

LGPD E A IMPORTÂNCIA DOS DADOS NAS PEQUENAS E MÉDIAS EMPRESAS DE TECNOLOGIA

Marques, Caio¹

Centro Universitário Academia – UniAcademia

RODRIGUES, Isabella Stroppa²

Centro Universitário Academia – UniAcademia

Linha de Pesquisa: Gestão de Tecnologia e Inovação

RESUMO

A transformação digital intensificou o uso de dados pessoais, tornando-os ativos estratégicos nas esferas econômica e social, mas também levantando preocupações sobre privacidade e segurança. Em resposta, o Brasil sancionou a Lei Geral de Proteção de Dados (LGPD) em 2018, em vigor desde 2020, com o objetivo de regulamentar o tratamento de dados e garantir transparência, segurança e respeito aos direitos dos cidadãos. Para pequenas e médias empresas (PMEs) de tecnologia, a adequação à LGPD representa um desafio significativo, dado o uso intensivo de dados e a limitação de recursos técnicos e financeiros. Contudo, a conformidade legal pode ser uma oportunidade estratégica para fortalecer a reputação, aumentar a confiança do mercado e adotar práticas de governança mais sustentáveis. Este trabalho analisa os impactos da LGPD nas PMEs incubadas pelo CRITT/UFJF, investigando como essas empresas interpretam e aplicam os princípios da lei, os mecanismos implementados para garantir a segurança da informação e os benefícios percebidos com a conformidade. Busca-se, ainda, entender como a gestão responsável dos dados pode impulsionar a inovação. A pesquisa visa contribuir para o debate acadêmico e oferecer soluções práticas para o setor, ainda em processo de adaptação à nova legislação.

Palavras-chave: Dados Pessoais. Proteção de Dados. LGPD. PMEs. Transformação Digital. Segurança.

1 INTRODUÇÃO

Nas últimas décadas, o avanço acelerado da transformação digital e a consolidação da sociedade da informação têm provocado mudanças profundas na forma como indivíduos, empresas e instituições públicas interagem, comunicam e operam. Nesse novo contexto, os dados pessoais passaram a ocupar uma posição

¹ Graduando em Administração pelo Centro Universitário Academia – UniAcademia.

² Professor orientador do curso de Administração pelo Centro Universitário Academia – UniAcademia.

estratégica e central nas dinâmicas econômicas, tecnológicas e sociais. O uso intensivo de tecnologias da informação, como plataformas digitais, serviços em nuvem, inteligência artificial e big data, transformou os dados em um dos ativos mais valiosos da atualidade. No entanto, ao mesmo tempo em que o tratamento massivo de dados oferece inúmeras oportunidades de inovação e personalização de serviços, ele também levanta questões complexas relacionadas à privacidade, à segurança da informação e ao uso ético dos dados.

Diante desse cenário, foi sancionada no Brasil, em 2018, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em setembro de 2020. Inspirada em regulamentações internacionais, como o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, a LGPD estabelece um conjunto de princípios, direitos e obrigações destinados a disciplinar o tratamento de dados pessoais em todo o território nacional. Seu objetivo é garantir maior transparência, controle e segurança às informações dos cidadãos, assegurando que qualquer uso de dados pessoais ocorra com base em fundamentos legais claros e com o devido respeito à dignidade e à liberdade dos indivíduos. Além disso, a lei também introduz penalidades para organizações que descumprirem suas disposições, o que tem exigido mudanças estruturais e culturais dentro das empresas brasileiras.

No caso das pequenas e médias empresas (PMEs), especialmente aquelas de base tecnológica, os impactos da LGPD são particularmente sensíveis. Estas organizações, embora representem uma parcela expressiva da economia nacional e desempenhem papel crucial no desenvolvimento da inovação, muitas vezes não dispõem da estrutura, do conhecimento técnico e dos recursos financeiros necessários para implementar as mudanças exigidas pela legislação. Além disso, por lidarem frequentemente com grandes volumes de dados de usuários, clientes e parceiros, essas empresas se veem diante de um paradoxo: ao mesmo tempo em que necessitam inovar e crescer rapidamente, precisam também garantir conformidade legal, segurança da informação e respeito à privacidade.

A conformidade com a LGPD, nesse sentido, vai além de uma simples obrigação jurídica. Ela pode representar uma oportunidade estratégica para as PMEs, ao permitir o fortalecimento da reputação institucional, o aumento da

confiança de clientes e stakeholders, e a consolidação de práticas organizacionais mais eficientes, transparentes e sustentáveis. A adoção de políticas claras de proteção de dados e boas práticas de governança pode, inclusive, posicionar essas empresas de forma mais competitiva frente ao mercado, tanto nacional quanto internacional, especialmente em um cenário global onde a proteção da privacidade digital tornou-se critério decisivo para consumidores e investidores.

O presente trabalho tem como objetivo analisar os efeitos e implicações da LGPD nas pequenas e médias empresas de tecnologia incubadas pelo Centro Regional de Inovação e Transferência de Tecnologia da Universidade Federal de Juiz de Fora (CRITT/UFJF). O foco nesse recorte se justifica por duas razões principais: primeiro, pela natureza inovadora e tecnológica das empresas vinculadas à incubadora, que frequentemente operam com soluções digitais baseadas em dados; segundo, pela necessidade concreta de compreender como essas organizações estão enfrentando os desafios da adequação legal dentro de um ecossistema de inovação e empreendedorismo.

Especificamente, pretende-se investigar como essas empresas estão interpretando os princípios da LGPD, quais mecanismos técnicos e administrativos têm sido implementados para garantir a segurança e a integridade dos dados, e quais benefícios internos e externos estão sendo percebidos com a adoção de práticas de conformidade. Também se busca compreender de que forma os dados são utilizados como insumos para inovação, revelando como a gestão responsável e estratégica da informação pode impulsionar o desenvolvimento de novos produtos, serviços e soluções.

A escolha desse tema se sustenta na urgência de oferecer contribuições práticas e acadêmicas a um debate ainda em amadurecimento no Brasil. Embora a LGPD esteja em vigor, ainda são poucos os estudos que analisam, sob a perspectiva das PMEs tecnológicas, os reais efeitos da legislação, os entraves enfrentados e as soluções viáveis para alcançar a conformidade sem comprometer a inovação. Nesse sentido, o trabalho busca preencher uma lacuna na literatura, ao mesmo tempo em que propõe uma abordagem aplicada, conectada à realidade de empreendedores e gestores que precisam lidar com múltiplas demandas, riscos e oportunidades.

2 REFERENCIAL TEÓRICO

Nossa era é definida pela exponencial geração e fluxo de informações, onde a transformação digital alterou completamente as interações sociais e econômicas. Nesse contexto, os dados pessoais emergiram como um ativo de imenso valor estratégico para as organizações, fundamentais para a inovação, otimização de serviços e processos decisórios, conforme destacam Amaral e Ribeiro (2017). Entretanto, essa crescente valorização dos dados acarreta, simultaneamente, uma exposição constante dos indivíduos a riscos relacionados à privacidade e ao uso potencialmente inadequado de suas informações pessoais. Investigar como as empresas, particularmente as pequenas e médias do setor de tecnologia, navegam neste cenário desafiador exige uma fundamentação teórica sólida, essencial para a condução de pesquisas metodologicamente consistentes, como orienta Vergara (1998).

