Revista GCTI
Gestão do Conhecimento e Tecnologia da Informação
RGCTI 6:61-72, 2022
ISSN: 2526-8384

Modelo de maturidade de compliance à LGPD – Lei Geral de Proteção de Dados Pessoais

LGPD Compliance Maturity Model - General Law for the Protection of Personal Data

Joel Mateus Lopes Ferreira[a], João Souza Neto[b], Edilson Ferneda[c]

[a] *joel.jfx@gmail.com*

[b] *sznetoj@gmail.com*

[c] *eferneda@gmail.com*

Resumo: Diversas nações identificaram a necessidade de rever suas legislações com intuito de viabilizar a proteção de dados aos titulares e usuários, a exemplo do Brasil, com a publicação da Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD). Esta pesquisa propõe um modelo para identificar, em uma organização, o nível de maturidade de compliance à LGPD. A pesquisa foi classificada como exploratória, de natureza aplicada e com abordagem qualitativa. Adicionalmente, foi empregada metodologia para construção do modelo de maturidade, aliada com técnica de análise de conteúdo e aplicação de survey. O modelo inicialmente proposto foi avaliado por grupo de especialistas por meio da técnica de discussão de grupo focal, gerando insumos para revisão e proposição do modelo final. Ao ser aplicado o modelo na organização, será possível identificar o estágio de maturidade de compliance à LGPD, possibilitando que a empresa realize ações de melhoria contínua.

Palavras-chave: Modelo de Maturidade, LGPD, Compliance, Conformidade. Proteção de Dados.

Abstract: Several nations identified the need to revise their legislation in order to make data protection feasible for holders and users, as in Brazil, with the publication of Law no. 13.709 / 18 - General Law for the Protection of Data. Personal Data (LGPD). This research proposes a model to identify, in an organization, the level of compliance maturity to LGPD. The research was classified as exploratory, applied a qualitative approach. In addition, a methodology was used to build the maturity model, combined with the technique of content analysis and survey application. The initially proposed model was evaluated by a group of experts using the focus group discussion technique, generating inputs for review and proposition of the final model. When the model is applied in the organization, it will be possible to identify the stage of maturity of compliance with the LGPD, allowing the company to carry out continuous improvement actions.

Keywords: Maturity Model, LGPD, Compliance, Data Protection.

1. Introdução

A proteção de dados pessoais, ao longo do tempo, tornou-se um tema cada vez mais relevante. O rápido desenvolvimento tecnológico, devido ao progresso da capacidade de processamento e de armazenamento, possibilitou às empresas coletarem e processarem os dados, com a utilização em vários propósitos (Tikkinen-Piri, Rohunen, & Markkula, 2018).

Cada vez mais, as empresas tendem a usar esses dados para aplicações em serviços personalizados e marketing, por exemplo. O contínuo crescimento e a evolução da tecnologia ocorreram a tal ritmo que foi necessário adaptar os marcos legais relacionados à proteção de dados (Tikkinen-Piri *et al.*, 2018; Diamantopoulou, Tsohou, & Karyda, 2020)

2. Proteção de dados

Em que pese a relevância cada vez maior sobre a proteção de dados, no Brasil, o Código de Defesa do Consumidor (CDC), publicado em 1990, já abordava questões relacionadas às informações e cadastro de consumidores (Brasil, 1990). O CDC estabelece que a abertura de cadastro ou registro de dados pessoais deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. Adicionalmente, sempre

que o consumidor encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção (Brasil, 1990).

Outro marco regulatório importante no Brasil sobre esse tema é o Marco Civil da Internet (Brasil, 2014), o qual estabeleceu garantias e deveres para o uso da Internet no Brasil. Em seu 3º artigo, são apresentados os princípios que a regem, dentre eles, a proteção à privacidade e a proteção dos dados pessoais

Na União Europeia, a Diretiva 95/46 de 1995 (DIR95), estabeleceu uma ampla matéria sobre proteção de dados pessoais, a qual já abordava a definição de conceitos sobre processamento de informações e a aplicação dos princípios e leis de proteção à privacidade individual (União Europeia, 1995).

A DIR 95 foi substituída pelo Regulamento Geral de Proteção de Dados - *General Data Protection Regulation* (GDPR), aprovado em abril de 2016 e aplicável a todos estados membros da União Europeia. A partir dos princípios e regras desse regulamento, o GDPR amplia os direitos dos titulares dos dados, motivando empresas a protegerem seus sistemas para evitar violações de dados e relatar efetivamente sobre quando a mitigação falhar (Zerlang, 2017). Seus principais avanços em relação à DIR95 estão relacionados à definição de categorias especiais de dados pessoais, a responsabilidades do controlador de dados, à gestão do consentimento e à notificação da violação (Diamantopoulou *et al.*, 2020).

No Brasil, após os marcos do CDC e o Marco Civil da Internet, foi publicada em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), com início da vigência em setembro de 2020 (Brasil, 2018). A LGPD permeia sua aplicabilidade a entes públicos e privados, regulando danos individuais e coletivos, e tem por objetivo proteger os direitos fundamentais da pessoa natural, como privacidade, intimidade, honra, direito de imagem e dignidade (Pinheiro, 2018).

Na LGPD, também são estabelecidos conceitos como, por exemplo, o de dados sensíveis e tratamento de dados. A partir da LGPD, passa a ficar claro o que é ou não dado pessoal, assim como todos os processos, as técnicas e os procedimentos relativos ao tratamento de dados (Pinheiro, 2018). Maldonado *et al.* (2019) salientam que o conceito de tratamento de dados na LGPD é abrangente e inclui todas operações relativas aos dados pessoais, desde sua coleta até a sua extinção. Os autores destacam que o mero armazenamento está inserido, por definição legal, como atividade de tratamento, de sorte que a simples posse dos dados determina, por si só, a observância dos dispositivos legais.

