



## COMPONENTES DE GOVERNANÇA DA PRIVACIDADE FRENTE AOS REQUISITOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

**Luciana Carvalho de Brito Prados**

Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília, Brasil.

E-mail: [luciana.c.br@gmail.com](mailto:luciana.c.br@gmail.com)

**Alex Rabello**

Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília, Brasil.

E-mail: [alexrabello@gmail.com](mailto:alexrabello@gmail.com)

**João Souza Neto**

Doutor em Engenharia Elétrica pela Universidade de Brasília, Brasil.

Professor da Universidade de Brasília, Brasil.

E-mail: [szneto@gmail.com](mailto:szneto@gmail.com)

**Tomás Roberto Cotta Orlandi**

Doutor em Ciência da Informação pela Universidade de Brasília, Brasil.

Professor da Universidade Correios, Brasil.

E-mail: [tomasroberto@gmail.com](mailto:tomasroberto@gmail.com)

### Resumo

O presente relato de pesquisa teve como objetivo identificar quais são os componentes de um modelo de governança da privacidade que atenda à Lei Geral de Proteção de Dados Pessoais – LGPD, para apoio à governança corporativa, na tarefa de orientar as organizações na adoção ou adequação de políticas e práticas de governança para promover compliance com a LGPD. O levantamento dos componentes desse modelo de governança está fundamentado no artigo 50 da lei 13.709/2018 que trata da governança da privacidade. A pesquisa constitui em uma pesquisa descritiva, lança mão de comparação com modelos existentes a partir da revisão da literatura, de natureza básica e com abordagem quantitativa e qualitativa, fazendo uso de técnicas de pesquisa bibliográfica por meio da qual elabora-se o modelo conceitual da governança da privacidade, análise de conteúdo para categorizar os componentes, survey para obter subsídios e compor o modelo proposto e discussão de grupo focal para avaliação do modelo. O resultado produzido por este trabalho foi um constructo capaz de servir de instrumento de apoio às organizações para estarem em compliance com a LGPD por sustentar-se nos princípios da governança da privacidade proposta por esta regulamentação e por atender aos requisitos dispostos na lei.

**Palavras-chave:** modelo de governança; privacidade; Lei Geral de Proteção de Dados Pessoais; compliance; proteção de dados pessoais.

### **PRIVACY GOVERNANCE COMPONENTS IN RELATION TO THE REQUIREMENTS OF THE GENERAL PERSONAL DATA PROTECTION LAW**

### Abstract

*This research project aimed to identify the components of a privacy governance model that complies with the General Law on Protection of Personal Data - LGPD, to support corporate governance, in the task of guiding organizations in adopting or adapting policies and practices governance to promote*

*compliance with the LGPD. The survey of the components of this governance model is based on Article 50 of Law 13.709/2018, which deals with privacy governance. The research constitutes descriptive research, of a basic nature and with a quantitative and qualitative approach, making use of bibliographic research techniques, content analysis, survey and focus group discussion. The result produced by this work was a construct capable of serving as a support tool for organizations to be in conformity with the LGPD because it is based on the privacy governance principles proposed by this regulation and for meeting the requirements set out in the law.*

**Keywords:** *governance model; privacy. General Law on Protection of Personal Data; compliance; data protection*

## 1 INTRODUÇÃO

O Brasil coopera com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) desde o início da década de 1990 e atualmente muitos dos ministérios e órgãos do governo estão de alguma forma envolvidos na cooperação com a organização. A partir de 2015 outros acordos foram assinados e permitiram aprofundar e sistematizar a relação bilateral, assim, em 2017, o Brasil solicitou adesão aos “Códigos de Liberalização de Movimento de Capital e de Operações Correntes Intangíveis da OCDE”. Os Códigos de Liberalização são um dos principais documentos do arcabouço normativo da OCDE. A aceitação de um país como um membro significa o reconhecimento internacional dos esforços recentes do governo brasileiro de promover um ambiente aberto, estável e atraente para investimentos estrangeiros (Itamaraty, 2020).

Contudo, para o ingresso de um país na OCDE, precisa-se cumprir diversos requisitos técnicos e legais, e o Brasil, que submeteu sua candidatura para integrar a essa organização, aprovou a lei nº 13.709/2018, a LGPD – Lei Geral de Proteção de Dados, um passo considerado importante neste sentido pois, aos olhos da OCDE, um país que legisla sobre a proteção de dados pessoais e informações garante o mínimo de segurança à partir de princípios como transparência, finalidade, uso necessário e outros (Itamaraty, 2020).

A LGPD e a General Data Protection Regulation (GDPR), regulamento europeu sobre privacidade de dados, são leis que dispõem sobre o tratamento de dados pessoais, versam na mesma direção, de modo que, relações comerciais, financeiras e operacionais na região ou com empresas da região serão facilitadas se as empresas brasileiras estiverem em compliance com a LGPD.

Para além das oportunidades para o ambiente de negócio no Brasil com a regulamentação da LGPD e a própria obrigatoriedade do cumprimento desta. Destaca-se a abrangência da aplicabilidade, para pessoa física ou jurídica que gerencie bases com fins classificados como econômicos. Onde também são definidos os princípios para o tratamento dos dados e, apresentados novos conceitos na busca por identificar e segmentá-los conforme impactos quando do uso ou compartilhamento. Destaque para, sob risco de penalidade em caso de não conformidade. Assim, é importante que, considerada a relação entre o tratamento e os dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, as organizações incorporem a proteção de dados pessoais, se assim entender necessários, no seu planejamento estratégico, mas principalmente, na estrutura de governança corporativa e de TI estabelecida na organização (BRASIL, 2018).

No artigo 50 da lei 13.709/2018, observadas a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos para os titulares dos dados, encontramos a recomendação para as organizações adotarem um modelo de Governança que cumpra com as diretrizes estabelecidas na lei:

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 de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018).

Lunardi, Becker e Macada (2008) explicam que a governança vem da palavra grega *kubernan*, e significa segundo palavras do autor “navegação ou o processo de continuamente orientar e ajustar”.

Sobre governança da privacidade, Swartz, Veiga e Martins (2019), afirmam que esta apoia a gestão na definição de responsabilidades e papéis, na recomendação do monitoramento contínuo de conformidade, além de, estabelecer as políticas de privacidade.

E em tempos de leis e regulamentações sobre proteção de dados pessoais, é importante que as organizações tenham acesso aos componentes que devem compor um modelo de governança da privacidade que sirva de complemento para a governança de TI e, conseqüentemente, instrumento para a governança corporativa, no cumprimento do seu papel de orientar, avaliar e ajustar, e assim, garantir conformidade da organização mediante a leis e regulamentações, além de gerar valor ao negócio.

A lei 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD) publicada em 14 de agosto de 2018 rege o assunto proteção de dados no Brasil, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, em todo território nacional. (BRASIL, 2018) O General Data Protection Regulation (GDPR) – Regulamento Geral de Proteção de Dados, aprovada em 15 de abril de 2016 entrou em vigor em 25 de maio de 2018, trata da proteção de dados na União Europeia (União Europeia, 2016).

E essa é a nova realidade. As empresas precisam cumprir com as diretrizes da Lei Geral de Proteção de dados, porém, é necessário também lidar com a escassez de artefatos que apoiem na orientação para implementar ou adequar as ações, e assim, estar em compliance com a lei. Essa pesquisa se propôs a responder a seguinte pergunta: “Quais são os componentes de um modelo de governança da privacidade que atenda aos requisitos da LGPD?”.

O objetivo desta pesquisa foi identificar os componentes de um modelo de governança da privacidade que atenda aos requisitos da LGPD, especificamente as instruções recomendadas no artigo 50 da Lei Geral de Proteção de Dados.

## **2 REFERENCIAL TEÓRICO**

A conscientização sobre privacidade tem aumentado, por isso, leis e regulamentações têm sido elaboradas por governos e associações, a fim de, atribuir as devidas responsabilidades aos envolvidos em uma operação onde há tratamento de informações de dados pessoais.

A LGPD, aprovada pelo Senado Federal em julho de 2018, foi sancionada em 14 de agosto. Oficialmente chamada de Lei 13.709, esta altera a Lei 12.965 (Marco Civil da Internet). O principal objetivo da Lei Geral de Proteção de Dados é fortalecer a segurança corporativa e do consumidor, por meio do gerenciamento transparente de informações.

E na busca por mapear um modelo de governança que possa apoiar as empresas no sentido de cumprir as recomendações da LGPD, é preciso entender em conceito geral a

privacidade, governança, governança corporativa, governança de TI, governança da privacidade

## 2.1 Privacidade

A LGPD, oficialmente chamada de Lei 13.709, altera a Lei 12.965 (Marco Civil da Internet). O principal objetivo da Lei Geral de Proteção de Dados é fortalecer a segurança corporativa e do consumidor, por meio do gerenciamento transparente de informações.

O conceito de privacidade tem seu ponto de partida no ensaio denominado “*The right to privacy*” de autoria de Samuel D. Warren e Louis D. Brandeis, publicado no ano de 1890 em *Harvard Law Review*. (Maldonado *et al.*, 2019)

Segundo Decew (2018), não é recente a conceito de privacidade, ela existe há séculos, cita como exemplo a concepção de privacidade idealizada por Aristóteles, que formulou a diferença entre a coisa pública e a coisa privada.

