Matriz de referência para implementação da lei geral de proteção de dados pessoais e a ABNT NBR ISO/IEC 27001

Reference matrix for implementation of the LGPD and ABNT NBR ISO/IEC 27001

DOI:10.34117/bjdv8n11-231

Recebimento dos originais: 24/10/2022
Aceitação para publicação: 22/11/2022

Washington Fabio de Souza Ribeiro
Mestre em Gestão do Conhecimento e Tecnologia da Informação
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: washington.ribeiro@uniceplac.edu.br

Gilmar Severino Lucena de Souza
Mestre em Engenharia Biométic
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: gilmar.souza@uniceplac.edu.br

Jorge Alberto dos Santos
Mestre em Psicologia Educacional
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: jorge.alberto@uniceplac.edu.br

Osmam Bras de Souto
Doutor em Tecnologias Educaionais
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: osmam.souto@uniceplac.edu.br

Wilton Marinho Carneiro Souza
Mestre em Governança, Tecnologia e Inovação
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: wilton.souza@uniceplac.edu.br

Gustavo Gomes dos Anjos Novais
Graduado em Sistemas de Informação
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: gustavogomesdosanjos@hotmail.com

João Pedro Silva Araújo
Graduado em Sistemas de Informação
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: jpedro_s@live.com

Júlio Anderson Marques de Souza
Graduado em Sistemas de Informação
Instituição: Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC)
Endereço: Siga Área Especial para Indústria, Lote 2-3, Sce St. Leste Industrial, Gama, Brasília - DF, CEP: 72445-020
E-mail: julioandersonf@hotmail.com

RESUMO
Este artigo tem como objetivo apresentar uma matriz de categorização com recomendações para auxiliar na implementação da Lei Geral de Proteção de Dados(LGPD) dentro das organizações em consonância com a ABNT NBR ISO/IEC 27001 através de um estudo de classificação, categorização e comparação das normativas presentes nesses dois documentos. Os testes de conformidade da matriz realizados com profissionais de tecnologia na estrutura atual das organizações indicou que esse instrumento tem grande potencial para auxiliar na adequação dos negócios à nova legislação de proteção de dados pessoais.

Palavras-chave: LGPD, matriz, ABNT NBR ISO 27001, Organizações.

ABSTRACT
This article aims to present a categorization matrix with recommendations to assist in the implementation of the General Data Protection Law (LGPD) within organizations in line with ABNT NBR ISO/IEC 27001 through a study of classification, categorization and comparison of the regulations present in these two documents. The matrix compliance tests carried out with technology professionals in the current structure of organizations indicated that this instrument has great potential to assist in the adaptation of businesses to the new legislation on personal data protection.

Keywords: LGPD, matrix, ABNT NBR ISO 27001, organizations.

1 INTRODUÇÃO

A segurança da informação tem se destacado como foco principal das organizações, uma vez que a quantidade de informações alocadas tem aumentado, assim como os riscos associados ao armazená-las e processá-las indevidamente. A democratização do acesso aos sistemas de informação com o uso de tecnologias digitais têm potencializado esse problema, uma vez que a coleta de dados pessoais se tornou fator determinante nos ambientes de negócios de natureza estatal e privada.

Esse fato impulsionou a modernização das legislações para garantir os direitos dos cidadãos que fornecem os dados, assim como estabelecer as obrigações, os limites de responsabilidades e sanções em virtude de descumprimento das normas estabelecidas. Nesse contexto, em 2018, a Lei Geral de Proteção dos Dados (Brasil, 2020) que, inspirada na General Data Protection Regulation Europeia (GDPR), busca garantir a proteção e segurança de dados pessoais e dados sensíveis por parte das organizações que fornecem bens e serviços no Brasil.

A segurança jurídica proporcionada pela LGPD torna o ambiente de negócio mais propício para as empresas, pois diante de regras mais claras e ressonantes com as legislações da União Europeia preserva e fortalece a confiança dos consumidores. Do ponto de vista dos cidadãos, a legislação reafirma o compromisso com a confidencialidade e liberdade na tomada de decisão sobre o uso de seus dados. Neste contexto, Pinheiro (2020) afirma que a LGPD ajudou a

> [...] resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante a proteção e a garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos.