Para Maldonado *et al.* (2019), a promulgação do GRPR influenciou diretamente a elaboração da LGPD. Erickson (2019) complementa que a LGPD tem semelhanças com o GDPR, uma vez que ambas estabelecem conceitos para dados pessoais, bem como exigem o consentimento do titular dos dados para coleta e tratamento. Para o autor, a LGPD é menos extensa e menos prescritiva que o GDPR, o que torna a LGPD mais flexível. Em contrapartida, a falta de prescrição e a ausência de textos explicativos podem causar incerteza para as organizações que se preparam para entrar em conformidade com a referida Lei (Erickson, 2019).

As regulamentações de proteção de dados têm implicações nas estruturas de governança e nos aspectos relacionados à transparência e prestação de contas (Ingley & Wells, 2016). Enquanto a adesão aos regulamentos pode ser um processo caro para as organizações, a implementação pode ir além da conformidade, visto que as empresas podem tirar proveito desse processo, utilizando ferramentas avançadas para análise dos dados (Zerlang, 2017).

No contexto de proteção de dados, alguns estudos foram realizados com a proposição de *framework* para verificar a conformidade com o GDPR, a exemplo de Antignac, Scandariato e Schneider (2016), Ayala-Rivera e Pasquale (2018) e Lisiak-Felicka *et al.* (2020).

Ayala-Rivera e Pasquale (2018) elaboraram um guia, com abordagem sistemática, contendo seis etapas para apoiar as empresas para obter os requisitos que garantam a conformidade com as obrigações impostas pelo GDPR. O referido guia vincula os requisitos do GDPR com os requisitos de controles de privacidade que podem ser implementados dentro da organização. Nesse mesmo sentido, Antignac *et.al.* (2016) apresentaram os aspectos técnicos que devem ser considerados para o desenvolvimento de um software, sob a ótica da legislação e das melhores práticas. Os autores elaboraram um modelo conceitual a partir da legislação do GDPR e da ISO 29100.

Por fim, Lisiak-Felicka *et al.* (2020) avaliaram o grau de implementação do GDPR na administração do governo local da Polônia e República da Lituânia. Os resultados da pesquisa

foram submetidos à análise estatística e após esse processo, foram identificadas algumas lacunas ocorridas no momento da implementação.

No Brasil, Rapôso *et al*. (2019) realizaram uma revisão sistemática sobre o tema LGPD. Nesse estudo, segundo os autores, não foram localizadas pesquisas relacionadas à aplicabilidade da Lei nas empresas, bem como as ações necessárias para entrar em *compliance* com a LGPD. Adicionalmente, os autores propõem como estudo futuro o desenvolvimento de artefatos que apoiem as organizações e cidadãos a lidar com a LGPD.

3. *Compliance* e modelos de maturidade

No que tange ao conceito de c*ompliance*, este pode ser definido como conformidade de um conjunto de regras. Além disso, é um conceito que está associado com os entendimentos das relações com a lei e seus comportamentos (Kingsbury, 1998). Há autores que afirmam que as leis não podem ser avaliadas sob o aspecto binário de "conformidade" e "não conformidade" (Chayes & Chayes, 1995 *apud* Kingsbury, 1998). Para eles, "*compliance*" de determinada lei pode ser avaliada sob graus de conformidade em conjunto com as circunstâncias de comportamento.

Para avaliar os níveis de compliance de uma determinada lei, pode-se utilizar um modelo de maturidade, a exemplo de Gheorghe *et al*. (2009), que construíram um artefato para avaliar o nível de maturidade de governança e *compliance* de um processo.

Król e Zdonek (2020) definem um modelo de maturidade como um guia que, a partir de critérios e indicadores, define o estado atual para o desenvolvimento de um processo ou atividade. Além disso, o modelo fornece critérios e características que precisam ser atendidos para se atingir um determinado nível de maturidade.

Além do conceito de maturidade, existem cinco conceitos importantes identificados para compor um modelo de maturidade (Monteiro & Maciel, 2020):

- **Níveis de maturidade:** também conhecidos como estágios, níveis, pontuação de maturidade; utilizados para descrever o resumo geral ou a maturidade da entidade a ser avaliada.
- **Dimensões ou Domínios:** também chamadas de variáveis de referência, áreas de processo, capacidade e fatores críticos de sucesso.
- **Subcategorias ou Subdomínios:** são variáveis de segundo nível vinculadas às dimensões.
- **Caminho para maturidade:** os modelos podem ser avaliados seguindo um método linear, caminho unidirecional ou de menor para maior maturidade.
- **Questões de avaliação:** geralmente ligadas diretamente a subcategorias, com pontuação ou nível de maturidade.

Além de propor uma arquitetura para os modelos, estabelecendo uma estrutura genérica de um modelo de maturidade, Monteiro e Maciel (2020) Identificaram os fundamentos teóricos para desenvolvê-los. Nesse sentido, os autores sugerem três referências: *(i)* a abordagem dividida em seis etapas proposta por De Bruin *et al*. (2005); *(ii)* a abordagem dividida em oito etapas ou requisitos, proposta por Becker, Knackstedt e Poppelbulb (2009) e *(iii)* a abordagem dividida em cinco estágios proposta por Solli-Saether e Gottschalk (2010).

4. Metodologia

Com o objetivo de desenvolver um modelo para avaliar o nível de maturidade de *compliance* à LGPD, foi aplicada a metodologia apresentada por Becker *et al*. (2009). A elaboração do modelo por meio de iterações e procedimentos multi-metodológicos, possibilita uma melhoria incremental a partir da observância e implementação dos requisitos, promovendo uma robustez para o processo de construção.