A crescente preocupação com a privacidade e o controle sobre as informações pessoais gerou a necessidade da criação de marcos regulatórios específicos em diversas partes do mundo. Como aponta Doneda (2006), houve uma evolução conceitual do direito à privacidade, tradicionalmente visto como o "direito de ser deixado em paz", para uma concepção mais ampla de proteção de dados pessoais, que engloba o controle do indivíduo sobre o fluxo de suas informações no ambiente digital e físico. Essa transição reflete uma adaptação do direito às novas realidades impostas pela tecnologia.

No Brasil, um passo fundamental nesse sentido foi a promulgação da Lei nº 12.965/2014, denominada como o Marco Civil da Internet. Esta legislação estabeleceu princípios, garantias, direitos e deveres para o uso da internet no país, sendo um marco ao abordar a proteção da privacidade e dos dados pessoais dos usuários online. O Marco Civil da Internet, ao consagrar a proteção aos dados pessoais e à privacidade (Art. 3º, II e III) como fundamentos e objetivos do uso da internet no Brasil, e ao estabelecer a necessidade do consentimento expresso do usuário para o tratamento de seus dados pessoais por provedores de aplicações (Art. 7º, VII, VIII e IX), já delineava uma preocupação legislativa com a autodeterminação informativa, ainda que não com a profundidade e especificidade que seriam posteriormente

trazidas pela LGPD. Ele pavimentou o caminho, portanto, para uma regulação mais robusta e detalhada sobre o tema.

Essa necessidade de regulamentação visa equilibrar os interesses econômicos e de inovação com a proteção dos direitos fundamentais dos cidadãos. A proteção de dados pessoais, portanto, não é apenas uma questão técnica ou jurídica, mas um ponto essencial para a confiança nas relações digitais e para a própria dignidade humana na era da informação, conforme ressaltado por diversos especialistas na área (Mendes, 2019; Wimmer, 2020).

No Brasil, a resposta mais completa a essa demanda global e local por segurança e transparência no tratamento de dados se materializou na Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Esta legislação estabelece um marco regulatório abrangente para o tratamento de dados pessoais, aplicável a qualquer operação realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, sob as condições especificadas na lei (Brasil, 2018, Art. 3º).

A LGPD, inspirada em leis internacionais como o RGPD (Regulamento Geral sobre a Proteção de Dados) da Europa, cria um sistema de regras detalhado para o tratamento de dados. Essas regras se baseiam em princípios muito importantes que devem guiar todas as formas de usar os dados. Vainzof (2020) e Valente (2020) mostram como esses princípios são a base da lei, o que exige que as empresas ajam com cuidado e responsabilidade. A lei define dez princípios principais em seu Artigo 6º – incluindo finalidade, necessidade, transparência e segurança (Brasil, 2018) – e seguir esses princípios é essencial para cumprir a lei.

QUADRO 01: Princípios e sua relação com a LGPD

Exigência/Obrigaçã Principal	Artigos Principais da LGPD (Referência)	Breve Descrição da Exigência
Observância dos Princípios	Art. 6º	Todo tratamento de dados deve seguir 10 princípios, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas.
Existência de Base Legal para Tratamento	Art. 7º (dados pessoais), Art. 11º (dados pessoais sensíveis)	O tratamento de dados pessoais só pode ser realizado se houver enquadramento em uma das bases legais previstas na lei (ex: consentimento, cumprimento de obrigação legal, execução de contrato, legítimo interesse, etc.).
Requisitos para o Consentimento	Art. 8º, Art. 9º	Quando a base legal for o consentimento, este deve ser livre, informado, inequívoco e para finalidades determinadas. O titular deve ter acesso fácil à informação sobre o tratamento.
Atendimento aos Direitos dos Titulares	Art. 9º, Art. 18º, Art. 19º, Art. 20º	Garantir que os titulares possam exercer seus direitos, como acesso aos dados, correção, anonimização, bloqueio, eliminação, portabilidade, informação sobre compartilhamento, revogação do consentimento, etc.
Manutenção de Registro das Operações de Tratamento	Art. 37º	As empresas devem manter registros detalhados de todas as operações de tratamento de dados pessoais que realizarem.
Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	Art. 5º, XVII; Art. 10º, §3º; Art. 38º	Documento que descreve os processos de tratamento de dados que podem gerar altos riscos às liberdades civis e aos direitos fundamentais, contendo medidas para mitigar esses riscos. Obrigatório em certas situações.
Indicação do Encarregado pelo Tratamento de Dados Pessoais (DPO)	Art. 5º, VIII; Art. 41º	Nomear uma pessoa (física ou jurídica, interna ou externa) para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Adoção de Medidas de Segurança, Técnicas e Administrativas	Art. 46º, Art. 47º, Art. 50º	Implementar medidas de segurança capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado.
Comunicação de Incidentes de Segurança	Art. 48º	Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o controlador deve comunicar à ANPD e ao titular em prazo razoável.
Aplicação de "Privacidade desde a Concepção" (Privacy by Design) e "Privacidade por Padrão" (Privacy by Default)	Art. 46º, §2º	Incorporar a proteção de dados desde a fase de concepção de produtos, serviços ou processos, e configurar sistemas com as opções mais protetivas à privacidade por padrão.

Transparência sobre o Tratamento de Dados	Art. 6º, VI; Art. 9º; Art. 23º, §5º	Fornecer informações claras, precisas e facilmente acessíveis aos titulares sobre como seus dados são tratados.
Observância das Regras para o Término do Tratamento de Dados	Art. 15º, Art. 16º	Definir e seguir procedimentos para o encerramento do tratamento de dados e sua eliminação segura, ressalvadas as hipóteses de conservação previstas na lei.
Cumprimento dos Requisitos para Transferência Internacional de Dados	Art. 33º a Art. 36º	Seguir as regras específicas caso haja necessidade de transferir dados pessoais para outros países ou organismos internacionais.
Implementação de Programa de Governança em Privacidade	Art. 50º	Adotar um programa que demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento da LGPD, aplicável a toda a organização.
Responsabilização e Ressarcimento de Danos	Art. 42º a Art. 45º	Os agentes de tratamento (controlador e operador) são responsáveis por danos patrimoniais, morais, individuais ou coletivos causados em violação à legislação de proteção de dados.
Demonstração de Adoção de Medidas Eficazes (Accountability)	Art. 6º, X; Art. 50º, §2º, I	Capacidade de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas adotadas.

Fonte: Elaborado pelo autor

O princípio da finalidade, por exemplo, determina que o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (Brasil, 2018, Art. 6º, I). Como Wimmer (2020) argumenta, a clareza na definição das finalidades é um dos fundamentos práticos essenciais para uma proteção de dados efetiva, evitando desvios e usos secundários não autorizados.

Intimamente ligados à finalidade estão os princípios da adequação e da necessidade. O primeiro exige compatibilidade do tratamento com as finalidades informadas, enquanto o segundo limita o tratamento ao mínimo necessário para a realização de suas finalidades (Brasil, 2018, Art. 6º, II, III). Estes princípios combatem a coleta indiscriminada de dados, promovendo uma gestão mais eficiente e focada, alinhada à ideia de dados como ativos de valor que precisam ser bem gerenciados para gerar resultados estratégicos, como defendem Amaral e Ribeiro (2017).

A transparência e o livre acesso são garantias essenciais para o titular, assegurando informações claras sobre o tratamento e consulta facilitada aos seus

dados (Brasil, 2018, Art. 6º, IV, VI). Para Mendes (2019), a transparência é condição sine qua non para um consentimento verdadeiramente informado e para o exercício efetivo dos demais direitos pelo titular, fortalecendo sua autonomia. As empresas precisam, portanto, estabelecer canais e procedimentos eficazes para atender a essas demandas informativas.