Entretanto, a implementação da LGPD, como toda nova legislação, tem se tornado motivo de dúvidas tanto das pessoas, quanto das empresas o que se faz necessário criar uma base referencial que possa guiar as organizações para que estejam em conformidade com a lei e com as normativas da gestão da segurança da informação estabelecido na ISO 27001. Assim, o objetivo deste trabalho é apresentar uma matriz de referência baseada na LGPD e em conformidade com a ABNT NBR ISO 27001, utilizando como guia as convergências e conformidade entre as duas. O produto final desse trabalho poderá ser útil às empresas e organizações na implementação de políticas de proteção de dados.

2 REFERENCIAL TEÓRICO

2.1-HISTÓRICO E PRECEDENTES DA LEI GERAL DO PROTEÇÃO DOS DADOS (LGPD)

O ano de 2013 teve uma grande importância para a internet, com a criação da Lei do Marco Civil da Internet no mês de março, que foi uma lei responsável por regular o uso da internet no País.

No ano de 2018, foi exposto ao público através das mídias sociais o vazamento e a utilização de dados pessoais através das redes sociais, no qual o Regulamento Geral sobre a Proteção de Dados obrigou grandes empresas como Facebook e Google a mudarem a forma como tratam os dados dos usuários de seus serviços através de uma legislação vigente.

No ano de 2018, foi aprovada a LGPD com o intuito de prosseguir e complementar as norma regulativas das leis já criadas anteriormente, porém dando mais segurança jurídica aos usuários e apoio às empresas, uma vez que tornou as regras, direitos e obrigações mais claras com relação ao uso, a guarda e ao tratamento dos dados pessoais.

2.2 ESTRUTURAÇÃO DA LGPD

A Lei Geral de Proteção de Dados Pessoais, também conhecida como LGPD, é a Lei nº 13.709 que foi aprovada no dia 17 de agosto de 2018 com a vigência no ano de 2020. É uma lei que possui o objetivo de padronizar e normatizar as práticas voltadas para a proteção dos dados pessoais dos cidadãos do país.

A lei estabelece que qualquer tipo de organização com atividades em território brasileiro com sede localizada dentro ou fora do país deverá tratar os dados pessoais de forma segura, garantindo a integridade dos usuários e zelando pelos direitos fundamentais do cidadão.

Com relação a estrutura da referida legislação, os tópicos a seguir estão presentes: 1- Dados Pessoais; 2-Proteção à Privacidade; 3-Transparência; 4-Padronização de Normas; 5-Operador e Controlador; 6-Organizações.

Os dados pessoais são relativos aos que podem ser utilizados para identificar uma pessoa, de acordo com o artigo 1º da Lei 13.709/2018

> Esta Lei dispõe 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, 2020).

Assim, a legislação se estabelece na proteção desses dados, indicando que a tomada de decisão nas organizações nas relações com os clientes deve ser pautada pela privacidade, resguardando a pessoa, seja ela no âmbito corporativo ou pessoal.

Na legislação em discussão, a transparência dos dados está diretamente ligada a forma clara e concisa sobre como os dados estão sendo utilizados, tratados e disponibilizados aos interessados, de acordo com o artigo 6º, VI, da Lei 13.709/2018 "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respetivos agentes de tratamento, observados os segredos comercial e industrial."(BRASIL, 2020).

A LGPD, em conformidade com o regime jurídico brasileiro, apresenta a padronização das normas no artigo 1º parágrafo único da Lei 13.709/2018 "As normas gerais contidas nesta lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios." (BRASIL, 2020). E como um aspecto inovador, cria a figura do Operador e Controlador. Assim, com a nova lei se tornou necessário ter um responsável (Operador) local pelos dados contidos das pessoas, com a função de monitorar e registrar os dados pessoais e ser o responsável por tratar os dados mediante instruções do Controlador, conforme citado no artigo 39º da Lei 13.709/2018 "O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria." (BRASIL, 2020)

O Controlador, por sua vez, também conhecido como DPO que é a sigla em inglês de Data Protection Officer (Oficial de Proteção de Dados) é o encarregado de guiar e supervisionar o Operador com relação ao tratamento dos dados, conforme citado no artigo 41º da Lei 13.709/2018 "O controlador deverá indicar encarregado pelo tratamento de dados pessoais." (BRASIL, 2020)

Neste contexto, as empresas passam a ter estes responsáveis que atuarão em sincronia sobre os dados tratados e utilizados pela empresa, conforme citado no artigo 37º da Lei 13.709/2018 "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse." (BRASIL, 2020).