Estudos realizados por Friedewald, Finn e Wright (2013) ao trabalho concretizado por Clark (1997), estabeleceram sete categorias de privacidade: privacidade da pessoa, abrange o direito de manter as funções e características corporais. A privacidade de comportamento e ação, inclui questões sensíveis como preferências e hábitos sexuais, política atividades e práticas religiosas, diz respeito a atividades que acontecem no espaço público, bem como no espaço privado. Privacidade de comunicação, visa evitar a interceptação de comunicações. Privacidade de dados e imagens, preocupações em garantir que os dados dos indivíduos não estejam automaticamente disponíveis para outros. Privacidade de pensamentos e sentimentos, as pessoas têm o direito não compartilhar pensamento e sentimentos. Privacidade de localização e espaço, direito de se movimentarem em espaços públicos e privados sem serem identificados. E, por fim, privacidade de associação, direito de se associarem a quaisquer grupos sem serem monitorados.

Diamantopoulou, Tsohou e Karyda (2019), consideram que os dados pessoais é a principal fonte de força das sociedades para se desenvolver, interagir e tomar decisões. Novos e crescentes desafios surgiram para a proteção de dados pessoais com o desenvolvimento tecnológico e a globalização, e, embora estes tragam grandes benefícios para empresas e consumidores, também geram riscos a privacidades (Tikkine-Piri; Rohunen; Markkula, 2018). E esse é o objetivo da LGPD: proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas. Com base nesta definição, alguns requisitos da lei refletem o respeito pelos direitos do proprietário. O consentimento é um requisito muito forte da lei.

Segundo Maldonado *et al.* (2019), a LGPD, assim como outras leis de proteção de dados, tende a reduzir determinadas práticas criminosas de comercialização de dados, contribuem com a redução de vazamento de informações, estabelecem responsabilidades mais claras para as empresas que utilizam dados pessoais e geram oportunidade de maior engajamento de clientes e consumidores.

Nesse sentido, a LGPD potencializa a criação de novos profissionais de TI, como o *Data Protection Officer* (DPO), conhecido como delegado ou supervisor de dados, um especialista em gestão de tratamento dos dados (Cordeiro, 2019).

## 2.2 Governança

Segundo Gonçalves (2005), o termo “governança” parece ser amplamente utilizado sem estar cercado pela atenção analítica que requer e, à luz dessa conclusão, afirma ser necessário especificar o significado, acrescentando que a governança precisa ser levada em consideração em diferentes áreas e de maneiras diferentes.

Para Roth *et al.* (2011), o conceito de governança tem sido utilizado a partir de várias perspectivas de pesquisa organizacional, sendo um termo usado com mais frequência em consonância com a teoria do agente principal e tem como objetivo monitorar e controlar o comportamento dos gerentes por meio da separação entre propriedade e controle.

Lunardi (2008) explica que o termo “governança” é utilizado em vários campos, mas seu significado nem sempre é claro, principalmente porque seu uso é interdisciplinar. O autor refere-se à área de gestão para ilustrar como a governança navega em diferentes áreas.

### 2.2.1 Governança corporativa

Segundo Oliveira (2006), a governança corporativa otimiza o desempenho corporativo de produtos e serviços, protegendo todos os stakeholders, incluindo acionistas, clientes, fornecedores, credos, funcionários e governo, de forma justa, em um conjunto de práticas de gestão.

A governança corporativa se preocupa em garantir que a administração gerencie a empresa de boa fé e com eficácia, a fim de garantir retornos justos e aceitáveis para aqueles que investiram recursos na empresa. Seu surgimento, aliado às boas práticas, deve-se ao desejo das empresas em modernizar suas operações e é visto como diferenciado no mercado financeiro (Silva, 2006).

E quanto a governança corporativa e sua relação com a governança de TI temos (Putri e Surendo 2015e) onde afirmam que, a governança de TI é parte integrantes da governança corporativa.

### 2.2.2 Governança de TI

Para Bloem *et al.* (2006), a tecnologia é amplamente identificada como um dos principais componentes das grandes organizações. A governança de TI é também referida como governança corporativa de TI, ou seja, participante intrínseca da alta gestão. Os autores refletem que separar as iniciativas de tecnologia e TI é muito difícil porque a tecnologia existe em todos os lugares e envolve quase todos na organização de forma que o papel da governança de TI, tem inclusive importância legal, em relação aos controles internos da organização, principalmente após a entrada em vigor da Lei Sarbanes-Oxley em 2002 (Kaarst-Brown; Kelly, 2005), que faz parte do processo de mitigação de risco criado pelo governo norte-americano (REIS, 2019).

Segundo Lunardi (2008), a gestão de TI lida com a tecnologia da informação, enquanto a governança de TI lida com a relevância da informação de TI e a importância nos negócios ligados a TI, mas isso não diminui a importância e a complexidade do tema e, diante do presente e do futuro, a governança de TI, conceito mais amplo, acontece interna e externamente.

A tecnologia da informação se faz presente em todas as rotinas das organizações, participando desde o suporte de TI até na habilitação da estratégia das organizações, e por isso essa prevalência exige que a governança da TI seja um imperativo organizacional (ISO 38501, 2015).

E para implementar a governança de TI, segundo Putri e Surendo (2015), a ISO 38500 deve servir de referência para as organizações atingir as melhores condições e processos nesse sentido.

A ISO 38500 é o padrão internacional que fornece princípios, definições de um modelo para boa governança de TI, para ajudar aqueles no mais alto nível das organizações a compreender e cumprir suas obrigações legais, regulatórias e éticas com relação ao uso de TI por suas organizações (ISO, 2008).

### 2.2.3 Governança da Privacidade

Conforme Swartz, Veiga e Martins (2019) para *Information Systems Audit Control Association* (ISACA), governança de privacidade significa que os diretores de uma organização devem direcionar, avaliar e monitorar os requisitos de privacidade e a visão com base nas necessidades do negócio. Para esses autores a governança da privacidade deve discutir e decidir sobre as diretrizes e estratégias da privacidade em uma organização. Ela está vinculada à política de privacidade de uma organização, que deve reger a proteção e o processamento de informações pessoais. Segundo os autores, Conforme Swartz, Veiga e Martins (2019), a governança de privacidade é, portanto, uma abordagem estratégica da administração para comunicar os valores centrais do processamento e da proteção de informações pessoais às partes interessadas.

Swartz, Veiga e Martins (2019) afirmam que uma política de responsabilidade clara é um requisito fundamental para uma boa governança de privacidade, reforçam a importância de especificar quem é responsável pelas várias funções e aspectos dos programas de gerenciamento de privacidade.

Quando não há uma estrutura de privacidade em vigor é difícil avaliar se todas as diretrizes ou critérios de privacidade de um programa de privacidade foram implementados com sucesso (Wright, 2012).

A função de cada funcionário na gestão da privacidade deve ser estabelecida em uma estrutura de governança da privacidade para garantir que a parte responsável seja responsabilizada, esclarece, Swartz, Veiga e Martins (2019). Pelkola (2012) reitera essa ideia quando afirma que as estruturas de governança de privacidade reforçam a responsabilidade, estabelecem políticas de privacidade, desenvolvem procedimentos e manuais de privacidade automatizados, usam monitoramento contínuo de conformidade, e, por último, fornecem informações para treinamento de privacidade.

Na seção II das Boas Práticas e Governança, da lei 13.709/2018, recomenda que seja considerada em relação ao tratamento e aos dados: a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, e ainda observados: a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados (BRASIL, 2018).

### 2.2.4 Governança corporativa, governança de TI, governança da privacidade

A Tabela 1 resume o relacionamento entre as governanças Corporativa, de TI e da Privacidade, de modo a levar à compreensão como elas se correlacionam e se complementam, a fim de, apoiar na construção do modelo de governança da privacidade que sirva como um artefato de apoio as organizações no sentido de estar em compliance com a LGPD do Brasil.

**Tabela 1:** Conceitos e princípios das governanças

GOVERNANÇA	CONCEITO	PRINCÍPIOS
GOVERNANÇA CORPORATIVA	Governança Corporativa é o sistema pelo qual <b>as organizações</b> são direcionadas, monitoradas e incentivadas, envolvendo relações entre proprietários, conselho de administração e órgãos de controle.	Transparência
		Equidade
		Prestação de contas
		Responsabilidade
GOVERNANÇA	A governança de TI envolve a definição	Responsabilidade

DE TI	de objetivos, estratégias e políticas a serem adotadas pelos membros da organização para garantir que o uso da TI atenda aos <b>objetivos de negócios</b> .	Estratégia
		Aquisição
		Desempenho
		Conformidade
		Comportamento Humano
GOVERNANÇA DA PRIVACIDADE	Abordagem estratégica da administração das organizações para comunicar os valores centrais do processamento e da proteção de informações pessoais às <b>partes interessadas</b> .	Adequação
		Necessidade
		Livre acesso
		Qualidade dos dados
		Transparência
		Segurança
		Prevenção
		Não discriminação
Responsabilização e Prestação de contas		

Fonte: Adaptado pelos autores extraído do IBGC (2009), ISO 38500 (2015) e LGPD (2018).