A segurança e a prevenção são princípios que impõem a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais (BRASIL, 2018, Art. 6º, VII, VIII; Art. 46). A implementação e manutenção dessas medidas técnicas demandam uma estrutura de governança de TI bem definida, como preconizado por Fernandes e Abreu (2016), para garantir sua eficácia e alinhamento com os objetivos de negócio e conformidade. Isso conecta a LGPD diretamente às disciplinas de segurança da informação e gestão de riscos corporativos.

Fundamental para a efetividade da lei é o princípio da responsabilização e prestação de contas (accountability), que exige que o agente de tratamento demonstre a adoção de medidas eficazes (Brasil, 2018, Art. 6º, X). Isso se alinha diretamente aos conceitos de governança de dados, que estabelecem frameworks de responsabilização para o manejo adequado dos dados, como exposto por Barbieri (2016), exigindo uma postura proativa e documentada das organizações.

A LGPD exige que haja sempre uma base legal válida para qualquer tratamento de dados pessoais, conforme listado no Artigo 7º. O consentimento do titular é a base legal mais conhecida (Brasil, 2018, Art. 5º, XII; Art. 8º), no entanto, é apenas uma entre dez hipóteses legais. Bioni (2019) analisa os detalhes e os limites da aplicação do consentimento.

Para que o consentimento seja considerado válido, ele precisa ser dado de forma livre, com informação clara, sem ambiguidades e para uma finalidade específica (Brasil, 2018, Art. 8º). Garantir essas condições no ambiente digital pode ser complexo, pois muitas vezes há uma diferença de informação e poder entre as partes. Autores como Bioni (2019) e Mendes (2019) destacam essa complexidade e questionam se o modelo de consentimento é sempre suficiente em determinados contextos digitais.

Além do consentimento, a lei prevê outras bases legais como o cumprimento de obrigação legal, a execução de contrato, o exercício regular de direitos e a proteção

da vida (Brasil, 2018, Art. 7º). A escolha da base legal adequada, como aponta Valente (2020), depende crucialmente do contexto e da finalidade específica do tratamento, exigindo análise caso a caso pela empresa.

O legítimo interesse do controlador ou de terceiro (Brasil, 2018, Art. 7º, IX; Art. 10) é outra base legal relevante, porém sua aplicação demanda um teste de balanceamento criterioso e transparência. O objetivo dessa análise cuidadosa e da transparência é garantir que os direitos do titular sejam respeitados. Vainzof (2020) destaca que é importante documentar, ou seja, registrar essa análise feita para fins de "accountability", que é a capacidade de demonstrar que a empresa adotou medidas eficazes para cumprir a lei.

A LGPD também fortalece significativamente os direitos dos titulares dos dados, listados no Artigo 18. Estes incluem a confirmação da existência do tratamento, o acesso aos dados e a correção de informações incorretas (Brasil, 2018, Art. 18, I, II, III). Garantir o exercício desses direitos de forma eficaz é um desafio operacional para muitas empresas.

Outros direitos incluem a anonimização, bloqueio ou eliminação de dados desnecessários ou tratados ilicitamente, a portabilidade dos dados e a eliminação de dados tratados com base no consentimento (Brasil, 2018, Art. 18, IV, V, VI). A operacionalização da portabilidade, em particular, pode exigir esforços significativos de padronização e compatibilidade entre sistemas.

O titular tem ainda o direito à informação sobre compartilhamento de dados, sobre as consequências de não consentir, e à revogação do consentimento (Brasil, 2018, Art. 18, VII, VIII, IX). O direito de oposição ao tratamento (Brasil, 2018, Art. 18, §2º) também é uma ferramenta importante de controle para o cidadão, reforçando a necessidade de as empresas estarem preparadas para gerenciar essas solicitações. A amplitude desses direitos reflete a evolução do conceito de proteção de dados discutida por Doneda (2006).

Para operacionalizar a conformidade, a LGPD define os agentes de tratamento: o controlador e o operador (Brasil, 2018, Art. 5º, VI, VII). A clara definição de papéis e responsabilidades entre eles, preferencialmente por meio de contrato, é essencial para evitar ambiguidades e garantir a proteção adequada dos dados, conforme interpretação de Vainzof (2020).

A figura do encarregado pelo tratamento de dados pessoais (DPO) (Brasil, 2018, Art. 5º, VIII; Art. 41) é central, atuando como ponte entre a empresa, os titulares e a ANPD (Autoridade Nacional de Proteção de Dados). Além de suas funções formais, o encarregado pode desempenhar um papel crucial na promoção de uma cultura de privacidade e na conscientização interna, alinhando-se aos modelos de conformidade baseados em awareness propostos por Siponen e Vance (2014).

A implementação da LGPD exige uma mudança cultural profunda. Não se trata apenas de cumprir regras, mas de incorporar a privacidade na estratégia e operações. Peck (2020) argumenta que o Direito Digital Aplicado, como no caso da LGPD, requer uma visão dinâmica e multidisciplinar, integrando conhecimentos jurídicos, tecnológicos e de gestão para uma adequação efetiva e contínua.

A adequação à LGPD está intrinsecamente ligada a práticas robustas de governança de dados e de TI. A governança de dados é crucial para gerenciar os dados como ativos de valor (Amaral; Ribeiro, 2017), estabelecendo políticas e responsabilidades claras que são fundamentais para atender aos requisitos da lei, como a manutenção de registros de tratamento e a garantia da qualidade dos dados.

A implementação de um framework de governança de dados, como os discutidos por Barbieri (2016), ajuda a estruturar processos como mapeamento de dados, classificação da informação e gestão de metadados, atividades essenciais para a conformidade com a LGPD e para a demonstração de accountability perante a ANPD e os titulares.

Paralelamente, a governança de TI fornece a estrutura para alinhar a tecnologia com os objetivos de negócio e com os requisitos de segurança e privacidade (Fernandes e Abreu, 2016). Uma boa governança de TI e de dados facilita o cumprimento de diversas exigências da LGPD, como a implementação e gestão contínua das medidas de segurança técnica e administrativa.

A LGPD determina explicitamente que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais (Brasil, 2018, Art. 46). A definição dessas medidas deve considerar a natureza dos dados, o contexto e a finalidade do tratamento, os riscos envolvidos e as tecnologias disponíveis, exigindo uma análise de risco contínua.

Um conceito importante introduzido pela lei é o de "privacy by design" e "privacy by default" (Brasil, 2018, Art. 46, §2º). Isso impacta diretamente o ciclo de desenvolvimento de software, exigindo que as equipes de tecnologia incorporem considerações de privacidade desde as fases iniciais, um desafio e uma oportunidade para a inovação responsável no setor tech. A natureza aplicada e prática do Direito Digital, como abordada por Peck (2020), é evidente neste requisito.

Em caso de incidentes de segurança relevantes, a comunicação à ANPD e ao titular é obrigatória (Brasil, 2018, Art. 48). A gestão de incidentes e a capacidade de resposta rápida são, portanto, componentes críticos da conformidade, com impactos diretos na reputação e na responsabilidade da empresa.

A LGPD também estabelece regras para a transferência internacional de dados pessoais (Brasil, 2018, Art. 33 e seguintes), um tema complexo e de grande relevância para empresas de tecnologia que operam em um mercado globalizado ou utilizam infraestrutura internacional. A adequação a essas regras é vital para a legalidade das operações transfronteiriças.

