação para obtenção do dado pessoal estiver respaldada por alguma das bases legais.

O consentimento pode ser revogável a qualquer momento e deve ser fornecido pelo titular dos dados de forma inequívoca, manifesta e livre, podendo ser retirado a qualquer tempo.

Ao processar dados pessoais, um site, empresa ou organização deve apresentar uma base legal específica ou tratar devidamente o consentimento do titular dos dados pessoais

Todo o processamento de dados pessoais deve ser documentado desde a coleta inicial até o término. Também é obrigatória a apresentação de um relatório de impacto a proteção de dados, onde constará uma descrição de que tipo de dados são coletados, o objetivo da coleta e processamento, seu tempo de retenção e com quem os dados podem ser compartilhados. Isso também deve fazer parte de uma política de privacidade de fácil acesso aos titulares de dados pessoais.

3.3 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A LGPD estabelece uma autoridade nacional de proteção de dados (ANPD) e obriga empresas e organizações a nomear um oficial de proteção de dados.

Os principais objetivos da ANPD serão estabelecer normas, padrões técnicos, supervisionar e auditar, educar sobre a lei e suas implicações, lidar com notificações de violações de dados e aplicar suas sanções.

Para a ANPPD a competência fiscalizatória da ANPD será essencial para todo o firmamento da lei, de modo que a ANPD tem seu protagonismo na discussão e na interpretação perante a LGPD. Porém, deve-se ficar atento quanto a sua função, não antepondo ou misturando outras leis que já estão consolidadas no país, como por exemplo, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet, além de outras regulações especificas existentes para cada proposito em si.

Brazilian Journals of Business

Desta maneira, segundo a ANPPD, a ANPD se fará presente e atuante, demonstrando sua competência técnica de conhecimentos bem direcionados e com a devida proficiência de causa, sem a interferência de outras entidades de fiscalização que venham a sobrepor ou descontinuar suas decisões, uma vez que a própria ANPD já fez sua interpretação da lei carimbando nesta a sua designação.

A autoridade nacional de proteção de dados possui dois órgãos - o Conselho de Administração, composto por cinco membros com experiência no campo da privacidade e proteção de dados, e o Conselho Nacional, um conselho consultivo de 23 membros, com representação do governo, sociedade civil, instituições de pesquisa e setor privado.

3.4 ENCARREGADO DE DADOS

A LGPD também determina a necessidade da contratação do Encarregado de Dados ou *Data Protection Officer* – DPO por empresas que realizam o tratamento de dados pessoais.

Para Ferreira (2020), a exigência do encarregado, ou DPO, como o mercado já convencionou chamar, cria mais dúvidas que certezas. O texto da LGPD não é claro sobre o porte das empresas que deverão obrigatoriamente contratar um DPO.

A função do Encarregado de Dados consiste em determinar os tratamentos de dados pessoais da empresa, cabendo a ele o papel de harmonizar o uso dos dados pessoais com as necessidades destes dados para o negócio, bem como ser canal de comunicação perante os usuários titulares dos dados pessoais e autoridades governamentais controladoras e, de forma geral, prestar assistência sobre as práticas de tratamento de dados, bem como, verificar se estas estão em conformidade com a legislação e políticas internas.

Desta forma, as atividades de um Encarregado de Dados consistem basicamente em: Receber reclamações e comunicações dos titulares dos dados pessoais; Prestar esclarecimentos e orientar sobre as providências; Receber comunicações de órgãos reguladores e adotar as providências que couberem; Orientar os funcionários envolvidos no tratamento de dados pessoais dos usuários; Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais dos usuários, e; Manter registros de todas as práticas de tratamento de dados pessoais conduzidas pela empresa, incluindo o propósito de todas as atividades desenvolvidas.

Mas é fato que todos os tipos e portes de negócios deverão promover o contato com os titulares dos dados pessoais que utilizam, de forma a que eles possam demandar o cumprimento de seus direitos. Ainda que não se contrate alguém com o nível de senioridade de um DPO, será preciso

definir um departamento, uma equipe ou um colaborador, que seja responsável por fazer a ponte entre autoridade nacional, titular dos dados e a empresa (FERREIRA, 2020).

3.5 PENALIDADES PREVISTAS NA LEI

A LGPD é clara quando se trata das consequências do não cumprimento da lei. O sistema de penalidades varia de:

- Advertência;
- Multa simples de até 2% do faturamento da empresa ou grupo econômico, limitada à R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração;
- Eliminação dos dados pessoais a que se refere a infração, até;
- Eventuais sanções administrativas, civis e penais definidas em legislação específica.

3.6 ASPECTOS GERAIS

A nova lei quer criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja confusão, a lei estabelece o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os dados sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação (SERPRO, 2020).

