UNIVERSIDADE PAULISTA
PROGRAMA DE MESTRADO EM ENGENHARIA DE PRODUÇÃO

SUELY DOS SANTOS SOUSA

DESENVOLVIMENTO DE INDICADORES E ARTEFATO DIGITAL PARA APOIO ÀS EMPRESAS NA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS

SÃO PAULO
2024

SUELY DOS SANTOS SOUSA

DESENVOLVIMENTO DE INDICADORES E ARTEFATO DIGITAL PARA APOIO ÀS EMPRESAS NA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS

Defesa de Mestrado para obtenção do título de Mestre em Engenharia de Produção, apresentado à Universidade Paulista – UNIP. A linha de pesquisa: 1- Redes de Empresas e Planejamento da Produção e aderente no projeto 19- Tecnologias digitais e inovação tecnológica em sistemas de operação.
Orientador: Prof. Dr. Marcelo Tsuguio Okano

SÃO PAULO
2024

Sousa, Suely dos Santos.
Desenvolvimento de indicadores e artefato digital para apoio às empresas na conformidade com a Lei Geral de Proteção de Dados / Suely dos Santos Sousa. – 2024.
81 f. : il. color. + CD-ROM.

Dissertação de Mestrado Apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista, São Paulo, 2024.
Área de concentração: Gestão de Sistemas de Operação.
Orientador: Prof. Dr. Marcelo Tsuguio Okano.

1. LGPD. 2. DSR. 3. Indicadores. 4. Artefato. I. Okano, Marcelo Tsuguio (orientador). II. Título.

Ficha elaborada pelo Bibliotecário Rodney Eloy CRB8-6450

DEDICATÓRIA

Dedico, primeiramente, este trabalho a Deus. Depois, aos meus pais, Ana Madalena dos Santos Souza e José Dias de Souza, por terem me ensinado o valor da persistência diante das dificuldades. Em sequência, dedico-o ao meu filho, Gael Emídio Sousa, em quem busco forças e inspiração para conseguir alcançar os meus objetivos. Mesmo com todas as lágrimas na alegria ou na dificuldade, tudo compensa, tudo vale a pena devido a este ser especial na minha vida. Então, novamente, dedico este trabalho ao meu filho por, de fato, eu não imaginar minha vida sem ele.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois sem Ele eu não teria conseguido mais uma vez traçar e conquistar os meus objetivos.

Agradeço imensamente aos meus pais, Ana e José, pelo incentivo à busca de conhecimentos desde a minha infância e ao apoio incondicional de ambos no momento mais difícil da minha vida. Que os valores e a educação transmitidos por eles sejam os pilares que me guiam e me fortalecem no dia a dia. Respeitar as pessoas como eu gostaria de ser respeitada é um mote vindo deles e que o tempo todo ecoa em mim.

Agradeço a todos os membros da minha família e amigos por terem me apoiado e ficado ao meu lado nas horas em que eu mais precisava de alento.

Agradeço em especial ao meu orientador, Marcelo Tsuguio Okano, que me apoiou no momento difícil que vivi durante o desenvolvimento deste projeto e me compreendeu. A ele também agradeço por me transmitir seus conhecimentos, por fazer esta experiência positiva, por confiar em mim, por estar sempre me orientando e dedicando parte do seu tempo ao meu trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – PROSUP Financiamento, entidade à qual muito agradeço.

LISTA DE TABELAS

SUMÁRIO

UTILIDADE DA PESQUISA

A implementação da LGPD traz mudanças significativas às responsabilidades das empresas quanto à proteção de dados pessoais. Para garantir conformidade com a legislação, é essencial criar uma ferramenta de mensuração da maturidade da LGPD. Esse artefato ajudará a identificar e a classificar o grau de adequação das empresas. Ele permite a correção de lacunas e a mitigação de riscos legais. Além disso, ele mostra o compromisso da organização com a proteção de dados, fortalece a confiança com clientes e parceiros. Em um ambiente focado em privacidade e segurança, a ferramenta contribuirá para a transparência, a responsabilidade e a melhoria contínua dos processos, alinhando-se aos Objetivos de Desenvolvimento Sustentável ODS 16.

RESUMO

O avanço tecnológico tem transformado todos os aspectos da vida, e o seu uso vem gerando um grande volume de dados que são coletados e utilizados por empresas para se tomar decisões. Com a crescente conectividade, a proteção de dados se tornou crucial, de maneira que os países passaram a adotar leis de proteção aos dados pessoais. A exemplo, temos o Brasil que criou a lei Nº 13.709, DE 14 DE AGOSTO DE 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que segue o modelo do *General Data Protection Regulation* (GDPR) europeu. A LGPD visa a proteger dados pessoais e a garantir a privacidade, impondo obrigações a organizações que lidam com esses dados. Nesse contexto, o objetivo deste trabalho é criar um *framework* com indicadores que possam colaborar para relatórios e os gerar ou *dashboards* que apresentem um diagnóstico da organização analisada. O intuito é sempre auxiliar na identificação de em qual grau de maturidade está a organização, além de colaborar para o monitoramento e aperfeiçoamento dos dados coletados. O *framework* permitiu acompanhar todo o processo de implantação, desde os primeiros estágios de maturidade até os mais avançados da LGPD nas empresas. Os resultados evidenciam que o desenvolvimento, a aplicação e a evolução contínua de tais ferramentas são fundamentais para o fortalecimento da cultura de privacidade nas organizações e para o cumprimento das obrigações legais estabelecidas pela LGPD. A conscientização sobre a importância da privacidade e a segurança dos dados é essencial, pois algumas pessoas não entendem os riscos associados ao compartilhamento de informações sensíveis e, por isto, implementar a LGPD é um desafio. Exige mudanças culturais e investimentos em segurança da informação. As empresas devem se manter atualizadas sobre a lei para garantir conformidade e evitar sanções.

Palavras chaves: LGPD, DSR, Indicadores, Artefato.

ABSTRACT

Technological advancements have transformed all aspects of life, generating a large volume of data that companies collect and use to make decisions. With increasing connectivity, data protection has become crucial, leading countries to adopt laws to protect sensitive data. For instance, Brazil created Law No. 13,709 of August 14, 2018—the General Data Protection Law (LGPD), which follows the European General Data Protection Regulation (GDPR) model. The LGPD aims to protect personal data and ensure privacy by imposing obligations on organizations that handle such data. In this context, the objective of this work is to create a framework with indicators that can generate reports or dashboards, providing a diagnostic of the organization to help identify its maturity level. This framework will aid in monitoring and improving the collected data, supporting the entire implementation process from initial to advanced maturity stages of the LGPD in companies. The results highlight that the development, implementation, and continuous evolution of such tools are essential for strengthening the culture of privacy within organizations and ensuring compliance with the legal obligations established by the LGPD. Awareness of the importance of data privacy and security is essential, as some people do not understand the risks associated with sharing sensitive information. Implementing the LGPD is challenging, requiring cultural changes and investments in information security. Companies must stay updated on the law to ensure compliance and avoid sanctions.

Keywords: LGPD, DSR, Indicators, Artifact.

CAPÍTULO I

1 CONSIDERAÇÕES INICIAIS

1.1 Introdução

A tecnologia no mundo contemporâneo tem evoluído de forma exponencial, e isso impacta diretamente em todos os aspectos da nossa vida, pois a tecnologia está presente em todas as atividades. No entanto, isso gera um grande volume de dados que são coletados por empresas e organizações que os utilizam para analisar tendências, identificar *insigths* e tomar decisões.

Com a sociedade cada vez mais conectada, as interações sociais e as comunicações acontecem em grande parte por meio de plataformas digitais, e o fluxo de dados nesses meios se tornou crucial para as organizações. Assim, a proteção de dados despontou como uma preocupação na mesma medida. Logo, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já têm, como são os casos, para exemplo, da Coreia do Sul, do Chile, da Tailândia, da Índia, da Indonésia e do Brasil. Já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo (*CONSUMERS INTERNATIONAL*, 2018, p. 2).

A proteção de dados tem se tornado um desafio cada vez maior, pois as organizações operam em territórios globais. Nesse contexto, é essencial que as empresas e as organizações compreendam e gerenciem de forma ética e responsável o uso desses dados coletados, para que o desenvolvimento da tecnologia possa ser benéfico para todos. A Lei de Proteção de Dados Pessoais (LGPD) e grande parte das recentes legislações de proteção de dados têm como base o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, em vigor desde maio de 2018. Portanto, ambos os documentos apresentam características similares, como legislação geral e abrangente; proteção de direitos individuais; autoridade supervisora independente (IRAMINA, 2020).

Com a crescente dependência da tecnologia, a segurança cibernética e a proteção da privacidade tornaram-se preocupações críticas à LGPD. O objetivo é proteger os dados pessoais de pessoas naturais, físicas ou jurídicas, que sejam tratadas por pessoas físicas ou jurídicas de direito público ou privado. O intuito é garantir a privacidade, a liberdade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A privacidade é um direito fundamental das pessoas, e a LGPD é uma ferramenta importante para garantir esse direito. A mesma legislação também contribui para a proteção dos dados pessoais, que são cada vez mais valiosos e importantes para as pessoas. A LGPD é uma legislação importante que promove a proteção da privacidade e dos direitos fundamentais das pessoas. A conscientização sobre ela é fundamental para que as pessoas possam usufruir de seus benefícios (DONEDA, 2020).

A temática Lei Geral de Proteção de Dados pessoais no Brasil é um assunto de grande relevância para o país, pois a Lei nº 13.709, de 2018, está em adequação progressiva nas empresas, para tratar da proteção de dados pessoais coletados e produzidos. A LGPD estabelece uma série de obrigações para as empresas e organizações que tratam dados pessoais, com a intenção de garantir a privacidade e os direitos fundamentais das pessoas (BRASIL, 2018).

O tratamento de dados também enfrenta alguns desafios específicos. Um deles é a falta de conscientização sobre a importância da privacidade e da segurança dos dados. Muitas pessoas não entendem os riscos associados ao compartilhamento de seus dados pessoais e não tomam medidas para proteger sua privacidade. Isso pode causar impactos que podem ser positivos, pois está tornando o mundo mais conectado, mais eficiente e mais inteligente. Ao mesmo tempo, também pode causar impactos negativos quanto à quantidade de dados de pessoas físicas e jurídicas está disponível nas plataformas digitais.

Nesse contexto, a Lei Geral de Proteção de Dados é uma legislação que regula o tratamento de dados pessoais no Brasil. Estabelece diretrizes para a coleta, para o armazenamento, para o processamento e o compartilhamento de informações pessoais por organizações, sejam elas públicas ou privadas (BRASIL, 2018).

A LGPD é válida para todas as ações de tratamento realizada por pessoa natural ou entidade jurídica, tanto públicas, quanto privadas, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados. A garantia vem da Lei 13.709, em seu Art. 3º, episódio que também trata das exceções (BRASIL, 2018).

A Lei 13.709, no seu Art. 1º, trata [...] “de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” Ela é uma lei recente, e ainda é preciso acompanhar sua implementação e evolução no Brasil (BRASIL, 2018).

É importante que as empresas e as organizações se mantenham atualizadas sobre as mudanças na lei, para garantir o cumprimento das obrigações. Também é importante que o governo continue a promover a conscientização sobre a LGPD, para que as pessoas entendam seus direitos e como os proteger.

É uma lei complexa e abrangente, e as empresas e organizações que tratam dados pessoais precisam se adequar à mesma lei para evitar sanções administrativas. Um dos principais desafios da LGPD no Brasil é o desconhecimento dos seus conteúdos de proteção. Muitas empresas e organizações ainda não estão familiarizadas com o fato e suas obrigações, pois a lei exige uma mudança na cultura organizacional das empresas. A intenção é garantir a proteção dos dados pessoais. Sua adequação, porém, pode exigir investimentos significativos.

A tecnologia, portanto, poderá ser uma ferramenta de conexão fundamental para pessoas físicas e pessoas jurídicas. Todas as organizações, entretanto, precisam se adaptar à Lei nº13.709, de 2018, e cumprir suas exigências ou serão penalizadas (BRASIL, 2018).

A LGPD é legislação recente, e ainda é preciso acompanhar sua real implementação e evolução no Brasil. É importante que as empresas e organizações, como já se disse, se mantenham atualizadas sobre as mudanças na lei, para garantir o cumprimento de suas obrigações. Também é importante que o governo continue a promover a conscientização sobre a LGPD, para que as pessoas entendam sua importância e ainda seus direitos e como os proteger.

1.2 Problema da Pesquisa

Na era da informação e da tecnologia, o tratamento de dados pessoais tornou-se uma questão crítica para empresas e organizações em todo o mundo. No Brasil, a Lei Geral de Proteção de Dados (doravante apenas LGPD na continuidade do texto) estabeleceu diretrizes para a coleta, para o armazenamento, para o processamento e o compartilhamento de informações pessoais. O fato visa a proteger a privacidade e os direitos dos dados pessoais.

Muitas organizações enfrentam desafios significativos na adaptação aos requisitos da LGPD e na garantia de conformidade com suas disposições. A identificação e a classificação do grau de maturidade no tratamento de dados pessoais tornaram-se uma tarefa complexa e crucial para empresas de todos os setores. Diante do cenário em que os dados se fizeram os

ativos mais importantes nas organizações, houve a necessidade de regulamentar as operações de tratamento e de processamento das informações. Deste modo, este estudo tem a seguinte questão de pesquisa: como identificar e como classificar o grau de maturidade das empresas no tratamento de dados pessoais, de acordo com os requisitos estabelecidos pela LGPD.

Nesse cenário, é preciso definir quais são os indicadores que permitem identificar e classificar o grau de maturidade das organizações. Para esse cálculo, foram determinados os seguintes parâmetros:

- Governança,
- Conformidade legal e respeito aos princípios,
- Transparência e direitos do titular,
- Rastreabilidade,
- Adequação de contratos e de relações com parceiros,
- Segurança da informação,
- Violação de dados.

1.3 Justificativa

Os principais objetivos de um projeto de adequação à LGPD servem para que as organizações possam mitigar os riscos, gerar políticas e procedimentos internos para implementar a adequação de governança. O intuito é ainda conseguir controle, monitoramento e avaliação de dados, além de identificar e melhorar as práticas continuamente.

A questão é que as empresas lidam diariamente com grandes quantidades de dados pessoais, e, quando ocorre algum incidente de segurança com vazamento de informações, a privacidade fica comprometida. Nesse contexto, atender as exigências da LGPD é de extrema importância. Avaliar, todavia, o seu nível de adequação e maturidade é essencial para que a política de privacidade e o processo de governança sejam eficazes.

A identificação e a classificação do grau de maturidade no tratamento de dados pessoais são temas fundamentais para a conformidade com a LGPD. Diversos autores e especialistas destacam a importância de indicadores e de critérios para avaliar essa maturidade.

Para começar, autores, como Machado (2020), argumentam que a maturidade no tratamento de dados pessoais pode ser avaliada com base em indicadores relacionados à

conformidade com os princípios da LGPD, como finalidade, necessidade, transparência e segurança. Esses indicadores refletem o compromisso da organização com a proteção dos dados pessoais e com o cumprimento dos requisitos legais.

Além disso, Lima (2019) ressalta a importância de critérios, como a existência de políticas e de procedimentos claros para o tratamento de dados. A finalidade é a designação de um encarregado de proteção de dados (DPO) e a implementação de medidas técnicas e organizacionais para garantir a segurança dos dados.

Outro aspecto relevante é a capacitação dos colaboradores, conforme discutido por Araújo (2021), que destaca a importância de programas de conscientização sobre proteção de dados. O que se quer é garantir uma cultura organizacional voltada à privacidade e à segurança da informação.

Por fim, autores, como Rezende (2020), enfatizam a necessidade de avaliação contínua e a realização de avaliações de impacto à proteção de dados (PIA). Identificar e mitigar riscos relacionados ao tratamento de dados pessoais valida-se sempre como fundamental.

A literatura, em suma, destaca a importância de indicadores e critérios para identificar e classificar o grau de maturidade no tratamento de dados pessoais de acordo com os requisitos estabelecidos pela LGPD. Isto fornece orientações valiosas para as organizações que buscam garantir a conformidade e a proteção eficaz dos dados pessoais.

A implementação da LGPD nas empresas é um processo complexo e desafiador. Ela exige mudanças significativas na cultura, nos processos e nas tecnologias de uma organização. Por isso, um *framework* para acompanhar o processo de implantação auxiliaria com um conjunto de diretrizes e recomendações para acompanhar o processo de implementação da LGPD nas empresas.

Auxiliar as empresas é preciso. A ação é para que elas possam identificar e monitorar os processos que estão sendo implementados, mas sempre de forma sistemática e eficiente, de acordo com as conformidades exigidas pela Lei.

O gerenciamento desse processo de implantação envolve todos os níveis de uma organização. Ele considera a importância de garantir a conformidade, pois a LGPD prevê sanções administrativas. Portanto, as empresas que desejam implementar a Lei de forma eficaz e eficiente podem (deveriam) considerar o uso de um *framework* para auxiliar nesse processo.

1.4 Objetivos

Geral

O objetivo mais abrangente é para seria o de desenvolver os indicadores e os critérios que permitam analisar o processo de implantação da LGPD em todos os níveis da organização por meio de um artefato tecnológico. Essa análise servirá de parâmetro e auxiliará o direcionamento da empresa sobre o processo de implantação e sobre os níveis de melhoria para a mesma implementação.

Específicos

- Criar os indicadores, com base no arcabouço teórico, para analisar o grau de maturidade da implantação da LGPD nas empresas,
- Desenvolver o artefato tecnológico de acordo com os indicadores criados,
- Testar o artefato nas empresas.

1.5 Composição da Dissertação

Esta dissertação encontra-se dividida nos seguintes capítulos: o Capítulo 1 apresenta uma introdução ao trabalho, a identificação do problema da pesquisa, os objetivos e uma justificativa de pesquisa. O Capítulo 2 contribui com referencial teórico utilizado na pesquisa; descreve as áreas relacionadas ao tema do trabalho, as quais são as plataformas digitais, a LGPD e o seu processo de implantação nas empresas.