Quanto à classificação, esta pesquisa é aplicada, uma vez que objetiva gerar conhecimento a partir de uma aplicação prática de um modelo de maturidade para um problema específico, relacionado ao regulamento de proteção de dados pessoais, e também pode ser classificada como exploratória, uma vez que tem por objetivo abordar um problema recente, de modo a fornecer informações para uma investigação mais precisa.

5. Etapas da pesquisa

Para a elaboração do modelo de maturidade serão utilizados os oito requisitos apresentados no método construído por Becker *et al*. (2009), conforme Quadro 1.

Quadro 1. Descrição das etapas da pesquisa.

Etapas	Descrição
1. Definição do problema (R6)	O problema pode ser definido por meio da seguinte questão: "Quais são os principais elementos e características que compõem um modelo de avaliação de maturidade quanto à *compliance* à Lei Geral de Proteção de Dados Pessoais - LGPD?" De forma complementar, salienta-se que a proposta do trabalho está delimitada pela avaliação de maturidade de *compliance* à Lei brasileira, LGPD, limitando o escopo de desenvolvimento à Lei nº 13.709/18.
2. Relevância do problema (R5)	A LGPD se aplica à operação de tratamento de dados pessoais realizada no território nacional, com penalidades previstas envolvendo desde advertência a multas pecuniárias, tal fato reforça a importância e a relevância de se identificar o estágio de maturidade de uma organização quanto à *compliance* à LGPD.
3. Comparação com modelos existente (R1)	Por meio da pesquisa bibliográfica não foram identificados modelos de avaliação de maturidade à legislação de proteção de dados. Entretanto, foi localizado um *framework* de avaliação de maturidade em privacidade, elaborado pelo Departamento de assuntos internos, vinculado ao Governo de Nova Zelândia, em conjunto com a consultoria KPMG.
4. Procedimentos iterativos (R2)	a. Design: elaboração de domínios e subdomínios a partir de Análise de Conteúdo (R4) da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/18; b. Seleção de abordagem: elaboração de questões vinculadas a cada subdomínio por meio de análise à Lei nº 13.709/18. Definição da escala de pontuação por meio de pesquisa bibliográfica (R4); c. Elaboração de pesos dos domínios e subdomínios a partir da aplicação de *survey* (R4) na comunidade acadêmica e em uma rede social voltada para contatos profissionais e empresas; d. Elaboração dos níveis de maturidade com as respectivas descrições a partir de pesquisa bibliográfica (R4); e. Avaliação (R3) do modelo a partir de discussão por meio de grupo focal (R4) com especialistas da área; f. Análise dos resultados da discussão do Grupo Focal e eventual ajuste no modelo de maturidade (R2).

Fonte: Os autores.

Além das etapas apresentadas no Quadro 1, a metodologia proposta por Becker *et al*. (2009) também contempla a etapa de apresentação dos resultados e conclusões (R7) e documentação de todas fases e procedimentos da pesquisa (R8).

5.1 Análise de conteúdo

Para a elaboração do modelo de maturidade de *compliance* à LGPD, a primeira etapa consistiu na aplicação da metodologia de Análise de Conteúdo.

A Análise de Conteúdo é uma técnica de análise das comunicações, que avalia o que foi dito nas entrevistas ou observado pelo pesquisador, buscando classificá-lo em temas ou categorias que auxiliam na compreensão do que está no conteúdo das mensagens (Bardin, 1977; Silva & Fossá, 2015).

A Análise de Conteúdo pode ser sintetizada nas seguintes etapas (Silva & Fossá, 2015):

(i) Leitura geral do material coletado;
(ii) Codificação para formulação de categorias de análise;
(iii) Recorte do material em unidades de registro (palavras, frases, parágrafos) comparáveis e com o mesmo conteúdo semântico;
(iv) Estabelecimento de categorias que se diferenciem, tematicamente, nas unidades de registro;
(v) Agrupamentos das unidades de registro em categorias comuns;
(vi) Agrupamento progressivo das categorias (iniciais, intermediárias, finais);
(vii) Inferência e interpretação, respaldadas no referencial teórico.

O material utilizado será a Lei nº 13.709/18, que rege a LGPD (etapa *"i"*). Considerando a estrutura da Lei, não foi necessário codificar os textos (*"ii"*). Adicionalmente, os artigos foram definidos como unidades de registro (*"iii"*).

Dessa forma, inicialmente foram definidas 65 unidades de registro, correspondendo aos 65

artigos da Lei nº 13.709/18. Por meio da análise do pesquisador, foi estabelecida uma categoria inicial para cada unidade de registro (etapas *"iv"* e *"v'*). Salienta-se que, após a elaboração do *design* do modelo, a referida estrutura será apresentada e discutida por meio de um grupo focal, composto por especialistas da área.

No processo de vinculação das categorias iniciais, foram identificados artigos que foram vetados por ajuste de Lei anterior, esses foram excluídos para o trabalho de análise de categorias intermediárias e categorias finais.

A partir da construção das categorias iniciais, vinculadas a cada artigo da Lei, foram construídas as categorias intermediárias, que correspondem ao agrupamento das categorias iniciais. Por sua vez, após a elaboração das categorias intermediárias, estas foram agrupadas originando as categorias finais, concluindo a etapa *"vi"* da Análise de Conteúdo. O Quadro 2 apresenta as categorias finais.

Dessa forma, por meio do estudo realizado, verifica-se que as categorias finais vinculadas à Lei são: "Dispositivos da Lei", "Gestão de Dados", "Gestão do Consentimento", "Gestão de Riscos", "Gestão de Segurança" e "Governança".

Considerando que a categoria final "Dispositivos da Lei" se refere a artigos intrínsecos da Lei e, por consequência, não permitiriam diferenciar o nível de maturidade de *compliance* à LGPD, este foi excluído para a elaboração do modelo.