Embora a LGPD se aplique a organizações de todos os portes, sua implementação apresenta desafios particulares para as Pequenas e Médias Empresas (PMEs), especialmente as de tecnologia. Recursos limitados, falta de expertise interna e a complexidade inerente ao tratamento de dados no setor são barreiras significativas. A necessidade de investimentos em tecnologia e consultoria pode ser proibitiva para algumas PMEs.

A falta de conhecimento aprofundado sobre a lei e a necessidade de uma mudança cultural são obstáculos adicionais. Neste contexto, a conscientização em segurança e privacidade torna-se vital. A criação de uma cultura organizacional que valorize a proteção de dados, como implícito nos modelos de Siponen e Vance (2014), é um fator chave para a conformidade sustentável, especialmente em PMEs onde cada colaborador tem um papel relevante.

Apesar dos desafios, a adequação à LGPD oferece oportunidades. A conformidade pode aumentar a confiança de clientes e parceiros, fortalecer a reputação da marca e tornar-se um diferencial competitivo (Wimmer, 2020). Em um mercado cada vez mais consciente sobre privacidade, demonstrar respeito aos dados é um fator de atração e retenção de clientes.

O processo de adequação frequentemente leva à otimização de processos internos e à melhoria da qualidade dos dados (Valente, 2020). O mapeamento de dados e a revisão de fluxos informacionais podem revelar ineficiências e oportunidades de melhoria que transcendem a mera conformidade legal.

A implementação de medidas de segurança robustas não só cumpre a lei (Brasil, 2018, Art. 46), mas também aumenta a resiliência do negócio contra incidentes, evitando custos financeiros e reputacionais associados a vazamentos e as severas sanções administrativas previstas no Artigo 52 da LGPD.

As sanções por descumprimento da LGPD podem ser severas, incluindo multas significativas e até a proibição de atividades de tratamento (Brasil, 2018, Art. 52), reforçando a importância econômica e estratégica da conformidade para a sobrevivência e prosperidade das empresas no longo prazo.

Além de evitar sanções, a conformidade pode facilitar o acesso a novos mercados e parcerias, sinalizando maturidade em governança e gestão de riscos. Portanto, para as PMEs de tecnologia incubadas, como as do CRITT UFJF, encarar a LGPD estrategicamente pode transformar um desafio regulatório em uma alavanca para o crescimento. A análise desses desafios e oportunidades, à luz do referencial teórico construído, guiará a pesquisa empírica, buscando respostas concretas no contexto específico estudado, seguindo as boas práticas de elaboração de projetos de pesquisa (Vergara, 1998).

3 METODOLOGIA

A metodologia adotada neste trabalho segue a classificação proposta por Vergara (1998), sendo caracterizada como uma pesquisa de natureza qualitativa, de caráter descritivo e exploratório. O estudo foi estruturado em duas etapas complementares: uma pesquisa bibliográfica e uma pesquisa de campo.

Na primeira etapa, foi realizada uma ampla revisão bibliográfica com o objetivo de reunir e analisar materiais já publicados, como livros, artigos científicos, legislações e documentos oficiais que tratam da Lei Geral de Proteção de Dados (LGPD) e sua aplicação em pequenas e médias empresas (PMEs) do setor tecnológico. Essa abordagem permitiu o levantamento de diferentes perspectivas teóricas e práticas sobre o tema, constituindo uma base sólida para o

desenvolvimento da pesquisa empírica. As principais fontes consultadas incluíram obras de autores renomados na área, como Danilo Doneda (2006), Patricia Peck Pinheiro (2020), Bruno Bioni (2019), Rony Vainzof (2020), Laura Schertel Mendes (2019), Miriam Wimmer (2020) e Mariana Valente (2020). A análise dos dados secundários foi conduzida com base na técnica de análise de conteúdo, que possibilitou a identificação e interpretação de conceitos, desafios e estratégias associadas à adequação das empresas à LGPD.

Na segunda etapa, foi realizada uma pesquisa de campo com o objetivo de coletar dados primários que complementassem as informações obtidas na etapa anterior. Essa investigação empírica ocorreu durante os meses de maio e junho de 2025, tendo como foco 8 empresas de base técnica e tecnológica alocadas no Centro Regional de Inovação e Transferência de Tecnologia (CRITT) da Universidade Federal de Juiz de Fora (UFJF). Por meio dessa etapa, buscou-se compreender de que forma essas empresas estão implementando as diretrizes da LGPD em suas rotinas operacionais, bem como identificar as principais dificuldades enfrentadas nesse processo de conformidade.

A análise dos dados primários também foi realizada por meio da técnica de análise de conteúdo, permitindo categorizar e interpretar as informações coletadas de forma sistemática, com vistas a identificar padrões, tendências e boas práticas relacionadas à proteção de dados pessoais no contexto das PMEs tecnológicas.

3.1 PESQUISA DE CAMPO

Foi realizado uma pesquisa de campo com 8 empresas incubadas no Centro Regional de Inovação e Transferência de Tecnologia situada na Universidade Federal de Juiz de Fora. O CRITT-UFJF é um órgão institucional que se dedica a impulsionar a inovação e a transferência de tecnologia, contribuindo para o desenvolvimento regional e nacional. Ele atua como um Núcleo de Inovação Tecnológica (NIT), gerenciando a política de inovação da UFJF e coordenando a Incubadora de Base Tecnológica (IBT).

A análise prevista do questionário tem como objetivo identificar o grau de maturidade das empresas incubadas no CRITT/UFJF em relação à adequação à Lei Geral de Proteção de Dados (LGPD). Por meio de perguntas estruturadas em blocos

temáticos — como conhecimento da legislação, práticas de conformidade, governança de dados e percepção de benefícios — espera-se mapear os principais avanços, lacunas e desafios enfrentados por essas organizações. A abordagem quantitativa, complementada por interpretações qualitativas, permitirá compreender não apenas o estágio atual de adequação, mas também os fatores que influenciam a implementação das diretrizes legais no contexto das pequenas e médias empresas de base tecnológica.

Espera-se que os resultados obtidos revelem padrões de comportamento organizacional diante da LGPD, destacando tanto boas práticas quanto pontos críticos que demandam atenção. A análise dos dados será conduzida com base em frequências, percentuais e cruzamentos entre variáveis, possibilitando a identificação de correlações relevantes, como a relação entre o nível de conhecimento e a adoção de medidas práticas. Com isso, pretende-se oferecer subsídios para a formulação de estratégias de apoio e capacitação, contribuindo para o fortalecimento da cultura de proteção de dados e para a consolidação da conformidade como diferencial competitivo no ambiente de inovação.

4 ANÁLISE DOS RESULTADOS

Pergunta 1: Em uma escala de 1 (muito baixo) a 5 (muito alto), como você classifica o nível de conhecimento geral da sua empresa sobre os requisitos e as implicações da Lei Geral de Proteção de Dados (LGPD)?

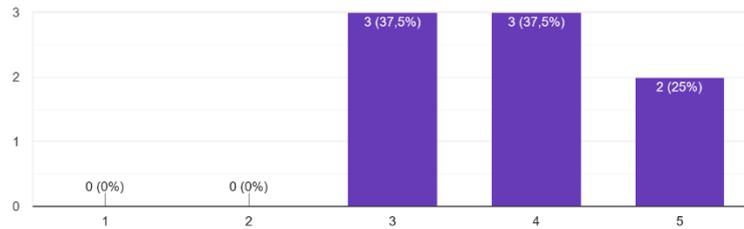
A maioria das empresas avaliou seu conhecimento sobre a LGPD como “alto” ou “médio” (ambos com 37,5%), enquanto 25% indicaram “muito alto”. Nenhuma se classificou nos níveis mais baixos, conforme Gráfico 1.