O Capítulo 3 mostra os procedimentos metodológicos utilizados para realizar a pesquisa. O Capítulo 4 apresenta os resultados e as respectivas análises e o Capítulo 5 aborda os objetivos alcançados e as considerações realizadas em relação à continuidade da pesquisa.

CAPÍTULO II

2. REFERENCIAL CONCEITUAL

2.1 Ecossistemas Digitais

Ecossistemas digitais são ambientes formados pela interação entre diferentes tecnologias, plataformas digitais, serviços e usuários, que criam e compartilham valor de forma interligada. Como corroboram Jacobides, Cennamo e Gawer (2018), "um ecossistema digital consiste em um grupo de empresas interdependentes e outras entidades que compartilham padrões comuns e dependem de uma infraestrutura tecnológica compartilhada para alcançar seus objetivos".

Os ecossistemas digitais são caracterizados pela complexidade e pela interconectividade de seus componentes. Lima (2020) descreve os ecossistemas digitais como "estruturas complexas e interconectadas, nas quais uma variedade de plataformas, de dispositivos, de aplicativos, de serviços e usuários interagem e trocam informações de maneira dinâmica". Essa definição enfatiza a multiplicidade de elementos que compõem esses sistemas e a importância da conectividade para um funcionamento eficaz.

Considerando ambientes que desempenham um papel central na economia digital contemporânea, que moldam significativamente as interações sociais e profissionais na era da tecnologia, afirma-se que são fundamentais no mundo presente. Tais ecossistemas desempenham um papel crucial ao fomentar o desenvolvimento da economia digital e ao influenciar os padrões de vida, de trabalho e de comunicação das pessoas e entre elas.

Os ecossistemas digitais têm se tornado uma parte essencial da infraestrutura tecnológica moderna. Segundo Lima (2020), a quem repetimos por sua importância, "ecossistemas digitais são estruturas complexas e interconectadas, nas quais uma variedade de plataformas, dispositivos, aplicativos, serviços e usuários interagem e trocam informações de maneira dinâmica". Essa definição sublinha a natureza multifacetada e interativa dos ecossistemas digitais; destaca a importância da conectividade e da integração de diferentes componentes tecnológicos.

De acordo com Barbosa e Silva (2018), a formação de ecossistemas digitais envolve não apenas a tecnologia, mas também aspectos sociais e econômicos, que são fundamentais

para a criação de valor. Eles argumentam que "a interconectividade desses sistemas permite a inovação contínua e a adaptação às mudanças nas demandas dos usuários" (BARBOSA; SILVA, 2018, p. 45). Isso reflete a ideia de que ecossistemas digitais não são estáticos, mas evoluem com o tempo, influenciados pelas interações entre seus diversos elementos.

Além disso, Ferreira e Gomes (2019) apontam que a eficiência dos ecossistemas digitais depende da capacidade de seus componentes de se comunicar e de operar de forma harmoniosa. Eles afirmam que "a interoperabilidade é crucial para o sucesso de um ecossistema digital, pois permite a troca de informações sem barreiras e a coordenação eficaz entre diferentes plataformas e serviços" (FERREIRA; GOMES, 2019, p. 78). Portanto, a interoperabilidade se destaca como um fator determinante para a funcionalidade e a competitividade dos ecossistemas digitais.

Os ecossistemas digitais são uma realidade crescente na infraestrutura tecnológica contemporânea. Eles representam a convergência de diversas plataformas, de dispositivos, de aplicativos e de serviços, interligados para criar um ambiente de interação e de troca de informações de maneira dinâmica e contínua (LIMA, 2020).

Além disso, Barbosa e Silva (2018) ressaltam que a formação de ecossistemas digitais envolve aspectos tecnológicos, sociais e econômicos. Eles afirmam que "a interconectividade desses sistemas permite a inovação contínua e a adaptação às mudanças nas demandas dos usuários" (BARBOSA; SILVA, 2018, p. 45). Isso indica que os ecossistemas digitais são influenciados tanto pelas tecnologias emergentes, quanto pelas necessidades e pelos comportamentos dos usuários.

A dinâmica dos ecossistemas digitais é caracterizada pela interação contínua entre seus componentes. Repetindo Ferreira e Gomes (2019), novamente se afirma que "a interoperabilidade é crucial para o sucesso de um ecossistema digital, pois permite a troca de informações sem barreiras e a coordenação eficaz entre diferentes plataformas e serviços" (FERREIRA; GOMES, 2019, p. 78). A interoperabilidade facilita a comunicação entre diferentes sistemas; ela permite que se trabalhe de maneira coesa e eficiente.

Além disso, a dinâmica dos ecossistemas digitais é impulsionada pela inovação. Silva (2021) argumenta que "a capacidade de adaptação e de evolução constante é essencial para a sustentabilidade dos ecossistemas digitais" (SILVA, 2021, p. 32). Isso significa que as

tecnologias e as práticas nesses ecossistemas precisam ser continuamente atualizadas e aprimoradas para se manterem relevantes e competitivas.

Embora os ecossistemas digitais ofereçam muitas vantagens, eles também apresentam desafios significativos. A interoperabilidade é um desses desafios, conforme destacado por Ferreira e Gomes (2019). A necessidade de que diferentes sistemas e plataformas se comuniquem de maneira eficaz é fundamental para o sucesso do ecossistema. A falta de padrões comuns, entretanto, pode dificultar essa comunicação.

Outro desafio crítico é a segurança. Segundo Costa e Pereira (2021), "os ecossistemas digitais são vulneráveis a ataques cibernéticos devido à sua natureza interconectada e à quantidade de dados sensíveis que circulam entre os sistemas" (COSTA; PEREIRA, 2021, p. 85). A proteção dos dados e a implementação de medidas de segurança robustas são essenciais para garantir a integridade e a confiabilidade dos ecossistemas digitais.

Os ecossistemas digitais são pedra angular na economia contemporânea por facilitar a inovação aberta, por aumentar a eficiência e promover o desenvolvimento de novos mercados e modelos de negócios. Eles permitem que as organizações colaborem e compartilhem recursos de maneira mais eficaz, e isto resulta em uma maior criação de valor para todos os participantes.

2.2 Plataformas digitais

As tecnologias digitais estão mudando substancialmente os processos das organizações, e isso provoca mudanças em todo o cenário, fato, na sua vez, que faz que as empresas procurem se adaptar a essas mudanças. As plataformas digitais emergiram como elementos centrais na economia e na sociedade contemporâneas. Elas representam ambientes digitais em que usuários, empresas e outras entidades interagem e realizam transações, trocam informações e criam valor de forma coletiva.

As plataformas digitais são um fenômeno complexo e estão em constante evolução, marca cada vez mais importante no mundo dos negócios. As plataformas estão transformando a sociedade e impactando diretamente a forma como vivemos, como trabalhamos e nos relacionamos.

Além disso, as plataformas digitais desempenham um papel crucial na economia de compartilhamento. Botsman e Rogers (2010) destacam que "a economia de compartilhamento

é impulsionada por plataformas digitaisque conectam fornecedorese consumidores de maneira eficiente, o que permite o uso compartilhado de recursos".

Plataformas digitais são modelos de negócios que funcionam por meio da tecnologia. Elas conectam usuários e empresas de diversos setores; permitem uma relação de troca, muito além da simples compra e venda. “As plataformas, em termos simples, são baseadas em algum tipo de infraestrutura que facilita a troca de valor entre fornecedores e consumidores” (Parker *et al*., 2016 apud Grisoldi, 2023). O termo *plataforma* digital ainda é muito recente, conforme Okano *et al*. (2021) e, nesse contexto, existem várias definições para o vocábulo de acordo com a Tabela 1.

Tabela 1 - Definições e características da plataforma

Plataforma digital pode ser definida como plataforma externa baseada em software. Ela consiste em uma base de código extensível que fornece a principal funcionalidade compartilhada pelos módulos que interagem com ela e pelas interfaces por meio das quais eles interatuam. Os aplicativos (parte executável do software) das plataformas oferecem serviços ou sistemas aos usuários finais.	Tiwana *et al*., (2010) Ghazawneh e Henridsson (2013)
Uma plataforma digital também pode ser caracterizada como um conjunto sociotécnico. Ela engloba os elementos técnicos (de software e hardware) e os processos e padrões organizacionais associados.	Tilson *et al*., (2012).
As plataformas digitais são “ações de uma rede de empresas com competências complementares para co-inovar novos modelos de negócios”. Os modelos se baseiam intrinsecamente em recursos de informação e tecnologia.	Venkatraman *et al*., (2014)
A plataforma digital multifacetada é uma organização. O aplicativo cria valor ao permitir comunicação direta e interações entre dois ou mais grupos diferentes de usuários.	Hagiu e Wright (2015)
As plataformas digitais fornecem um conjunto comum de regras de *design* e uma infraestrutura digital. O fim é facilitar as trocas entre vários usuários que, de outra forma, nunca teriam a oportunidade de interagir uns com os outros.	Ondrus *et al*., (2015)
A plataforma é construída em princípios e arquiteturas baseados em serviços. Ou seja, ela visa a criar um conjunto de serviços que podem ser reunidos para produzir aplicativos e fluxos de trabalho	Le Hong *et al*., (2016)
Uma plataforma digital é um espaço tecnológico em que diferentes participantes, empresas ou consumidores se conectam, geram e trocam valor entre si. Exemplos incluem mídias sociais (Facebook, Instagram), plataformas de economia compartilhada (AirBnb, Uber), *marketplaces* de comércio eletrônico (Amazon, Mercado Livre) e serviços de streaming (Netflix, Spotify, Youtube Music).	Castellani, (2016)
Uma plataforma digital é um modelo de negócios habilitado para tecnologia que cria valor ao facilitar as trocas entre dois ou mais grupos interdependentes.	Morvan, Hintermann,

Mais comumente, a plataforma reúne usuários finais e produtores para realizar transações uns com os outros. Ela também permite que as empresas compartilhem informações para melhorar a colaboração ou a inovação para novos produtos e serviços.	Vazirani, (2016)
Uma plataforma digital é um modelo de negócios com tecnologia habilitada. Ela permite que produtores e consumidores troquem valor.	Mancha *et al*., (2018)
Na plataforma digital, as relações econômicas digitais são construídas com base em um ambiente de rede transparente. Ou seja, o aspecto social da confiança é fornecido por uma rede social, que é, entre outras coisas, um poderoso fator de autodesenvolvimento para todo o sistema. Na plataforma, os mecanismos de infraestrutura de mercado devem ser devidamente implementados.	Kozhevnikov e Korolev (2018)
As plataformas digitais diferem em finalidade e complexidade. Isto vai desde nos conectar em nossas vidas pessoais, até nos conectar com nossos clientes, colegas e parceiros de negócios. Mais especificamente, as plataformas analisam a interação entre o mundo digital e o mundo real. Analisam ainda o potencial de transformação digital; tentam cumprir o objetivo de uma organização *multistakeholder*.	(Bonollo & Poopuu, (2019)

Fonte: Okano *et al*., (2021).

A Tabela 1 apresenta definições e características de plataformas digitais, conforme descrito por diversos autores ao longo dos anos. As definições convergem para descrever plataformas digitais como sistemas baseados em *softwares* que facilitam interações entre usuários e/ou organizações, o que gera benefícios por meio dessas conexões. São elas

Aspectos técnicos e organizacionais: alguns conceitos enfatizam a combinação de elementos técnicos (*hardware* e *software*) com processos e padrões organizacionais associados;

Inovação e criação de valor: as descrições concordam ao descrever plataformas digitais como sistemas fundamentados em programas de computador que facilitam a comunicação entre usuários e/ou organizações, o que gera benefícios por meio dessas conexões;

Facilitação de interações: as plataformas digitais têm o intuito de facilitar a comunicação e a interação entre grupos diversos de usuários, muitas vezes por meio de regras de *design* comuns e infraestrutura digital;

Modelo de negócio habilitado para tecnologia: muitas definições destacam que as plataformas digitais são modelos de negócios habilitados para a tecnologia e, por isto, modelos que facilitam trocas de valor entre diferentes grupos de usuários;

Transparência e confiança: alguns autores mencionam a importância da transparência e da confiança nas relações econômicas digitais e, desse modo, enfatizam o papel das redes sociais e dos mecanismos de infraestrutura de mercado;

Diversidade de propósitos: as definições também reconhecem a diversidade de propósitos das plataformas digitais que vão desde conectar indivíduos em suas vidas pessoais até facilitar interações entre empresas e clientes.

As plataformas digitais são sistemas ou infraestruturas que permitem a interação, a transação e a colaboração entre diferentes usuários, empresas e dispositivos por meio da Internet. Essas definições e características destacam a natureza multifacetada e em constante evolução das plataformas digitais. A situação reflete a complexidade e o impacto significativos que elas têm nos negócios e na sociedade em geral.

Uma característica essencial das plataformas digitais é a sua capacidade de gerar efeitos de rede. Rochet e Tirole (2003) afirmam que "os efeitos de rede ocorrem quando o valor de um serviço aumenta à medida em que mais pessoas o utilizam". Esse fenômeno é crucial para o sucesso das plataformas digitais, pois incentiva a sua adoção em massa e fortalece a posição competitiva das mesmas plataformas no mercado.

Apesar dos benefícios significativos, as plataformas digitais também enfrentam vários desafios. Um dos principais deles é a governança da plataforma. Boudreau e Hagiu (2009) discutem que "a governança das plataformas envolve o estabelecimento de regras e normas que regulam as interações entre os participantes da plataforma". A governança eficaz é crucial para manter a confiança dos usuários e garantir a sustentabilidade a longo prazo do recurso tecnológico.

Outros desafios importantes são a privacidade e a segurança dos dados. De acordo com Acquisti, Taylor e Wagman (2016), "as plataformas digitais coletam e processam grandes quantidades de dados pessoais, o que levanta preocupações sobre privacidade e segurança". A proteção desses dados é essencial para preservar a confiança dos usuários e para cumprir as regulamentações legais.

As plataformas digitais não impactam apenas a economia. Portam também profundas implicações sociais e culturais. Shirky (2008) argumenta que "as plataformas digitais mudaram a maneira como as pessoas se comunicam, colaboram” entre si “e consomem informações".

Redes sociais, como *Facebook e Twitter*, transformaram a comunicação interpessoal e a disseminação de notícias, enquanto plataformas, como *YouTube* e *Instagram*, criaram formas novas de expressão cultural.

As plataformas digitais são componentes fundamentais da infraestrutura tecnológica e econômica moderna. Elas facilitam a criação de valor, promovem a inovação e transformam indústrias inteiras. No entanto, esses benefícios vêm acompanhados de desafios significativos em termos de governança, de privacidade e de concorrência. Além disso, as plataformas digitais têm um impacto profundo nas dinâmicas sociais e culturais, o que exige uma consideração cuidadosa de suas implicações a longo prazo.

2.3 *Privacy by Design*

Privacy by Design (Privacidade por Projeto) é uma abordagem para o desenvolvimento de sistemas, produtos e processos desde sua concepção inicial, considerando-se a proteção da privacidade como um elemento de centro. Essa abordagem visa a integrar considerações de privacidade em todas as etapas do ciclo de vida do projeto, desde a fase de planejamento até as suas implementação e manutenção. O objetivo é o de garantir que os dados pessoais sejam protegidos de maneira eficaz desde o início.

A privacidade tornou-se uma preocupação de centro na era digital. Nela, a coleta e o processamento de dados pessoais são comuns. Para enfrentar os desafios associados à proteção de dados, o conceito de *Privacy by Design* (Privacidade desde a Concepção) foi desenvolvido. Essa abordagem propõe a integração de medidas de privacidade ao longo de todo o ciclo de vida dos sistemas e dos processos de informações. O ensaio explora a origem, os princípios e a implementação do *Privacy by Design*, bem como seus benefícios e desafios.

O conceito de *Privacy by Design* é definido por Cavoukian (2010) como "uma abordagem que integra a privacidade ao desenvolvimento inicial e aos processos operacionais de sistemas, de redes e de práticas de negócios" (CAVOUKIAN, 2010, p. 2). Essa definição sublinha a necessidade de considerar a privacidade como um componente fundamental e não um complemento no desenvolvimento de tecnologias e de processos.

Privacy by Design não é apenas uma prática recomendada. É um princípio essencial incorporado em regulamentações de proteção de dados, como o Regulamento Geral sobre a

Proteção de Dados (GDPR) da União Europeia. De acordo com o GDPR, as organizações são obrigadas a implementar medidas de proteção de dados já na fase de concepção de novos produtos e serviços (*EUROPEAN UNION*, 2016).

Privacy by Design é baseada em sete princípios fundamentais, conforme descritos por Cavoukian (2010):

> **Proativo, não Reativo; Preventivo, não Corretivo** – a abordagem proativa visa a prever invasões de privacidade; visa, então, a preveni-las obviamente antes que ocorram;
> **Privacidade como Configuração Padrão** – os sistemas devem ser configurados para proteger automaticamente a privacidade dos indivíduos sem a necessidade de intervenção do usuário;
> **Privacidade Incorporada ao Projeto** – a proteção de dados deve ser integrada ao *design* e à arquitetura dos sistemas e processos;
> **Funcionalidade Total – Positivo-Soma, não Soma-Zero** – a abordagem deve buscar um equilíbrio em que tanto a privacidade, quanto outros objetivos possam ser alcançados simultaneamente;
> **Segurança de Extremidade a Extremidade – Proteção ao Longo do Ciclo de Vida** – os dados devem ser protegidos durante todo o seu ciclo de vida, desde a coleta até a destruição;
> **Visibilidade e Transparência** – todas as práticas e tecnologias devem ser transparentes para permitir a verificação independente do cumprimento das políticas de privacidade; **Respeito pela Privacidade do Usuário – Centricidade no Usuário** – os interesses e a privacidade dos indivíduos devem estar no centro das práticas de proteção de dados.