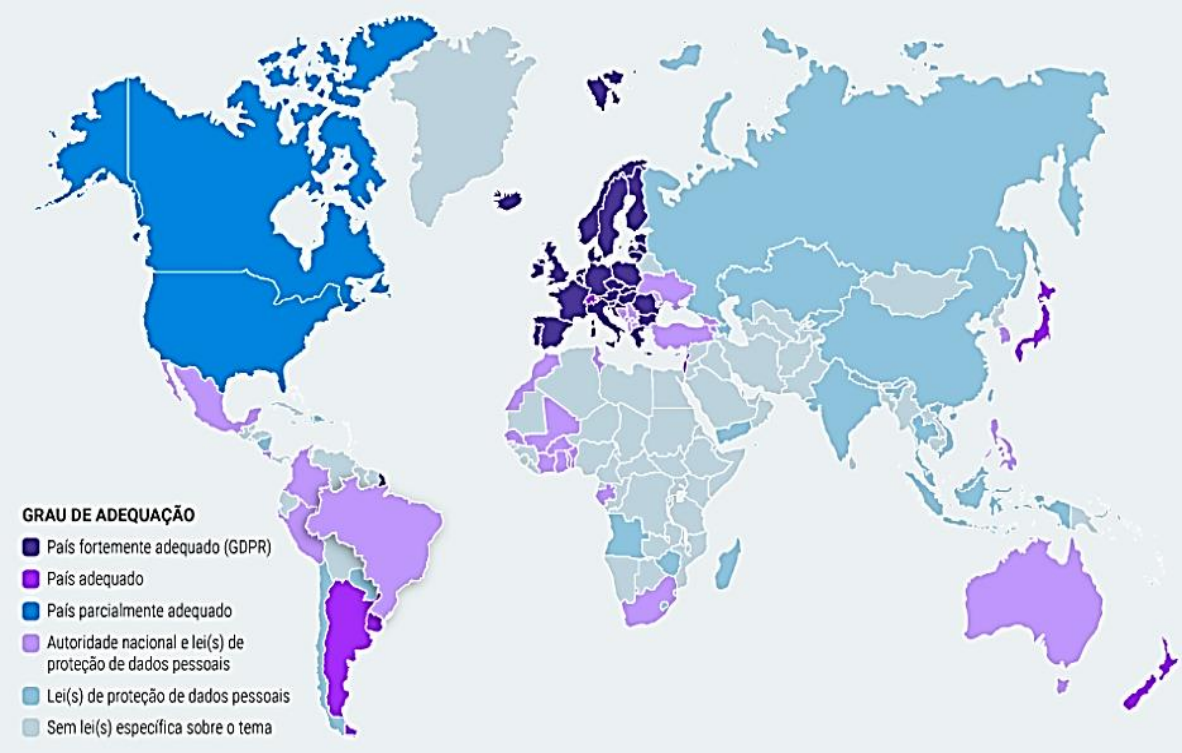
Segundo o SERPRO (2020) a LGPD estabelece ainda que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida. Determina também que é permitido compartilhar dados com organismos internacionais e com outros países, desde que isso ocorra a partir de protocolos seguros e/ou para cumprir exigências legais. A Figura 5 apresenta os principais aspectos da lei:

Brazilian Journals of Business

Fonte: SERPRO (2020)

O SERPRO (2020) ressalta que a LGPD permite a transferência de dados além-fronteira, desde que seja: com o consentimento específico do titular dos dados; a pedido do titular para que esse possa executar pré-contrato ou contrato; para proteger a vida e a integridade física do titular ou de terceiro; para ajudar na execução de política pública; para país ou organismo internacional que projeta dados pessoais de forma compatível com o Brasil; para cooperar juridicamente com órgãos públicos de inteligência, investigação, ou por conta de compromisso assumido via acordo internacional; para cumprir obrigação legal; com a autorização da ANPD; comprovado que o controlador segue a LGPD na forma de normas globais, selos, certificados e códigos de conduta. A Figura 6 apresenta o grau de adequação à proteção de dados pessoais ao redor do mundo:

Brazilian Journals of Business



Fonte: SERPRO (2020)

Peixoto (2019), membro do Comitê de Conteúdo da ANPPD, aponta que a entrada em vigor da LGPD em nosso pais, possivelmente será um divisor de águas para a transformação e inovação tecnológica, não apenas pelo simples viés de proteção à privacidade que se deseja obter, mas também para uma mudança de paradigmas na forma como grande parte dos produtos e serviços serão desenvolvidos dentro dos conceitos *Privacy by design* e *Privacy by default* ao qual o modelo de negócio de muitos fornecedores precisará ser revisto.