Por se tratar de um novo cenário, o impacto e as mudanças necessárias gerou adaptações nas empresas, e o papel da organização neste contexto, é tratar de maneira clara e correta os dados de seus colaboradores e clientes.

2.3 A ABNT NBR ISO/IEC 27001

A NBR ISO/IEC 27001 (ABNT, 2013) é uma norma de padrão internacional que orienta e normatiza como deve-se ser implementada um Sistema de Gestão de Segurança da Informação (SGSI), auxiliando na aplicação das ações compromissadas com a proteção da informação. Essa certificação representa um considerável nível de tranquilidade para as organizações certificadas, uma vez que faz parte do arcabouço teórico que inspiraram a LGPD.

Essa normativa é utilizada para avaliar, descobrir e solucionar problemas relacionados à informação dos dados. Os processos ligados a SGSI são adaptáveis ao estilo de cada organização, não sendo um modelo sistemático, podendo fornecer uma estrutura para sua implementação após a coleta do diagnóstico de risco que leva em consideração as necessidades e objetivos da organização, os requisitos de segurança, os processos empregados, o tamanho e estrutura do negócio.

Dentre as conformidades da norma, os principais pontos que norteiam a ISO são a análise de risco; o comprometimento de alta gestão; a definição de objetivos e estratégias; os recursos e competências; a documentação da informação; o acompanhamento de desempenho e as melhorias contínuas.

A norma solicita que a empresa realize uma análise dos riscos de segurança sempre que há alguma mudança significativa definida e com uma periodicidade. Sendo essa análise aplicada corretamente com o estabelecimento de critérios de aceitação e medição dos riscos. Verificando as possíveis consequências e níveis desses riscos encontrados. Para que esse processo se efetive, é exigido dos níveis mais altos dos administradores um comprometimento com o SGSI, sendo a parte responsável pelo conhecimento da segurança da informação e por assegurar que os recursos estejam completamente disponíveis para a sua implementação. Guiando colaboradores para total adaptação ao sistema.

Entretanto, esse processo deve ser guiado pelo planejamento baseado nos objetivos de segurança e nas justificativas para atingi-los e requer que todos os recursos, tanto para implementação, quanto manutenção estejam totalmente disponíveis. Estabelece ainda quais as competências e qualificações comprovadas por certificações os responsáveis deverão possuir.

Uma etapa fundamental na implementação do SGSI é a documentação do processo.É exigido que todo e qualquer dado seja documentado corretamente, os

identificando e definindo e o seu formato. Essas informações demandam uma atualização, sempre que possuir uma mudança na descrição inicial do projeto, sendo essas alterações necessárias a passar por aprovações, antes de serem devidamente implementadas. De acordo com os objetivos determinados, deverá haver uma medição e acompanhamento por meio de aplicações de ferramentas que indicam a viabilidade e adequação do sistema. Dessa forma, é necessário que a empresa realize a implementação e manutenção do sistema de melhorias contínuas para que tenha a possibilidade de correção de não conformidades. Podendo ser implementada com o uso de auditorias internas e análises críticas pela direção. Todo esse processo, é guiado pelo conhecido ciclo padrão PDCA (Plan, Do, Check, Action).

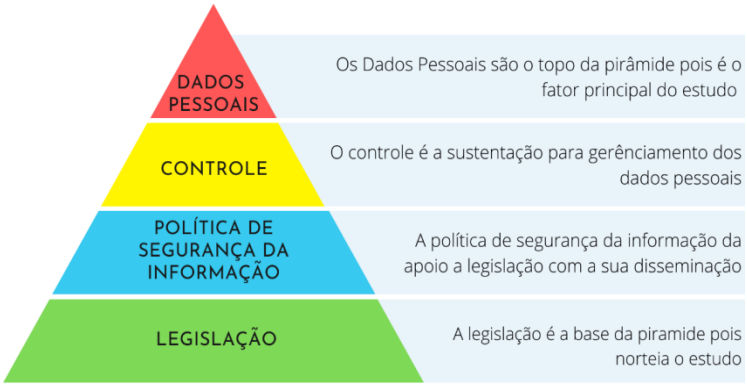
3 DESENVOLVIMENTO

O desenvolvimento do estudo foi fundamentado na organização de uma matriz hierárquica taxonômica seguida de um teste de usabilidade e eficiência da mesma.