Esses princípios formam a base para a implementação eficaz do *Privacy by Design* em sistemas e processos organizacionais. A implementação do sistema requer uma abordagem multidisciplinar que envolva não apenas a tecnologia, mas também a governança, as políticas e os procedimentos organizacionais. De acordo com Schaar (2010), "a aplicação prática de *Privacy by Design* envolve a integração de medidas técnicas e organizacionais desde as fases iniciais de desenvolvimento de projetos e de processos" (SCHAAR, 2010, p. 18).

A adoção de tecnologias, que garantam a privacidade, como criptografia, anonimização e pseudonimização de dados, se tornou fundamental na atualidade. Pfitzmann e Hansen (2010)

destacam a importância dessas tecnologias ao afirmar que "a aplicação de criptografia e de anonimização pode significativamente reduzir os riscos de violação de dados" (PFITZMANN; HANSEN, 2010, p. 12).

É crucial implementar políticas e procedimentos organizacionais que suportem a privacidade. Isso inclui a realização de avaliações de impacto sobre a privacidade (*Privacy Impact Assessments - PIAs*). Inclui ainda a nomeação de oficiais de proteção de dados (*Data Protection Officers - DPOs*) e a realização de treinamentos regulares para funcionários sobre práticas de privacidade.

A adoção de *Privacy by Design* oferece vários benefícios tanto para as organizações, quanto para os indivíduos. A implementação do recurso pode levar a uma redução nos riscos de violações de dados e nas suas consequentes penalidades. Cavoukian (2010) argumenta que "a adoção de práticas proativas de privacidade pode aumentar a confiança do consumidor e a reputação da marca, o que resulta em vantagem competitiva" (CAVOUKIAN, 2010, p. 5).

Para os indivíduos, *Privacy by Design* garante maior controle sobre seus dados pessoais e, na extensão, proteção contra abusos. Isso é especialmente relevante em um contexto em que os dados pessoais são frequentemente usados para fins de *marketing* e outras atividades não autorizadas. De acordo com Solove (2006), "os indivíduos se beneficiam de uma maior transparência, de um maior controle sobre como seus dados são coletados, usados e compartilhados" (SOLOVE, 2006, p. 24).

A integração de medidas de privacidade pode ser complexa e onerosa. Pfitzmann e Hansen (2010) observam que "a implementação de tecnologias de privacidade, como criptografia e anonimização, pode exigir recursos significativos e *expertise* técnica" (PFITZMANN; HANSEN, 2010, p. 15). Organizacionalmente, porém, a resistência à mudança e a falta de conscientização sobre a importância da privacidade podem dificultar a adoção de *Privacy by Design*. Schaar (2010), como já afirmado, sugere que "a criação de uma cultura organizacional que valorize a privacidade requer um comprometimento contínuo da liderança e um investimento em treinamento e educação" (SCHAAR, 2010, p. 20).

Em termos regulatórios, a conformidade com múltiplas jurisdições e os regulamentos de privacidade podem ser desafiadores. A complexidade das leis de privacidade, como a LGPD no Brasil, o GDPR na Europa e a CCPA na Califórnia, exige que as organizações mantenham uma compreensão atualizada e detalhada das suas obrigações legais (CAVOUKIAN, 2010).

Privacy by Design representa uma abordagem essencial para a proteção de dados pessoais na era digital. Integrando a privacidade desde a concepção dos sistemas e processos, as organizações podem cumprir com os requisitos regulatórios, como ainda ganhar a confiança dos consumidores e melhorar sua reputação. No entanto, a implementação efetiva de *Privacy by Design* requer um compromisso significativo e uma abordagem integrada, o que envolve medidas técnicas, organizacionais e culturais.

2.4 *General Data Protection Regulation* (GDPR)

O GDPR, ou *General Data Protection Regulation*, é uma legislação europeia que entrou em vigor em maio de 2018 e tem aplicação em todos os países membros da União Europeia. Ainda tem aplicação em organizações que processam dados de cidadãos europeus, independentemente de sua localização geográfica.

Este regulamento visa a proteger os direitos à privacidade e à proteção de dados dos cidadãos europeus. Ela estabelece regras estritas para a coleta, para o processamento e para o armazenamento de informações pessoais, como já se afirmou.

O GDPR exige que as organizações obtenham consentimento explícito dos titulares dos dados para processar suas informações, que forneçam transparência nas práticas de tratamento de dados e que notifiquem as autoridades competentes sobre violações de dados em até 72 horas após a descoberta. Além disso, ele concede aos titulares dos dados o direito de acessar, de retificar, de apagar ou de exportar seus dados pessoais e impõe multas substanciais para empresas que não estejam em conformidade com suas disposições.

A LGPD (Lei Geral de Proteção de Dados) e o GDPR (Regulamento Geral de Proteção de Dados) são marcos regulatórios cruciais no campo da privacidade de dados. Eles estabelecem diretrizes e regulamentações para o tratamento de informações pessoais em ambientes digitais. Embora sejam distintos em suas origens e aplicações geográficas, ambos compartilham o objetivo central de proteger a privacidade e os direitos dos indivíduos em um mundo cada vez mais orientado pela tecnologia.

Ambos, a LGPD e o GDPR, têm desempenhado um papel fundamental na promoção da privacidade de dados e na conscientização sobre a importância da proteção das informações pessoais em um cenário digital cada vez mais complexo. A legislação estabelece um padrão

para o tratamento de dados pessoais, além de incentivar as organizações a adotar medidas robustas de segurança e conformidade para proteger os direitos e a privacidade dos indivíduos.

O Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* - GDPR) é uma legislação da União Europeia (UE) que estabelece diretrizes rigorosas para a proteção de dados pessoais e para a privacidade dos cidadãos europeus. Implementado em 25 de maio de 2018, o GDPR substituiu a Diretiva de Proteção de Dados, de 1995, e introduziu um conjunto de obrigações mais rígidas para as organizações que processam dados pessoais.

A necessidade de uma legislação robusta sobre proteção de dados na UE surgiu devido ao rápido avanço tecnológico e ao aumento das transações digitais, que expuseram as limitações da Diretiva de Proteção de Dados, de 1995. De acordo com Costa e Silva (2019), "o GDPR foi desenvolvido para harmonizar as leis de proteção de dados em toda a UE, reforçando os direitos dos indivíduos e proporcionando maior clareza e previsibilidade para as empresas" (COSTA; SILVA, 2019, p. 45).

O GDPR aplica-se em todas as organizações que processam dados pessoais de residentes da UE, independentemente da localização da empresa. Essa extraterritorialidade garante que os dados protegidos dos cidadãos europeus em qualquer lugar sejam do mundo (*EUROPEAN UNION*, 2016).

O GDPR é construído sobre seis princípios fundamentais que orientam o processamento de dados pessoais (*EUROPEAN UNION,* 2016):

Licitude, lealdade e transparência: os dados pessoais devem ser processados de maneira lícita, justa e transparente em relação ao titular dos dados;

Limitação das finalidades: os dados pessoais devem ser coletados para finalidades determinadas, explícitas e legítimas; não devem ser tratados de maneira incompatível com essas finalidades;

Minimização dos dados: os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário em relação às finalidades para as quais são processados;

Exatidão: os dados pessoais devem ser exatos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados inexatos sejam apagados ou retificados sem demora;

Limitação da conservação: os dados pessoais devem ser mantidos de forma a se permitir a identificação dos titulares dos informes apenas durante o período necessário para as finalidades para as quais são processados;

Integridade e confidencialidade: os dados pessoais devem ser processados de maneira a garantir a segurança adequada dos mesmos dados, e isso inclui proteção contra processamento não autorizado ou ilícito e contra perda, destruição ou dano acidental.

O GDPR fortalece os direitos dos indivíduos em relação aos seus dados pessoais; proporciona-lhes maior controle e transparência sobre o material. Entre os principais direitos garantidos pelo GDPR estão

Direito de Acesso aos dados: os titulares dos dados têm o direito de obter da organização a confirmação de que seus dados pessoais estão sendo processados e, se for o caso, têm o direito de acessar esses dados e outras informações relacionadas (EUROPEAN UNION, 2016); de acordo com Almeida e Santos (2018), "o direito de acesso garante transparência e permite que os indivíduos conheçam e verifiquem a legalidade do processamento de seus dados" (ALMEIDA; SANTOS, 2018, p. 33);

Direito à Retificação: os indivíduos têm o direito de obter a retificação de dados pessoais inexatos e o direito de completar dados pessoais incompletos (EUROPEAN UNION, 2016); este direito assegura que os dados mantidos pelas organizações sejam precisos e atualizados;

Direito ao Esquecimento: conhecido formalmente como direito ao apagamento, este direito permite que os indivíduos solicitem a exclusão de seus dados pessoais quando não houver mais necessidade de processamento deles ou quando o consentimento for retirado (EUROPEAN UNION, 2016); segundo Costa e Silva (2019), "o direito ao esquecimento é fundamental para proteger a privacidade dos indivíduos e evitar a retenção desnecessária de dados pessoais" (COSTA; SILVA, 2019, p. 50);

Direito à Portabilidade dos Dados: os indivíduos têm o direito de receber os dados pessoais que lhes digam respeito, que tenham fornecido a uma organização, em um formato estruturado, de uso comum e leitura automática; têm ainda o direito de transmitir esses dados a outra organização (EUROPEAN UNION, 2016); este direito facilita a transferência de dados entre provedores de serviços;

Direito de Oposição: os titulares dos dados têm o direito de se opor ao processamento de seus dados pessoais em determinadas circunstâncias, incluindo o processamento para fins de *marketing* direto (EUROPEAN UNION, 2016); este direito permite que os indivíduos controlem como seus dados são utilizados.

As organizações que processam dados pessoais têm várias obrigações sob o GDPR. Nisto se inclui a designação de um Encarregado de Proteção de Dados (DPO). Organizações que realizam monitoramento regular e sistemático de indivíduos em larga escala ou que processam categorias especiaisde dados devem nomear um Encarregado de Proteção de Dados (DPO). O intuito é a garantia da conformidade com o GDPR (EUROPEAN UNION, 2016).

As organizações são ainda obrigadas a realizar Avaliações de Impacto sobre a Proteção de Dados (DPIAs) quando o processamento de dados pode resultar em alto risco para os direitos e liberdades dos indivíduos (*EUROPEAN UNION*, 2016). As DPIAs ajudam a identificar e a mitigar riscos relacionados ao processamento de dados pessoais.

Em caso de violação de dados pessoais, as organizações devem notificar a autoridade de supervisão competente sem demora indevida e, em alguns casos, notificar também os titulares dos dados afetados (EUROPEAN UNION, 2016). Segundo Monteiro (2019), "a notificação rápida de violações de dados é essencial para minimizar os impactos negativos sobre os indivíduos" (MONTEIRO, 2019, p. 78).

O GDPR teve um impacto significativo em como as organizações lidam com dados pessoais e na conscientização sobre a privacidade. De acordo com Braga e Oliveira (2020), "a implementação do GDPR aumentou a transparência e a responsabilidade no processamento de dados, fortaleceu a confiança dos consumidores nas organizações" (BRAGA; OLIVEIRA, 2020, p. 65).

As empresas tiveram que adaptar suas práticas de processamento de dados para cumprir com os requisitos do GDPR, o que envolveu a revisão de políticas de privacidade, a implementação de novas medidas de segurança e a realização de treinamentos para funcionários (BRAGA; OLIVEIRA, 2020). Embora esses ajustes iniciais tenham gerado um custo alto inicialmente, ainda assim muitos argumentam que a implantação dessas práticas proporcionou benefícios a longo prazo, como a mitigação de riscos e a melhoria da reputação.

Para o indivíduo, o GDPR trouxe maior controle sobre seus dados pessoais e aumentou a transparência das práticas de processamento de dados (ALMEIDA; SANTOS, 2018). Os indivíduos agora têm mais poder para questionar e entender como seus dados são usados, bem como poder para exercer seus direitos de privacidade de forma mais eficaz.

O GDPR representa um marco significativo na proteção de dados e na privacidade dos indivíduos na era digital. Ao estabelecer princípios claros e direitos robustos, o mesmo GDPR reforça a proteção dos dados pessoais e promove práticas responsáveis de processamento de dados. No entanto, a conformidade com o GDPR também apresenta desafiossignificativos para as organizações, que devem investir em medidas técnicas e organizacionais adequadas para garantir a proteção contínua dos dados pessoais.

2.5 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados - LGPD, também conhecida como Lei nº 13.853/2018, é uma legislação brasileira promulgada em 2018. A sua vigência, no entanto, começou apenas em agosto de 2020, e as sanções previstas passaram a valer em agosto de 2021 (BRASIL, 2018).

Seu propósito principal é regulamentar o tratamento de dados pessoais nas organizações, sejam elas públicas ou privadas. O mesmo intuito estabelece diretrizes claras para a coleta, para o armazenamento, para o processamento e o compartilhamento de informações pessoais de cidadãos brasileiros:

> A LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país no qual estejam localizados os dados, desde que a operação de tratamento de dados seja realizada no Brasil; a atividade de tratamento tem por objetivo a oferta de bens ou serviços ou o manejo de dados de indivíduos localizados no país; ou, ainda, que os dados pessoais objeto do tratamento tenham sido coletados em território nacional (BRASIL, 2018).

A LGPD visa a proteger a privacidade e os direitos dos indivíduos; garante a transparência nas operações que envolvem dados pessoais e impõe sanções em caso de violações. Ela concede aos titulares dos dados o direito de acessar, corrigir, eliminar ou retirar

seu consentimento em relação aos seus dados pessoais, bem como promove a nomeação de um encarregado de proteção de dados nas organizações. Os princípios fundamentais da LGPD estão expressos no art. 2º de acordo com a Tabela 2:

Tabela 2 - Princípios fundamentais da LGPD.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:	
I – O respeito à privacidade.	Respeitar a privacidade significa garantir que as informações pessoais de alguém (como dados financeiros, históricos médicos ou detalhes íntimos) sejam protegidas e não sejam divulgadas ou usadas sem consentimento. Isso inclui proteger a vida privada das pessoas de intrusões não autorizadas (DONEDA, 2006).
II – A autodeterminação informativa.	Autodeterminação informativa é o direito que as pessoas têm de controlar seus próprios dados pessoais. Isso quer dizer que cada pessoa deve ter a capacidade de decidir quais as suas informações que serão coletadas, como serão usadas e quem terá acesso a elas. Seria ter controle e transparência sobre os próprios dados (MENDES, 2019).
III – A liberdade de expressão, de informação, de comunicação e de opinião.	Isso significa que as pessoas têm o direito de se expressar livremente, de buscar, de receber e de compartilhar informações, de comunicar- se com os outros e ter suas próprias opiniões sem medo de censura ou represálias. Esta essência é a base de uma sociedade aberta e democrática em que todos podem participar do debate público (LEMOS; SOUZA, 2008).
IV - A inviolabilidade da intimidade, da honra e da imagem.	Este princípio protege a dignidade pessoal de cada indivíduo; ele garante que sua intimidade (aspectos mais privados da vida), sua honra (reputação e respeito) e sua imagem (como é visto pelos outros) sejam preservadas e não alvo de ataques injustos ou exposição indevida (MORAES, 2003).
V - O desenvolvimento econômico e tecnológico e a inovação.	Este item destaca a importância de promover o crescimento econômico, os avanços tecnológicos e a inovação. Isso significa incentivar a criação de novas tecnologias, de serviços e de produtos que possam melhorar a qualidade de vida, criar empregos e fomentar o progresso da sociedade (CARBONI, 2020).
VI - A livre iniciativa, a livre concorrência e a defesa do consumidor.	Esses princípios se referem à liberdade de empreender e criar negócios (livre iniciativa), competir de forma justa no mercado (livre concorrência) e proteger os consumidores contra práticas abusivas ou enganosas. Isso cria um ambiente econômico saudável e justo;

	beneficia tanto empresários, quanto consumidores (MARQUES, 2019).
VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	Este item enfatiza a importância de respeitar e de garantir os direitos humanos básicos; permite que cada pessoa possa desenvolver plenamente sua personalidade e viver com dignidade. Além disso, assegura que todos possam participar ativamente na sociedade, exercendo seus direitos e deveres como cidadãos (PIOVESAN, 2013).

Fonte: A própria autora, 2024,

A importância da LGPD para as organizações é multifacetada. Primeiramente, ela promove uma cultura de proteção de dados; incentiva as empresas a que implementem políticas robustas de segurança da informação. De acordo com Doneda (2020), a conformidade com a LGPD não é apenas uma exigência legal; é também uma oportunidade para que as empresas reforcem sua credibilidade e sua confiança com os clientes, os parceiros e os investidores.

A LGPD introduz o conceito de governança de dados, que se refere à administração e à supervisão das informações na organização. Esse aspecto é crucial, pois permite que as empresas otimizem processos internos, reduzam riscos de vazamentos e de fraudes e melhorarem a eficiência operacional (LEMOS; SOUZA, 2020). A implementação de práticas de governança de dados pode levar a uma maior agilidade na tomada de decisões e a um aprimoramento na gestão estratégica das informações.

Os impactos da LGPD também se refletem nos custos e na estrutura organizacional. As empresas precisam investir em tecnologias de segurança da informação, em capacitação de funcionários e, muitas vezes, na criação de novas funções, como a de Encarregado de Proteção de Dados (DPO). Segundo Carboni (2020), esses investimentos, embora inicialmente elevados, tendem a gerar benefícios a longo prazo, como a prevenção de multas e danos reputacionais. A conformidade com a LGPD também pode abrir novas oportunidades de negócios, especialmente em mercados que valorizam a proteção de dados.

A adaptação à LGPD implica um esforço contínuo de adequação e de monitoramento. As organizações devem realizar auditorias regulares, revisar políticas de privacidade e manter um diálogo constante com os titulares dos dados (MARQUES, 2019). Esse processo dinâmico de conformidade ajuda a criar uma base sólida para a inovação e o desenvolvimento tecnológico, ao mesmo tempo que assegura a proteção dos direitos dos indivíduos.