Peixoto (2019) também defende que com a entrada em vigo da lei, as empresas deverão se concentrar em informações realmente necessárias e relevantes ao cliente, de maneira que o relacionamento com o consumidor deva se pautar por uma maior transparência em relação à coleta e uso de seus dados. Ou seja, em algumas ocasiões ter que remodelar seu processo de negócio, sua forma de atuação, abordagem e captação. Reconfigurar ou até mesmo mudar o tipo de ferramenta tecnológica para fazer tão somente o que deve ser feito, nada mais que isso.

Para Peixoto (2019), os incidentes não serão apenas operacionais ou de segurança. Vão cada vez mais apontando para a proteção e privacidade dos dados pessoais e sensíveis. Nesse novo contexto não bastará apenas cumprir *SLAs*, mas sobretudo, atender efetivamente com um verdadeiro plano de resposta a incidentes que dê as devidas informações de satisfação ao cliente, com a contenção imediata da causa raiz voltada agora principalmente aos direitos e liberdade do titular dos dados.

Para o Gartner (2020) a fim de evitar sanções regulatórias e impulsionar o crescimento dos clientes, os líderes em segurança e gerenciamento de riscos devem adotar as melhores práticas para desenvolver e manter um programa eficaz de gerenciamento de privacidade.

Segundo o Portal Terra (2019), de acordo com consultas feitas junto a clientes do Gartner, as três principais preocupações em relação à privacidade das informações são: sofrer impacto financeiro por violações de dados, excluindo multas (46%), perder clientes (45%) e sofrer danos à reputação (44%). As sanções regulamentares por descumprimento ficam em apenas quarto lugar, ainda que as multas possam chegar a R$ 50 milhões.

Willemsen (2019) afirma que proteção à privacidade é infinitamente maior do que apenas um problema de TI ou de segurança e que a LGPD afeta toda a organização. Diz ainda que embora os *CIOs* tenham um papel de liderança na orientação de suas organizações para armazenamento de dados em locais mais seguros, a privacidade deve ser um esforço de toda a empresa.

Antes de 2023, mais de 80% das empresas no mundo estarão sujeitas a pelo menos um regulamento de proteção de dados com foco em privacidade. Dessa forma, Neiva (2019), *Research Vice President* do Gartner, cita como aspecto essencial da LGPD o fato de que as empresas terão de mudar de postura e que ao invés de sair tentando capturar a maior quantidade de informações, elas deverão capturar apenas os dados que servem a um propósito deliberadamente iniciado.

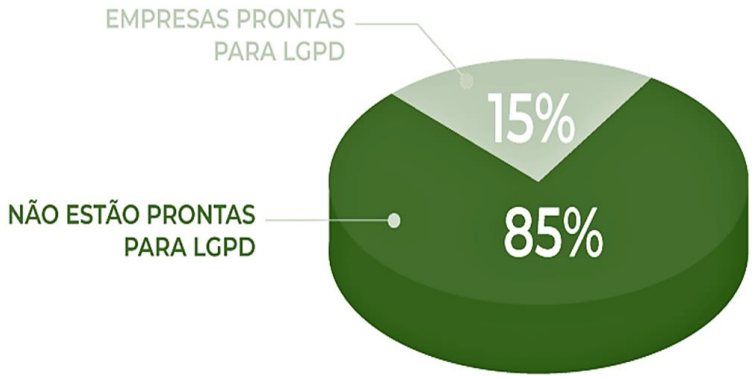
Para Neiva (2019), os líderes de TI devem estar atentos em sua preparação para os desafios de conformidade promovidos pela LGPD, de preferência seguindo estas cinco melhores práticas de gestão: 1. Nomear um diretor de proteção de dados ou diretor de privacidade que atue fora da organização de TI ou de segurança, estabelecendo uma função satélite que seja capaz de supervisionar, sem conflito de interesses, e alinhar claramente as linhas de relatório à liderança; 2. Desenvolver um diagnóstico do real estágio de privacidade em que a companhia se encontra para criar um roteiro de ação totalmente baseado em riscos e demandas, estabelecendo objetivos claros em colaboração com os proprietários (os obrigatórios e os responsáveis) dos processos nas áreas de negócios; 3. Implementar políticas claras e plausíveis de retenção de dados trabalhando com os proprietários dos processos legais e de negócios; 4. Formalizar a governança do programa de gerenciamento de privacidade, fornecendo orientações sobre os papéis e as responsabilidades de cada uma das partes interessadas que participam dos programas de gerenciamento de privacidade; 5. Desenvolver um plano separado para resposta à violação de dados, alinhando e aprendendo com os fluxos de trabalho tradicionais de resposta a incidentes de segurança.