Isso demonstra familiaridade geral com a lei, mas também aponta para a ausência de domínio técnico mais aprofundado, o que pode limitar a aplicação prática da legislação.

Diante disso, é importante investir em capacitações que ajudem as empresas a transformar esse conhecimento inicial em ações efetivas de conformidade.

Gráfico 1: Dados estatísticos referentes à pergunta 1

Em uma escala de 1 (muito baixo) a 5 (muito alto), como você classifica o nível de conhecimento geral da sua empresa sobre os requisitos e as imp...ações da Lei Geral de Proteção de Dados (LGPD)?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 2: Na sua opinião, qual a importância da adequação à LGPD para a sustentabilidade e o sucesso da sua empresa no mercado atual?

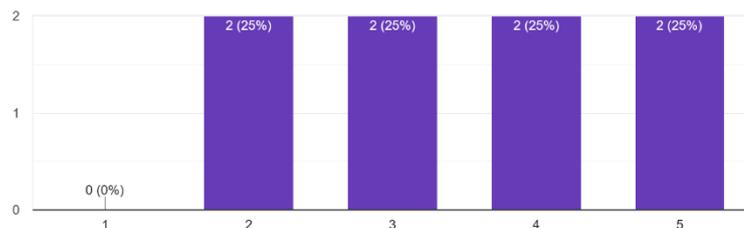
Conforme o Gráfico 2, as respostas foram distribuídas igualmente entre os níveis 2, 3, 4 e 5, cada um representando 25% das empresas. Nenhuma atribuiu nota mínima, o que indica que todas reconhecem algum grau de relevância na adequação à LGPD.

Essa distribuição uniforme revela que, embora haja consciência sobre a importância da conformidade, ainda existe incerteza quanto aos seus efeitos práticos no desempenho empresarial. A falta de consenso pode refletir diferentes níveis de maturidade organizacional e compreensão estratégica da legislação.

Diante disso, é essencial reforçar o papel da LGPD como instrumento de sustentabilidade e competitividade. Ações educativas e orientações práticas podem ajudar as empresas a perceberem a conformidade não apenas como obrigação, mas como oportunidade de fortalecimento institucional.

Gráfico 2: Dados estatísticos referentes à pergunta 2

Na sua opinião, qual a importância da adequação à LGPD para a sustentabilidade e o sucesso da sua empresa no mercado atual?
 8 respostas



Fonte: Dados da pesquisa, 2025.

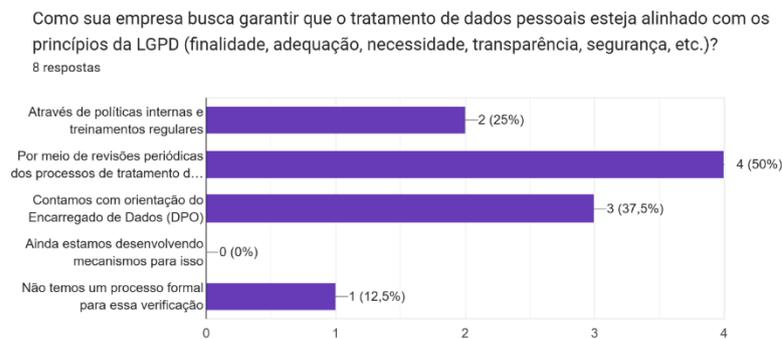
Pergunta 3: Como sua empresa busca garantir que o tratamento de dados pessoais esteja alinhado com os princípios da LGPD (finalidade, adequação, necessidade, transparência, segurança, etc.)?

Segundo o Gráfico 3, 50% das empresas realizam revisões periódicas dos processos de tratamento de dados, enquanto 37,5% contam com a atuação de um DPO. Outras 25% adotam políticas internas e treinamentos, e 12,5% não possuem processos formais.

Esses dados mostram que há esforço por parte das empresas para garantir conformidade, mas também revelam lacunas na padronização e formalização das práticas. A diversidade de abordagens reflete diferentes níveis de estrutura e recursos disponíveis.

Para fortalecer a governança de dados, é recomendável incentivar a troca de boas práticas e o acesso a consultorias especializadas. A consolidação de processos claros e contínuos é essencial para garantir segurança jurídica e maturidade organizacional.

Gráfico 3: Dados estatísticos referentes à pergunta 3



Fonte: Dados da pesquisa, 2025

Pergunta 4: Em que estágio se encontra o processo de adequação da sua empresa à LGPD?

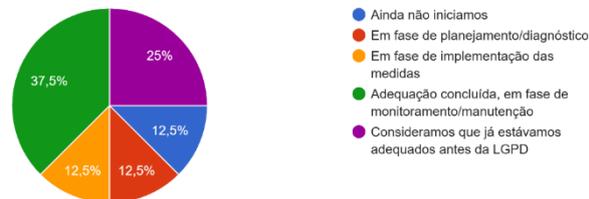
Como mostra o Gráfico 4, 37,5% das empresas já concluíram o processo de adequação e estão na fase de monitoramento. Outras 25% afirmaram estar adequadas desde antes da vigência da LGPD. Os demais se dividem entre planejamento, implementação e ausência de ações (cada um com 12,5%).

Essa distribuição revela que, embora parte das empresas tenha avançado significativamente, ainda há um grupo relevante em estágios iniciais ou sem iniciativas concretas. Isso evidencia desigualdade na capacidade de adaptação à legislação.

Para ampliar a conformidade, é necessário promover ações de apoio técnico e sensibilização, especialmente voltadas às empresas que ainda não iniciaram o processo. O incentivo à capacitação pode acelerar a adequação e garantir maior segurança jurídica no setor.

Gráfico 4: Dados estatísticos referentes à pergunta 4

Em que estágio se encontra o processo de adequação da sua empresa à LGPD?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 5: Sua empresa mantém um registro atualizado das operações de tratamento de dados pessoais (data mapping / inventário de dados), conforme exigido pela LGPD (Art. 37)?

Conforme o Gráfico 5, 37,5% das empresas afirmaram não manter um registro atualizado das operações de tratamento de dados pessoais, enquanto 25% possuem registros incompletos ou desatualizados. Apenas 12,5% mantêm esse controle de forma completa e regular, e o restante está em fase de elaboração ou planejamento.

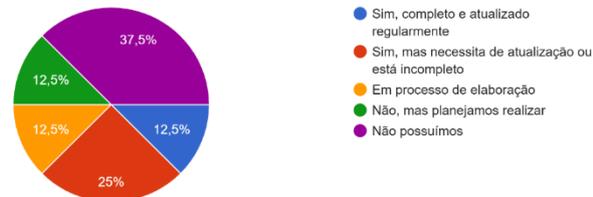
Esses dados revelam que, embora algumas empresas já tenham iniciado esse processo, a maioria ainda enfrenta dificuldades para atender plenamente ao Art. 37 da LGPD. A ausência ou precariedade desses registros compromete a capacidade de demonstrar conformidade, responder a incidentes e garantir os direitos dos titulares.

Diante disso, é essencial reforçar a importância do data mapping como ferramenta estratégica de governança. A oferta de modelos práticos, ferramentas acessíveis e capacitações específicas pode facilitar a implementação e promover maior segurança jurídica.