2.6 Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) é uma entidade fundamental no cenário de proteção de dados pessoais no Brasil. Foi estabelecida pela Lei Geral de Proteção de Dados Pessoais (LGPD) para supervisionar, regulamentar e fiscalizar as práticas de tratamento de dados no país.

A referida ANPD foi criada pela Lei no. 13.853, de 8 de julho de 2019, que alterou a LGPD (Lei no. 13.709/2018) para incluir a criação da autoridade. A instituição da ANPD foi vista como um passo crucial para garantir a implementação e o cumprimento eficaz da LGPD (BRASIL, 2019).

Segundo Doneda (2020), "a criação da ANPD representa um marco na regulação da privacidade e da proteção de dados no Brasil, similar às autoridades de proteção de dados existentes na União Europeia e em outros países" (DONEDA, 2020, p. 45). A ANPD é um órgão da administraçãopública federal, integrante da Presidência da República, com autonomia técnica e decisória, essencial para a efetiva aplicação das normas de proteção de dados.

A ANPD é composta por diversos órgãos internos, incluindo

01. **Conselho Diretor**: órgão máximo de deliberação colegiada, composto por cinco diretores, incluindo o Diretor-Presidente;
02. **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**: órgão consultivo, composto por representantes de diversos setores da sociedade, incluindo governo, setor empresarial, academia e sociedade civil;
03. **Ouvidoria**: órgão responsável por assegurar a transparência e a comunicação entre a ANPD e os cidadãos;
04. **Corregedoria**: órgão responsável por apurar infrações cometidas por servidores da ANPD;
05. **Unidades administrativas**: representações divididas em coordenações e diretorias responsáveis pela execução das atividades técnicas e administrativas da ANPD (BRASIL, 2019).

A ANPD possui um amplo espectro de funções e atribuições que visam a garantir a proteção dos dados pessoais e a privacidade dos titulares de dados no Brasil. Entre suas principais atribuições estão

Regulamentação: a ANPD é responsável por editar normas e procedimentos para a implementação da LGPD, bem como orientar e interpretar as disposições da lei; isso inclui a elaboração de regulamentos detalhados que explicam como os princípios e obrigações da LGPD devem ser aplicados na prática (BRASIL, 2019);

Fiscalização e Supervisão: a ANPD exerce o papel de fiscalização do cumprimento da LGPD por parte das organizações, realizando auditorias, requisição de relatórios de impacto à proteção de dados e outras medidas de controle; segundo Lima (2021), "a capacidade da ANPD de fiscalizar efetivamente as práticas de tratamento de dados é essencial para assegurar a conformidade com a LGPD" (LIMA, 2021, p. 92);

Aplicação de Sanções: a ANPD tem autoridade para aplicar sanções administrativas em casos de descumprimento da LGPD; as sanções podem variar de advertências a multas significativas, incluindo a suspensão parcial ou total do funcionamento de bancos de dados (BRASIL, 2019); Oliveira (2020) destaca que "a aplicação de sanções pela ANPD é uma ferramenta crucial para incentivar a conformidade e responsabilizar as organizações por violações" (OLIVEIRA, 2020, p. 110);

Promoção da Cultura de Proteção de Dados: a ANPD também desempenha um papel educativo – promove a conscientização sobre a importância da proteção de dados pessoais; isso inclui a realização de campanhas informativas, a promoção de boas práticas e a realização de eventos e seminários sobre o tema (BRASIL, 2019);

Cooperação Internacional: a ANPD busca colaborar com autoridades de proteção de dados de outros países e organismos internacionais para harmonizar normas e práticas de proteção de dados e facilitar a cooperação em casos transnacionais (BRASIL, 2019); de acordo com Santos (2021), "a cooperação internacional é fundamental para enfrentar os desafios globais da proteção de dados em um mundo cada vez mais interconectado" (SANTOS, 2021, p. 135);

Desafios Enfrentados pela ANPD: apesar de sua importância, a ANPD enfrenta diversos desafios que podem impactar sua eficácia na proteção de dados pessoais no Brasil;

Recursos e Autonomia: a ANPD foi inicialmente criada como um órgão vinculado à Presidência da República, o que gerou preocupações sobre sua autonomia financeira e administrativa; segundo Doneda (2020), "a independência da ANPD é crucial para garantir que ela possa atuar de maneira imparcial e eficiente, sem interferências políticas" (DONEDA, 2020, p. 50);

Capacidade Técnica e Infraestrutura: a construção da capacidade técnica e da infraestrutura necessária para desempenhar suas funções é outro desafio significativo; isso inclui a contratação de pessoal qualificado, a criação de sistemas de informação robustos e a implementação de processos eficazes de fiscalização e regulamentação (LIMA, 2021);

Educação e Conscientização: promover uma cultura de proteção de dados em um país com grandes desigualdades educacionais e digitais é um desafio considerável; a ANPD precisa desenvolver estratégias eficazes para alcançar diversos públicos e setores; ela garante que todos compreendam e cumpram a LGPD (SANTOS, 2021).

Desde sua criação, a ANPD tem desempenhado um papel crucial na promoção e na implementação da proteção de dados no Brasil. Sua atuação tem impactos significativos em diversas áreas.

A presença de uma autoridade de fiscalização como a ANPD incentiva as empresas a adotar práticas de conformidade com a LGPD, incluindo a implementação de políticas de privacidade, medidas de segurança e treinamentos para funcionários (OLIVEIRA, 2020). Isso não apenas ajuda a evitar sanções; também melhora a confiança dos consumidores e a reputação das empresas.

Para os consumidores, a ANPD oferece uma camada adicional de proteção e um mecanismo de recurso em casos de violação de dados pessoais. Isso fortalece os direitos dos indivíduos e aumenta a transparência das práticas de tratamento de dados (SILVA; SILVA, 2019).

A ANPD também tem um impacto significativo no ambiente regulatório brasileiro. Suas regulamentações e diretrizes ajudam a clarificar e a padronizar as práticas de proteção de dados; promove um ambiente de maior segurança jurídica e previsibilidade para todos os atores envolvidos (DONEDA, 2020).

A Autoridade Nacional de Proteção de Dados desempenha um papel essencial na garantia da proteção de dados pessoais no Brasil. Embora enfrente desafios significativos, sua atuação é crucial para a implementação eficaz da LGPD e para a promoção de uma cultura de privacidade e segurança. O sucesso da ANPD dependerá de sua capacidade de manter autonomia, de desenvolver capacidade técnica e de promover a conscientização pública sobre a importância da proteção de dados.

2.7 Indicadores Propostos nesta Dissertação

Os indicadores desempenham várias funções cruciais. Primeiramente, eles são utilizados para monitorar e controlar atividades e processos; garantem que atividades e processos estejam alinhados com os objetivos estabelecidos. Em segundo lugar, eles permitem a avaliação do desempenho; ajudam a identificar se as metas estão sendo atingidas e destacam áreas que necessitam de melhorias (Kaplan; Norton, 1996). Além disso, os indicadores fornecem dados essenciais para a tomada de decisões; facilitam escolhas estratégicas baseadas em evidências concretas (Parmenter, 2015). Com base no arcabouço teórico obtido na revisão da literatura, os indicadores propostos neste ensaio são:

Governança

A governança corporativa é um componente crucial para a gestão eficaz e eficiente das organizações, especialmente em um contexto de complexidade regulatória. Segundo Silva (2020), a governança corporativa pode ser definida como "um sistema pelo qual as empresas são dirigidas e controladas, envolvendo um conjunto de relações entre a administração, seu conselho, seus acionistas e outras partes interessadas". Essa definição enfatiza a importância de mecanismos que assegurem a transparência, a responsabilidade e a equidade nas práticas empresariais.

A Lei Geral de Proteção de Dados (LGPD), promulgada no Brasil em 2018, insere-se nesse cenário como uma peça fundamental que demanda das empresas a implementação de robustos sistemas de governança da informação. De acordo com Oliveira e Santos (2021), "a conformidade com a LGPD requer que as empresas estabeleçam políticas claras de proteção de dados, incluindo a nomeação de um encarregado de dados e a realização de avaliações

regulares de impacto sobre a privacidade". Essas exigências refletem a necessidade de uma estrutura de governança que não apenas cumpra os requisitos legais, mas que também promova uma cultura organizacional voltada à proteção dos dados pessoais.

Nesse contexto, a adoção de boas práticas de governança pode contribuir significativamente para a mitigação de riscos associados à privacidade e à segurança da informação. Conforme ressaltado por Almeida (2019), "uma governança da informação bem estruturada permite que as empresas não apenas evitem penalidades legais, mas também construam uma reputação de confiança junto aos seus clientes e parceiros". A governança corporativa, quando alinhada com os princípios da LGPD, oferece uma abordagem integrada que fortalece a resiliência organizacional frenteàs exigências regulatórias e às expectativas do mercado.

Conformidade Legal e Respeito aos Princípios

A conformidade legal e o respeito aos princípios constituem a base para a governança de dados. Segundo a Lei Geral de Proteção de Dados (LGPD), as organizações devem observar rigorosamente as disposições legais ao tratar dados pessoais; deve garantir que todas as atividades estejam em conformidade com a legislação aplicável. A aderência aos princípios da finalidade, da adequação, da necessidade e da segurança é essencial para evitar sanções e assegurar a proteção dos dados pessoais dos indivíduos (BRASIL, 2018).

Transparência e Direitos do Titular

A transparência é crucial para a construção de uma relação de confiança entre as organizações e os titulares dos dados. Conforme a LGPD, os titulares têm direito à informação clara e acessível sobre o tratamento de seus dados, incluindo a finalidade, os meios e a duração desse tratamento. Além disso, os titulares têm o direito de acessar, de corrigir e de eliminar seus dados pessoais; eles reforçariam o controle sobre suas informações pessoais (BRASIL, 2018). Essa transparência não só fortalece a confiança, mas também cumpre requisitos legais; promove uma gestão de dados ética e responsável (NIST, 2020).

Rastreabilidade

A rastreabilidade refere-se à capacidade de acompanhar a trajetória dos dados desde a sua coleta até seu descarte. Este princípio é fundamental para garantir a integridade e a segurança dos dados; permite a identificação de possíveis pontos de vulnerabilidade ou

incidentes de segurança ao longo do ciclo de vida dos dados. Implementar mecanismos de rastreabilidade efetivos é uma prática recomendada pelas diretrizes do *National Institute of Standards and Technology* - NIST, que enfatiza a importância de registros detalhados e auditáveis para a governança de dados (NIST, 2020).

Adequação de Contratos e de Relações com Parceiros

A adequação dos contratos e das relações com parceiros comerciais é um aspecto crítico da governança de dados. As organizações devem garantir que todos os contratos de prestação de serviços ou parcerias incluam cláusulas específicas sobre a proteção de dados, assegurem que os parceiros também estejam em conformidade com a LGPD. A revisão e a atualização periódica desses contratos são necessárias para acompanhar mudanças regulatórias e tecnológicas, para minimizar riscos de exposição indevida de dados pessoais (BRASIL, 2018).

Segurança da Informação

A segurança da informação é um dos pilares da proteção de dados. As organizações devem implementar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, contra destruição, contra perda, contra alteração ou qualquer forma de tratamento inadequado ou ilícito. Segundo as diretrizes do NIST, um programa robusto de segurança da informação deve incluir controles de acesso, criptografia, monitoramento contínuo e respostas a incidentes para prevenir e mitigar riscos (NIST, 2020).

Gestão da Violação de Dados

A gestão de violações de dados é um aspecto crucial na governança de dados. As organizações devem estar preparadas para detectar, para responder e notificar violações de dados de forma eficaz. A LGPD exige que, em caso de violação, as autoridades competentes e os titulares sejam notificados prontamente, detalhando a natureza da violação, os dados comprometidos e as medidas adotadas para mitigar os efeitos do incidente (BRASIL, 2018). Uma resposta rápida e transparente a violações de dados pode minimizar danos e preservar a confiança dos titulares de dados.

Esses princípios não só asseguram o cumprimento das obrigações legais, como também promovem a confiança dos titulares de dados e fortalecem a reputação das organizações.

CAPITULO III

3. METODOLOGIA

Os principais métodos utilizados nesta pesquisa foram o levantamento de dados, a pesquisa bibliográfica e o *Design Science Research*. Estes são os recursos para a elaboração do arcabouço teórico e do artefato.

A metodologia de uma pesquisa é definida como o conjunto de estratégias e procedimentos sistemáticos utilizados para alcançar os objetivos propostos e responder às questões de investigação. De acordo com Gil (2010), a metodologia consiste em um planejamento detalhado que orienta o pesquisador na escolha das técnicas mais adequadas para a coleta, para a análise e a interpretação dos dados. Isto garante o rigor científico e a validade dos resultados. É o essencial para assegurar a confiabilidade e a coerência dos resultados. É o que possibilita a análise rigorosa e fundamentada em relação ao tema abordado.

Essa pesquisa teve como base a análise descritiva, que é uma abordagem que busca descrever as características de determinado fenômeno ou população, sem, no entanto, estabelecer relações de causa e efeito. Segundo Gil (2010), a pesquisa descritiva tem como principal objetivo observar, registrar, analisar e correlacionar fatos ou fenômenos sem os manipular. Essa abordagem é amplamente utilizada para estudar variáveis em seu estado natural, pois proporciona uma visão detalhada e sistemática dos aspectos investigados. Dessa forma, a análise descritiva fundamenta-se na coleta rigorosa de dados e na sua interpretação criteriosa e, deste modo, assevera a fidelidade das informações apresentadas.

3.1 Levantamento bibliográfico e indicadores

A metodologia utilizada nesta dissertação, iniciou-se com um levantamento bibliográfico de artigos, livros, revistas e sites relacionados ao tema LGPD, com o intuito de conhecer o nível de implantação e maturidade do assunto nas organizações. A bibliografia relacionada ao tema serviu como fundamentação teórica, agregando valor à pesquisa e contribuindo para o desenvolvimento do *framework* que auxiliou no projeto de pesquisa.

Após identificar e selecionar fontes relevantes sobre a LGPD, foram desenvolvidos os indicadores de conformidade, um conjunto deles para medir o nível de conformidade das

empresas com a LGPD. A criação desses indicadores foi baseada em referências normativas, guias de melhores práticas e consultas a especialistas. São eles

- Governança;
- Conformidade legal e respeito aos princípios;
- Transparência e direitos do titular;
- Rastreabilidade;
- Adequação de contratos e de relações com parceiros;
- Segurança da informação;
- Violação de dados.

Após a elaboração inicial, os indicadoresforam validados e refinados por meio de consultas a profissionais da área. Foram, então, consultados dois profissionais que trabalham na área de Segurança da Informação e um DPO (*Data Protection Officer*). Segue a experiência dos especialistas de validação via quadro sintetizador, ver Quadro 1.

Quadro 1 - Experiência dos especialistas.

Profissional	Área de Atuação	Início na Área	Posição Atual	Responsabilidades
Profissional de Direito	Direito	2011	DPO (Data Protection Officer)	Consultoria e implantação da LGPD nas empresas.
Profissional de Tecnologia 2	Segurança da Informação	2020	Administrador de Datacenter	Administração e manutenção de datacenters.
Profissional de Tecnologia 1	Segurança da Informação	2021	Analista de Governança em Segurança da Informação	Gestão e governança em segurança da informação.

Fonte: Autoria Própria, 2024.

Os indicadores apresentados visam a avaliar o nível de adequação de um processo, sistema ou organização a um determinado padrão ou requisito de acordo com a Tabela 3.

Tabela 3 - Adequação de processo.

Indicadores de desempenho	Nível de adequação	Índice de adequação
Não	0 a 0,9	Inicial
Baixo	1,0 a 1,9	Básico
Médio	2,0 a 2,9	Intermediário
Alto	3,0 a 3,9	Aprimoramento
Completo	4	Completo
Fórmula de cálculo de Média Aritmética	$MA = (n1 + n2 + n3 + n4 + n5)/5$	

Fonte: Autoria Própria, 2024.

Nível de Adequação: define a etapa em que o processo se encontra, desde o início até a completa adequação.

Índice de Adequação: um valor numérico que quantifica o nível de adequação; variando de 0 a 4, facilita a comparação e a interpretação de dados; a divisão em faixas numéricas e a correspondência com níveis de adequação (inicial, básico, intermediário, aprimoramento e completo) tornam a avaliação mais intuitiva.

Fórmula da Média Aritmética: é utilizada para calcular a média do índice de adequação de diferentes itens ou processos; a fórmula da média aritmética é simples e eficaz para calcular um valor representativo do índice de adequação de um conjunto de itens; ao calcular a média, é possível obter uma visão geral do desempenho global.

O valor da média é uma métrica importante para avaliar o estágio de adequação dos processos. Uma média próxima de 0 indica que, em geral, os processos estão em um estágio inicial de adequação, ou seja, há uma necessidade significativa de melhorias e ajustes. Por outro lado, uma média próxima de 4 sugere que os processos estão altamente adequados, o que reflete um nível avançado de maturidade. Valores intermediários indicam diferentes níveis de maturidade;

eles permitem identificar áreas específicas que podem precisar de mais atenção para alcançar uma maior eficiência.

O desvio padrão é outra métrica importante que indica a dispersão dos dados em torno da média. Um alto desvio padrão significa que os processos apresentam grande variabilidade em termos de adequação, o que pode sinalizar inconsistências ou a necessidade de ajustes para garantir uma maior uniformidade nos resultados.

Ao analisar a distribuição dos valores por faixa de índice de adequação, é possível identificar tanto os pontos fortes, quanto os fracos do processo. Por exemplo, se a maioria dos valores estiver concentrada na faixa "básico", isso pode indicar que há um grande potencial de melhoria e que é necessário investir em aperfeiçoamentos para alcançar níveis mais avançados de adequação.