Adicionalmente, por meio da análise das categorias intermediárias, foi possível elaborar os subdomínios vinculados a cada domínio. O Quadro 3 apresenta os Domínios e Subdomínios construídos a partir da Análise de Conteúdo.

5.2 Escala da avaliação das questões

Modelos de maturidade foram projetados para avaliar a competência ou a capacidade de um domínio selecionado. A forma mais comum para avaliar a maturidade é uma escala de pontuação, sendo que a maior pontuação

Quadro 2. Categorias Finais da lei 13.709/18 – LGPD.

Categorias Iniciais agrupadas (Artigos)	Categoria Intermediária	Categoria Final
2 - 17 - 21 - 44	Princípios da Lei	Dispositivos da Lei
5 – 12	Definição de Termos	
30 - 60 - 61 - 64 - 65	Dispositivos da Lei	
58	Estrutura da ANPD	
42 - 43 - 52 - 53 - 54	Penalidades	
29 - 31 - 34 - 35 - 40 - 51 - 55 - 62 - 63	Responsabilidades da ANPD	
1 - 3 - 4 - 7 - 22 - 24 - 45	Escopo da Lei	
13 - 14 - 15 - 16 - 23 - 26 - 33 - 36	Escopo de tratamento	Gestão de dados
6 [Inciso I a V e IX] - 10 - 11 - 25 - 37 - [50 Parágrafo 2º Inciso I: "b"]	Tratamento de dados	
9 - 18 - 19 - 20	Direitos do titular	Gestão do consentimento
6 [Inciso VI]	Transparência ao titular dos dados	
8 - 27	Consentimento	
50 [Parágrafo 2º Inciso I: "e"]	Comunicação com o titular	
32 - 38	Relatório de impacto	Gestão de riscos
50 [Parágrafo 2º Inciso I: "d"]	Avaliação de impacto e risco à privacidade	
6 Inciso VII e VIII - 47	Segurança da informação	Gestão de segurança
48 - 50 [Parágrafo 2º Inciso I: "g"]	Incidentes de segurança	
46	Medidas de segurança	
49	Requisitos de segurança	
6 [Inciso X]	Responsabilização	Governança
39 - 41 - 50 [Parágrafo 1ª]	Responsabilidades	
50 [Parágrafo 2º Inciso I: "a", "c", "f" e "h"]	Programa de governança em Privacidade	
50 [Parágrafo 2º Inciso II e Parágrafo 3º]	Efetividade do programa de governança	

Fonte: Os autores.

Quadro 3. Estrutura do Modelo de Maturidade.

Domínios	Subdomínios
Gestão de Dados	escopo de tratamento
	tratamento de dados
Gestão do Consentimento	consentimento
	comunicação com o titular dos dados
Gestão de Riscos	relatório de impacto
	avaliação de riscos à privacidade
Gestão de Segurança	medidas de segurança
	incidentes de segurança
Governança	programa de governança em privacidade
	responsabilidades e responsabilizações

Fonte: Os autores.

Quadro 4. Elaboração de questões vinculadas ao artigo 8ª da LGPD.

Questão	Descrição	A maturidade da organização referente a essa questão é:
1	Nas situações previstas no Inciso I do artigo 7º, a organização colhe o consentimento do Titular dos Dados por escrito ou por outro meio que demonstre a manifestação de vontade do Titular.	( ) 1 ( ) 2 ( ) 3 ( ) 4
2	Nas situações em que o consentimento é fornecido por escrito, a organização possui uma cláusula destacada das demais cláusulas contratuais.	( ) N/A ( ) 1 ( ) 2 ( ) 3 ( ) 4
3	Nas situações de alteração de finalidade do tratamento em que o consentimento é exigido, a organização possui procedimento especifico para informar ao Titular dos Dados, podendo revogar o consentimento caso discorde da alteração.	( ) 1 ( ) 2 ( ) 3 ( ) 4

Fonte: Os autores.

representa o nível mais alto de maturidade (De Bruin *et al.*, 2005).

O uso de escalas de pontuação pode melhorar a confiabilidade e a consistência da resposta e permite que os resultados sejam facilmente mapeados para os estágios de maturidade (De Bruin *et al.*, 2005).

Diante do exposto, com intuito de avaliar o estágio de maturidade da organização em relação a cada questão, optou-se por utilizar uma escala de pontuação, utilizando-se como referência o COBIT 5 (ISACA, 2013).

A partir da referência citada, foi construída uma escala de quatro níveis, com pontuação de 1 a 4, apresentada a seguir:

- **Pontuação 1:** atendimento mínimo, básico, do que foi determinado pela Lei.
- **Pontuação 2:** atendimento básico, com a organização buscando novas soluções estruturantes para o aprimoramento do procedimento ou quesito.
- **Pontuação 3:** atendimento pleno com procedimentos e práticas formalizados.
- **Pontuação 4:** atendimento pleno da determinação da Lei, bem como a aplicação das melhores práticas de mercado, estabelecendo diretrizes e referências para os demais *stakeholders*.

Dessa forma, por meio da escala proposta, quanto maior for a pontuação, maior será o nível de maturidade da organização frente à questão avaliada.

5.3 Elaboração das questões

As questões do modelo de maturidade foram construídas a partir dos artigos da LGPD, vinculados a cada subdomínio. A título de ilustração, a partir do artigo 8º, vinculado ao domínio "Gestão do Consentimento" e subdomínio "Consentimento", foram elaboradas as questões apresentadas no Quadro 4.

De forma análoga ao procedimento mencionado, foram elaboradas as demais questões

Tabela 1. Estrutura do Modelo de Maturidade e quantidade de questões.