Podemos observar que os princípios que regem as governanças de TI e da privacidade são complementares e estão contidos no propósito da governança corporativa, assim, as governanças são regidas por princípios que buscam atingir os objetivos das organizações de forma a atender as partes interessadas.

Os recursos de TI são os recursos por meio dos quais são realizadas, na quase totalidade, as operações das organizações, de modo que, os princípios que orientam a governança de TI, também o faz, no sentido de estar em conformidade com a governança corporativa. E, se na quase totalidade do trânsito dos dados realizadas nas mais diferentes relações entre as partes, e a estes incluem os dados pessoais, ocorre por meio de recursos tecnológicos, logo, os princípios que orientam a governança da privacidade devem estar alinhados com a governança de TI e, também o faz, no sentido de estar em conformidade com a governança corporativa. Dessa forma, a relação entre as governanças de TI e privacidade são complementares e respondem à governança corporativa.

### 3 PROCEDIMENTO METODOLÓGICOS

#### 3.1 A Metodologia da pesquisa

Para identificar os componentes de um modelo de governança da privacidade, que sirva de instrumento para a governança de TI e, conseqüentemente, para a governança corporativa como guia de implementação ou adequação da governança da privacidade, foram utilizados como referência os requisitos da proteção de dados pessoais da LGPD para critério de seleção dos modelos para estudo e identificação dos componentes de um modelo de governança da privacidade, capaz de atender os requisitos da lei e servir de orientação para as empresas estarem em compliance com as exigências previstas na lei quanto aos tratamento de dados pessoais. Para tanto, as etapas da pesquisa são:

1. Comparação com modelos existentes, a partir da revisão da Literatura;
2. Elaboração do modelo conceitual da governança da privacidade a partir da pesquisa bibliográfica;
3. Uso de Análise de Conteúdo para categorizar os componentes;

4. Aplicação de survey para obter subsídios e compor o modelo proposto;
5. Avaliação do modelo a partir de discussão por meio de grupo focal com especialistas da área;
6. Apresentação dos Resultados e Conclusões;
7. Documentação de todas as etapas da pesquisa;

Esta pesquisa ainda pode ser classificada como básica, uma vez que, objetiva gerar conhecimento a partir do conhecimento levantado na pesquisa e dessa forma servir para ampliar o conhecimento sobre a governança da privacidade sob a óptica da LGPD face a necessidade da adequação as organizações mediante a implantação de lei.

Pode ser classificada como uma pesquisa qualitativa e quantitativa. Qualitativa, uma vez que será realizada a atividade de discussão em grupo focal e quantitativa, pois será empregada técnica estatística como o survey para o desenvolvimento do modelo e a análise dos dados.

Tem por objetivo descrever as características de um modelo de governança da privacidade como guia para as organizações implementarem ou adequarem à governança da privacidade e assim estarem em compliance com a lei de proteção de dados pessoais, portanto, essa pesquisa pode ser classificada como descritiva.

E, adota como procedimento técnico de investigação a pesquisa bibliográfica, levantamento e pesquisa participantes como instrumento para buscar dados que irão subsidiar as análises para identificar os componentes de um modelo de governança da privacidade capaz de atender os requisitos da LGPD.

### **3.2 Análise de conteúdo**

Bardin (1977) traz informações sobre como a análise de conteúdo se desenvolveu, esclarecendo que, no início do século, o rigor científico era pautado na medida e que os materiais analisados à época eram apenas quanto aos aspectos jornalísticos, tendo avançado para a imprensa e propaganda com H. Lasswell, 1915.

Trazendo para tempos mais recentes, afirma Puglisi (2005) que a análise de conteúdo passou a ser utilizada para produzir inferências acerca de dados verbais ou simbólicos, contudo, estes observados e obtidos a partir do interesse de um determinador pesquisador.

Continuando, Puglisi (2005), ao utilizar a análise de conteúdo, o primeiro desafio do autor é definir Unidades de Análise, para a qual, faz-se necessário dividir em Unidades de Registro e Unidades de Contexto. A Unidade de Registro é definida como a menor parte do conteúdo e a Unidade de Contexto é considerada o “pano de fundo”, que imprime significado às Unidades de Registro.

Tendo como referência os conceitos acima, na busca por conteúdos relevantes para realizar a análise de conteúdo, foram realizadas pesquisas com os termos:

1. Governance;
2. Privacy;
3. GDPR;
4. privacy governance;
5. GDPR governance;
6. Governança;
7. Privacidade; e
8. LGPD.

Os termos de pesquisa estão em inglês e português, sendo GDPR, General Data Protection Regulation, em português RGPD, Regulamento Geral de Proteção de Dados, regulamento europeu sobre privacidade de dados, e LGPD, Lei Geral de Proteção de Dados, regulamento brasileiro, e ambos são leis que dispõem sobre o tratamento de dados pessoais.

Os termos pesquisados foram buscados nas bases por todos os campos que compõem o documento. Na Tabela 2 constam a quantidade de documentos encontrados por termo pesquisado nas duas bases consultadas.

**Tabela 2:** Resultado da quantidade de documentos encontrados resultado das pesquisas por palavra-chave, realizada em 21/08/2020

TERMOS	CAPE – base Scopus	BDTD
Governance	163.617	4.259
Privacy	132.569	743
GDPR	1.731	0
Governança	342	4.259
Privacidade	54	788
LGPD	15	31

Fonte: os autores

A pesquisa mostra que há uma grande quantidade de material relacionado a governança e privacidade, o contrário ocorre com os termos GDPR e LGPD. Diante dessa ocorrência foi realizado um novo filtro para verificar se há uma convergência desses termos, uma vez que, o objetivo é localizar artigos referente a modelo de governança da privacidade relacionados à regulamentação da proteção de dados.

Ao combinar os termos são localizados poucos documentos que tratam sobre governança da privacidade de dados sob à óptica da regulamentação de proteção de dados.

Dos 42 documentos encontrados foram selecionados os 5 mais relevantes, e como relevantes foram considerados aqueles que tratam do tema governança da privacidade, ainda que, não tratem especificamente de regulamentação ou leis de tratamento de dados, como o caso da LGPD e GDPR. São eles:

- i. MILBERG, Sandra J., SMITH, Jeff H., BURKE, Sandra J. *Information Privacy: Corporate Management and National Regulation. Organization Science*, 11(1), pp. 35-57, 2000.
- ii. SEERDEN, Xander, SALMELA, Hnnu T.T., RUTKOWSKI, Anne F. *Privacy Governance and the GDPR: How are Organizations Taking Action to Comply with the Privacy Regulation in Europe? Proceedings of the 14th European Conference on Management, Leadership and Governance*, EMLG 2018, pp. 371-378, 2018.
- iii. MODARESNEZHAD, Minoo, PAIVA, Prashant C. *The Efficacy of is Privacy and Security Governance Structure. 19th Americas Conference on Information Systems*, AMCIS 2013 – Hyperconnected World: Anything, Anywhere, Anytime 5, pp. 3339 – 3349, 2013.
- iv. BAMBERGER, Kenneth, MULLIGAN, Deirde K. *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*. *George Washington Law Review*, 81(5), pp. 1529-1664, 2013.
- v. SWARTZ, Paulus, DA VEIGA, Adele, MARTINS, Nico. *A conceptual privacy governance framework. Conference on Information Communications Technology and Society ICTAS*, 2019.

Destaque para o artigo v onde os autores desenvolveram um framework de governança da privacidade face a necessidade das organizações de incorporar a proteção de informações pessoais em seu planejamento estratégico e administrá-la em toda a organização. No estudo são comparadas as estruturas de governança de privacidade existentes, são elas: OIPC (*Officer Informantion Privacy Commissioner*), IPC (*Information and Privacy Commission*), CCIM (*Community Care Information Management*), OAIC (*Office of the Australian Information Commissioner*), e proposto uma estrutura consolidada que incorpora um conjunto abrangente de componentes de privacidade que podem ajudar o gerenciamento a governar a privacidade em uma organização. Concluem dizendo que uma estrutura de governança da privacidade pode ajudar a reforçar a proteção da privacidade, melhorar a reputação da organização,

fomentar uma cultura de privacidade e garantir a conformidade com os requisitos regulamentares de privacidade.

### 3.3 Pesquisa survey

Para Freitas, Oliveira, Saccol e Mascarola (1999), o pesquisador não tem obrigação de eleger apenas um método de pesquisa a ser aplicado, devendo estar mais preocupado em fazer a escolha em coerência e associado ao objetivo da sua pesquisa e, se for necessário, combiná-los, ou seja, aliando o quantitativo ao qualitativo, o que chamam de multimodo. Para esses autores, ambos métodos possuem vantagens e desvantagens.

A obtenção de dados ou informações sobre características, ações ou opiniões de um determinado grupo de pessoas, indicado como um representante de uma população-alvo, por meio de uma pesquisa, normalmente um questionário, é conhecida como pesquisa survey segundo Freitas *et al.* (1999).