Ao analisar o valor da média e o desvio padrão, foi fundamental considerar também o porte da empresa para compreender melhor os vieses presentes nos resultados. Empresas de diferentes portes tendem a ter características e necessidades distintas, o que pode influenciar a forma como os processos são avaliados e como a maturidade é alcançada.

Em empresas de menor porte, os processos podem estar mais centralizados e, consequentemente, podem estar em um estágio inicial de adequação, o que refletiria uma média mais próxima de 0. Por outro lado, em empresas de maior porte, é possível que os processos estejam mais desenvolvidos e adaptados a uma estrutura complexa, o que pode levar a uma média mais próxima de 4. Isto indicaria processos altamente adequados.

Grandes empresas, porém, podem ter áreas ou processos específicos que necessitam de melhorias, o que pode ser identificado por meio de valores intermediários ou até mesmo por um desvio padrão alto. O fato sinaliza variações significativas na adequação entre diferentes departamentos ou unidades.

3.2 O artefato

Foi criada uma ferramenta digital ou artefato para coletar dados e auxiliar a pesquisa junto às empresas. O mesmo instrumento ainda permitiu que os dados fossem analisados. Assim, tornou-se possível saber em qual nível de maturidade está a implantação da LGPD nas

empresas. O método utilizado para conduzir a criação do artefato foi o *Design Science Research*.

O método *Design Science Research* (DSR) consiste em construir artefatos. *Design Science Research* (DSR) é um enfoque sistemático voltado à criação e à avaliação de artefatos projetados para resolver problemas identificados e melhorar o entendimento das questões em estudo. Ele tem ainda como propósito aprofundar a análise sobre a importância da caracterização de Classes de Problemas e sobre a tipologia global de artefatos. O intuito é poder explorar e conduzir pesquisas na Ciência do *Design Research*, visando a fortalecer a avaliação dos artefatos e, consequentemente, o conhecimento produzido (Lacerda et al, 2013).

O processo de DSR pode ser dividido em várias fases fundamentais: identificação do problema, definição dos objetivos da solução, *design* e desenvolvimento, demonstração, avaliação e comunicação (DRESCH, LACERDA & ANTUNES, 2015). Cada uma dessas fases é crucial para garantir que o artefato resultante não só resolva o problema identificado, mas também contribua para o corpo de conhecimento científico existente.

Segundo Dresch *et al*. (2015), o DSR se distingue por seu compromisso com a dualidade entre o rigor acadêmico e a relevância prática. Ele promove a construção e a avaliação de artefatos inovadores e utilitários, como modelos, métodos, instâncias, e teorias que abordam problemas complexos no contexto da engenharia de produção. Esse método envolve um ciclo iterativo de construção, de avaliação e de comunicação dos resultados. Nele, cada etapa é rigorosamente documentada e analisada para assegurar tanto a validade, quanto a aplicabilidade dos resultados.

Abaixo, seguem as etapas referidas e suas respectivas responsabilidades. As fases acontecem em número de seis.

01 **Identificação do Problema**: esta fase inicial envolve a identificação e a descrição detalhada do problema que será abordado. É fundamental compreender o contexto e os requisitos do problema para assegurar que o artefato projetado seja relevante e aplicável.

02 **Definição dos Objetivos da Solução:** após identificar o problema, define-se o que a solução deve alcançar; estes objetivos devem ser claros, mensuráveis e alinhados com as necessidades do contexto de aplicação.

03 ***Design* e Desenvolvimento:** nesta fase, o artefato é projetado e desenvolvido; isto pode incluir a criação de novos modelos e métodos e sistemas ou processos que irão atender aos objetivos definidos anteriormente.

04 **Demonstração:** o artefato é então demonstrado em um contexto real ou simulado; o intuito é verificar sua funcionalidade e sua eficácia na resolução do problema identificado.

05 **Avaliação:** a avaliação rigorosa do artefato é essencial para determinar se ele atende aos objetivos da solução e se identifica as melhorias (quaisquer melhorias) necessárias; este passo pode envolver uma série de métodos de avaliação, incluindo testes experimentais, estudos de caso e simulações.

06 **Comunicação:** finalmente, os resultados do DSR, incluindo o artefato desenvolvido e os *insights* obtidos durante o processo, são levados à comunidade científica e aos praticantes da área; esta comunicação é fundamental para garantir que os conhecimentos adquiridos possam ser utilizados e validados por outros.

De acordo com Lacerda, Dresch e Antunes (2013), o DSR não tem apenas o seu foco na criação de soluções práticas. Ele também busca contribuir para o conhecimento teórico por meio da formulação de novas teorias ou da extensão de teorias existentes. O papel do pesquisador no DSR é, portanto, duplo: solucionador de problemas práticos e contribuidor para a literatura científica.

O metódo do *Design Science Research*, portanto, representa uma abordagem robusta e iterativa. Ela facilita a criação de artefatos que são tanto inovadores, quanto cientificamente sólidos. Atendendo as necessidades práticas, ele promove o avanço do conhecimento teórico (DRESCH *et al*., 2015; LACERDA, DRESCH & ANTUNES, 2013).

3.2.1 - Etapas para desenvolvimento do artefato do projeto de acordo com o DSR 01 Identificação do Problema

Foram realizadas reuniões com os especialistas em LGPD (Quadro 1), para garantir que todas as expectativas e requisitos sejam compreendidos e documentados.

Em seguida, foram identificados os objetivos do artefato, as funcionalidades principais e os requisitos específicos do cliente. Dessa forma, garantiu-se a necessidade de profissionais das áreas de Segurança da Informação e do Direito.

02 Definição dos Objetivos da Solução

Realizou-se entrevistas com os especialistas e *stakeholders*. Em seguida, foram realizadas as análises de documentos para identificar os requisitos necessários.

Assim, permitiu-se coletar e documentar todos os requisitos do sistema. Isso inclui requisitos funcionais (o que o sistema deve fazer) e requisitos não funcionais (como desempenho, segurança, usabilidade etc.).

Os requisitos foram detalhados e documentados de forma clara e concisa. Isso inclui a descrição de cada requisito, seus critérios de aceitação, de dependências e restrições.

Utilizou-se uma linguagem clara e objetiva para evitar ambiguidades e garantir que todos os envolvidos no projeto entendam os requisitos da mesma forma.

Desta forma, definiu-se o objetivo do artefato.

03 *Design* e Desenvolvimento

Para o desenvolvimento do artefato foi utilizado o *Firebase* para o *backend* e o armazenamento de dados. Trata-se de plataforma de desenvolvimento de aplicativos que oferecem serviços de banco de dados em tempo real, autenticação, hospedagem e funções em nuvem, o que proporciona uma solução escalável e segura para a aplicação.

A linguagem de programação principal para o desenvolvimento foi *JavaScript*, complementada por *TypeScript*. O *hardware* utilizado para desenvolvimento incluiu computadores pessoais com sistemas operacionais *Windows*, competência capaz de executar ambientes de desenvolvimento integrados (IDEs), como *Visual Studio Code*, além de suportar emuladores e dispositivos físicos para testes.

O artefato foi instalado no domínio *http://applgpd.com.br* e disponibilizado para o público em geral. Nesta primeira fase, o *site* contém somente o aplicativo para a coleta de dados e a indicação do nível de maturidade. Na segunda fase, porém, apresentar-se-ão os dados coletados da pesquisa.

O artefato desenvolvido foi fundamental na coleta de dados necessários para embasar a dissertação. Ao fornecer uma estrutura sistemática para avaliar o nível de maturidade da LGPD nas empresas, esse artefato permitiu a coleta de informações precisas e relevantes sobre as práticas de proteção de dados em diferentes organizações. Esses dados foram essenciais para analisar o estado atual da conformidade dentro das organizações e, então, identificar tendências

e lacunas comuns e *indicar insights* valiosos para a dissertação. A utilização desse artefato, auxiliou na obtenção de uma visão abrangente e fundamentada sobre o panorama da conformidade com a LGPD nas empresas. Ela contribuiu significativamente para o avanço do conhecimento nessa área.

04 Demonstração

Foram coletadas cento e vinte e três respostas, no período de vinte e dois de novembro a vinte nove de novembro de 2024. Com o objetivo de analisar os resultados obtidos, foram consideradas oitenta e uma respostas que atendiam todos os requisitos da pesquisa, fornecendo uma interpretação que reflete o grau de conformidade das empresas. A análise dos resultados permitiu identificar pontos fortes e áreas críticas no processo de implementação. Ainda ofereceu *insights* para as empresas que buscam melhorar a gestão da privacidade e a proteção de dados pessoais.

05 Avaliação

A avaliação do artefato foi realizada por especialistas, incluindo profissionais da área de Segurança da Informação e um DPO *(Data Protection Officer*). Foram utilizados testes experimentais para verificar sua conformidade com os objetivos inicialmente estabelecidos. Esse processo possibilitou identificar oportunidades de melhoria e ajustes necessários para que o artefato atendesse plenamente aos requisitos propostos.

06 Comunicação

Os resultados da pesquisa foram divulgados a comunidade cientifica por meio desta dissertação que ficará disponível na página do PPGEP na Internet e no Repositório Digital da UNIP, além das publicações realizadas durante o desenvolvimento deste mestrado:

Artigo cientifico: *How do consultants understand the privacy of personal data in Brazilian financial institutions?* Submetido ao periodico Contemporary Economics e em fase revisão final de acordo com as exigências do periodico

Artigo científico: *Digital Innovation through LGPD Compliance* aceito e será apresentado no *22nd AIMS International Conference on Management* em janeiro de 2025.

CAPÍTULO IV

4. Análise e discussão de resultados

Para avaliar a adesão das empresas à LGPD, foi realizada uma pesquisa com profissionais que estão atuando nas organizações para analisar os diferentes estágios de implementação da LGPD. A amostra foi escolhida por acessibilidade ou conveniência, e segundo Schiffman e Kanuk (2000), uma amostra por conveniência é um tipo de amostragem não probabilística em que os elementos são selecionados com base em sua disponibilidade ou pela facilidade de acesso ao pesquisador.Esse método é amplamente utilizado quando há restrições de tempo, recursos ou quando não é possível determinar com precisão uma população-alvo. Foi desenvolvida uma *framework* para a coleta dessas respostas que foram classificadas em cinco categorias: “Não”, "Baixo", "Médio", "Alto" e "Completo", cada uma representando um grau diferente de adequação às exigências da LGPD.

A tabela do Anexo 1 organiza as respostas em níveis de conformidade e permite análise detalhada das práticas de privacidade e segurança. A análise desses dados já foi realizada detalhadamente para cada pergunta. A Tabela 4 apresenta a estatística descritiva das repostas.

Tabela 4 - Análise estatística descritiva das respostas.

Questões	Total de respostas	Média	Mediana	Desvio Padrão	Míniimo	Máximo
resposta1	81	16,2	19	6,87	5	23
resposta2	81	16,2	14	9,34	6	31
resposta3	81	16,2	17	5,12	10	22
resposta4	81	16,2	17	6,18	6	22
resposta5	81	16,2	16	4,49	10	21
resposta6	81	16,2	17	3,7	10	20
resposta7	81	16,2	16	6,76	9	23
resposta8	81	16,2	15	6,1	8	24
resposta9	81	16,2	14	4,49	12	22
resposta10	81	16,2	15	5,76	10	24
resposta11	81	16,2	17	7,46	5	25
resposta12	80	16	16	4,53	11	21
resposta13	80	16	18	5,43	8	21
resposta14	76	15,2	16	6,18	5	21

resposta15	73	14,6	15	4,56	10	20
resposta16	74	14,8	14	4,6	10	22
resposta17	74	14,8	17	3,77	9	18
resposta18	72	14,4	15	3,29	11	18
resposta19	71	14,2	13	6,91	7	24
resposta20	71	14,2	14	5,93	8	22
resposta21	71	14,2	15	4,32	7	18
resposta22	70	14	16	3,24	10	17
resposta23	70	14	15	4,47	8	19
resposta24	68	13,6	13	1,82	12	16
resposta25	67	13,4	12	3,36	11	19
resposta26	65	13	13	2,55	10	17
resposta27	64	12,8	14	2,77	8	15
resposta28	63	12,6	12	2,88	9	16
resposta29	63	12,6	14	1,95	10	14
resposta30	63	12,6	10	5,77	7	21

Fonte : Autoria própria, 2024.

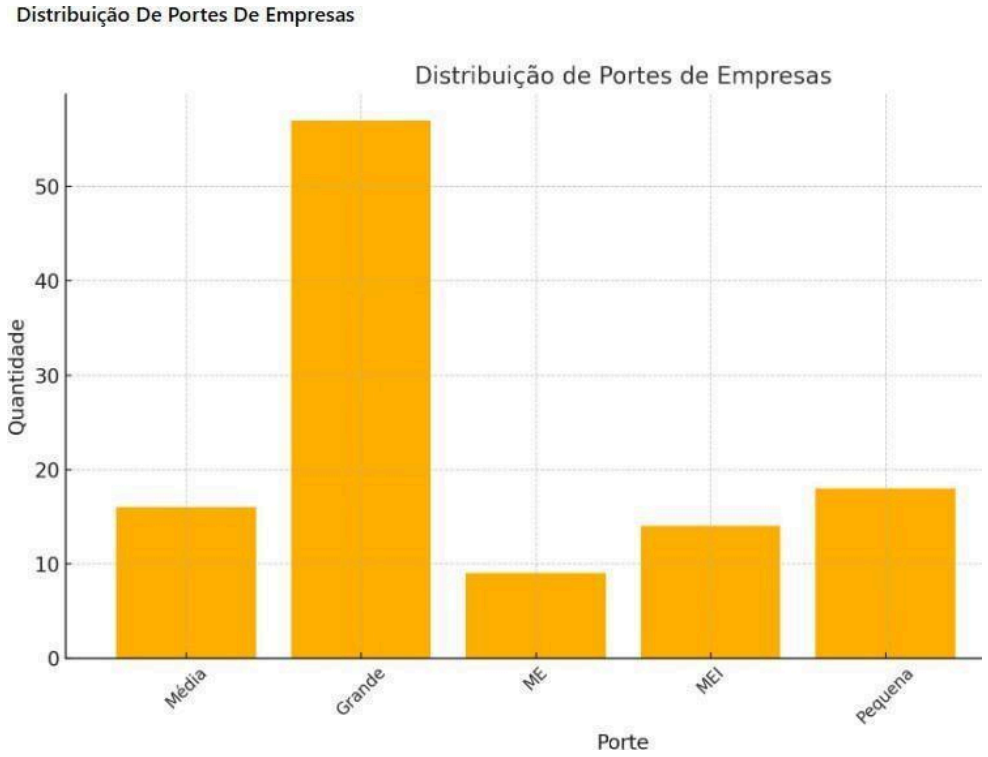
A análise global sobre a implementação da LGPD nas empresas revela progressos significativos em governança e consentimento, com destaque para altos níveis de comprometimento e boas práticas. Áreas, no entanto, como monitoramento, capacitação e segurança da informação, ainda apresentam lacunas relevantes, refletidas em baixos índices de conformidade.

Há necessidade de melhorias no rastreamento de dados, na notificação de violações e no treinamento regular de colaboradores. Apesar dos avanços, investimentos direcionados nessas áreas críticas são essenciais para fortalecer a proteção de dados pessoais e consolidar a conformidade com a legislação.

4.1 Porte da empresa

Ao analisar a distribuição dos valores por faixa de índice de adequação, é importante levar em consideração o porte da empresa, pois empresas de diferentes tamanhos podem ter realidades muito distintas. E mais: o que pode ser considerado uma alta adequação para uma empresa de pequeno porte pode não ser o suficiente para uma empresa maior, pois ela tem mais recursos e processos mais complexos. Assim, ao identificar áreas que precisam de mais atenção, é preciso contextualizar o porte da empresa para entender a especificidade de adequação dos processos. O Gráfico 1 apresenta o porte das empresas pesquisadas:

Gráfico 1 - Porte das empresas.



Fonte: Autoria própria, 2024.

Os dados coletados mostram que a análise das respostas pode ter um viés, considerando que estão distribuídos entre grandes, médias, pequenas, microempresas e MEIs, devido à desigualdade na representação dos diferentes portes.

Com 50 empresas grandes, 14 médias e pequenas e apenas 10 microempresas e 10 MEIs, há um risco de que as empresas maiores, com processos mais estruturados, dominem os resultados, inflacionando a média de adequação. As microempresas e MEIs, por sua vez, tendem a ter processos mais informais ou em estágios iniciais de maturação. Assim, o fato pode resultar em uma subestimação de suas necessidades de adequação e distorcer a percepção global da amostra.

Além disso, o desvio padrão pode ser impactado pelo porte das empresas, uma vez que as grandes empresas geralmente apresentam processos mais estáveis e com menor variabilidade. Já as microempresas e MEIs, com características mais diversificadas, podem mostrar uma maior dispersão nos dados.

4.2 A implementação da LGPD na empresa

Sobre a implementação da LGPD, nota-se que as empresas estão em um nível médio de implementação. A dispersão dos dados aponta para uma grande diferença entre as empresas, com algumas mais avançadas e outras ainda começando a se ajustar. Em média, 50% das empresas obtiveram uma pontuação de 19 ou mais na Média. Em outras palavras, metade das empresas já avançaram consideravelmente em suas experiências de adesão e adequação à LGPD.

O valor elevado do desvio padrão de 6,87, que reflete grande dispersão dos dados, indica que as empresas estudadas estão em diferentes estágios de maturidade em relação à LGPD. Elas variam em diversos aspectos, como porte, setor de atuação, de investimento em tecnologia e de cultura organizacional. Isso é confirmado pela grande variabilidade dos dados, com o valor mínimo sendo 5,00 e o máximo, 23,00 em termos de amplitude. Algumas empresas estão no início da implementação da LGPD. Outras já realizam operações de um programa de privacidade muito mais maduro.