Domínios	Subdomínios	Qtde. de questões
Gestão de Dados	Escopo de Tratamento	10
	Tratamento de Dados	10
Gestão do Consentimento	Consentimento	4
	Comunicação com o Titular dos Dados	6
Gestão de Riscos	Relatório de Impacto	2
	Avaliação de Riscos à Privacidade	1
Gestão de Segurança	Medidas de Segurança	4
	Incidentes de Segurança	2
Governança	Programa de Governança em Privacidade	5
	Responsabilidades e Responsabilizações	4
	Total	**48**

Fonte: Os autores.

Quadro 5. Exemplo de perguntas utilizadas no *survey*.

Pergunta	Descrição da pergunta
Pergunta 1	Qual o peso que você estabeleceria para cada domínio? [a soma dos pesos deve resultar em 100] ( ) Gestão de Dados ( ) Gestão de Consentimento ( ) Gestão de Riscos ( ) Gestão de Segurança ( ) Governança
Pergunta 2	No domínio "Gestão de Dados", qual peso você estabeleceria para cada subdomínio? [a soma dos pesos deve resultar em 100] ( ) Escopo de Tratamento ( ) Tratamento de Dados

Fonte: Os autores.

relacionadas aos artigos vinculados aos domínios e subdomínios do modelo de maturidade.

Após a elaboração das questões vinculadas a cada subdomínio, a estrutura do modelo de maturidade de compliance à LGPD pode ser apresentada como na Tabela 1.

5.4 Definição de pesos dos domínios e subdomínios

Uma vez estabelecido o critério de avaliação das questões, é possível apurar um cálculo de pontuação por domínios e definir, por consequência, um nível de maturidade para a organização. Para isso, é possível considerar uma média simples das pontuações vinculadas às questões ou aplicar pesos, a serem atribuídos por meio de outros critérios (New Zealand Government, 2014).

Nesse sentido, de forma a avaliar a pontuação de cada domínio (Gestão de Dados, Gestão do Consentimento, Gestão de Riscos, Gestão de Segurança e Governança) foi realizado um *survey* com o objetivo de colher informações para definição de pesos para os domínios e subdomínios do modelo de maturidade.

O *survey* foi distribuído livremente por meio de um *link* para a comunidade acadêmica e em uma rede social voltada para contatos profissionais e de empresas. Adicionalmente, foram elaboradas perguntas de forma que os cidadãos pudessem estabelecer peso para cada domínio e subdomínio, conforme exemplo apresentado no Quadro 5.

De forma análoga à pergunta 2, referente ao peso para os subdomínios vinculados a "Gestão de Dados", apresentado no Quadro 5, foram elaboradas as demais perguntas para os subdomínios restantes.

Para a apuração dos pesos dos domínios e subdomínios, foram selecionados os questionários vinculados aos cidadãos com participação em cursos relacionados à LGPD ou profissionais com atuação na área de proteção de dados (perguntas contempladas no *survey* para seleção do perfil do público), resultando na seleção de 70 respondentes.

Tabela 2. Estatísticas das respostas às perguntas do *survey* sobre domínios.

Domínios	Qtde. Respostas	Média	Mediana	Mínimo	Máximo
Gestão de Dados	70	23,3	20	5	65
Gestão do Consentimento	70	17,1	15	5	40
Gestão de Riscos	70	19,1	20	5	50
Gestão de Segurança	70	20,2	20	5	50
Governança	70	20,3	20	5	50

Fonte: Os autores.

Tabela 3. Estatísticas das respostas às perguntas do *survey* sobre subdomínios.

Subdomínios	Qtde. Respostas	Média	Mediana	Mínimo	Máximo
Escopo de tratamento	70	47,9	50	10	80
Tratamento de dados	70	52,1	50	20	90
Consentimento	70	58,1	55	20	95
Comunicação com o titular dos dados	70	41,9	45	5	80
Relatório de impacto	70	39,4	40	10	70
Avaliação de riscos à privacidade	70	60,6	60	30	90
Relatório de impacto	70	39,4	40	10	70
Avaliação de riscos à privacidade	70	60,6	60	30	90
Medidas de segurança	70	64,2	60	10	95
Incidentes de segurança	70	35,8	40	5	90
Programa de governança em privacidade	70	57,3	60	10	90
Responsabilidades e responsabilizações	70	42,7	40	10	90

Fonte: Os autores.

Dos 70 questionários, foram construídas as estatísticas de média, mediana, valor mínimo e valor máximo dos pesos informados para cada questão.

Pela ótica dos valores médios (estatística média), verifica-se que o domínio com maior peso, segundo os respondentes, é "Gestão de Dados", seguido dos domínios: "Governança", "Gestão de Segurança", "Gestão de Riscos" e, por fim, "Gestão do Consentimento", como apresentado na Tabela 2.

Mesma análise foi realizada para os subdomínios, conforme apresentado na Tabela 3.

Por fim, o estudo também foi contemplado com a análise de *outliers*, onde não foram identificadas distribuições significativamente dispersas para as pontuações dos domínios e subdomínios. Além disso, partindo da premissa que a soma das pontuações dos subdomínios seja 100, uma vez que o respondente declare um peso elevado para um determinado subdomínio, para o outro subdomínio, o peso, por consequência, será baixo. Tal dinâmica contribuiu para a amplitude de pontuações (distância entre o valor mínimo e valor máximo) das dimensões analisadas.

Considerando o *survey* realizado e a seleção do perfil dos respondentes, foram estabelecidos os pesos dos domínios e subdomínios a partir dos valores médios das respostas dos 70 questionários. Tal critério estaria alinhado com a percepção média dos respondentes.

5.5 Elaboração dos níveis de maturidade

Após o processo de estabelecimento de pesos e cálculo de maturidade para os domínios e subdomínios, a etapa seguinte consiste na definição dos níveis de maturidade.