Nesse cenário, o Gartner (2019) destaca que os líderes de segurança e gestão de riscos devem observar as seguintes previsões para garantir a transparência e a garantia de privacidade aos clientes

Brazilian Journals of Business

e a seus negócios: 1) Até 2020, o backup e o arquivamento de dados pessoais representarão a maior área de risco de privacidade para 70% das organizações, contra 10% em 2018; Até 2022, 75% dos *blockchains* públicos sofrerão "envenenamento por privacidade"; 3) Até 2023, mais de 25% das implementações de prova de consentimento baseadas no GDPR irão envolver a tecnologia *blockchain*, em comparação com menos de 2% em 2018.

Segundo pesquisa da Serasa Experian (2019), 85% das empresas brasileiras afirmaram que ainda não estão preparadas para garantir os direitos e deveres em relação ao tratamento de dados pessoais exigidos pela LGPD. O Gráfico 1 apresenta este resultado:



Fonte: Elaborado pelos autores (2020)

A pesquisa foi realizada em março de 2019 e ouviu executivos de 508 companhias de diferentes portes e segmentos em todas as regiões do país e mostrou também que 72% das companhias com mais de 100 funcionários pretendem contratar uma pessoa de mercado especializada ou uma consultoria/assessoria para se adequarem à primeira lei federal voltada exclusivamente à proteção de dados.

Para Ferreira (2020), a LGPD reforça o uso das melhores práticas de segurança da informação. Aspectos tratados há anos pela gestão de TI agora adquirem uma urgência que tornam obrigatórios investimentos antes considerados altos. E quem não os fizer incorrerá em riscos que podem comprometer o futuro dos negócios.

Entender melhor e desde já a nova legislação é importante para ajudar o país na missão coletiva de assegurar a privacidade a qual é um direito fundamental do indivíduo e, portanto, deve ser salvaguardada com o máximo de cuidado, eficiência e qualidade (SERPRO, 2020).

4 RESULTADOS E DISCUSSÃO

A documentação estudada identificou que a demanda por controles de privacidade e segurança vem aumentando muito nos últimos anos, devido a iniciativa de diversos países para que as empresas instaladas em seus territórios estejam adequadas a privacidade.

No Brasil, tem-se ouvido o relado de muitas empresas a respeito das dificuldades de entendimento sobre como implementar os controles previstos na lei e se essa implementação é realmente necessária.

Mas a privacidade dos dados pessoais é importante para as organizações? O que ela atinge de fato nos negócios? Uma resposta simples: ela afeta o que é mais importante, seus consumidores e funcionários. Ter os dados dessas pessoas expostos e utilizados de maneira nociva pode ser muito prejudicial para a imagem das empresas, além de acarretar multas conforme os critérios estabelecidos pela lei.

Para ilustrar um caso que reforça a necessidade de uma lei que proteja a privacidade de dados pessoais, em 2016 a Cambridge Analytica usou os dados de mais de 50 milhões de pessoas para fazer propaganda política sem consentimento prévio. Esses dados pessoais foram obtidos através de um aplicativo lançado no Facebook.

Uma vez que a lei direciona apenas alguns mecanismos (e outros não) necessários para aderir aos seus requisitos, uma alternativa é a realização de um *benchmarking* em empresas da União Europeia que já implementaram a GDPR (*General Data Protection Regulation*).

A metodologia para mapeamento dos requisitos listados na LGPD proposta neste artigo contém mapeamento detalhado e algumas orientações específicas para implementar os requisitos e controles requeridos pela lei brasileira.

Para o mapeamento dos requisitos temos um total de 325 controles que classificamos entre mandatórios e altamente recomendáveis.

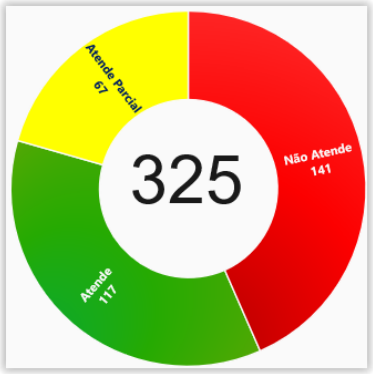
Os requisitos mandatórios se referem explicitamente a privacidade de dados e são necessários para conformidade com a LGPD.

Os requisitos altamente recomendáveis se referem a segurança da informação tal como descrito nas normas ISO IEC 27001 e ISO IEC 27002.