4.3 A empresa possui um setor específico responsável para implementar e monitorar as diretrizes da LGPD

A média 16,20 implica que existe um departamento ou uma divisão dentro da empresa responsável pela implementação e acompanhamento das diretrizes da LGPD. Embora a média seja relativamente alta, também é imperativo observar a dispersão dos dados para estabelecer se a grande maioria das empresas possui uma hierarquia de estrutura burocrática e, assim, não consegue cumprir a LGPD.

Com o coeficiente da mediana sendo 14,00, pode-se notar que, embora a média tenha sido 16,20, a média indicada tem muitas respostas da parte inferior da distribuição das frequências de resposta. O fato sugere que muitas empresas não instalaram um departamento exclusivo para o propósito da implementação de licenciamento, uma vez que, por definição, a mediana é menor que a média.

O desvio padrão 9,34 deve ter um valor próximo de zero para sugerir que a população é homogênea. Neste caso, com o desvio padrão igual a 9,34, mostra-se que as respostas estão bastante espalhadas. Nelas, alguns respondentes afirmam ter departamentos específicos dedicados à adoção e ao monitoramento da LGPD. Outros, contudo, podem não ter nenhum

departamento para esse propósito. O grande desvio padrão pode indicar um alto nível de não uniformidade em termos de conformidade das práticas empresariais.

4.4 Análise sobre adoção de boas práticas de governança em privacidade de dados

Para analisar esse cenário, a coleta de dados evidenciou que uma média de 16,20 indica que as empresas apresentam um nível relativamente elevado de conformidade em governança de privacidade de dados. Há no caso, entretanto, limitações, evidenciadas pela diferença em relação à mediana (17,00). Enquanto a mediana sugere que a maior parte das organizações está alinhada às boas práticas, a discrepância entre os dois indicadores revela a existência de empresas com níveis menos desenvolvidos. Cria-se, assim, um cenário de maturidade variada na implementação de políticas de proteção de dados.

O desvio padrão de 5,12 aponta para uma maior homogeneidade nas práticas, indicando que as organizações estão convergindo para padrões mais consistentes de governança. Contudo, os valores extremos (mínimo de 10,00 e máximo de 22,00) destacam disparidades: algumas empresas ainda possuem práticas incipientes; simultaneamente, outras adotam políticas robustas e eficazes. Esses resultados sugerem progresso geral, mas ressaltam a necessidade de esforços para reduzir as desigualdades entre as empresas em relação à proteção de dados pessoais.

4.5 Setores envolvidos no tratamento de dados pessoais em seu Programa de Proteção de Dados

A pesquisa indica que, na maioria das empresas, há um entendimento da importância de definir as responsabilidades de cada setor em relação à proteção de dados. A média, neste caso, é de 16,20. No entanto, ela – a média – evidencia que há espaço para aprimorar a clareza e a formalização dessas obrigações, garantindo uma gestão mais eficiente e em conformidade com a LGPD.

A mediana de 17,00 reforça essa percepção. Destaca que a maior parte das empresas adota práticas alinhadas a boas diretrizes de governança, embora ainda haja diferenças sutis na maturidade das abordagens adotadas. Por outro lado, o desvio padrão relativamentealto (6,18)

reflete uma dispersão considerável nas práticas empresariais, com organizações variando de estruturas bem definidas a processos vagos ou inexistentes.

Essa heterogeneidade é confirmada pelos valores extremos. Enquanto o mínimo de 6,00 evidencia empresas com pouca ou nenhuma especificação de responsabilidades, o máximo de 22,00 aponta para aquelas com estruturas robustas e detalhadas. Esses dados mostram um cenário desigual, no qual algumas empresas lideram com boas práticas. Outras, na sua vez, permanecem em estágios iniciais de conformidade.

4.6 Capacitações e treinamentos sobre a proteção de dados pessoais

A análise dos dados sobre treinamentos em proteção de dados pessoais revela um panorama de implementação relativamente avançado entre as empresas. A média de 16,20 reflete um nível significativo de adesão a práticas de capacitação; indica que muitas organizações realizam treinamentos regularmente.

Essa média, contudo, sugere que, apesar da frequência dessas iniciativas, pode haver lacunas na abrangência dos conteúdos abordados ou na regularidade dos intervalos, o que limita a efetividade completa dessas ações. A proximidade entre a média e a mediana (16,00) reforça que a maioria das empresas apresenta uma distribuição equilibrada no engajamento dos funcionários, com práticas consistentes de treinamento.

Por outro lado, o desvio padrão de 4,49 aponta que, embora exista certa uniformidade, há variações importantes nas práticas de treinamento entre as organizações. Os valores extremos evidenciam essa disparidade: o mínimo de 10,00 destaca empresas com iniciativas insuficientes ou pouco priorizadas; o máximo de 21,00 mostra organizações que possuem sistemas robustos e bem estruturados, que cobrem amplamente as necessidades de capacitação.

Esse contraste demonstra um progresso significativo no geral, mas ressalta a necessidade de maior padronização na qualidade e na frequência dos treinamentos. É preciso garantir maior alinhamento às melhores práticas em proteção de dados.

4.7 A sua empresa tem responsáveis pelo tratamento de dados que facilitam a comunicação rápida e acessível sobre questões relacionadas à LGPD?

O panorama da comunicação corporativa sobre questões relacionadas à LGPD mostra um nível moderado de eficácia, conforme indicado pela média aritmética de 16,20. Esse valor demonstra que muitas empresas já adotam práticas eficazes de comunicação, embora ainda exista margem para melhorias, especialmente em termos de acessibilidade e agilidade nas interações.

A mediana de 17,00, ligeiramente superior à média, reforça a percepção de que a maioria das organizações possui práticas estruturadas e razoavelmente eficazes, indicando uma tendência positiva em direção a uma comunicação mais adequada e alinhada aos princípios da LGPD. O desvio padrão de 3,70 reflete uma homogeneidade nas práticas de comunicação entre as empresas; sugere que elas adotam estratégias similares, como designação clara de responsáveis e respostas rápidas e eficientes para questões relacionadas à LGPD.

No entanto, os valores – mínimo (10,00) e máximo (20,00) – evidenciam disparidades. Enquanto o valor mínimo revela a ausência de práticas claras em algumas empresas, o valor máximo indica a existência de organizações com estratégias altamente eficazes e bem implementadas. O fato demonstra um alto nível de maturidade organizacional em termos de conformidade e de comunicação sobre proteção de dados.

4.8 Comprometimento com o tratamento de dados coletados e sua privacidade

A análise dos dados revela que a média aritmética de 16,20 reflete um nível moderado de comprometimento das empresas com a privacidade de dados e a conformidade com a LGPD. Esse valor sugere que, embora muitas organizações adotem práticas adequadas de proteção de dados, a consistência dessas práticas pode variar entre áreas e departamentos, e isto aponta espaço significativo para melhorias. A mediana de 16,00, próxima à média, reforça que a percepção geral dos respondentes é de um comprometimento moderado, com uma avaliação equilibrada das práticas, sem extremos marcantes nas respostas.

O desvio padrão de 6,76 indica uma considerável variação nas percepções; reflete que a conformidade com a LGPD e o comprometimento com a privacidade não são tratados de

maneira uniforme. Essa discrepância pode ocorrer entre diferentes setores ou até mesmo no interior de um mesmo departamento.

Os valores extremos, mínimo de 9,00 e máximo de 23,00, mostram que algumas empresas apresentam níveis insatisfatórios de comprometimento, com ausência de políticas claras ou medidas adequadas. Outras demonstram maturidade organizacional elevada, adotando práticas exemplares de proteção e governança de dados pessoais. Esses indicadores apontam para a necessidade de esforços mais consistentes para garantir a uniformidade e a eficácia das práticas em toda a organização.

4.9 A sua empresa mapeia os dados pessoais em tratamento e estabelece procedimentos que respeitam os princípios legais da LGPD

As empresas tem-se comprometido com a privacidade de dados e a conformidade com a LGPD tem se tornado uma prioridade crescente no cenário corporativo, mas ainda apresenta desafios variados. A média aritmética de 16,20 aponta para um nível moderado de engajamento; sugere que muitas empresas adotam práticas adequadas, embora essas iniciativas possam não ser consistentes em todas as áreas e departamentos.

Ainda há uma margem considerável para melhorias, especialmente na uniformidade e no alcance das políticas de proteção de dados. A mediana de 16,00, próxima à média, indica uma percepção geral equilibrada entre os respondentes, com a maioria avaliando o comprometimento como moderado, sem grandes extremos ou distorções nas respostas.

Apesar desse panorama geral, a análise do desvio padrão e dos valores extremos revela diferenças significativas no tratamento da privacidade de dados entre as empresas. O desvio padrão de 6,76, relativamente alto, reflete uma disparidade marcante na percepção dos respondentes, com algumas áreas ou setores demonstrando práticas estruturadas e outras enfrentando dificuldades importantes.

Essa heterogeneidade é corroborada pelos valores mínimo (9,00) e máximo (23,00), que mostram um contraste entre empresas com práticas insatisfatórias e outras que alcançam um alto nível de maturidade em governança de dados. Isso evidencia um progresso notável em algumas organizações, mas também a necessidade de maior uniformidade e consistência nas políticas de privacidade e proteção de dados.

4.10 Realização de monitoramento regular das práticas de privacidade de dados

O monitoramento das práticas de privacidade de dados nas empresas é um elemento essencial para a conformidade com a LGPD, e os dados analisados refletem um desempenho moderado nesse aspecto. A média de 16,20 sugere que existe um esforço perceptível na supervisão das políticas e práticas de proteção de dados, mas ainda distante de um nível elevado de excelência. Esse número indica uma percepção positiva, mas aponta para a necessidade de maior rigor e consistência nas atividades de monitoramento.

A mediana de 14,00, inferior à média, revela uma assimetria na distribuição das respostas. Ela indica uma parcela significativa dos colaboradores avalia negativamente o monitoramento; destaca a necessidade de tornar os processos mais robustos e eficazes.

O desvio padrão de 4,49, relativamente elevado, evidencia uma disparidade considerável nas percepções dos respondentes. Isso sugere que o monitoramento é realizado de forma desigual entre diferentes departamentos ou níveis hierárquicos, ou ainda que sua eficácia não é igualmente reconhecida por todos.

Os valores extremos reforçam essa discrepância. O mínimo de 12,00 reflete empresas com monitoramento insuficiente ou irregular. Já o máximo de 22,00 indica organizações que adotam práticas robustas, como auditorias regulares e revisões contínuas, garantindo a consistência na proteção de dados. Esses resultados mostram avanços significativos em algumas empresas, mas ressaltam a necessidade de maior uniformidade nos processos de monitoramento.

4.11 Processo de conscientização das áreas envolvidas na coleta e o tratamento de dados

Garantir o consentimento do titular para a coleta e o tratamento de dados é um princípio central da conformidade com a LGPD, e os dados analisados indicam avanços e desafios nesse processo. A média de 16,20 revela que as empresas possuem um nível razoável de conscientização sobre essa exigência; reflete esforços para atender as normas, embora a implementação não seja igualmente eficaz em todas as áreas da organização.

A mediana de 15,00, ligeiramente inferior à média, aponta para percepções mais críticas por parte de alguns respondentes. Ela sugere que, embora o consentimento seja amplamente reconhecido como fundamental, ainda há espaço para práticas mais sistemáticas e uniformes.

As variações nas práticas também são evidenciadas pelo desvio padrão de 5,76, que demonstra discrepâncias significativas entre setores e hierarquias dentro das empresas. Enquanto algumas áreas possuem um entendimento claro e procedimentos estruturados, outras apresentam abordagens menos rigorosas, indicando a necessidade de maior alinhamento interno.

Os valores extremos (mínimo de 10,00 e máximo de 24,00) reforçam essa disparidade. O valor mínimo reflete práticas insuficientes e riscos legais. O máximo destaca organizações com políticas bem definidas e mecanismos eficazes para assegurar a transparência e o registro do consentimento. Esses dados, na sua vez, indicam progresso, mas também a necessidade de maior consistência na aplicação das práticas.

4.12 Permissão de retificação de dados

Os mecanismos de retificação de dados pessoais são fundamentais para garantir a conformidade com a LGPD, e os dados analisados mostram um panorama misto em sua implementação. O valor médio de 16,20 indica que a maioria das empresas possui algum processo para permitir que os titulares corrijam suas informações, mas a eficácia e eficiência desses mecanismos ainda não são uniformes em todas as áreas organizacionais.

A mediana de 17,00, superior à média, sugere uma percepção geral positiva, com muitas empresas sendo avaliadas como capazes de oferecer retificação de dados de forma adequada. No entanto, a pequena diferença entre os dois indicadores aponta para áreas em que a implementação ainda pode ser melhorada, resultando em avaliações menos favoráveis.

A inconsistência na aplicação desses mecanismos é reforçada pelo desvio padrão de 7,46, que evidencia uma variação significativa nas percepções dos respondentes. Essa disparidade sugere práticas não uniformes entre diferentes departamentos ou níveis hierárquicos, possivelmente decorrentes de abordagens descentralizadas ou inconsistentes.

Os valores – mínimo de 5,00 e máximo de 25,00 – destacam ainda mais essa discrepância: enquanto algumas empresas apresentam dificuldades significativas ou até a ausência de mecanismos eficazes, outras mostra um alto nível de maturidade, com processos bem estruturados e ágeis para a retificação de dados pessoais. Esses resultados ressaltam a importância de padronizar e fortalecer as práticas de retificação em todas as áreas das organizações.

4.13 Clareza e objetividade sobre o Programa de Proteção de Dados Pessoais

A análise das percepções sobre a clareza e a objetividade das informações fornecidas pelas empresas em relação ao Programa de Proteção de Dados Pessoais revela uma avaliação moderada. A média de 16,00 sugere que, embora as informações não sejam amplamente vistas como confusas ou inadequadas, também não são consideradas excepcionalmente eficazes.

A mediana de 16,00, igual à média, reflete uma distribuição equilibrada entre os respondentes. Ela indica que metade dos resultados percebe as informações como suficientemente claras e objetivas; a outra metade as avalia ligeiramente abaixo ou acima desse ponto.

Considerando o desvio padrão de 4,53, o fato indica uma variação considerável nas percepções. Ela sugere que algumas empresas se destacam ao comunicar de forma clara e objetiva seu Programa de Proteção de Dados, enquanto outras enfrentam dificuldades em proporcionar o mesmo nível de transparência.

Os valores – mínimo (11,00) e máximo (21,00) – reforçam essa discrepância. O menor valor aponta para problemas significativos de comunicação em algumas organizações, o que torna as informações confusas ou inadequadas. Já o maior valor evidencia empresas que se destacam ao fornecer dados que são claros e eficientes, o que mostra excelência na divulgação de seus programas de proteção de dados.

4.14 Política de Privacidade acessível

A comunicação da política de privacidade da empresa apresenta sinais de progresso, mas ainda há pontos a serem aprimorados. A média de 16,00 sugere que a empresa já atingiu um patamar razoável de entendimento por parte dos colaboradores, mas há espaço para tornar a linguagem e a formatação do documento mais acessíveis. A mediana de 18,00 confirma que a maioria dos colaboradores compreende os principais aspectos da política. Entretanto, termos mais técnicos ou conceitos específicos ainda podem dificultar o entendimento de alguns

O desvio padrão de 5,43, que evidencia uma grande variação nas percepções, aponta para a necessidade de abordagens mais personalizadas na comunicação, adaptadas aos diferentes perfis e níveis de conhecimento dos colaboradores. Os valores extremos, variando de um mínimo de 8,00 a um máximo de 21,00, ressaltam essa disparidade e reforçam a importância de revisar a política de privacidade para garantir que ela seja clara e compreensível para todos. Isto promoveria maior uniformidade e eficácia na transmissão das informações.

4.15 Garantia de informação aos titulares de dados sobre a Política de Privacidade

A comunicação eficaz da Política de Privacidade é essencial para assegurar transparência e conformidade com a LGPD, mas as percepções sobre sua aplicação variam consideravelmente. A média de 15,20 e a mediana de 16,00 indicam que, enquanto muitas empresas conseguem fornecer informações razoavelmente satisfatórias sobre suas políticas, há deficiências que comprometem a clareza e a abrangência da comunicação em alguns casos. O desvio padrão de 6,18 destaca essa inconsistência, mostrando que algumas organizações são bem avaliadas nesse aspecto; outras enfrentam dificuldades significativas, o que resulta em percepções negativas sobre elas.

Os valores extremos reforçam essa disparidade. Empresas no menor patamar (5,00) apresentam sérias falhas de comunicação, arriscando a confiança dos titulares e o cumprimento das obrigações legais. Aquelas no maior patamar (21,00) mostram excelência na comunicação, com práticas claras e acessíveis. Esses dados evidenciam a necessidade de maior uniformidade e padronização para que todas as empresas assegurem que os titulares de dados compreendam seus direitos e como seus dados são tratados.

4.16 Rastreabilidade dos dados tratados

A rastreabilidade dos dados é um elemento crítico para a conformidade organizacional e a segurança das informações, mas apresenta desafios em termos de aplicação uniforme. A média de 14,60 e a mediana de 15,00 indicam uma percepção moderada dessa prática. Ela sugere que as empresas possuem processos implementados, mas que ainda não atingem níveis satisfatórios de eficácia em todas as áreas. Essa avaliação consistente entre média e mediana reflete um cenário de rastreabilidade presente, mas ainda com espaço para melhorias.

A alta dispersão apontada pelo desvio padrão de 4,56, juntamente com os valores extremos (mínimo de 10,00 e máximo de 20,00) revelam diferenças significativas entre setores e departamentos. Algumas áreas enfrentam dificuldades, como falta de infraestrutura ou capacitação; outras são vistas como exemplares, com processos bem estruturados. Esses dados reforçam a necessidade de harmonizar as práticas de rastreabilidade, de promover maior uniformidade e eficiência em toda a organização.