Gráfico 5: Dados estatísticos referentes à pergunta 5

Sua empresa mantém um registro atualizado das operações de tratamento de dados pessoais (data mapping / inventário de dados), conforme exigido pela LGPD (Art. 37)?

8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 6: Sua empresa identifica e documenta formalmente a base legal (Art 7º e 11º da LGPD) para cada uma de suas atividades de tratamento de dados pessoais?

De acordo com o Gráfico 6, apenas uma parte das empresas realiza a identificação da base legal para todas as atividades de tratamento. A maioria o faz apenas para a maioria ou algumas atividades, e há empresas que não realizam esse processo de forma sistemática.

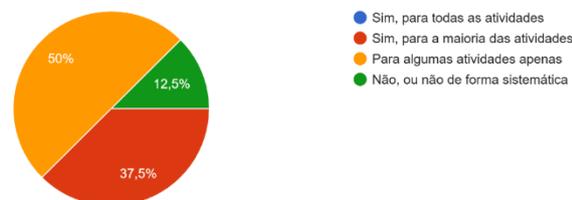
Essa falta de padronização representa um risco jurídico relevante, pois a ausência de documentação clara dificulta a prestação de contas à ANPD e compromete a transparência com os titulares dos dados.

É recomendável que as empresas estruturem processos formais para identificar e registrar a base legal de cada operação. Essa prática fortalece a segurança jurídica, facilita auditorias e reforça o compromisso com a conformidade legal.

Gráfico 6: Dados estatísticos referentes à pergunta 6

Sua empresa identifica e documenta formalmente a base legal (Art 7º e 11º da LGPD) para cada uma de suas atividades de tratamento de dados pessoais?

8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 7: Sua empresa designou um Encarregado pelo Tratamento de Dados Pessoais (DPO - Data Protection Officer), conforme Art. 41 da LGPD?

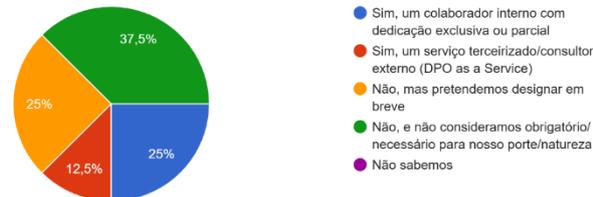
De acordo com o Gráfico 7, 37,5% das empresas ainda não designaram um DPO, por não considerarem essa medida obrigatória. Por outro lado, 25% já contam com um colaborador interno nessa função, 12,5% optaram por um serviço terceirizado, e outros 25% pretendem nomear um DPO em breve.

Esses dados revelam que, embora haja avanços, muitas empresas ainda subestimam o papel estratégico do DPO na governança de dados. A ausência desse profissional pode comprometer a efetividade das ações de conformidade e o relacionamento com os titulares e a ANPD.

É fundamental ampliar a conscientização sobre a importância do DPO e oferecer alternativas viáveis, como modelos compartilhados ou consultorias especializadas, especialmente para pequenas e médias empresas com recursos limitados.

Gráfico 7: Dados estatísticos referentes à pergunta 7

Sua empresa designou um Encarregado pelo Tratamento de Dados Pessoais (DPO - Data Protection Officer), conforme Art. 41 da LGPD?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 8: A empresa já realizou ou identificou a necessidade de realizar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) para atividades de tratamento consideradas de alto risco (Art. 38 da LGPD)?

Segundo o Gráfico 8, metade das empresas desconhece a exigência de elaboração de Relatórios de Impacto à Proteção de Dados (RIPD), enquanto 37,5% identificaram a necessidade, mas ainda não os realizaram. Apenas 12,5% já elaboraram esse tipo de relatório.

Esse cenário evidencia uma lacuna significativa de conhecimento e prática em relação à avaliação de riscos em atividades de tratamento de dados sensíveis. A ausência de RIPDs pode comprometer a capacidade de prevenção e resposta a incidentes.

Diante disso, é essencial promover a disseminação de informações sobre o RIPD e incentivar sua adoção como ferramenta de responsabilidade proativa. Capacitações e modelos simplificados podem facilitar sua aplicação, mesmo em empresas com estrutura reduzida.

Gráfico 8: Dados estatísticos referentes à pergunta 8

A empresa já realizou ou identificou a necessidade de realizar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) para atividades de trat...to consideradas de alto risco (Art. 38 da LGPD)?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 9: Sua empresa possui um programa de governança em privacidade (conforme Art. 50 da LGPD), que estabeleça políticas, procedimentos, ações educativas e mecanismos de supervisão interna e mitigação de riscos?

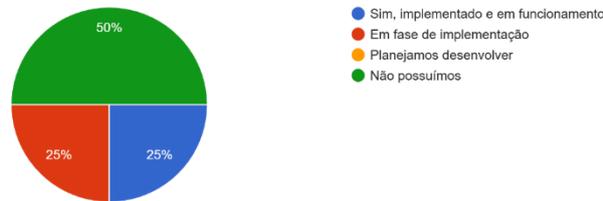
Conforme o Gráfico 9, a maioria das empresas ainda não possui um programa estruturado de governança em privacidade. Algumas estão em fase de planejamento ou implementação, e apenas uma pequena parcela já conta com um programa completo em funcionamento.

Esses dados mostram que, embora haja uma crescente conscientização sobre o tema, muitas organizações ainda enfrentam dificuldades para estruturar políticas, ações educativas e mecanismos de supervisão. A ausência de um programa robusto compromete a maturidade em proteção de dados.

Para avançar nesse aspecto, é recomendável fomentar a adoção de programas de governança adaptados à realidade das pequenas empresas. O acesso a modelos práticos, capacitação e suporte técnico pode acelerar a implementação e fortalecer a cultura de privacidade.

Gráfico 9: Dados estatísticos referentes à pergunta 9

Sua empresa possui um programa de governança em privacidade (conforme Art. 50 da LGPD), que estabeleça políticas, procedimentos, ações educati...os de supervisão interna e mitigação de riscos?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 10: Para o processo de adequação à LGPD, sua empresa buscou ou utiliza algum tipo de apoio externo (ex: consultoria jurídica, consultoria de TI especializada)?

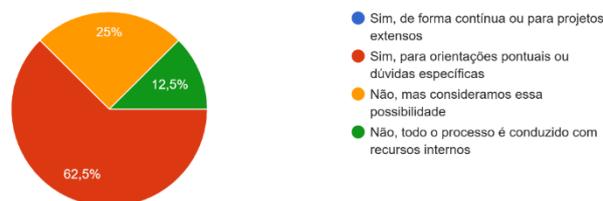
Conforme o Gráfico 10, 62,5% das empresas buscaram apoio externo pontual, como consultorias jurídicas ou de TI, para esclarecer dúvidas durante a adequação à LGPD. Outras 25% ainda não utilizaram esse suporte, mas consideram essa possibilidade, enquanto 12,5% conduzem todo o processo com recursos internos.

Esses dados mostram que, mesmo entre empresas que internalizam a maior parte das ações, há reconhecimento da importância de suporte técnico especializado. A complexidade da legislação torna o apoio externo um recurso estratégico para garantir segurança e eficiência na conformidade.

Diante disso, é recomendável ampliar o acesso a consultorias, parcerias institucionais e materiais orientativos. A combinação entre esforços internos e suporte externo pode ser decisiva para uma adequação mais segura e alinhada às exigências legais.

Gráfico 10: Dados estatísticos referentes à pergunta 10

Para o processo de adequação à LGPD, sua empresa buscou ou utiliza algum tipo de apoio externo (ex: consultoria jurídica, consultoria de TI especializada)?
 8 respostas



Fonte: Dados da pesquisa, 2025.