Para a elaboração dos níveis de maturidade utilizou-se como referência o modelo desenvolvido pelo Governo de Nova Zelândia. A partir da referência mencionada, foram estabelecidos quatro níveis de maturidade. Adicionalmente, a escala de pontuação (de 1 a 4) foi dividida em quartis, com faixas incrementais de 0,75 em cada estágio de maturidade:

- **Iniciante:** a pontuação final do modelo se encontra no intervalo de 1,00 a 1,75. Políticas, processos e práticas, relacionados ao tratamento de dados pessoais, não estruturados. A *compliance* à LGPD depende principal-

mente de iniciativas individuais e não de processos.

- **Em Desenvolvimento:** a pontuação final do modelo se encontra no intervalo de 1,76 a 2,50. Políticas, processos e práticas parcialmente estruturados e documentados, os quais possuem abordagens e aplicações isoladas em alguns setores da empresa.
- **Consolidado:** a pontuação final do modelo se encontra no intervalo de 2,51 a 3,25. Políticas, processos e práticas possuem definições claras e abrangentes. A empresa possui uma abordagem de *compliance* à LGPD holística e proativa.
- **Avançado:** a pontuação final do modelo se encontra no intervalo de 3,26 a 4,00. Políticas, processos e práticas, relacionadas ao escopo da LGPD, são amplamente consolidados, com uma cultura organizacional de melhoria continua. A organização é vista pelos *stakeholders* e usuários como referência em boas práticas de tratamento de dados pessoais e *compliance* à LGPD.

5.6 Avaliação do modelo de maturidade

Para a avaliação do modelo de maturidade proposto foi aplicado o método de discussão de Grupo Focal.

A discussão de grupo focal contou com a participação de cinco especialistas em assuntos correlatos à proteção de dados. Quanto à análise e contribuições do Grupo Focal sobre o modelo proposto, os especialistas declararam que o modelo está bem fundamentado e realizaram as seguintes sugestões:

- Revisão da escala de pontuação das questões;
- Inclusão de um quinto nível de maturidade e revisão dos pontos de corte da pontuação para estabelecimento de cada nível;
- Revisão da nomenclatura dos níveis de maturidade;
- Revisão do descritivo do último nível de maturidade do modelo, incluindo o processo de retroalimentação.

5.7 Ajuste do modelo de maturidade

Após a avaliação do modelo por meio da reunião de Grupo Focal, o modelo foi revisto, com objetivo de implementar as sugestões realizadas pelo grupo de especialistas. Tal dinâmica, além de estar em linha com a metodologia proposta por Becker *et al*. (2009), possibilita uma maior robustez na construção do modelo.

Quanto à escala das questões, inicialmente foi proposta com gradação entre um a quatro pontos. Considerando as contribuições dos especialistas, onde foi sugerida a revisão da escala, por meio da ampliação das gradações, seria de propor a seguinte escala para a pontuação das questões:

- **Pontuação 0:** não atendimento do que foi determinado pela Lei.
- **Pontuação 1:** atendimento parcial e não satisfatório do que foi determinado pela Lei.
- **Pontuação 2:** atendimento mínimo, básico, do que foi determinado pela Lei.
- **Pontuação 3:** atendimento básico, com a organização buscando novas soluções estruturantes para o aprimoramento do procedimento ou quesito.
- **Pontuação 4:** atendimento pleno com procedimentos e práticas formalizados.
- **Pontuação 5:** atendimento pleno da determinação da Lei, bem como a aplicação das melhores práticas de mercado, estabelecendo diretrizes e referências para os demais *stakeholders*. Adicionalmente, para o referido atributo, a organização possui monitoramento e acompanhamento constante, viabilizando a retroalimentação do processo e a melhoria contínua.

A nova escala proposta foi elaborada utilizando como referência o COBIT 2019 (ISACA, 2019). Este framework apresenta o conceito de maturidade para avaliação de um conjunto de objetivos de governança e gestão, denominado área de foco.

Quanto aos níveis de maturidade, considerando as contribuições dos especialistas, onde foi sugerida a inclusão de um quinto nível de maturidade e a revisão da semântica dos níveis, optou-se por realizar uma revisão abrangente das nomenclaturas dos estágios.

Nesse sentido, utilizando-se como referência os níveis de maturidade do *framework* de avaliação de Privacidade, elaborado pelo Governo de Nova Zelândia, e também as contribuições dos especialistas do Grupo Focal, seria de propor os seguintes níveis de maturidade: “Conscientização”, “Em Desenvolvimento”, “Estruturado”, “Consolidado” e “Otimizado”.

No que tange à definição de pontos de corte de pontuação para delimitação dos níveis, ponderando que não foi identificada na literatura

Tabela 4. Modelo Final – Estrutura do Modelo de Maturidade e quantidade de questões.

Domínios		Subdomínios		Qtde. de Questões
Descrição	Peso	Descrição	Peso	
Gestão de Dados	23,3	Escopo de Tratamento	47,9	10
		Tratamento de Dados	52,1	10
Gestão do Consentimento	17,1	Consentimento	58,1	4
		Comunicação com o Titular dos Dados	41,9	6
Gestão de Riscos	19,1	Relatório de Impacto	39,4	2
		Avaliação de Riscos à Privacidade	60,6	1
Gestão de Segurança	20,2	Medidas de Segurança	64,2	4
		Incidentes de Segurança	35,8	2
Governança	20,3	Programa de Governança em Privacidade	57,3	5
		Responsabilidades e Responsabilizações	42,7	4
				48

Fonte: Os autores.

Quadro 6. Modelo Final - Níveis de Maturidade do Modelo de *Compliance* à LGPD.