4.17 Classificação adequada de dados pessoais e dados sensíveis

A classificação de dados pessoais e sensíveis é um componente crucial para a gestão de informações, mas os dados sugerem que sua aplicação nas empresas é irregular. A média de 14,80 reflete um entendimento moderado da importância dessa prática, enquanto a mediana de 14,00 aponta que metade dos respondentes percebe as práticas como menos eficazes, o que evidencia lacunas na uniformidade e na consolidação do processo em diferentes áreas da organização.

A alta variação, evidenciada pelo desvio padrão de 4,60 e pelos valores extremos (mínimo de 10,00 e máximo de 22,00), indica disparidades significativas. Algumas áreas apresentam processos bem estruturados e exemplares; outras enfrentam falhas ou desconhecimento. Apesar de haver setores que podem servir de modelo para o restante da organização, os resultados ressaltam a necessidade de padronização das políticas, das ferramentas e da capacitação, fato que garantiria maior consistência na separação de dados pessoais e sensíveis.

4.18 Manutenção de registros detalhados das atividades de tratamento de dados pessoais

A manutenção de registros detalhados das atividades de tratamento de dados pessoais é essencial para a conformidade organizacional, e os dados analisados apontam avanços, mas também desafios. A média de 14,80 reflete uma percepção moderada; indica que a empresa realiza esforços nesse sentido, embora eles possam não ser suficientemente uniformes ou abrangentes em todas as áreas. A mediana de 17,00, significativamente superiorà média, revela que uma parte relevante dos respondentes avalia essas práticas de forma positiva, enquanto a média é influenciada por respostas mais críticas.

O desvio padrão de 3,77, relativamente baixo, sugere que a percepção dos respondentes é mais homogênea, com menor dispersão entre as respostas. Os valores extremos reforçam essa avaliação: o mínimo de 9,00 indica que, em algumas áreas, os registros podem ser insuficientes ou inexistentes; o máximo de 18,00 reflete que, para certos avaliadores, a prática de manutenção de registros detalhados é considerada muito satisfatória. Esses dados destacam a necessidade de ampliar e padronizar as práticas de registro, garantindo que elas sejam consistentes em todos os setores da empresa.

4.19 Rastreamento do fluxo e uso dos dados pessoais

A capacidade de rastrear eficientemente o fluxo e o uso de dados pessoais é um aspecto crucial para garantir transparência e conformidade nas empresas. A média de 14,40 indica uma percepção intermediária; sugere que essa prática está presente, mas pode não ser aplicada de forma totalmente eficaz ou consistente em todos os setores.

A mediana de 15,00, levemente superior à média, aponta que a maioria das respostas está alinhada ou acima desse nível, indicando uma percepção geral satisfatória do rastreamento em muitas áreas. O desvio padrão de 3,29, relativamentebaixo, demonstra uma homogeneidade maior nas opiniões dos avaliadores, refletindo percepções próximas sobre a eficiência do rastreamento.

Os valores extremos reforçam essa análise: o mínimo de 11,00 destaca dificuldades significativas em algumas áreas ou processos; o máximo de 18,00 reflete boas práticas em setores que são avaliados de forma bastante positiva. Esses resultados indicam a necessidade

de expandir as melhores práticas para toda a organização, promovendo maior consistência na eficiência do rastreamento de dados pessoais.

4.20 Adequação de contratos vigentes em conformidade com a LGPD

A adequação dos contratos à LGPD é crucial para a conformidade organizacional, mas ainda apresenta desafios. A média de 14,20 reflete um progresso intermediário; indica que os esforços estão em andamento, que não estão plenamente consolidados. A mediana de 13,00, inferior à média, sugere que em algumas áreas a percepção de adequação ainda é insatisfatória, que exige melhorias específicas.

A alta variação nas percepções, evidenciada pelo desvio padrão de 6,91 e pelos valores extremos (mínimo de 7,00 e máximo de 24,00), destaca disparidades entre setores. Enquanto algumas áreas estão avançadas na conformidade, outras mostram pouca ou nenhuma adequação. Esses resultados apontam para a necessidade de maior uniformidade e padronização nos esforços de adequação contratual.

4.21 Atendimento aos requisitos da LGPD em contratos com terceiros

A inclusão de cláusulas específicas sobre proteção de dados nos contratos com terceiros é fundamental para garantir a conformidade com a LGPD. A média de 14,20 reflete uma percepção moderada, indicando que a prática está presente, mas ainda carece de uniformidade e consolidação em toda a organização. A mediana de 14,00, praticamente igual à média, sugere que a percepção geral é consistente entre os respondentes, reforçando um nível intermediário de conformidade.

No entanto, o desvio padrão de 5,93 revela variações significativas nas percepções; indica que a inclusão de cláusulas de proteção de dados é irregular entre setores e tipos de contratos. Os valores extremos evidenciam essa disparidade: o mínimo de 8,00 aponta para contratos com lacunas ou inadequações; o máximo de 22,00 destaca práticas robustas e até superiores aos requisitos legais. Isso reforça a importância de padronizar as cláusulas de proteção de dados em toda a organização.

4.22 Revisões regulares com os parceiros para atender conformidade com a LGPD?

A prática de revisão da conformidade dos parceiros comerciais é essencial para o cumprimento da LGPD, mas ainda apresenta desafios de consistência em sua execução. A média de 14,20 revela um nível moderado de aplicação. Indica que a prática é realizada em parte, mas não cobre integralmente todas as relações comerciais. Já a mediana de 15,00, ligeiramente superior, sugere que a revisão é bem avaliada em boa parte da organização, mostrando esforços mais concentrados em algumas áreas.

O desvio padrão de 4,32 aponta para uma variação significativa nas percepções, evidenciando diferenças no grau de efetividade da revisão entre os setores ou processos. Os valores extremos reforçam essas desigualdades: o mínimo de 7,00 indica que algumas áreas ainda carecem de revisões adequadas; já o máximo de 18,00 destaca setores em que o processo é executado com maior frequência e rigor, atendendo melhor às exigências legais.

4.23 Controles de segurança e monitoramento para gerenciar vulnerabilidades e riscos relacionados aos serviços que lidam com dados pessoais

A segurança no monitoramento e no gerenciamento de vulnerabilidades em serviços que lidam com dados pessoais é essencial, mas apresenta níveis variados de eficácia. A média de 14,00 reflete uma aplicação moderada, enquanto a mediana de 16,00 indica que muitos setores possuem controles bem avaliados, apesar de existirem percepções mais críticas que impactam a média.

O desvio padrão de 3,24 demonstra variações entre setores, com áreas que implementam boas práticas (máximo de 17,00) e outras com controles considerados insuficientes (mínimo de 10,00). Esses dados reforçam a importânciade padronizar e fortalecer as práticas de segurança para maior consistência organizacional.

4.24 Planeja e implementa medidas de segurança desde a fase inicial

O planejamento e a implementação de medidas de segurança desde o início de serviços ou projetos são práticas essenciais, mas ainda apresentam inconsistências na aplicação. A média de 14,00 reflete um nível intermediário de adoção, indicando que as práticas existem, mas carecem de maior consistência. Já a mediana de 15,00, superior à média, aponta que a maioria das percepções é mais positiva, com avaliações satisfatórias em diversas áreas.

O desvio padrão elevado de 4,47 evidencia variações significativas entre setores ou projetos. O valor máximo de 19,00 sugere que algumas áreas realizam o planejamento de forma robusta e proativa, enquanto o mínimo de 8,00 revela lacunas importantes, com ausência de medidas desde as etapas iniciais. Esses dados reforçam a necessidade de padronizar as práticas de segurança para garantir maior uniformidade e eficácia em toda a organização.

4.25 Informações detalhadas e de fácil compreensão sobre a coleta de dados pessoais

A prática de fornecer informações claras e detalhadas sobre a coleta e o tratamento de dados é crucial para garantir a transparência e a confiança no tratamento de informações pessoais. A média de 13,60 reflete uma percepção moderada dessa prática. Ela indica que, conquanto esforços estejam sendo feitos, ainda há espaço significativo para melhorias. A mediana de 13,00, muito próxima à média, sugere que os respondentes compartilham uma avaliação uniforme, considerando as informações fornecidas razoáveis, mas não ideais.

A consistência nas percepções é reforçada pelo desvio padrão de 1,82, que indica pouca variação entre as respostas. No entanto, os valores extremos evidenciam diferenças entre áreas. O mínimo de 12,00 revela setores em que as informações são insuficientes ou pouco claras. O máximo de 16,00 mostra que boas práticas já são aplicadas em algumas partes da organização. Esses dados destacam a importância de padronizar a comunicação, garantindo que todas as áreas ofereçam informações compreensíveis e detalhadas sobre a coleta e o tratamento de dados.

4.26 Informação aos titulares dos dados sobre seus direitos e as formas de exercê-los

Garantir que os titulares de dados sejam informados sobre seus direitos e como exercê- los é um pilar essencial da conformidade com a LGPD, mas os dados apontam desafios nesse aspecto. A média de 13,40 reflete uma percepção moderada, indicando que, embora esforços estejam sendo feitos, a prática ainda não é totalmente eficiente ou abrangente. A mediana de 12,00, inferior à média, sugere que uma parte significativa dos respondentes percebe lacunas ou inconsistências na comunicação.

O desvio padrão de 3,36 evidencia variações significativas entre setores ou canais da empresa, indicando falta de uniformidade nas práticas de comunicação. Os valores extremos reforçam essa disparidade. O mínimo de 11,00 aponta para áreas em que as informações são insuficientes, dificultando o entendimento e o acesso aos direitos. O máximo de 19,00 destaca setores que se sobressaem, proporcionando informações claras e acessíveis. Esses dados ressaltam a necessidade de padronizar e fortalecer as práticas de comunicação para garantir que todos os titulares sejam adequadamente informados.

4.27 Processo de notificação sobre violações de dados pessoais e administração dos incidentes

O processo de notificação de violações e administração de incidentes é percebido como moderadamente eficaz, com uma média e mediana de 13,00, indicando avaliações equilibradas entre os respondentes. Apesar de práticas estabelecidas, ainda há espaço para melhorias em eficiência e uniformidade.

O desvio padrão de 2,55 revela variações moderadas. Algumas áreas apresentam processos alinhados às melhores práticas (máximo de 17,00). Outras enfrentam insuficiências que podem expor a empresa a riscos (mínimo de 10,00). Esses dados destacam a importância de padronizar e fortalecer o processo em toda a organização.

4.28 Sistema para a detecção e resposta rápida a incidentes de violação de dados

O processo de notificação de violações e gestão de incidentes é considerado moderadamente eficaz, com uma média e mediana de 13,00, o que reflete avaliações consistentes entre os respondentes. Mesmo existindo procedimentos estabelecidos, há oportunidades para aprimorar a eficiência e a uniformidade em sua aplicação.

Com um desvio padrão de 2,55, as respostas mostram variações moderadas. Algumas áreas mostram práticas bem estruturadas e alinhadas aos padrões ideais (máximo de 17,00). Outras revelam fragilidades que podem gerar riscos à empresa (mínimo de 10,00). Esses resultados ressaltam a necessidade de harmonizar e fortalecer o processo em toda a organização.

4.29 Processos para notificação e mitigação de violações de dados

Os processos de notificação e mitigação de violações de dados mostram um nível moderado de eficácia, conforme indicado pela média de 12,60. Isso sugere que, apesar de existir práticas estabelecidas, elas não são amplamente percebidas como claras ou consistentemente aplicadas em toda a organização. A mediana de 12,00, próxima à média, reflete uma percepção geral uniforme, com a maioria dos respondentes considerando os processos adequados, mas ainda distantes de ser ideais.

O desvio padrão de 2,88 indica uma variação moderada nas percepções, o que sugere que a aplicação dos processos não é homogênea entre os setores. Algumas áreas mostram maior alinhamento e comprometimento com os processos. Outras podem enfrentar desafios, como falta de clareza ou padronização na execução.

Os valores extremos reforçam essas diferenças: o mínimo de 9,00 aponta para setores em que os processos são percebidos como insuficientes ou inexistentes. O máximo de 16,00 destaca áreas com práticas bem estabelecidas e robustas. Esses setores podem servir como exemplos para ampliar e padronizar as melhores práticas em toda a organização, garantindo maior consistência e eficácia no tratamento de violações de dados.

4.30 Na sua visão, sua empresa disponibiliza um canal apropriado para receber denúncias de irregularidades e falhas na segurança?

Os canais de denúncia para irregularidades e falhas na segurança da empresa são considerados moderadamente eficazes, com uma média de 12,60 refletindo a existência de práticas estabelecidas, mas com espaço para aprimoramentos. A mediana de 14,00, superior à média, indica que boa parte dos respondentes avalia os canais como adequados, mas a média foi influenciada por percepções mais críticas.

O desvio padrão de 1,95 aponta para uma percepção uniforme entre os respondentes, sugerindo que as opiniões sobre a eficácia dos canais de denúncia são consistentes. Apesar disso, há disparidades nos níveis de eficácia percebidos em diferentes áreas ou situações, como indicado pelos valores extremos.

A pontuação mínima de 10 revela que, em algumas situações, os canais de denúncia são vistos como insuficientes ou inadequados. Já o máximo de 14 mostra que, em outros casos, os canais são considerados apropriados e eficazes. Esses resultados ressaltam a importância de uniformizar e fortalecer os canais de denúncia, garantindo que todos sejam eficazese acessíveis em toda a organização.

4.31 Encarregado de Dados Pessoais na empresa

A percepção sobre a nomeação de um Encarregado de Dados Pessoais (DPO) é moderada, com uma média de 12,60, o que indica que a prática existe, mas apresenta limitações em sua implementação ou entendimento. A mediana de 10,00, significativamente mais baixa, sugere que, para a maioria dos respondentes, a nomeação ainda não é vista como clara ou funcional.

O desvio padrão de 5,77 reflete uma grande variação, indicando que, enquanto algumas áreas reconhecem um DPO ativo e eficaz (máximo de 21,00), outras percebem sua nomeação como inexistente ou frágil (mínimo de 7,00). O fato evidencia disparidades no cumprimento dessa função.

A predominância de respostas indicando a implementação média da LGPD pode ser interpretada como um indicativo de que, embora as empresas estejam cientes da importância da conformidade com a LGPD, muitas ainda estão em processo de implementação das medidas requeridas.

Seu foco inicial, entretanto, está mais na adaptação legal do que em uma transformação total dos seus processos. A existência de respostas em nível baixo pode apontar para áreas de risco que precisam ser endereçadas, como a falta de treinamento contínuo sobre proteção de dados ou deficiências na infraestrutura de TI para garantir a segurança.

Em termos acadêmicos, isso sugere que muitas empresas estão adotando uma abordagem incremental para a LGPD, ainda ajustando seus sistemas de governança de dados e assegurando que as medidas de *compliance* sejam abrangentes e eficientes. É crucial que, para uma conformidade efetiva e sustentável, as empresas ajustem os aspectos técnicos e legais, promovam uma cultura de privacidade organizacional robusta, alinhada às melhores práticas internacionais.

4.32 Índice de maturidade das empresas

O índice de maturidade organizacional foi calculado com base nos *scores* das empresas, refletindo o grau de conformidade em relação às práticas avaliadas. As empresas foram classificadas em três níveis: **Baixa Maturidade** (0,00 - 1,99), indicando lacunas significativas; **Maturidade Moderada** (2,00 - 3,49), representando avanços com oportunidades de melhoria; **Alta Maturidade** (3,50 - 4,00), evidenciando práticas consolidadas.

A Tabela 5 consolidada apresenta os *scores* médios das empresas agrupadas por porte (Grande, Média, Pequena, ME e MEI). Esses *scores*, calculados com base nos dados previamente analisados, refletem o nível médio de conformidade das organizações em relação às práticas avaliadas.

Tabela 5 - Score médio das empresas.

Categoria	Score Médio	Explicação
Porte - Grande	2.32	Média dos scores das empresas classificadas como 'Grande'.
Porte - ME	1.73	Média dos scores das empresas classificadas como 'ME'.
Porte - MEI	1.63	Média dos scores das empresas classificadas como 'MEI'.
Porte - Média	2.57	Média dos scores das empresas classificadas como 'Média'.
Porte - Pequena	1.84	Média dos scores das empresas classificadas como 'Pequena'.

Fonte: Autoria própria, 2024.

Empresas de Grande Porte: este grupo obteve o maior *score* médio (2,32), evidenciando maior adesão às boas práticas. Isso pode ser atribuído a uma maior disponibilidade de recursos financeiros, tecnológicos e humanos, bem como a uma necessidade de proteger operações mais complexas e amplas.

Empresas de Porte Médio: com um *score* médio de 2,57, as empresas de porte médio mostraram desempenho próximo ao das empresas de grande porte. A sugestão é a de que organizações intermediárias também têm investido significativamente em conformidade e governança, possivelmente em resposta às demandas do mercado e às regulamentações.

Empresas de Pequeno Porte (ME, MEI e Pequena): as empresas menores apresentaram *scores* médios mais baixos, variando entre 1,63 e 1,84. Isso indica que elas enfrentam maiores desafios para implementar práticas robustas de conformidade, frequentemente limitadas por recursos financeiros e organizacionais reduzidos.

O aplicativo desenvolvido atendeu plenamente ao objetivo de coletar e calcular os *scores* e índices relacionados à conformidade das empresas com as práticas avaliadas. Durante o período de análise, foram obtidas 123 respostas, das quais 81 foram selecionadas após um

processo criterioso de triagem. Essa etapa de descarte foi essencial para reduzir vieses e assegurar a integridade dos resultados, garantindo que os dados refletissem a realidade das organizações avaliadas.

As 81 empresas analisadas apresentaram variabilidade em seus *scores* médios como mostrado detalhadamente. Isto permitiu uma visão clara das tendências por porte e área de atuação. A ferramenta demonstrou eficácia na

1. **Coleta de Dados**: capturando respostas relevantes de empresas de diferentes tamanhos e segmentos;
2. **Cálculo dos *Scores***: gerando índices médios com base em uma metodologia consistente e validada;
3. **Identificação de Tendências**: revelando padrões que apontam os desafios e avanços relacionados à conformidade.