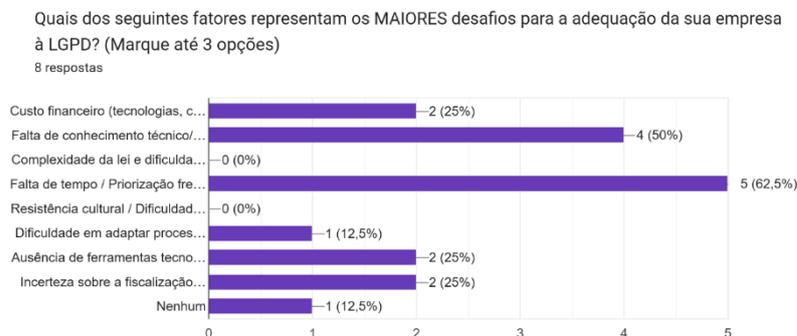
Pergunta 11: Quais dos seguintes fatores representam os MAIORES desafios para a adequação da sua empresa à LGPD? (Marque até 3 opções)

Segundo o Gráfico 11, o principal desafio apontado pelas empresas foi a falta de tempo ou dificuldade de priorização (62,5%), seguido pela carência de conhecimento técnico ou jurídico (50%). Outros obstáculos incluem custos financeiros, ausência de ferramentas tecnológicas e incertezas regulatórias (25% cada).

Esses dados evidenciam que os maiores entraves à conformidade estão ligados à limitação de recursos e à sobrecarga operacional, especialmente em pequenas e médias empresas. A dificuldade em adaptar processos internos também foi mencionada, embora em menor escala.

Para superar esses desafios, é fundamental investir em capacitação, apoio técnico acessível e políticas públicas que incentivem a adequação. A criação de soluções práticas e escaláveis pode facilitar o cumprimento da LGPD e fortalecer a cultura de proteção de dados.

Gráfico 11: Dados estatísticos referentes à pergunta 11



Fonte: Dados da pesquisa, 2025.

Pergunta 12: Em uma escala de 1 (muito fácil) a 5 (muito difícil), qual foi a dificuldade da sua empresa em traduzir os requisitos legais da LGPD em ações e controles práticos no dia a dia?

Conforme o Gráfico 12, 50% das empresas atribuíram nota 3 e 37,5% nota 4 para a dificuldade de aplicar os requisitos da LGPD no dia a dia. Apenas 12,5% indicaram nota 2, e nenhuma empresa considerou o processo muito fácil ou extremamente difícil.

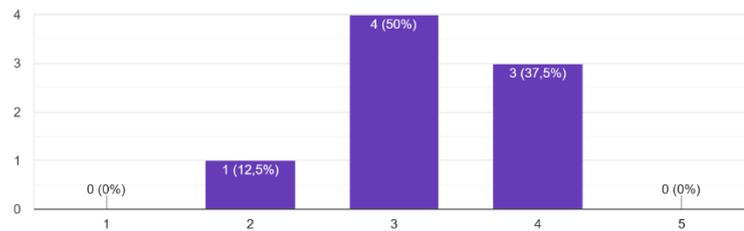
Esses dados indicam que a maioria das empresas percebe a adequação como um desafio moderado, o que pode estar relacionado à complexidade da legislação, à

falta de exemplos práticos e à dificuldade de adaptar rotinas internas. A ausência de notas extremas sugere que o problema não está na compreensão geral da lei, mas na sua operacionalização.

Para facilitar esse processo, é essencial disponibilizar materiais explicativos, guias práticos e modelos adaptados à realidade das pequenas e médias empresas. A tradução da LGPD em ações concretas é fundamental para garantir sua efetividade e a segurança jurídica das organizações.

Gráfico 12: Dados estatísticos referentes à pergunta 12

Em uma escala de 1 (muito fácil) a 5 (muito difícil), qual foi a dificuldade da sua empresa em traduzir os requisitos legais da LGPD em ações e controles práticos no dia a dia?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 13: Sua empresa possui procedimentos formais e canais de comunicação claros para receber e atender às requisições dos titulares de dados (Art. 18 da LGPD)? Qual o tempo médio de resposta?

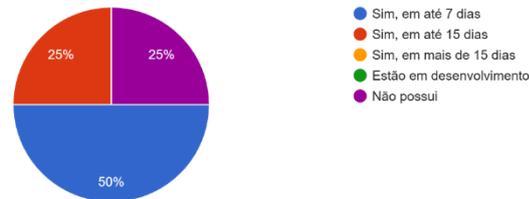
De acordo com o Gráfico 13, 50% das empresas afirmaram possuir canais formais para atender às requisições dos titulares, com tempo médio de resposta de até 7 dias. Outras 25% respondem em até 15 dias, enquanto os 25% restantes não possuem procedimentos estruturados.

Esses dados mostram que, embora a maioria das empresas tenha se organizado para cumprir o Art. 18 da LGPD, ainda há uma parcela significativa que precisa avançar nesse aspecto. A ausência de canais claros compromete a transparência e pode afetar a confiança dos titulares.

É recomendável que todas as empresas estabeleçam fluxos de atendimento bem definidos, com prazos razoáveis e comunicação acessível. Isso não apenas garante o cumprimento da lei, mas também fortalece a relação com os usuários e a reputação institucional.

Gráfico 13: Dados estatísticos referentes à pergunta 13

Sua empresa possui procedimentos formais e canais de comunicação claros para receber e atender às requisições dos titulares de dados (Art. 18 da LGPD)? Qual o tempo médio de resposta?
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 14: Quais medidas de segurança TÉCNICAS E ADMINISTRATIVAS (Art. 46 da LGPD) sua empresa implementou ou reforçou para proteger os dados pessoais? (Marque todas as aplicáveis)

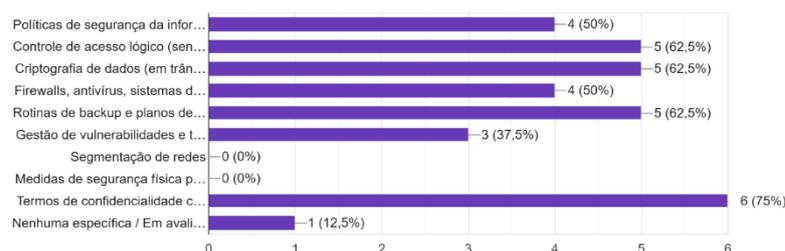
Segundo o Gráfico 14, 75% das empresas adotaram termos de confidencialidade com colaboradores, e 62,5% utilizam medidas como controle de acesso, criptografia e backup com plano de recuperação. Outras práticas, como políticas de segurança e testes de vulnerabilidade, também foram mencionadas.

Apesar do esforço evidente, nenhuma empresa relatou adotar segmentação de redes ou medidas de segurança física para dados em papel ou mídias removíveis, o que revela uma lacuna na proteção de dados não digitais. Apenas 12,5% afirmaram não ter implementado nenhuma medida ou estarem em fase de avaliação.

Esses dados reforçam a importância de uma abordagem integrada de segurança da informação. A ampliação das medidas técnicas e administrativas, incluindo proteção física e segmentação de redes, é essencial para mitigar riscos e garantir a conformidade com a LGPD.