Pontuação	Maturidade	Descrição
0,00 a 1,00	Conscientização	Políticas, processos e práticas, relacionados ao tratamento de dados pessoais, não são estruturados e não são satisfatórios.
1,01 a 2,00	Em desenvolvimento	Políticas, processos e práticas parcialmente estruturados e documentados, os quais possuem abordagens e aplicações isoladas em alguns setores da empresa.
2,01 a 3,00	Estruturado	Políticas, processos e práticas possuem definições claras e abrangentes. A empresa possui amplo conhecimento de gestão de privacidade.
3,01 a 4,00	Consolidado	Políticas, processos e práticas são consistentes em todas áreas da organização. A empresa possui uma abordagem de compliance à LGPD holística e proativa.
4,01 a 5,00	Otimizado	Políticas, processos e práticas, relacionadas ao escopo da LGPD, são amplamente consolidados e a organização é vista pelos stakeholders e usuários como referência em boas práticas de tratamento de dados pessoais e compliance à LGPD. Adicionalmente, a empresa possui monitoramento e acompanhamento dos seus processos, com retroalimentação constante, promovendo uma cultura organizacional de melhoria contínua.

Fonte: Os autores.

referência de critérios, e considerando que a escala das questões, após sua revisão, passou a ter seis pontos de amplitude (variação de zero a cinco pontos), foi estabelecida a variação de um ponto para cada nível de maturidade.

6. O modelo final

Após a revisão do modelo a partir das contribuições da avaliação do grupo de especialistas, o modelo de maturidade de *compliance* à LGPD pode ser representado conforme a Tabela 4. Quanto aos seus níveis de maturidade, estes são apresentados no Quadro 6.

A título de ilustração, a maturidade do domínio "Governança" pode ser calculada a partir da média ponderada dos subdomínios "Programa de Governança em Privacidade" e "Responsabilidades e Responsabilizações", e a pontuação final do modelo de *compliance* à LGPD, pela média ponderada das maturidades dos domínios.

7. Conclusão

Ao longo das últimas décadas, a aceleração da transformação digital, aliada com o aumento da capacidade de armazenamento de informações, propiciou o desenvolvimento de sistemas mais ágeis e robustos, corroborando para o uso intensivo de dados.

Em paralelo a essa transformação, diversas nações identificaram a necessidade de rever

suas legislações, adaptando-as ao novo contexto e impondo novas regras, com intuito de viabilizar a proteção de dados aos titulares e usuários.

Nesse sentido, de forma análoga à publicação do GDPR na Europa, no Brasil, foi publicada a LGPD, com vigência a partir setembro de 2020.

Considerando que a LGPD é aplicada para todas as empresas residentes no território nacional, as quais podem ter diversos níveis de *compliance* à Lei, vislumbrou-se a oportunidade de elaborar uma pesquisa relativa a esse tema.

Para atendimento dessa questão, foi realizada revisão bibliográfica a partir de buscas por palavras-chave vinculadas ao tema proteção de dados e modelo de maturidade. Nesse sentido, foram identificados os principais elementos e características que compõem um modelo de avaliação de maturidade de *compliance* à LGPD, dentre eles, as questões, subdomínios, domínios, pontuação do modelo e níveis de maturidade.

Diante desse contexto, o modelo proposto oferece uma contribuição que pretende ser significativa para indústria, uma vez que uma organização pode aplicar o modelo e identificar o estágio de maturidade de *compliance* em que se encontra, possibilitando, assim, a elaboração de ações de melhoria dos processos e mecanismos vinculados ao tema.

Adicionalmente, este trabalho buscou contribuir para a produção acadêmica, caracterizado também pelo seu caráter inovador, uma vez que não foi identificado na literatura modelo para avaliação de maturidade de *compliance* a legislações e regulamentos de proteção de dados.

No que tange às limitações do modelo, salienta-se que não foi identificado na literatura referência sobre critérios para definição do ponto de corte da pontuação para o estabelecimento dos níveis de maturidade. Dessa forma, a construção foi realizada a partir do critério definido pelo pesquisador, com a apreciação posterior dos especialistas do grupo focal.

Além disso, considerando que as questões foram elaboradas a partir dos artigos da Lei nº 13.709/18 (LGPD), eventual alteração da referida da Lei poderá implicar a revisão do modelo, inclusive nos pesos dos domínios e subdomínios.

De forma a mitigar as limitações identificadas, é necessário o acompanhamento e monitoramento constante do modelo. Nesse sentido, sugere-se como trabalhos futuros a aplicação do modelo em diversas organizações e setores da economia, com objetivo de avaliar se o resultado, quanto à maturidade LGPD da organização, está aderente com a percepção de especialistas e administradores da empresa.

A partir dessas aplicações e avaliação de resultados, sugere-se que os níveis de maturidade, com os respectivos pontos de corte da pontuação, pesos dos domínios e subdomínios, sejam constantemente recalibrados e aprimorados, gerando a retroalimentação no modelo e promovendo melhoria contínua.

Além disso, para a calibragem dos pesos de domínios e subdomínios, sugere-se a utilização do método de análise hierárquica *Analytic Hierarchy Process* (AHP), em uma eventual substituição à calibragem do modelo via *survey*.

Por fim, é possível utilizar a solução em questão como referência para a construção de modelo de maturidade de *compliance* ao GDPR e também como ponto de partida para a construção de um modelo de maturidade de privacidade.

Referências

Antignac, T., Scandariato, R., & Schneider, G. (2016). A privacy-aware conceptual model for handling personal data. In T. Margaria & B. Steffen (Orgs.), *Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques* (Vol. 9952, p. 942–957). Springer International Publishing. https://doi.org/10.1007/978-3-319-47166-2_65.