No caso da Empresa Ômega aplicamos os 325 controles que foram analisados com o apoio de uma equipe multidisciplinar formada por especialistas em risco corporativo, segurança da informação, governança, jurídico, tecnologia da informação e áreas de negócio demandadas conforme necessidade. Após a análise detalhada desse material foi constatado que a empresa atende plenamente

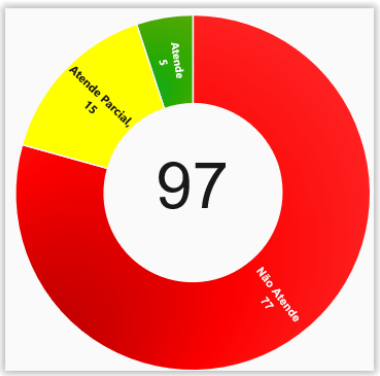
Brazilian Journals of Business

a 117 controles, são atendidos parcialmente 67 controles e 141 controles para aderência a lei não são atendidos. O Gráfico 2 apresenta o panorama geral da análise:



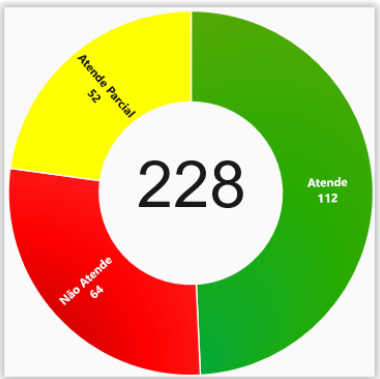
Fonte: Elaborado pelos autores (2020)

O Gráfico 3 apresenta o detalhamento especificamente para os requisitos mandatórios:



Fonte: Elaborado pelos autores (2020)

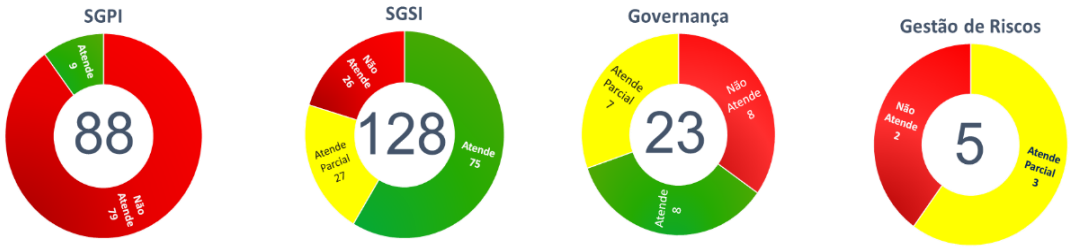
O Gráfico 4 apresenta o detalhamento especificamente para os requisitos altamente recomendáveis (baseados nas ISO IEC 27001 e ISO IEC 27002 – Segurança da Informação):



Fonte: Elaborado pelos autores (2020)

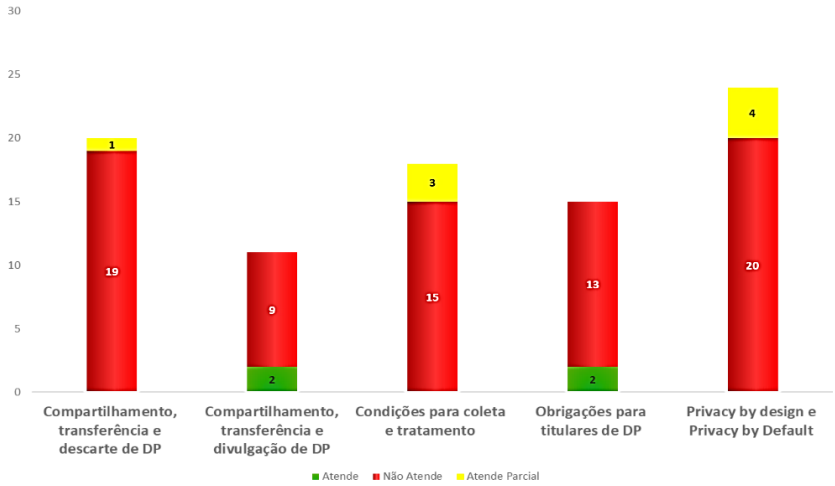
Brazilian Journals of Business

A aplicação dos 325 controles junto com a equipe multidisciplinar em conjunto com as áreas de negócio, nos permitiu uma análise mais profunda onde cada um dos departamentos e áreas da organização foram analisados. Destaque para quatro áreas que apresentaram maior risco de não conformidade, conforme apresentado no Gráfico 5:



Fonte: Elaborado pelos autores (2020)

A metodologia também nos permitiu explorar de maneira analítica controles específicos de Segurança da Informação e Privacidade. O Gráfico 6 apresenta o resultado da análise dos controles específicos do Sistema de Gestão da Privacidade da Informação (SGPI):



Fonte: Elaborado pelos autores (2020)

Baseado no detalhamento dos controles da metodologia foi possível a elaboração de um plano de ação priorizado por temas elencados através do mapeamento dos requisitos listados na LGPD. O plano de ação para orientar os ajustes necessários no ambiente foi elaborado como base nos controles apresentados no diagnóstico, com desdobramento em ações para os níveis estratégico, tático e operacional.