Esses dados confirmam que, embora existam avanços em governança e conformidade, pequenas empresas necessitam de maior apoio para aprimorar suas práticas. O aplicativo desenvolvido foi fundamental para medir o índice de maturidade e identificar tendências, fornecendo uma base sólida para ações futuras de melhoria contínua.

Além disso, a robustez da análise possibilitou *insights* importantes, como a relação entre o porte das empresas e a sua capacidade de implementação de práticas, destacando a necessidade de suporte para organizações menores. Esse processo não apenas validou o funcionamento do aplicativo, mas também forneceu um panoramaconfiável e fundamentado para futuras tomadas de decisão. Ele evidenciou que o aplicativo se mostrou uma ferramenta útil, eficiente, capaz de entregar resultados consistentes e alinhados com os objetivos propostos. O mesmo processo será atualizado conforme os *feedbacks* recebidos.

CAPÍTULO IV

5 CONSIDERAÇÕES FINAIS

5.1 Conclusões Finais

Os objetivos foram plenamente alcançados com o desenvolvimento de um índice de maturidade e seus indicadores associados, que mostraram eficácia prática ao auxiliar empresas na adequação à LGPD. A ferramenta proporcionou diagnósticosprecisos, priorização de ações corretivas e categorização dos níveis de maturidade, reafirmando sua utilidade como um recurso estratégico de gestão.

O desenvolvimento do índice de maturidade e dos indicadores associados foi realizado com rigor metodológico, fundamentado em referenciais teóricos e validados por especialistas da área, incluindo-se entre eles profissionais de Segurança da Informação e *Data Protection Officers* (DPO). Esse processo resultou na criação de um artefato digital estratégico, capaz de auxiliar empresas na adequação às exigências da Lei Geral de Proteção de Dados (LGPD).

Os indicadores desenvolvidos foram testados em 81 empresas, o que proporcionou um diagnóstico claro e quantitativo do nível de conformidade com a LGPD. Esse artefato demonstrou sua eficácia ao medir, monitorar e avaliar políticas de proteção de dados, permitindo que as organizações identificassem lacunas e priorizassem ações corretivas. Além disso, foi possível categorizar os níveis de maturidade das empresas, com destaque às diferenças entre portes e áreas de atuação, o que reforça sua aplicabilidade prática como ferramenta de gestão.

Para atender as necessidades em constante evolução dos clientes, estão previstas atualizações no artefato. Uma das melhorias planejadas é a inclusão de relatórios detalhados direcionados ao responsável pela implementação e monitoramento da LGPD nas organizações. Esses relatórios oferecerão *insights* personalizados para facilitar o acompanhamento contínuo da conformidade e a tomada de decisões estratégicas.

Esses resultados evidenciam que o desenvolvimento, a aplicação e a evolução contínua de tais ferramentas são fundamentais para o fortalecimento da cultura de privacidade nas organizações e para o cumprimento das obrigações legais estabelecidas pela LGPD.

REFERÊNCIAS BIBLIOGRÁFICAS

ACQUISTI, Alessandro; TAYLOR, Curtis R.; WAGMAN, Liad. *The Economics of Privacy*. Journal of Economic Literature, v. 54, n. 2, p. 442-492, 2016.

ALMEIDA, J. R. *Governança da Informação e Segurança dos Dados*. Revista de Gestão Empresarial, v. 45, n. 2, p. 123-137, 2019.

ALMEIDA, Joana; SANTOS, Pedro. *Direitos dos titulares de dados no GDPR*: uma análise crítica. Revista de Proteção de Dados, v. 2, n. 1, p. 30-50, 2018.

ARAÚJO, P. Gestão de Dados Pessoais: *O Impacto da LGPD nas Empresas*. São Paulo: Editora Atlas, 2021.

BARBOSA, João; SILVA, Maria. *Interconectividade em Ecossistemas Digitais*. São Paulo: Editora Tecnológica, 2018.

BONOLLO, Nicolas; POOPUU, Preedik. The impact of digital platforms on roles and responsibilities in value creation among stakeholders of an ecosystem. 2019.

BOTSMAN, Rachel; ROGERS, Roo. *What's Mine Is Yours: The Rise of Collaborative Consumption*. New York: HarperCollins, 2010.

BOUDREAU, Kevin J.; HAGIU, Andrei. *Platform Rules*: Multi-Sided Platforms as Regulators. Cambridge: MIT Press, 2009.

BRAGA, Luís; OLIVEIRA, Carlos. *Impactos do GDPR nas empresas e nos consumidores*. Jornal de Direito Digital, v. 5, n. 2, p. 60-80, 2020.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a criação da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, DF, 9 jul. 2019.

BROWN, A.; GRANT, D. *Framing the frameworks*: A review of IT governance research. Communications of the Association for Information Systems, v. 15, n. 1, p. 696-712, 2005.

CARBONI, Guilherme. *Inovação e regulação na economia digital.* São Paulo: Saraiva, 2020.

CASTELLANI, S. Everything you need to know about Digital Platforms. Disponível em: <http://stefano-castellani.net/wp-content/uploads/2019/09/Everything-you-need-to-know-about-Digital-Platforms-190920.pdf>. Acesso em: 29 maio 2024.

CAVOUKIAN, A. Privacy by Design: The 7 Foundational Principles. Privacy by Design: The 7 Foundational Principles, 2009. Disponível em: <https://www.ipc.on.ca/wp- content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 29 maio 2024.

CAVOUKIAN, A.; JONAS, J. *Privacy by design in the age of big data*. Information and Privacy Commissioner of Ontario, Canada, 2011.

CONSUMERS INTERNATIONAL**.** *The State of Data Protection Rules Around the World*. London: Consumers International, 2018. Disponível em: <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf.> Acesso em: 12 set. 2023.

COSTA, Maria; SILVA, João. *A nova era da proteção de dados*: entendendo o GDPR. Revista de Direito Europeu, v. 4, n. 1, p. 40-55, 2019.

COSTA, Ricardo; PEREIRA, Helena. *Segurança em Ecossistemas Digitais*. Porto Alegre: Editora Segurança Digital, 2021.

DEUTSCH, Karl; NEUMANN, John Von. *The Digital Future*: How the Data Economy is Transforming Business. Harvard Business Review, v. 86, n. 7, p. 46-56, 2017.

DONEDA, D. (2006). Privacidade e proteção de dados pessoais na sociedade da informação. Editora FGV.

DONEDA, Danilo. *Privacidade e proteção de dados pessoais na sociedade da informação*. São Paulo: Editora FGV, 2020.

DONEDA, Danilo. *A proteção de dados pessoais no Brasil*: da regulação à prática. Revista de Direito e Tecnologia, v. 12, n. 2, p. 40-60, 2020.

DRESCH, A.; LACERDA, D. P.; ANTUNES, J. A. V. *Design Science Research*: método de pesquisa para a engenharia de produção. Porto Alegre: Bookman Editora, 2015.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR). Official Journal of the European Union, 2016.

FERREIRA, Carlos; GOMES, Ana. *Interoperabilidade em Sistemas Digitais*. Rio de Janeiro: Editora de Sistemas, 2019.

FINK, E.; HOFFMANN, I. *The economic benefits of data protection–Case studies*. EDPS Economic Paper, 2015.

FRIEDMAN, T. The World is Flat: *A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux, 2005.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5. ed. São Paulo: Atlas, 2010.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa.* 5. ed. São Paulo: Atlas, 2010. Disponível em: https://ria.ufrn.br/jspui/handle/123456789/1236. Acesso em: 2 nov. 2024.

GOMES, A. I. *Desafios da Segurança de Dados em Ecossistemas Digitais*. Journal of Information Security, v. 14, n. 3, p. 235-255, 2021.

HAGIU, & Wright. Multi-Sided Platforms. International Journal Of Industrial Organization, 43(C), 162-174. (2015).

HUSSAIN, Muhammad. YOLO-v1 to YOLO-v8, the Rise of YOLO and Its Complementary Nature toward Digital Manufacturing and Industrial Defect Detection. Machines, v. 11, n. 7, p. 677, 2023. Disponível em: <https://www.mdpi.com/2075-1702/11/7/677>. Acesso em: 29 maio 2024.

IRAMINA, D. P. *A Lei Geral de Proteção de Dados (LGPD) e os principais impactos para as empresas brasileiras*. Revista Jurídica, v. 6, n. 2, p. 45-60, 2020.

JACOBIDES, M. G.; KNOPP, E. S. *How Ecosystem Strategies Reshape the Boundaries of Firms*. Journal of Management Studies, v. 57, n. 5, p. 27-49, 2020.

JACOBIDES, Michael G.; CENNAMO, Carmelo; GAWER, Annabelle. *Rumo a uma teoria dos ecossistemas*. Revista de gestão estratégica, v. 39, n. 8, p. 2255-2276, 2018.

KAPLAN, Robert S.; NORTON, David P. *The Balanced Scorecard: Translating Strategy into Action*. Harvard Business Review Press, 1996.

KOZHEVNIKOV, D. E.; Korolev, A. S. Digital Trust As a Basis For the Digital Transformation Of the Enterprise And Economy. 2018.

LACERDA, D. P.; DRESCH, A.; ANTUNES, J. A. V. *Design Science Research na prática*: revisão sobre as aplicações na Engenharia de Produção. Revista Gestão & Produção, 2013.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. *Liberdade de expressão na era digital*. Rio de

Janeiro: Zahar, 2020.

Lehong, H. Et Al. Building A Digital Business Technology Platform. Gartner, Inc, 2017.

LIMA, Marina. *Implementação da LGPD: desafios e oportunidades para as empresas*. Jornal de Direito Digital, v. 3, n. 1, p. 85-100, 2021.

LIMA, Pedro. *Estruturas e Dinâmicas dos Ecossistemas Digitais*. Brasília: Editora Digital, 2020.

LIMA, R. Proteção de Dados Pessoais: *A Nova Lei Brasileira e Seu Impacto nas Empresas*. São Paulo: Editora Saraiva, 2019.

MACHADO, F. *Lei Geral de Proteção de Dados*: Manual para Profissionais de TI. São Paulo: Editora Novatec, 2020.

MALLER, M. *Practical Applications of Platform-Based Business Models*. Management Review Quarterly, v. 69, n. 3, p. 125-140, 2020.

MANCHA, Ruben; Gordon, Steven; Iyer, Bala. Figayou Pursues A Platform Strategy: A Case Study Of Digital Platform Entrepreneurship. Journal Of Information Technology Case And Application Research, V. 20, N. 2, P. 55-70, 2018.

MARQUES, Claudia Lima. *Direito do consumidor e livre concorrência*. São Paulo: RT, 2019.

MENDES, Fernanda. *Inovação em Ecossistemas Digitais*. Curitiba: Editora Inovação, 2019.

MONTEIRO, Ricardo. *A importância da notificação de violações de dados no GDPR*. Revista de Segurança da Informação, v. 3, n. 3, p. 75-85, 2019.

MORAES, M. C. B. de. (2003). Direitos da personalidade: proteção à intimidade, vida privada, honra e imagem. Renovar.

MORVAN, L.; Hintermann, F.; Vazirani, M. Five Ways to Win with Digital Platforms. Accenture Research, Dublin, 2016.

NAMBISAN, Satish; SAWHNEY, Mohanbir. *Digital Innovation and the Changing Nature of Innovation Ecosystems*. Strategic Entrepreneurship Journal, v. 15, n. 1, p. 3-20, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, 2020.

OKANO, M. T., Antunes, S. N., & Fernandes, M. E. (2021). Digital transformation in the manufacturing industry under the optics of digital platforms and ecosystems. Independent Journal of Management & Production, 12(4), 1139-1159.

OLIVEIRA, M. S.; SANTOS, L. F. *Desafios da Conformidade com a LGPD*. Journal of Data

Protection, v. 12, n. 1, p. 45-59, 2021.

OLIVEIRA, Pedro. *A importância da notificação de violações de dados na LGPD*. Revista de Segurança da Informação, v. 4, n. 3, p. 110-125, 2020.

ONDRUS, J., Gannamaneni, A., & Lyytinen, K. The Impact Of Openness On The Market Potential Of Multi-Sided Platforms: A Case Study Of Mobile Payment Platforms Journal Of Information Technology, 30(3), 260–275. 2015.

PARMENTER, David. *Key Performance Indicators*: Developing, Implementing, and Using Winning KPIs. *John Wiley & Sons,* 2015.

PIOVESAN, F. (2013). Direitos humanos e cidadania. Saraiva.

REIS, Lucas; ALMEIDA, Joana. *A importância da notificação de violações de dados na LGPD*. Revista de Segurança da Informação, v. 4, n. 3, p. 110-125, 2020.

REZENDE, P. *Privacidade e Proteção de Dados*: Fundamentos e Aspectos Práticos da LGPD. Salvador: Editora Juspodivm, 2020.

ROCHET, Jean-Charles; TIROLE, Jean. *Platform Competition in Two-Sided Markets*. Journal of the European Economic Association, v. 1, n. 4, p. 990-1029, 2003.

SAMADI, S. *Data Protection in the GDPR and its impact on Business Models*. Business Law Review, v. 41, n. 4, p. 202-215, 2020.

SANTOS, Cláudia. *Cooperação internacional na proteção de dados*: desafios e perspectivas. Revista de Direito Internacional, v. 8, n. 2, p. 130-150, 2021.

SCHMIDT, E.; COHEN, J. *The New Digital Age*: Reshaping the Future of People, Nations and Business. New York: Knopf, 2013.

SILVA, João; SILVA, Maria. *Direitos dos titulares de dados na LGPD*: uma análise crítica. Revista de Proteção de Dados, v. 5, n. 1, p. 65-80, 2019.

SILVA, Lucas. *Adaptação e Sustentabilidade nos Ecossistemas Digitais*. Belo Horizonte: Editora Sustentável, 2021.

SILVA, R. T. *Fundamentos da Governança Corporativa*. São Paulo: Editora Acadêmica, 2020.

SOUZA, Thiago; ALMEIDA, Carla. *Eficiência Econômica e Ecossistemas Digitais*. Recife: Editora Economia Digital, 2020.

TILSON, D., Sørensen, C. And Lyytinen, K. Change And Control Paradoxes In Mobile

Infrastructure Innovation: The Android And Ios Mobile Operating Systems Cases, In: 45th Hawaii International Conference On System Science (Hicss 45), Maui, Hi. (2012).

TIWANA, A.; Konsynsky, B.; Bush, A.A. Platform Evolution: Coevolution Of Platform Architecture, Governance, And Environmental Dynamics. Information Systems Research 21(4): 675–687, 2010.

VIEIRA, T. A TRANSFORMAÇÃO DIGITAL SOB A ÓTICA DA ENGENHARIA DO CONHECIMENTO: UMA REVISÃO SOBRE O USO DE ONTOLOGIAS COMO
MODELO. Anais do Congresso Internacional de Conhecimento e Inovação–ciki, v. 1, n. 1, 2020.

WHEELER, S.; WEISS, M. *Data governance in the age of big data*: Challenges and opportunities. Journal of Information Technology Management, v. 27, n. 2, p. 40-55, 2020.

APÊNDICE – Respostas do nível de conformidade

Pergunta	Não	Baixo	Médio	Alto	Completo	Total
Como está implementada a LGPD na sua empresa?	5	15	23	19	19	81
A empresa possui um setor específico responsável pela implementação e pelo monitoramento da LGPD?	31	6	14	12	18	81
A empresa adota boas práticas de governança em privacidade de dados?	10	12	20	17	22	81
Como a empresa especifica obrigações de setores no Programa de Proteção de Dados?	6	17	20	16	22	81
A empresa realiza capacitações e treinamentos regulares?	20	10	16	21	14	81
Há responsáveis que facilitam a comunicação sobre LGPD?	17	10	20	17	17	81
A empresa demonstra comprometimento com privacidade e LGPD?	9	10	16	23	23	81
A empresa mapeia dados pessoais e respeita princípios legais da LGPD?	14	8	15	20	24	81
Há monitoramento regular de práticas de privacidade de dados?	13	12	22	20	14	81
A empresa conscientiza sobre a necessidade de consentimento?	10	12	15	24	20	81
A empresa permite a retificação de dados pelo titular?	14	5	17	20	25	81
A empresa informa claramente sobre o Programa de Proteção de Dados?	12	16	11	21	20	80
A Política de Privacidade é simples e acessível?	13	8	20	21	18	80
Os titulares dos dados são informados sobre a Política de Privacidade?	5	15	16	19	21	76
Há rastreabilidade dos dados tratados?	10	10	20	15	18	73
A classificação entre dados pessoais e sensíveis é adequada?	14	12	10	22	16	74

A empresa mantém registros detalhados das atividades de tratamento de dados?	9	13	18	17	17	74
Há rastreamento eficiente do fluxo e uso dos dados pessoais?	11	11	17	15	18	72
A empresa adequa contratos vigentes à LGPD?	7	9	13	18	24	71
Contratos com terceiros incluem cláusulas de proteção de dados?	9	8	14	22	18	71
A empresa revisa regularmente parceirospara conformidade com LGPD?	14	7	15	17	18	71
Há controles de segurança para monitorar riscos em serviços que lidam com dados pessoais?	10	11	16	16	17	70
Medidas de segurança são planejadas desde o início de projetos?	11	8	19	15	17	70
A empresa fornece informações claras sobre coleta e tratamento de dados?	12	12	13	15	16	68
Os titulares são informados sobre seus direitos e formas de exercê-los?	11	14	12	11	19	67
Há um processo eficaz para notificar sobre violações de dados?	13	10	12	13	17	65
Há um sistema para rápida resposta a incidentes de violação de dados?	15	8	14	13	14	64
Os processos para notificação e mitigação de violações são claros e seguidos?	12	9	15	11	16	63
Há um canal apropriado para denúncias de irregularidades na segurança?	14	11	14	14	10	63
A empresa realiza revisões regulares de parceiros para mitigar riscos relacionados à LGPD?	21	9	10	16	7	63

Fonte: Autoria Própria, 2024.