Ayala-Rivera, V., & Pasquale, L. (2018). The grace period has ended: An approach to operationalize gdpr requirements. *2018 IEEE 26th International Requirements Engineering Conference (RE)*, 136–146. https://doi.org/10.1109/RE.2018.00023.

Bardin, L. (2011). L'Analyse de contenu. Editora: Presses Universitaires de France, 1977. Ánalise de conteúdo. SP: Edições.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for it management: A procedure model and its application. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5.

Brasil (1990). Lei nº 8.078, de 11 de setembro de 1990. Presidência da República, Brasil.

Brasil (2014). Lei nº 12.965, de 23 de abril de 2014. Presidência da República, Brasil.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. Presidência da República, Brasil.

De Bruin, T., Rosemann, M., Freeze, R., & Kulkarni, U. (2005). Understanding the main phases of developing a maturity

assessment model. In *ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems* .

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From iso/iec27001:2013 and iso/iec27002:2013 to gdpr compliance controls. *Information & Computer Security*, *28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004.

Erickson, A. (2019). Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd. *Brooklyn Journal of International Law*, *44*(2), 859.

Gheorghe, G., Massacci, F., Neuhaus, S., & Pretschner, A. (2009). GoCoMM: A governance and compliance maturity model. *Proceedings of the First ACM Workshop on Information Security Governance - WISG '09*, 33. https://doi.org/10.1145/1655168.1655175.

Ingley, C., & Wells, P. (2019). Gdpr: Governance implications for regimes outside the eu. *Journal of Leadership, Accountability and Ethics*, *16*(1). https://doi.org/10.33423/jlae.v16i1.1361

Isaca - Informatio System Audit And Control Association (2013). *COBIT 5 for risk: Control Objectives for Information and Related Technologies*. Isaca.

Isaca - Informatio System Audit And Control Association (2019) *COBIT 2019 Framework: Introduction & Methodology*. Isaca.

Kingsbury, B. (1998). The concept of compliance as a function of competing conceptions of international law. *Michigan Journal of International Law*, *19*(2), 345–372.

Król, K., & Zdonek, D. (2020). Analytics maturity models: An overview. *Information*, *11*(3), 142. https://doi.org/10.3390/info11030142

Lisiak-Felicka, D., Szmit, M., & Department of Computer Science; Faculty of Management; University of Lodz, Lodz, Poland. (2021). GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis. *Journal of Economics and Management*, *43*, 5–25. https://doi.org/10.22367/jem.2021.43.01

Maldonado, V., Vieira, C., Prata, A., Lima, A., Junior, J., Silva, S., Vieira, E., Palhares, F., Capanema, W., Montanaro, D., & Junior, W. (2019). *LGPD – Lei Geral de Proteção de Dados Pessoais: Manual de Implementação*. São Paulo: Editora Thomson Reuters Revista dos Tribunais.

Monteiro, E. L. & Maciel, R. S. P. (2020). Maturity Models Architecture: A large systematic mapping. *iSys: Revista Brasileira de Sistemas de Informação*, *13*(2), 110-140.

New Zealand Government (2014). User Guide for the Privacy Maturity Assessment Framework (version 2.0).

Pinheiro, P (2018). Proteção de Dados Pessoais: Comentários à Lei n.13.709/2018 (LGPD). São Paulo: Editora Saraiva.

Rapôso, C., Lima, M., Oliveira, F., Silva, F., & Barros, E. (2019). LGPD - Lei Geral de Proteção de Dados Pessoais em tecnologia da informação: Revisão Sistemática. *RACE - Revista de Administração do Cesmac*, *4*, 2675-3766.

Silva, A., & Fossá, M. (2015) Análise de Conteúdo: Exemplo de aplicação da técnica para análise de dados qualitativos. *Qualit@s Revista Eletrônica*. *17*(1).

Solli-Sæther, H., & Gottschalk, P. (2010). The modeling process for stage models. *Journal of Organizational Computing and Electronic Commerce*, *20*(3), 279–293. https://doi.org/10.1080/10919392.2010.494535.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

União Europeia (1995). Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Luxemburgo: Parlamento Europeu.

União Europeia (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Luxemburgo: Parlamento Europeu.

Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security.*, *6*, 8–11.

Sobre os autores

Joel Mateus Lopes Ferreira

Graduado em Matemática pela Universidade Estadual de Campinas (2005), MBA em Gestão Econômica e Financeira de Empresas pela Fundação Getúlio Vargas (2008), Especialista em Estatística Aplicada pela Universidade do Distrito Federal (2013) e Mestre em Governança, Tecnologia e Inovação pela Universidade Católica de Brasília (2021). É Gerente de Divisão do Branco do Brasil.

João Souza Neto

Engenheiro Eletricista pela Universidade Estadual do Rio de Janeiro (1982), Mestre em Engenharia Eletrônica pelo Philips International Institute da Holanda (1984), Doutor em Engenharia Elétrica pela Universidade de Brasília (2003). É certificado CGEIT, CRISC, CDPSE, COBIT 2019 Design & Implementation, COBIT 5 Assessor, COBIT 5 Implementation, COBIT Certified Assessor, IT Risk Management, Digital Trust, CSX, PMP, RMP, FAIR, RCDD. É IEEE Senior Member e ISACA Platinum Member.

Edilson Ferneda

Graduado em Tecnologia de Computação pelo Instituto Tecnológico de Aeronáutica (1979), Mestre em Sistemas e Computação pela Universidade Federal da Paraíba (1988) e Doutor em Ciência da Computação pelo Laboratoire d'Informatique, Robotique et de Microélectronique de Montpellier – LIRMM/CNRS, França (1992). Desde 2000 é professor da Universidade Católica de Brasília, onde atua no Mestrado em Governança, Tecnologia e Inovação.