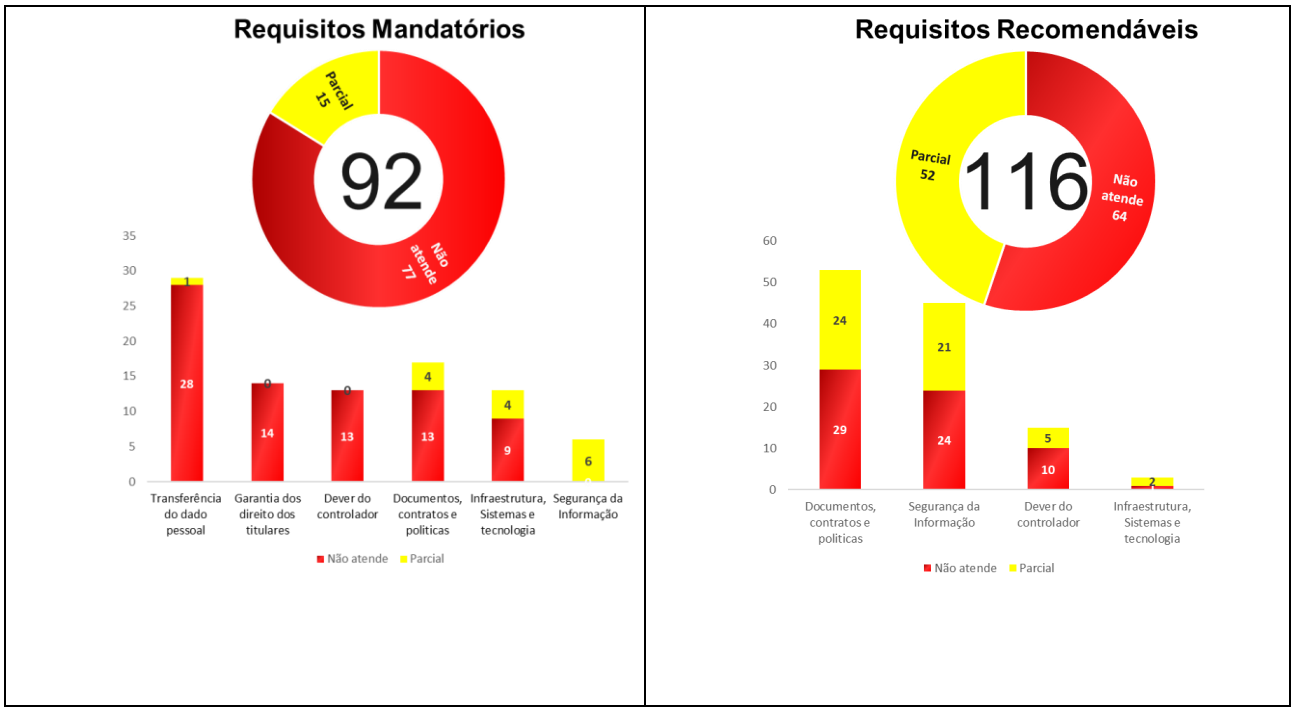
O plano está classificado conforme o nível de criticidade mapeado no diagnóstico e elencamos a prioridade de execução conforme itens mandatórios para a conformidade com a LGPD. Não foram

descartadas as análises de itens que já atendem a conformidade com a lei parcialmente. Para estes casos será necessário uma futura revisão detalhada e possíveis indicações de ajuste.

Existem desdobramentos de atividades para todas as áreas que fazem parte do ciclo de vida dos dados pessoais. Essas atividades vão desde debates para criação de novos processos para descarte, armazenamento e acesso a dados pessoais até criação de contratos e transferência de dados internacionais.

Esses direcionadores apoiaram na elaboração de outras documentações de projeto, como cronograma e plano orçamentário. São também os direcionadores que basearam a constituição e o direcionamento do plano de ação.

Relacionando os direcionadores do plano de ação com os controles levantados durante o diagnóstico foi possível fazer uma análise dos controles que deveriam ser atendidos pelo plano de ação. O Gráfico 7 apresenta este resultado:



Fonte: Elaborado pelos autores (2020)

Como estratégia de execução do plano de ação, foi definido percorrer todo o ciclo de vida do dado pessoal desde sua coleta no processo de originação ou de RH até o seu descarte, visitando todos os processos e corrigindo os problemas que foram destacados durante o diagnóstico.

Baseado nos direcionadores do plano de ação foi elaborado um cronograma para execução do plano de ação na Empresa Ômega, com ações de curto, médio e longo prazo.