Uma taxonomia, segundo Harper (2022) é o estudo para a classificação, categorização, organização e hierarquia de qualquer informação. Foi conceituada inicialmente para fazer a classificação e categorização de seres vivos no ramo da biologia nos meados do sec. XVII, porém com a amplitude dos estudos feitos ao decorrer dos séculos, se tornou um método podendo ser utilizado para qualquer área de conhecimento.

A matriz taxonômica do estudo foi construída tomando como base uma pirâmide hierárquica e a intersecção entre a LGPD e a NBR ISO 2700. A primeira, é composta por níveis que possui na base a legislação, seguida dos fundamentos das políticas de segurança que dá base para os mecanismos de controle e, finalmente no topo, os dados pessoais, que é o fator primordial do estudo. A figura 1, ilustra a pirâmide hierárquica adotada.

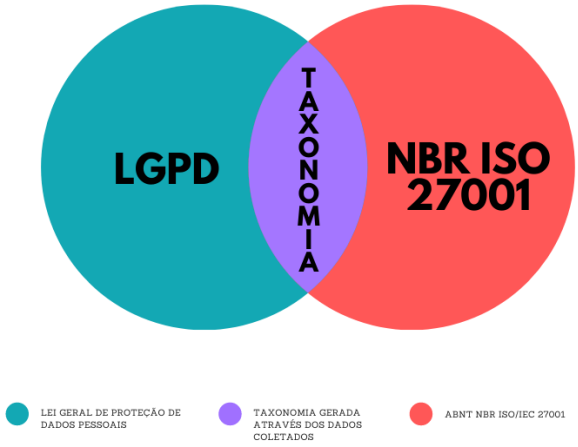
Figura 1 - Pirâmide da Hierárquica Taxonômica



Fonte: Os próprios autores.

A intersecção taxonômica entre a LGPD e a NBR ISO 27001 buscou conformidades entre as duas normativas, considerando que a primeira tem foco na proteção do cidadão e na definição de regras para às organizações e a segunda, a NBR ISO 27001, especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação, como está representado na figura 2.

Figura 2 – Composição da Intersecção taxonômica



Fonte: Os próprios autores.

A articulação da Pirâmide da Hierárquica com a Intersecção Taxonômica gerou a matriz representada na tabela 1, que cruza as informações presentes nas duas normativas considerando as categorias da pirâmide taxonômica.

NBR ISO/IEC 27001 – 2016	Lei Geral de Proteção de Dados Pessoais			Resultado da Inserção Taxonômica		
Registro	**Capítulo**	**Artigo**		**Categoria**	**Comentários Gerais**	**Resolução de Problemas**
A.7.1.2; A.1 3.2.4 - Definição da Função e Responsabilidade de Segurança	II	Art. 7º	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: 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;	Dados pessoais	A utilização dos dados pessoais deverão seguir acordos de confidencialidade e não divulgação sendo necessário a identificação e criticamente documentados	Ausência de definições e informações sobre os dados pessoais utilizados pela empresa
A.8.1.1 - Inventário de Ativos	VI	Art. 37º	O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.		A lei estabelece que os dados pessoais são tratados como ativos da organização, sendo necessário o devido controle e inventário, contendo o registro das operações	
A.8.1.3 - Uso Aceitável dos Ativos	IV	Art. 27º	A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada à autoridade nacional e dependerá de consentimento do titular.		A lei estabelece que a utilização dos dados pessoais deverá possuir consentimento do titular apoiados pelas autoridades competentes	
6.1.3, 6.2 - Plano de Tratamento de Riscos	VII	ART 50 - 1º	Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular.		A lei estabelece que o controlador e o operador deverão mitigar os riscos referente ao tratamento dos dados dos titulares.	
6.1.2 - Metodologia de Avaliação de Avaliação de Risco e Tratamento de Risco	IX	ART 55-J | XVI	Realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;	Controle	Segundo a lei as organizações deverão ter auditorias com intervalos constantes para manter as conformidades perante aos órgãos competentes	Controle correto dos dados
8.2, 8.3 - Relatório de Avaliação de Riscos e de	I	ART 5 º Parágrafo XVII	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		A lei estabelece que é necessário ter relatórios para descrever os impactos gerados através dos mecanismos de	