Continuando, para Freitas *et al.* (1999), a survey é apropriada como método de pesquisa, atuando sobre o que está acontecendo ou como e por que isso está acontecendo; quando não se tem interesse ou não se é possível controlar as variáveis dependentes e independentes; quando é possível estudar no ambiente natural do fenômeno de interesse e o objeto de interesse ocorre no presente ou em um passado próximo.

Por entender relevante o método survey para essa pesquisa, uma vez que, conforme pesquisa por conteúdo podemos considerar pequeno o volume de material criado sobre o tema e, portanto, fazendo necessário outros recursos para embasar a pesquisa foi realizado um survey com a pergunta: qual o grau de aderência dos componentes apresentados com os requisitos de governança da privacidade dispostos na LGPD?

No período de 15/11 a 30/11 de 2020, por meio de redes sociais, grupos de WhatsApp e palestras realizadas em ambientes acadêmicos, foi publicado um formulário eletrônico com trinta perguntas no total sendo as quatro primeiras de cunho demográfico, as demais pertinentes aos componentes identificados por meio da análise de conteúdo.

No total foram obtidas 23 respostas com as quais podemos avaliar o perfil demográfico dos participantes: quanto ao setor da organização nas quais os participantes trabalham temos, 56,52% trabalham na iniciativa pública e 43,48% na iniciativa privada. Sendo que 8,7% são da área jurídica, 43,48% da área de TI, 21,74% da área de administração e 26,09% de outras áreas não especificadas. E destes 17,39% possuem certificação DPO, os demais, 60,87% possuem curso sobre LGPD.

Os resultados obtidos foram consolidados por grau de relevância entre os componentes e os requisitos de governança da privacidade recomendado na LGPD.

### 3.4 O grupo focal

Os autores Backes, Colomé, Erdmann e Lunardi (2011) firmam que o campo da pesquisa qualitativa se constitui de diversas possibilidades metodológicas, as quais permitem um processo dinâmico de aderência a novas formas de coleta e de análise de dados. Eles explicam que dentre essas possibilidades, o grupo focal representa uma técnica de coleta de dados que, a partir da interação grupal, promove uma ampla problematização sobre um tema específico.

Backes *et al.* (2011) esclarecem que o grupo focal se originou no cenário da pesquisa social, aprendido como técnica de coleta de dados e que está sendo utilizada pela antropologia, ciências sociais, mercadologia e educação em saúde.

Essa técnica consiste em uma entrevista em grupo, na qual a interação configura-se como parte integrante do método. No processo, os grupos focais possibilitam aos participantes

explorarem seus pontos de vista, a partir de reflexões sobre um determinado fenômeno social, explicam Backes *et al.* (2011).

Para esses autores, o grupo focal pode atingir um nível reflexivo que outras técnicas não conseguem, revelando dimensões de entendimento que, frequentemente, permanecem inexploradas pelas técnicas convencionais de coleta de dados.

Explicam Borges e Santos (2005) que na realização de um levantamento (survey) que utilize tanto dados quantitativos como qualitativos, a técnica do grupo focal pode ser utilizada na obtenção de informações acerca de crenças e percepções dos sujeitos.

Considerando os conceitos acima para este estudo o resultado do survey foi apresentado a um grupo de especialistas convidados para debater o assunto em grupo focal, um encontro onde pudessem avaliar o modelo desenvolvido e responder algumas perguntas. Com o propósito de direcionar as discussões, a pesquisadora elaborou três perguntas, são elas: se os componentes eleitos pela pesquisa são componentes importantes para uma governança da privacidade que atenda aos requisitos da LGPD; se os componentes que não foram selecionados na pesquisa deveriam compor um modelo de governança da privacidade; e se o grupo conhece algum componente não avaliado na pesquisa que deveria compor a lista de componentes para a governança da privacidade.

Consideradas as recomendações dos especialistas foi montada a lista final dos componentes de uma governança da privacidade pautada nas recomendações da LGPD

#### 4. O Modelo de Governança da Privacidade Proposto

Objetivando identificar os componentes de um modelo de governança da privacidade, capaz de atender os requisitos da LGPD, recorreremos a revisão da literatura. Conforme Swartz, Veiga e Martins, (2019), neste artigo os autores desenvolveram um framework de governança da privacidade face a necessidade das organizações de incorporar a proteção de informações pessoais em seu planejamento estratégico e administrá-la em toda a organização. No estudo são comparadas as estruturas de governança de privacidade existentes e proposto uma estrutura consolidada que incorpora um conjunto abrangente de componentes de privacidade que podem ajudar o gerenciamento a governar a privacidade em uma organização. Concluem dizendo que uma estrutura de governança da privacidade pode ajudar a reforçar a proteção da privacidade, melhorar a reputação da organização, fomentar uma cultura de privacidade e garantir a conformidade com os requisitos regulamentares de privacidade.

Foram identificadas as estruturas abaixo:

- OIPC (*Officer Informantion Privacy Commissioner*);
- IPC (*Information and Privacy Commission*);
- CCIM (*Community Care Information Management*); e
- OAIC (*Office of the Australian Information Commissioner*), conforme Tabela 3.

**Tabela 3:** Presença dos componentes da governança da privacidade nas estruturas

COMPONENTES GOVERNANÇA PRIVACIDADE	OIPC	IPC	CCIM	OAIC
Oficial da privacidade	X	X		
Escritório da privacidade	X			
Comunicação interna	X	X	X	
Inventário de dados	X			
Políticas de privacidade	X	X	X	X
Avaliação de risco	X			

Treinamento	X		X	
Protocolos de incidentes	X	X	X	
Provedor de serviço	X	X		
Comunicação externa	X			
Operações			X	
Gerenciamento de consentimento			X	
Suporte privacidade do cliente			X	
Revisão contínua			X	X
Cultura da privacidade				X
Práticas e procedimentos				X
Garantia contínua				X

Fonte: Adaptado do artigo A conceptual Privacy Governance Framework, Swartz, Veiga e Martins (2019)

No passo seguinte, foram relacionados os componentes com maior similaridade com os requisitos de governança da privacidade descritos na LGPD. A Tabela 4 apresenta o resultado, onde requisitos da governança da privacidade foram relacionados.

**Tabela 4:** Requisitos da governança da privacidade sob a ótica da LGPD e os componentes das estruturas de governanças da privacidade da Tabela 3

REQUISITOS GOVERNANÇA DA PRIVACIDADE LGPD - ARTIGO 50	COMPONENTES DA GOVERNANÇA ENUMERADOS NA TABELA 3 UNIDADES DE REGISTRO
1 - Demonstra o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.	1 - Oficial da privacidade; 2 - Escritório da privacidade; 5 - Políticas de privacidade
2 - Aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta.	4 - Inventário de dados; - Provedor de serviço 9
3 - Adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.	4 - Inventário de dados; 6 - Avaliação de risco; 8 - Protocolos de incidentes
4 - Políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.	6 - Avaliação de risco; 8 - Protocolos de incidentes; 12 - Revisão contínua
5 - Estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular.	10 – Gerenciamento de consentimento; 11 - Suporte privacidade do cliente; 13 - Cultura da privacidade
6 - Integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos.	1 - Oficial da privacidade; 2 - Escritório da privacidade; 3 - Comunicação; 9 - Provedor de serviço; 13 - Cultura da privacidade
7 - Planos de resposta a incidentes e remediação.	5 - Políticas de privacidade; 6 - Avaliação de risco; 7 – Treinamento; 8 - Protocolos de incidentes;
8 - Atualizado constantemente com base em informações obtidas a partir de monitoramento	7 – Treinamento; 12 - Revisão contínua; 13 -

---

contínuo e avaliações periódicas.

Cultura da privacidade

---

Fonte: Os autores

Dos componentes, entende-se:

- Oficial da privacidade: pessoa que faz o planejamento do negócio quanto a avaliação e revisão do programa da privacidade. É encarregado por cuidar das questões relacionadas a proteção dos dados. Auxilia a empresa a adaptar seus processos para estruturar um programa de *compliance* com foco maior em segurança da informação.
- Escritório da privacidade: composto por diferentes membros da equipe de todas as áreas da organização. As principais responsabilidades do escritório de privacidade são: o desenvolvimento de políticas e procedimentos de privacidade, facilitar a conscientização e treinamento sobre privacidade, gerenciamento de violações de privacidade e incidentes, concepção e implementação de controles de privacidade e comunicação.
- Comunicação: a área responsável pela privacidade dos dados precisa manter uma comunicação aberta e transparente. As organizações têm a responsabilidade de informar aos proprietários dos dados sobre seus direitos de privacidade por meio de avisos de privacidade.
- Inventário de dados: a organização deve manter um registro dos dados pessoais que processam. Devem documentar e compreender como os dados pessoais são processados e onde e como são armazenados.
- Políticas da privacidade: planejamentos e ações desenvolvidas pela administração para direcionar a política da privacidade.
- Avaliação de risco: avaliação de impacto do risco da privacidade para apoiar as organizações no planejamento de ações para identificar e mitigar riscos da segurança da informação e dados.
- Treinamento: treinamento sobre privacidade dos dados para formar conhecimentos sobre privacidade da informação, riscos e responsabilidades aos funcionários e informar sobre quaisquer alterações nas políticas e procedimentos de privacidade
- Protocolo de incidentes: Violações e incidentes com a segurança dos dados e informações podem ocorrer devido a acessos não autorizados aos dados, negligência de funcionários e falta de critérios no tratamento dos dados.
- Provedor de serviço: O provedor de serviços deve cumprir com o acordo de nível de serviço ou contrato, que inclui adesão às políticas de privacidade da organização.
- Gerenciamento de consentimento: meios de gerenciar o consentimento do titular dos dados sobre a coleta e uso dos dados em conformidade com seus respectivos fins.
- Suporte privacidade do cliente: operação de atendimento ao titular do dado para esclarecimentos e suporte de qualquer natureza quanto aos dados coletados desde a coleta até o descarte.
- Revisão contínua: garantir que o programa de gerenciamento de privacidade seja monitorado e aplicado com objetivo de garantir que a política de privacidade seja cumprida por meio da efetiva execução dos processos para segurança da privacidade dos dados.
- Cultura da privacidade: um “ecossistema da privacidade”, onde todos os setores da organização que atuam com dados estão plenamente conscientes das

orientações para atender a legislação ou recomendações sobre a ciclo de vida dos dados enquanto em posse da empresa.

#### 4.1 A estrutura do modelo de governança da privacidade

##### 4.1.1 Análise de conteúdo da governança da privacidade disposta na LGPD

A primeira etapa da elaboração do modelo de governança da privacidade consistiu na análise do artigo 50 vinculado à Lei 13.709/18 – lei geral de proteção de dados pessoais, para isso, foi aplicada a metodologia análise de conteúdo.

O material utilizado foi a Lei 13.709, que rege a LGPD (etapa “i”) e, considerando a estrutura da Lei, não foi necessário codificar os textos (“ii”).

Dessa forma, inicialmente os treze componentes da Tabela 3 foram considerados unidades de registro. A Tabela 5, que organiza os componentes por requisitos de governança da privacidade da LGPD, define oito categorias intermediárias. A partir da análise do artigo 50 foram estabelecidas as componentes iniciais para cada requisito previsto na lei.

**Tabela 5:** Componentes iniciais da governança da privacidade

OS 8 REQUISITOS GOVERNANÇA DA PRIVACIDADE LGPD - ARTIGO 50 (conforme Tabela 4)	CATEGORIAS INTERMEDIÁRIAS
1	Recomendações sobre adoção de práticas para o cumprimento da lei e normas quanto a proteção de dados pessoais
2	Recomendação da abrangência da aplicação da gestão da proteção dos dados pessoais
3	Recomendação de proteção de dados em conformidade com a categoria de dados
4	Recomendação sobre a gestão do risco da privacidade
5	Recomendação à despeito da relação segura e transparente com o titular do dado
6	Recomendação quanto estrutura da governança da privacidade
7	Recomendação quanto a mecanismos de segurança e repostas a incidentes
8	Recomendação sobre processo contínuo de gestão da privacidade

Fonte: Os autores

Na etapa seguinte da análise de conteúdo, as categorias intermediárias foram vinculadas aos princípios da governança da privacidade, como mostrado na Tabela 6.

**Tabela 6:** Categorias intermediárias relacionadas aos princípios da governança da privacidade

CATEGORIAS INTERMEDIÁRIAS	PRINCÍPIOS DA GOVERNANÇA DA PRIVACIDADE
1 - Recomendações sobre adoção de práticas para o cumprimento da lei e normas quanto a proteção de dados pessoais	Responsabilização e Prestação de contas

2 - Recomendação da abrangência da aplicação da gestão da proteção dos dados pessoais	Transparência
3 - Recomendação de proteção de dados em conformidade com a categoria de dados	Necessidade; Qualidade dos dados
4 - Recomendação sobre a gestão do risco da privacidade	Segurança
5 - Recomendação à despeito da relação segura e transparente com o titular do dado	Livre acesso; Não discriminação
6 - Recomendação quanto estrutura da governança da privacidade	Responsabilização e Prestação de contas; Segurança
7 - Recomendação quanto a mecanismos de segurança e repostas a incidentes	Segurança; Prevenção
8 - Recomendação sobre processo contínuo de gestão da privacidade	Prevenção

Fonte: Os autores

A associação das categorias intermediárias aos princípios fez-se necessária para que fosse avaliada a capacidade de os componentes levantados na literatura de cumprirem com os requisitos dispostos na LGPD e, ao mesmo tempo, com os princípios de uma governança da privacidade. No passo seguinte, as unidades de registro foram relacionadas às categorias intermediárias e aos princípios, demonstrados na Tabela 7.

**Tabela 7:** Categorias, Princípios e Unidades de Registro

<b>CATEGORIAS INTERMEDIÁRIAS (conforme Tabela 6)</b>	<b>PRINCÍPIOS DA GOVERNANÇA DA PRIVACIDADE</b>	<b>UNIDADES DE REGISTRO</b>
1	Responsabilização e Prestação de contas	1 - Oficial da privacidade; 2 - Escritório da privacidade; 5 - Políticas de privacidade
2	Transparência	4 - Inventário de dados; 9 - Provedor de serviço
3	Necessidade; Qualidade dos dados	4 - Inventário de dados; 6 - Avaliação de risco; 8 - Protocolos de incidentes
4	Segurança	6 - Avaliação de risco; 8 - Protocolos de incidentes; 12 - Revisão contínua

5	Livre acesso; Não discriminação	10 – Gerenciamento de consentimento; 11 - Suporte privacidade do cliente; 13 - Cultura da privacidade
6	Responsabilização e Prestação de contas; Segurança	1 - Oficial da privacidade; 2 - Escritório da privacidade; 3 – Comunicação; 9 - Provedor de serviço; 13 - Cultura da privacidade
7	Segurança; Prevenção	5 - Políticas de privacidade; 6 - Avaliação de risco; 7 – Treinamento; 8 - Protocolos de incidentes;
8	Prevenção	7 – Treinamento; 12 - Revisão contínua; 13 - Cultura da privacidade

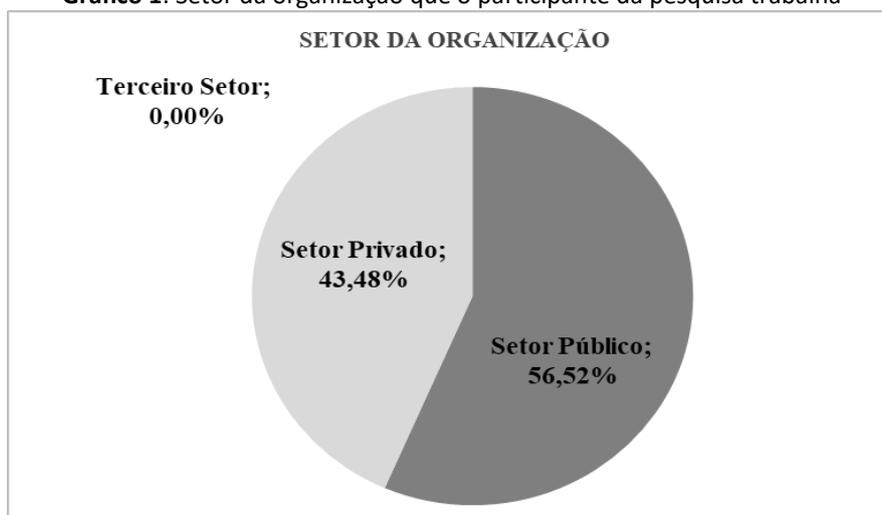
Fonte: Os autores

#### 4.1.2 Levantamento da relação entre os requisitos e os componentes

Com o objetivo de avaliar o grau de aderência entre os componentes e os requisitos, foi realizado um survey com a pergunta: “Qual o grau de aderência dos componentes apresentados com os requisitos de governança da privacidade dispostos na LGPD?”

Por meio de redes sociais e palestras realizadas em ambientes acadêmicos, foi publicado um formulário eletrônico com trinta perguntas, sendo as quatro primeiras de cunho demográfico. No total foram obtidas 23 respostas com as quais podemos avaliar o perfil demográfico dos participantes: 56,52% trabalham na iniciativa pública e 43,48% na iniciativa privada. O Gráfico 1 apresenta estes resultados.