A entrega do diagnóstico e do plano de ação com os resultados obtidos pelo mapeamento ocorreu em maio de 2020 após sete meses de projeto e trouxe como recomendação um conjunto de 29 ações para mitigar ao máximo a exposição do ambiente da Empresa Ômega ao risco de não conformidade com os requisitos da LGPD.

Cada ação de mitigação proposta possui objetivo, escopo, fase de planejamento e fase de execução com vistas a anular e, quando não possível, reduzir ao máximo determinado risco mapeado.

Caberá exclusivamente a Empresa Ômega a decisão de aplicar ou não, total ou parcialmente, as recomendações propostas por este trabalho.

5 CONSIDERAÇÕES FINAIS

A LGPD tem como objetivo proteger os direitos fundamentais de liberdade (Art. 1º) e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Essa ideia de proteção à privacidade é prevista até mesmo no artigo XII da Declaração Universal dos Direitos Humanos: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação” (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948). Todo ser humano, portanto, tem direito à proteção da lei contra tais interferências ou ataques.

Isso mostra que a privacidade não é um assunto tão recente e que alguns países já possuem leis de proteção à privacidade a muito tempo, com mecanismos e controles que podem ser utilizados para que os requisitos previstos em lei sejam atendidos de maneira adequada.

O processo de criação da metodologia descrita neste trabalho, foi construído a partir dos seguintes princípios:

- Análise e entendimento da LGPD sob o viés tecnológico, jurídico e de gestão de negócios corporativos;
- Definição dos controles necessários para mapeamento de todos os requisitos e escopo definido na LGPD;
- Definição do ciclo de vida, dinâmica e artefatos da metodologia;
- Validação da metodologia através de testagem em laboratório emulando a aplicação dela em um projeto LGPD bem como sua prática;
- Aprimoramento e melhoria da metodologia mediante os resultados obtidos para aplicação em um projeto real.

Antes de sua aplicação, cada fundamento da metodologia foi amplamente discutido, testado e validado entre os consultores responsáveis pela concepção do trabalho.

Após inúmeras reuniões de alinhamento, a equipe conseguiu materializar um modelo consonante aos requisitos da LGPD.

Dessa forma, foi possível aplicar com segurança e eficácia a metodologia na prática, e obter assim, um mapeamento e resultados com alto grau de aderência e assertividade perante os pressupostos e requisitos descritos na lei.

Os resultados mostram que dos 325 controles analisados na Empresa Ômega por equipe multidisciplinar, a partir da metodologia proposta neste trabalho, 117 atendem plenamente aos requisitos lei, 67 atendem apenas parcialmente e 141 controles não atendem aos requisitos determinados pela LGPD.

Constata-se dessa forma que há um elevado risco de exposição da Empresa Ômega em incorrer em não conformidades quando confrontada com a lei, uma vez que apenas 36% do seu ambiente atende plenamente aos requisitos legais, enquanto 21% atende somente parcialmente tais requisitos e 43% seguem desprotegidos ou descobertos de mecanismos (processuais, tecnológicos ou humanos) de proteção.

Destaca-se como principal elemento facilitador deste trabalho a interação e comunicação junto aos profissionais responsáveis pelas áreas de gestão de riscos, segurança da informação e jurídico bem como o acesso aos documentos, usuários, prestadores de serviço e materiais que a Empresa Ômega permitiu aos pesquisadores, que conduziram este trabalho como pesquisa-ação e estudo de caso de natureza exploratória.

Como principal dificuldade, citamos a falta de clareza sobre o prazo de entrada em vigor da lei bem como o estabelecimento material e efetivo da ANPD (Autoridade Nacional de Proteção de Dados) para a execução de suas atribuições, das quais o estabelecimento de novas normas, padrões técnicos e ações de educação junto as empresas.

O maior fator de contribuição deste trabalho foi a abertura de novos caminhos investigativos para futuras pesquisas a serem aplicadas em outras organizações, de segmento e portes distintos, uma vez que a legislação possui aplicação transversal e multisetorial, o que significa que se aplica aos setores público e privado, bem como online e offline, para empresas de todos os tamanhos.

Por fim, como aponta Peixoto (2019), com a entrada de modelos de governança de privacidade em nosso país, a LGPD possivelmente será um divisor de águas para a transformação e inovação tecnológica, não apenas pelo simples viés de proteção à privacidade que se deseja obter, mas também para uma mudança de paradigmas na forma como grande parte dos produtos e serviços serão desenvolvidos, respeitando integralmente a privacidade e o desejo do cidadão no que tange a todos os seus dados pessoais.

AGRADECIMENTO

Fábio Ferreira - CTO e sócio consultor da Lozinsky Consultoria de Negócios, São Paulo – SP/ Brasil.