Tratamento dos Riscos			como medidas, salvaguardas e mecanismos de mitigação de risco;		controle para mitigação de riscos, tal como avaliação dos mesmos	
5.2, 6.2 - Política e Objetivos de Segurança Da Informação	VII	ART 50	Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.	Política de Segurança da Informação	Segundo a lei os dados precisam ser tratados seguindo os padrões de segurança determinados pela as organizações unidos as boas práticas e governança mitigando os riscos e cumprindo as normas de segurança	Disseminação da Política de Segurança da Informação
A.9.1.1 - Política de Controle de Acesso	I	Art. 6º Parágrafo VII	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;		A lei estabelece que deverá ter documentado todos os níveis de acesso mediante aos requisitos de segurança da organização	
A.15.1.1 - Política de Segurança do Fornecedor	II	Art. 7º Parágrafo 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		Deverá ser documentado a utilização das informações repassadas a terceiros, seguindo o que foi definido em contrato	
A.16.1.5 - Procedimentos de Gestão de Incidentes	VII	Art. 48º	O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Legislação	A lei estabelece que deverá ser documentado os incidentes relacionados aos dados que possam causar qualquer tipo de risco aos titulares e deverão ser comunicados aos órgãos competentes	Adequação a LGPD
A.18.1.1 - Requisito Legais, Regulatórios e Contratuais	IX	Art. 55º-J.	Compete à ANPD		A lei estabelece que a ANPD deverá zelar, fiscalizar, aplicar e promover a observância no que tange aos requisitos regulatórios e contratuais.	

Fonte: Os próprios autores

Com relação aos testes, a metodologia utilizada envolveu uma pesquisa com perguntas realizada com profissionais da área de Tecnologia da Informação. Foram envolvidos dezoito entrevistados que se identificaram com o cargo e tempo de atuação na área. As perguntas versaram sobre a conformidade das organizações com relação às normativas e se as informações apresentadas na matriz estão em conformidade com o conhecimento dos colaboradores sobre as evidências funcionais do modelo que foi baseado na LGPD/ABNT ISO 27001. Segue a sequência de passos para a realização da metodologia de pesquisa:

1º Passo: Inicialmente foi criado um questionário com treze perguntas inerentes ao estudo para nortear a entrevista com profissionais da área de Tecnologia da Informação.

2º Passo: Foi enviado o questionário do Google Forms para os colaboradores de quatro empresas de ramos de atuação distintos através da ferramenta WhatsApp e E-mail.

3º Passo: Foram apresentados os dados coletados do resultado taxonômico do estudo.

4º Passo: Foram feitas perguntas citando os pontos descritos no estudo para buscar conformidade e viabilidade dentro das organizações em que os entrevistados atuam.

5º Passo: Foram coletadas as respostas e as opiniões inerentes ao estudo e armazenadas em um formulário.

4 ANÁLISE DOS DADOS

A compilação dos dados coletados evidenciou que 55,6% dos entrevistados possuem mais de sete anos de atuação na área tecnologia, porém 88,8% apresentam pouco conhecimento ou conhecimento básico sobre a LGPD. Esse fato desperta para a necessidade de instrumentos que facilitem e aproximem os profissionais da área das normativas, abrindo espaços para matrizes de referências como a proposta.

Observou-se que 77,8% dos entrevistados apontaram para a necessidade de fontes de pesquisas complementares que traduzam as normativas em ações práticas. Sendo assim é possível entender que grande parte dos entrevistados entendem que uma matriz como a apresentada contribui na implementação da LGDP nas organizações.

Dos entrevistados, 94,5% acreditam que é possível o tratamento correto dos dados através da política de segurança da informação é essencial e que a NBR 27001 possui processos que conseguem cobrir esses pontos de controle.

Ficou evidente a concordância mútua sobre a criação de uma proposta taxonômica baseada em uma norma brasileira. Pode ser visto que os entrevistados acreditam que a organização, classificação e hierarquia das informações junto a uma norma é possível obter conformidade com a lei, e a tabela taxonômica possui essa estrutura para a compreensão das informações.