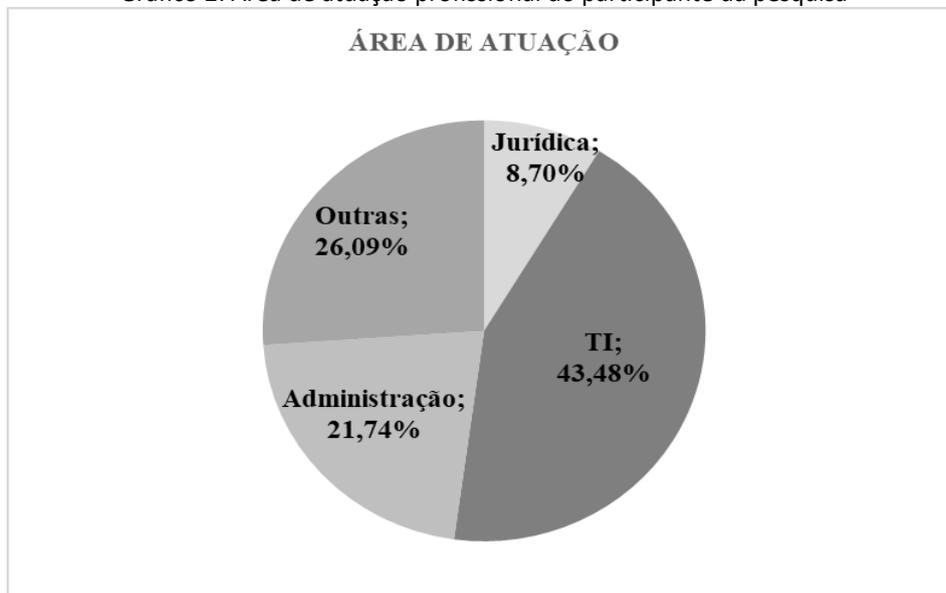
**Gráfico 1:** Setor da organização que o participante da pesquisa trabalha



Fonte: Os autores

Em relação à área de atuação, 8,7% são da área jurídica, 43,48% da área de TI, 21,74% da área de administração e 26,09% de outras áreas, não especificadas, conforme demonstrado no Gráfico 2.

Gráfico 2: Área de atuação profissional do participante da pesquisa



Fonte: Os autores

A Tabela 8 consolida os resultados obtidos do grau de relevância entre os componentes e os requisitos de governança da privacidade recomendado na LGPD.

**Tabela 8:** Tabela dos resultados da pesquisa sobre o grau de aderência entre os componentes de uma Governança da Privacidade com os requisitos da governança da privacidade segundo a LGPD

REQUISITOS DA LGPD	ID	COMPONENTES	GRAU DE ADERÊNCIA À LGPD			
			MUITO FORTE	FORTE	FRACO	MUITO FRACO
1	1	1 – Oficial da privacidade	6	13	3	1
	2	2 – Escritório da privacidade	7	11	5	0
	3	5 – Políticas da privacidade	12	7	4	0
2	4	4 - Inventário de dados	10	10	3	0
	5	9 - Provedor de serviço	4	10	9	0
3	6	4 - Inventário de dados	7	11	5	0
	7	6 - Avaliação de risco	3	8	9	3
	8	8 - Protocolos de incidentes	4	14	3	1
4	9	6 - Avaliação de	9	9	5	

		risco				
	10	8 - Protocolos de incidentes	6	13	4	0
	11	12 - Revisão contínua	6	10	7	0
5	12	10 – Gerenciamento de consentimento	7	14	2	0
	13	11 - Suporte privacidade do cliente	6	13	4	0
	14	13 - Cultura da privacidade	11	6	5	1
6	15	1 - Oficial da privacidade	7	11	5	0
	16	2 - Escritório da privacidade	3	15	4	0
	17	3 – Comunicação	4	11	6	1
	18	9 - Provedor de serviço	1	11	9	1
	19	13 - Cultura da privacidade	5	7	8	2
7	20	5 - Políticas de privacidade	7	12	4	0
	21	6 - Avaliação de risco	9	10	3	1
	22	7 - Treinamento	5	11	6	1
	23	8 - Protocolos de incidentes	7	11	5	0
8	24	7 - Treinamento	4	9	10	0
	25	12 – Revisão contínua	7	8	7	1
	26	13 - Cultura da privacidade	4	12	6	1

Fonte: Os autores

#### 4.1.3 Análise dos resultados

Para os valores foram encontrados o valor em percentual e, dos graus fraco e muito fraco foram desprezados, enquanto, os de forte e muito forte somados. Na Tabela 9 tem-se a consolidação do resultado do grau de relação entre o componente e o requisito com o qual está relacionado.

**Tabela 9:** Consolidação do resultado da pesquisa

1	2	3	4	5	6
1 – Oficial da privacidade	2 – Escritório da privacidade	5 – Políticas da privacidade	4 - Inventário de dados	9 - Provedor de serviço	4 - Inventário de dados
82,61%	78,26%	82,60%	86,96%	60,87%	78,26%
7	8	9	10	11	12

6 - Avaliação de risco	8 - Protocolos de incidentes	6 - Avaliação de risco	8 - Protocolos de incidentes	12 - Revisão contínua	10 – Gerenciamento de consentimento
47,82%	82,61%	78,26%	82,61%	69,57%	91,30%
13	14	15	16	17	18
11 - Suporte privacidade do cliente	13 - Cultura da privacidade	1 - Oficial da privacidade	2 - Escritório da privacidade	3 – Comunicação	9 - Provedor de serviço
82,61%	73,92%	88,26%	81,82%	68,18%	54,55%
19	20	21	22	23	24
13 - Cultura da privacidade	5 - Políticas de privacidade	6 - Avaliação de risco	7 - Treinamento	8 - Protocolos de incidentes	7 - Treinamento
54,55%	82,60%	82,61%	69,57%	78,26%	56,52%
25	26	-	-	-	-
12 – Revisão contínua	13 - Cultura da privacidade	-	-	-	-
65,21%	69,56%	-	-	-	-

Fonte: Os autores

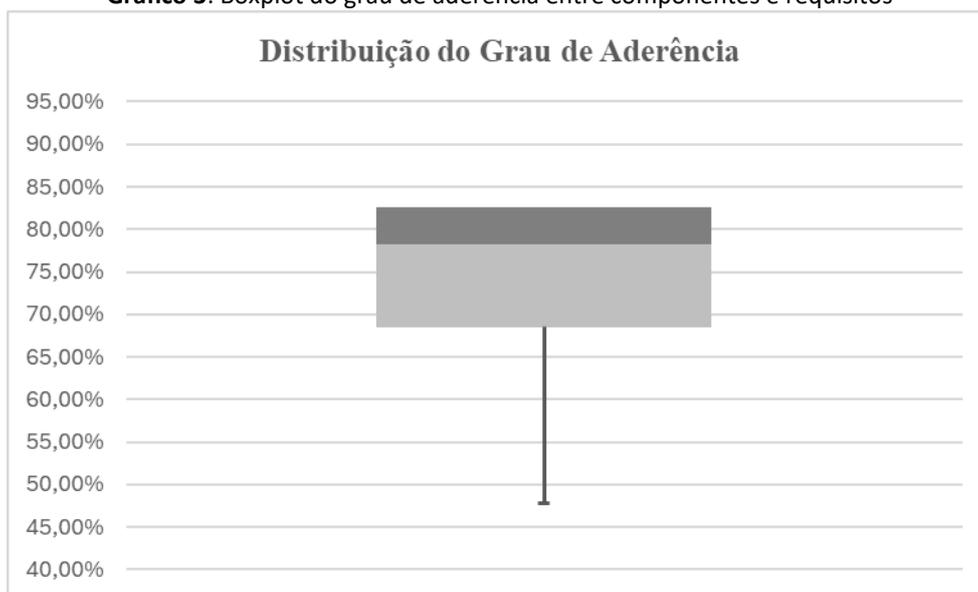
Na Tabela 9, encontramos percentuais distintos para um mesmo componente, isso deve-se a diferença do grau de relação que os respondentes entenderam haver de um componente quando associado a diferentes requisitos.

Para apresentar melhor como esse conjunto de dados está distribuído foi construída uma representação gráfica, o Boxplot, para representar a variação dos dados observados. De forma breve, é um diagrama que identifica onde estão localizados 50% dos valores mais prováveis, a mediana e os valores extremos. O Boxplot tem uma reta que estende-se verticalmente ou horizontalmente a partir da caixa, indicando a variabilidade fora do quartil superior e do quartil inferior. (Farias, 2008)

Neste estudo, para esse conjunto de dados, foram calculados os valores correspondentes ao valor mínimo, 1º quartil, mediana, 3º quartil e valor máximo: Mínimo = 47,82%, 1º Quartil = 68,53%, Mediana = 78,26, 3º Quartil = 82,61%, Máximo = 91,30%.

No Boxplot mostrado no Gráfico 3, no 3º quartil concentra-se a maior parte das observações, com pequenas variações (quartil estreito), enquanto, no 1º quartil encontram-se variações maiores e pequena densidade de observações. Essa distribuição indica que as respostas, em sua maioria, tiveram um caráter positivo, de confirmação da aderência.