REFERÊNCIAS

ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados. Manifesto pela tecnicidade dos membros do conselho diretor da Autoridade Nacional de Proteção de Dados, 2020. Disponível em: https://anppd.org/parecer/manifesto-pela-tecnicidade-da-anpd. Acesso em: 07 de agosto de 2020.

BARDIN, L. Análise de Conteúdo. Lisboa, Portugal; Edições 70, LDA, 2009.

BONOMA, T. V. Case Research in Marketing: Opportunities, Problems, and Process. Journal of Marketing Research, Vol XXII, May 1985.

DENZIN, N. K. The values of social sciences. Nueva York: Aldine, 1970.

FERREIRA, F. LGPD: por que você não pode mais esperar para se adaptar, 2020. Disponível em: https://lozinskyconsultoria.com.br/estrategia-e-gestao-de-ti/lgpd-por-que-voce-nao-pode-mais-esperar-para-se-adaptar/. Acesso em: 24 de janeiro de 2020.

GARTNER, INC. Beyond GDPR: 5 Best Practices for LGPD Compliance, 2020. Disponível em: https://www.gartner.com/guest/purchase/registration?resId=3903476. Acesso em: 09 de julho de 2020.
----------. Conferência Gartner Segurança e Gestão de Risco, 13 e 14 de agosto, 2019. São Paulo, SP.
Disponível em: https://www.gartner.com/pt-br/conferences/la/security-risk-management-brazil. Acesso em: 31 de julho de 2020.

GOODE, W. J.; HATT, P. K. - Métodos em Pesquisa Social. 3ªed., São Paulo: Cia Editora Nacional, 1969.

LIMA, M. C. O método de pesquisa-ação nas organizações: do horizonte político à dimensão formal. Revista Eletrônica de Gestão Organizacional, v. 3, n. 2, p. 139-153. 2005.

NEIVA, C. Portal Terra. Gartner prevê que menos de 30% das organizações irão cumprir totalmente a nova lei de proteção de dados até agosto de 2020, 2019.
Disponível em: https://www.terra.com.br/noticias/dino/gartner-preve-que-menos-de-30-das-organizacoes-irao-cumprir-totalmente-a-nova-lei-de-protecao-de-dados-ate-agosto-de-2020,94139bc2991002837d32286eae03eb2a1hcorayj.html. Acesso em: 09 de julho de 2020.

OLIVEIRA, S. L. Tratado de metodologia científica: projetos de pesquisa, TGI, TCC, monografias, dissertações e teses. 2. São Paulo: Pioneira. 2000.

ONU. Declaração Universal dos Direitos Humanos, 1948.
Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 10 de agosto de 2020.

PEIXOTO, M. ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados. Transformações e inovações junto à LGPD, 2020.
Disponível em: https://anppd.org/noticia/transformacoes-e-inovacoes-junto-a-lgpd. Acesso em: 07 de agosto de 2020.

PORTAL TERRA. Gartner prevê que menos de 30% das organizações irão cumprir totalmente a nova lei de proteção de dados até agosto de 2020, 2019.
Disponível em: https://www.terra.com.br/noticias/dino/gartner-preve-que-menos-de-30-das-organizacoes-irao-cumprir-totalmente-a-nova-lei-de-protecao-de-dados-ate-agosto-de-2020,94139bc2991002837d32286eae03eb2a1hcorayj.html. Acesso em: 09 de julho de 2020.

PRESIDÊNCIA DA REPÚBLICA. Secretaria Geral. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), 2018.
Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm . Acesso em: 09 de julho de 2020.

RICHARDSON, R. J. Pesquisa Social: Métodos e Técnicas. São Paulo: Atlas,1999.

SECURITY REPORT. Serasa Experian. 85% das empresas ainda não estão prontas para a LGPD. Pesquisa, 2019.
Disponível em: https://www.securityreport.com.br/overview/85-das-empresas-ainda-nao-estao-prontas-para-a-lgpd/#.XylVrq-Sk2w. Acesso em: 04 de agosto de 2020.

SERPRO. Glossário LGPD, 2020.
Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd. Acesso em: 09 de julho de 2020.
----------. O que muda com a LGPD, 2020.
Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 09 de julho de 2020
THIOLLENT, M. Metodologia da Pesquisa-ação. 7º edição. Editora São Paulo: Cortez; 1996.

WILLEMSEN, B. Gartner IT Symposium/Xpo 2019™, 2019. São Paulo, SP
Disponível em: http://www.gartner.com/br/symposium. Acesso em: 31 de julho de 2020.

YIN, R. K. Estudo de caso: planejamento e métodos. 3 editora. Porto Alegre: Bookman, 2006.