Os resultados revelaram também que todos os profissionais de tecnologia, e não apenas a equipe jurídica, deveriam estar cientes e ter uma difusão do tema de LGPD nas organizações. Para os entrevistados atuantes na área, é de grande importância que todos os colaboradores de tecnologia estejam coniventes com o assunto pressuposto e o nosso estudo reforça que é necessário que ambas as partes estejam juntas para tratar da nova lei.

Mais da metade dos entrevistados acreditam que através da política de segurança da informação é possível documentar todos os processos que envolvem os níveis de permissões dos colaboradores das empresas, porém creem que as empresas e os colaboradores não seguem as diretrizes como deveriam e que é necessário ter um controle efetivo dos acessos dos colaboradores mediante as legislações vigentes. Apontam também que as empresas não seguem à risca os processos voltados para a segurança da informação, e que estudos como o aqui apresentado reforçam a importância da disseminação da política de segurança da informação para reduzir os problemas de documentação encontrados nas organizações e os riscos de infringir a legislação, o que pode acarretar em pesadas multas.

Finalmente, 55,6% dos entrevistados concordam parcialmente, 38,9% totalmente e 5,6% indiferente, que a documentações referentes aos dados que possam causar algum dano a organização não estão em conformidade com a legislação, porém acreditam que existem outros meios para tratar esta questão no que se refere a dados sensíveis. Através das boas práticas de tecnologia da informação unida a disseminação da política de segurança da informação seria possível ter conformidade com os pontos citados pelos entrevistados

5 CONSIDERAÇÕES FINAIS

É notório que através de um processo taxonômico que consiste na comparação analítica da intersecção de uma norma internacional que possui processos que quando atrelados a nova Lei Geral de Proteção de Dados contribui com o entendimento e implementação de novas políticas de segurança. Porém apenas este guia não é suficiente para a aplicação total da lei nas organizações, sendo necessário também um apoio jurídico e técnico da equipe de tecnologia da informação, agregando valores para o sucesso da implementação da lei.

A matriz taxonômica apresentada foi de grande valia para entendimento dos processos e artigos citados em lei, pois através dela foi possível despertar os profissionais para a compreensão da cadeia sequencial da normativa.

A pesquisa mostrou resultados positivos na validação da matriz para futuras aplicações como um modelo guia para o entendimento e possível aplicação da LGPD nos negócios, porém com ressalvas que é necessário a disseminação da Política de Segurança da Informação para os colaboradores, juntamente com as documentações inerentes ao uso dos dados.

A pesquisa apontou que grande parte dos colaboradores da área de Tecnologia da Informação não possuem conhecimento concreto para a aplicação da LGDP, sendo de grande utilidade um guia que possa dar apoio para o entendimento dos registros apontados em lei mediante processos que podem ser encontrados em normas de segurança da informação.

O estudo mostrou também diversas problemáticas relacionadas a falta de familiaridade dos colabores com o assunto pressuposto. Dentre os problemas identificados nas organizações foram: dificuldade de compreensão da LGPD, ausência de definições e informações sobre os dados pessoais utilizados pela empresa, deficiente disseminação da Política de Segurança da Informação nas empresas, controle correto dos dados, adequação da Infraestrutura de TI para suprir as necessidades que a lei pede e ausência de documentação referente a utilização dos dados.

Como trabalho futuro, recomenda-se a utilização do modelo taxonômico com a matriz de processos e registros como um guia para auxiliar as empresas e os profissionais de Tecnologia da Informação na implementação da lei em conjunto com uma validação de aptidão das organizações relacionadas aos níveis de maturidade tangíveis a Lei Geral de Proteção de Dados Pessoais, ou seja, as empresas irão ponderar se é necessário a contração de uma consultoria externa para aplicabilidade da lei como um todo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC27001**. Rio de Janeiro, 2013.

BRASIL. Presidência da República. **Lei Geral de Proteção aos Dados**. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 30/10/2020.

HARPER, Douglas. **Taxonomy. Online Etymology Dictionary**. Disponível em: https://www.etymonline.com/. Acesso em: 30/10/2020.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD**. 2.ed. São Paulo: Saraiva, 2020.

ROCHA, Camila; CARNEIRO, Ana Valéria:; MEDEIROS, Marcus Vinícius: MELO, Alexandre. **Segurança Da Informação: A Iso 27.001 Como Ferramenta De Controle Para Lgpd**. Disponível em: <http://www.revistasfap.com/ojs3/index.php/tic/article/view/285>. Acesso em 20 de julho de 2022.