**Gráfico 3:** Boxplot do grau de aderência entre componentes e requisitos

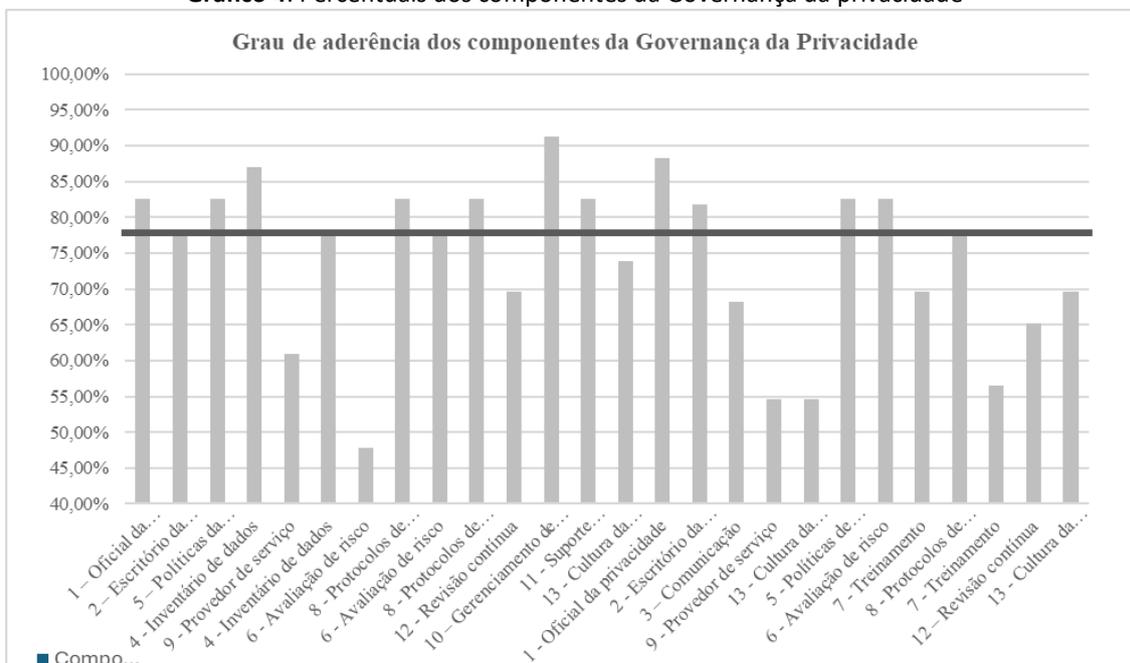


Fonte: Os autores

Aplicando-se o critério do terceiro quartil (observações maiores que a mediana - Gráfico 4) acima da barra vermelha da mediana estão os itens: 1, 2, 3, 4, 6, 8, 9, 10, 12, 13, 15, 16, 20, 21 e 23.

Para compor o modelo de governança da privacidade proposto, considera-se que, se em ao menos uma associação, ou seja, o componente relacionado a um requisito, tiver atingido a mediana, este, nesta etapa, está contido nos componentes da governança da privacidade, demonstrado no Gráfico 4.

**Gráfico 4:** Percentuais dos componentes da Governança da privacidade



Fonte: Os autores

Tomando a mediana como referência, um modelo de governança da privacidade que atenda aos requisitos da governança da privacidade dispostos na LGPD deve conter os componentes:

- Oficial da privacidade;
- Escritório da privacidade;
- Políticas da privacidade;
- Inventário de dados;
- Protocolos de incidentes;
- Avaliação de risco;
- Gerenciamento de consentimento e
- Suporte da privacidade do cliente

Nesta etapa, os componentes, Provedor de serviço, Revisão Contínua, Treinamento, Cultura da Privacidade e Comunicação foram eliminados porque não atingiram o percentual da mediana ou superior.

O resultado da pesquisa foi apresentado a um grupo de especialistas. Para os estes, os componentes oficiais da privacidade, escritório da privacidade e políticas da privacidade são importantes e afirmaram que, com termos diferentes, estes têm sido implementados em quase a totalidade das organizações que estão se adequando às exigências de normativos referentes à proteção de dados pessoais e, portanto, devem compor a lista de componentes.

Quanto aos componentes não selecionados, todos os especialistas foram unânimes em afirmar que provedor de serviço não deve estar na lista de componentes.

Outro componente não selecionado que foi compreendido pelos especialistas como importante para compor a lista dos componentes é a Cultura da Privacidade. Para estes, comunicação e treinamento estão contidos na cultura da privacidade e não devem ser tratados como componentes específicos.

#### 4.1.4 A lista dos componentes da governança da privacidade

Consideradas as recomendações dos especialistas, foi montada a lista final dos componentes de uma governança da privacidade pautada nas recomendações da LGPD:

- Oficial da privacidade;
- Escritório da privacidade;
- Políticas da privacidade;
- Inventário de dados pessoais;
- Gerenciamento de incidentes;
- Avaliação de risco de dados pessoais;
- Gerenciamento dos direitos dos titulares;
- Plataforma da privacidade do titular dos dados;
- Cultura da privacidade.

Com a lista final dos componentes, foi possível elaborar as categorias finais do modelo, conforme mostrado na Tabela 10.

**Tabela 10:** Categorias, Princípios e Unidades de Registro

CATEGORIAS FINAIS	PRINCÍPIOS DA GOVERNANÇA DA PRIVACIDADE	UNIDADES DE REGISTRO
Recomendações sobre adoção de práticas para o cumprimento da lei e normas quanto a proteção de dados pessoais	Responsabilização e Prestação de contas	1 - Oficial da privacidade; 2 - Escritório da privacidade; 5 - Políticas de privacidade

Recomendação da abrangência da aplicação da gestão da proteção dos dados pessoais	Transparência	4 - Inventário de dados;
Recomendação de proteção de dados em conformidade com a categoria de dados	Necessidade; Qualidade dos dados	4 - Inventário de dados; 6 - Avaliação de risco de dados pessoais; 8 - Gerenciamento de incidentes
Recomendação sobre a gestão do risco da privacidade	Segurança	6 - Avaliação de risco de dados pessoais; 8 - Gerenciamento de incidentes;
Recomendação à despeito da relação segura e transparente com o titular do dado	Livre acesso; Não discriminação	10 – Gerenciamento dos direitos dos titulares; 11 – Plataforma da privacidade do titular dos dados; 13 - Cultura da privacidade
Recomendação quanto estrutura da governança da privacidade	Responsabilização e Prestação de contas; Segurança	1 - Oficial da privacidade; 2 - Escritório da privacidade; 13 - Cultura da privacidade
Recomendação quanto a mecanismos de segurança e repostas a incidentes	Segurança; Prevenção	5 - Políticas de privacidade; 6 - Avaliação de risco de dados pessoais; 8 - Gerenciamento de incidentes;
Recomendação sobre processo contínuo de gestão da privacidade	Prevenção	13 - Cultura da privacidade

Fonte: Os autores

As categorias finais proposta para um modelo de governança da privacidade apresentada nesse constructo, teve origem nos achados acadêmicos que serviram de ponto de partida para o levantamento dos componentes da governança da privacidade e suas respectivas fontes. Portanto, esse produto final é um objeto com origem em modelos amplamente aplicados. Além da relevante origem dos componentes levantados por meio dos achados acadêmicos, estes passaram por outras diferentes etapas durante a metodologia que foram a análise de conteúdo, o survey e o grupo focal, que permitiram estabelecer o quão aderentes estes componentes são para a realidade da LGPD.

Cabe destacar também que, com a adoção de regulamentações sobre o tratamento de dados pessoais, a governança da privacidade adquire um caráter de importância no contexto estratégico das organizações, ainda que a depender da sensibilidade dos dados tratados por estas, da sua volumetria e da finalidade.

Portanto, implementar um modelo de governança da privacidade, conforme descrito no artigo 50 da LGPD, é uma recomendação para que as organizações consigam estar em

compliance com a lei, contudo, não se pode desconsiderar os custos financeiros do cumprimento destas regulamentações para as organizações.

É importante observar que, conforme o IBGC (2009), a governança corporativa no Brasil tem amadurecido a passos largos por motivos diversos, e isso é significativo para o cenário atual, uma vez que, sendo a governança da privacidade um instrumento da governança corporativa, pode-se inferir que o conhecimento destas organizações quanto à implementação, adequação e manutenção do modelo de governança pode ser considerado como um fator facilitador e mesmo de mitigação dos custos de implementação da governança da privacidade.

O mesmo pode-se afirmar sobre a governança de TI, que é amplamente adotada nas organizações e que também é um instrumento crítico para a governança corporativa, pois ela tem uma relação direta com a governança da privacidade. Como sabemos, hoje, estes dados transitam em sua quase totalidade por meio de recursos de TI, sendo assim, as governanças de TI e da privacidade estão estreitamente relacionadas, de modo que, a experiência e conhecimento com o modelo de governança de TI, assim como a expertise na governança corporativa, poderá servir para mitigar e absorver custos e possíveis dificuldades na implementação da governança da privacidade.

Diante do exposto, este instrumento contribui como ponto de partida para um modelo de governança da privacidade. Cabe destacar a possibilidade contida na proposta dos componentes de ser adaptado ao escopo e cenário que cada organização vivência.

## **5 CONCLUSÃO**

Com a aprovação da Lei Geral de Proteção de Dados no Brasil, faz-se necessário que, a depender da estrutura, escala e volume das operações de uma organização, seja adotado um modelo de governança da privacidade que cumpra com as diretrizes estabelecidas na Lei.

Propôs-se, então, como objetivo geral deste estudo, identificar os componentes da governança da privacidade que cumpram os requisitos dispostos na LGPD e, assim, sirvam de instrumento de apoio às organizações para estarem em compliance com as normas dispostas na Lei.

Para atingir o objetivo proposto, iniciou-se o levantamento dos componentes identificados na literatura, que, na sequência, foram submetidos às etapas de análise de conteúdo, onde foram avaliadas as primeiras inferências entre os componentes e os requisitos. Em seguida, para avaliar essas associações, foi realizada uma pesquisa survey que teve os resultados submetidos a uma análise estatística descritiva (Boxplot) e, por último, foi realizada uma discussão em grupo focal para avaliação da lista de componentes.

Dos resultados levantados em cada etapa da metodologia aplicada, para responder à questão de pesquisa, outras considerações significativas foram observadas tais como a relevância das fontes dos componentes levantados nos achados acadêmicos, a inferência entre os requisitos, componentes e princípios da governança da privacidade e, por último, a constatação da possibilidade de flexibilização para implementação dos componentes da governança da privacidade pelas organizações.

Ao longo desta pesquisa, também foram apresentados os modelos e fontes de governanças da privacidade que serviram como referência para o desenvolvimento de modelos locais; foi confirmada a aderência entre o modelo proposto e a governança da privacidade, uma vez que este mantém a base de sustentação dos princípios desta e, por fim, foi destacado o potencial da lista final de componentes de adequar-se ao cenário, escopo e estratégia de negócio das organizações. Para finalizar, com base nas considerações colocadas anteriormente, é possível afirmar que foi respondida a questão de pesquisa ao afirmar que o constructo produzido por este trabalho é capaz de servir de instrumento de apoio às

organizações para estarem em compliance com a LGPD por sustentar-se nos princípios da governança da privacidade proposta por esta regulamentação e por atender aos requisitos dispostos na lei.

Como sugestão para estudos futuros, fica a proposta da identificação dos subcomponentes destes componentes, de modo que possa ser elaborado um framework para esse fim.

## REFERÊNCIAS

BACKES, Dirce S; COLOMÉ, Juliana S; ERDMANN, Rolf H; LUNARDI, Valéria L. **Grupo focal como técnica de coleta e análise de dados em pesquisa qualitativa**. O Mundo da Saúde. São Paulo, p. 438-442, 2011.

BAMBERGER, Kenneth; MULLIGAN; Deirde K. Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. **George Washington Law Review**, 81(5), pp. 1529-1664, 2013.

BARDIN, L. L'Analyse de contenu. Editora: Presses Universitaires de France, 1977. Análise de conteúdo. SP: Edições 70, 2011.

BLOEM, J.; VAN DOORN, M.; MITTAL, P. Making IT governance work in a Sarbanes- Oxley world. New Jersey: John Wiley & Sons, 2006.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018].  
Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Acessado em 20/08/2023.

CARVALHO, Luiz; OLIVEIRA, Jonice; CAPPELLI, Claudia; MAJER, Violeta. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**. VII Workshop de Transparência em Sistemas. Porto Alegre: Sociedade Brasileira de Computação, p. 21-30, 2019.

CORDEIRO, Hélio. **Detalhes da LGPD e a relação com a segurança da informação**. 2019.  
Disponível em: <https://blog.daryus.com.br/detalhes-da-lgpd-e-a-relacao-com-seguranca-da-informacao/#:~:text=Al%C3%A9m%20do%20respaldo%20aos%20titulares,positivo%20na%20gest%C3%A3o%20de%20riscos>. Acessado em 01/09/2023.

DECEW, Judith. **Privacy**. **The Stanford Encyclopedia of Philosophy**. Spring 2018 Edition, Edward N. Zalta (ed.), 2018. Disponível em: <https://plato.stanford.edu/archives/spr2018/entries/privacy/>. Acessado em 01/09/2023.

DIAMANTOPOULOU, Vasiliki; TSOHOU, Aggeliki; KARYDA, Maria. **General Data Protection Regulation and ISO/IEC 27001:2013**: Synergies of Activities Towards Organizations' Compliance. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) pp. 94-109, 2019.

Farias, A. M. L.; Laurence, L. C. Estatística Descritiva, Apostila. Departamento de Estatística. Niterói: UFF, 2008. Disponível em: [http://www.professores.uff.br/anafarias//estdesc\\_2008.pdf](http://www.professores.uff.br/anafarias//estdesc_2008.pdf)

GONÇALVES, Arlindo. **O conceito de governança**. In: XV Congresso Nacional do CONPEDI/UEA - Manaus: Anais de Congresso. 2006.

GOUVEIA, Amauri Jr. **O Conceito de Modelo e sua Utilização nas Ciências do Comportamento: Breves notas Introdutórias**. Rev. Estudos de Psicologia, PUC-Campinas, v. 16, n. 1, p. 13-16, janeiro/abril 1999.

IBGC, Instituto Brasileiro de Governança Corporativa. **Código das Melhores Práticas de Governança Corporativa**. 4ª Ed. São Paulo: IBGC, 2009.

ITAMARATY. **O Brasil e a OCDE**. Disponível em: <http://www.itamaraty.gov.br/pt-BR/politica-externa/diplomacia-economica-comercial-e-financeira/15584-o-brasil-e-a-ocde>. Acesso em 15 jun. 2023.

ISO 38500:2008, International Organization for Standardization. **Corporate governance of information technology**, 2008.

ISO 38501:2015, International Organization for Standardization. **Information technology — Governance of IT — Implementation guide**, 2015.

ISO 38502:2017, International Organization for Standardization. **Information technology — Governance of IT — Framework and model**, 2017.

KAARST-BROWN, M.; KELLY, S. **IT governance and Sarbanes-Oxley: the latest pitch or real challenges for the IT function?** Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii, 2005.

LUNARDI, Guilherme Lerch; MACADA, João Luiz; GASTAUD, Antônio Carlos. **Um estudo empírico do impacto da governança de TI no desempenho organizacional**. vol.22, n.3, pp.612-624, 2012.

MALDONATO, Viviane; VIEIRA, Claudinei; PRATA, Alexandre; LIMA, Adriano; JUNIOR, Josmar; SILVA, Sergio; VEIRA, Elba; PALHARES, Felipe; CAPANEMA, Walter; MONTANARO, Domingo; JUNIOR, Washington. **LGPD – Lei Geral de Proteção de Dados Pessoais. Manual de Implementação**. 1. ed. São Paulo: Editora Thomson Reuters Revista dos Tribunais, 2019.

OLIVEIRA, Djalma de Pinho Rebouças. **Governança Corporativa na Prática: integrando acionistas, conselho de administração e diretoria executiva na geração de resultados**. São Paulo: Atlas, 2006.

OCDE. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**, 2020. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acessado em: 07/09/2023.

OCDE, Organização para a Cooperação e Desenvolvimento Econômico. **Health Statistics 2020: definitions, sources and methods**. Paris: OCDE, 2020. Disponível em: <http://www.oecd.org/els/health-systems/Table-of-Content-Metadata-OECD-Health-Statistics-2020.pdf>. Acessado em 04/09/2023.

PELKOLA, David. **A framework for managing privacy-enhancing technology**. IEEE Software. vol. 29, pp. 45–49, 2012.

PUGLISI, Maria Laura. **Análise de Conteúdo**. 2. ed. Brasília: Liber Livro, 2005.

PUTRI, Rahmi Eka; SURENDRO, Kridanto. **A Process Capability Assessment Model of IT Governance Based on ISO 38500**. 2015 International Conference on Information Technology Systems and Innovation (ICITSI) Bandung – Bali, November, p.p 16-19, 2015.

REIS, Thiago. **Lei Sarbanes-Oxley: entenda melhor como funciona essa regulação**, 2019. Disponível em: <https://www.sunoresearch.com.br/artigos/sarbanes-oxley/#:~:text=A%20Sarbanes%2DOxley%2C%20ou%20SOx,empresas%20como%20Xerox%20e%20Enron>. Acessado em 20/08/2023.

ROTH, Ana Lúcia; WEGNER, Douglas; JÚNIOR, José Antônio Valle Antunes; PADUA, Antônio Domingos. **Diferenças e inter-relações dos conceitos de governança e gestão de redes horizontais de empresas**: contribuições para o campo de estudos. Revista de Administração, v. 47, n. 1, pp.112-123, 2012.

SILVA, André Luiz Carvalhal da. **Governança Corporativa e sucesso empresarial**: melhores práticas para aumentar o valor da firma. São Paulo: Saraiva, 2006.

SILVA, A.; FOSSÁ, M. Análise de Conteúdo: Exemplo de aplicação da técnica para análise de dados qualitativos. **Qualit@s Revista Eletrônica**, v. 17, n. 1, 2015.

SWARTZ, Paulus, DA VEIGA, A., MARTINS, Nico. A conceptual privacy governance Framework. Conference on Information Communications Technology and Society ICTAS, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.POR&toc=OJ:L:2016:119:FULL](https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POR&toc=OJ:L:2016:119:FULL) . Acessado em 28 ago. 2023.

---

Recebido em/Received: 23/06/2021 | Aprovado em/Approved: 29/05/2024

---