Gráfico 14: Dados estatísticos referentes à pergunta 14

Quais medidas de segurança TÉCNICAS E ADMINISTRATIVAS (Art. 46 da LGPD) sua empresa implementou ou reforçou para proteger os dados pessoais? (Marque todas as aplicáveis)
 8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 15: Como a sua empresa garante a transparência aos titulares sobre o tratamento de seus dados pessoais (Art. 6º, VI e Art. 9º da LGPD)?

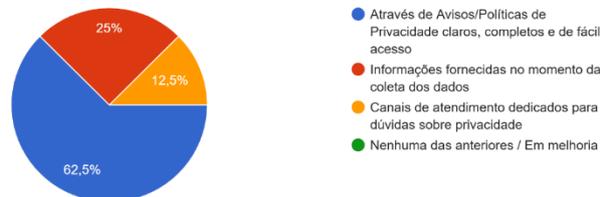
Segundo o Gráfico 15, 62,5% das empresas utilizam políticas de privacidade claras e acessíveis para garantir a transparência no tratamento de dados. Outras 25% informam os titulares no momento da coleta, e apenas 12,5% mantêm canais específicos para dúvidas sobre privacidade.

Esses dados mostram que a maioria das empresas adota práticas básicas de transparência, mas ainda há espaço para ampliar os canais de comunicação com os titulares. A presença de políticas acessíveis é um bom indicativo, mas o engajamento direto ainda é limitado.

Para fortalecer a confiança dos usuários e garantir conformidade com a LGPD, é recomendável combinar políticas claras com comunicação ativa e canais de atendimento dedicados. Essa abordagem integrada reforça a credibilidade e o compromisso com a proteção de dados.

Gráfico 15: Dados estatísticos referentes à pergunta 15

Como a sua empresa garante a transparência aos titulares sobre o tratamento de seus dados pessoais (Art. 6º, VI e Art. 9º da LGPD)?
8 respostas



Fonte: Dados da pesquisa, 2025.

Pergunta 16: Como sua empresa majoritariamente enxerga a LGPD?

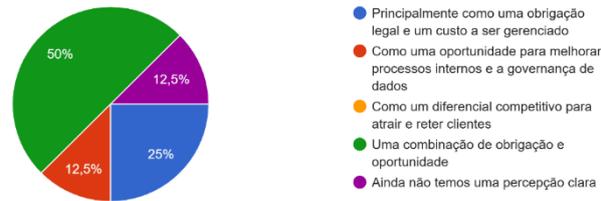
Como apresentado no Gráfico 16, 50% das empresas percebem a LGPD como uma combinação entre obrigação legal e oportunidade de melhoria. Essa visão demonstra um entendimento mais estratégico da legislação, reconhecendo seu potencial para fortalecer a governança de dados e agregar valor institucional.

Ainda segundo o gráfico, 25% das empresas veem a LGPD apenas como uma obrigação legal e um custo, enquanto 12,5% a consideram uma oportunidade para melhorar processos internos. Nenhuma empresa a identificou como diferencial competitivo, e 12,5% não têm uma percepção clara sobre o tema.

Esses dados reforçam a necessidade de ampliar o diálogo sobre os benefícios estratégicos da LGPD, especialmente no fortalecimento da confiança dos clientes, na mitigação de riscos e na construção de uma cultura organizacional orientada à privacidade.

Gráfico 16: Dados estatísticos referentes à pergunta 16

Como sua empresa majoritariamente enxerga a LGPD?
 8 respostas



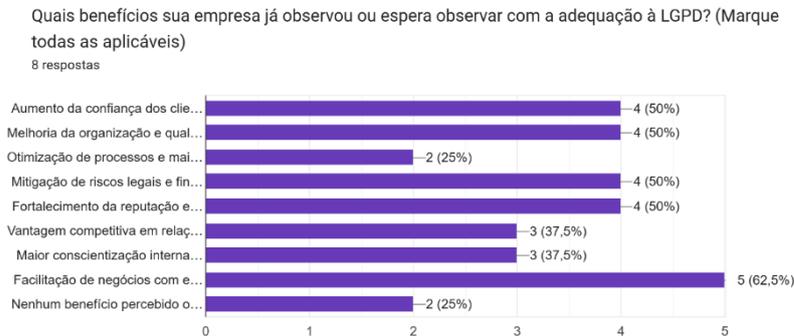
Fonte: Dados da pesquisa, 2025.

Pergunta 17: Quais benefícios sua empresa já observou ou espera observar com a adequação à LGPD? (Marque todas as aplicáveis)

De acordo com o Gráfico 17, o benefício mais citado pelas empresas foi a facilitação de negócios com parceiros internacionais (62,5%), seguido por aumento da confiança dos clientes, melhoria na qualidade dos dados, mitigação de riscos e fortalecimento da reputação (50%).

O gráfico também mostra que 37,5% das empresas identificaram como benefícios a vantagem competitiva frente a concorrentes não adequados e o aumento da conscientização interna. Apenas 25% mencionaram ganhos operacionais, e o mesmo percentual afirmou não ter percebido ou esperado benefícios até o momento.

Esses resultados indicam que a maioria das empresas já reconhece a adequação à LGPD como uma oportunidade estratégica. No entanto, ainda é necessário promover ações de sensibilização e compartilhar boas práticas para ampliar essa percepção e incentivar a adoção plena da legislação.

Gráfico 17: Dados estatísticos referentes à pergunta 17


Fonte: Dados da pesquisa, 2025.

Pergunta 18: Você acredita que a adequação eficaz à LGPD pode ser transformada em um diferencial competitivo para sua empresa no setor de tecnologia?

O Gráfico 18 mostra que 37,5% das empresas acreditam que a adequação à LGPD pode definitivamente se tornar um diferencial competitivo. Outras 25% consideram essa possibilidade viável, enquanto 25% adotam uma postura mais cautelosa, condicionando o impacto à percepção dos clientes.

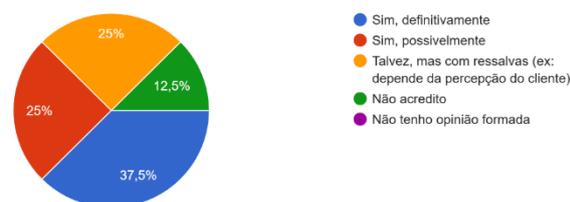
Apenas 12,5% das empresas não acreditam nesse potencial, o que indica que, apesar de algumas dúvidas, a maioria reconhece que a conformidade pode ir além da obrigação legal. A valorização da privacidade tende a crescer, especialmente em setores baseados em tecnologia e dados.

Para que a LGPD se torne um diferencial real, é necessário integrá-la à proposta de valor da empresa e comunicar esse compromisso de forma estratégica. A proteção de dados pode ser um elemento-chave para conquistar e fidelizar clientes em um mercado competitivo.

Gráfico 18: Dados estatísticos referentes à pergunta 18

Você acredita que a adequação eficaz à LGPD pode ser transformada em um diferencial competitivo para sua empresa no setor de tecnologia?

8 respostas



Fonte: Dados da pesquisa, 2025.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa objetivou analisar os efeitos e implicações da LGPD nas pequenas e médias empresas de tecnologia incubadas pelo Centro Regional de Inovação e Transferência de Tecnologia da Universidade Federal de Juiz de Fora (CRITT/UFJF). Neste sentido, buscou compreender como essas empresas têm interpretado e aplicado as diretrizes da LGPD, além de identificar os principais desafios e oportunidades envolvidos nesse processo de adequação.

A análise conjugada dos referenciais teóricos e dos dados empíricos revelou que, embora haja avanços na percepção sobre a importância da proteção de dados, persistem lacunas significativas na efetiva implementação dos dispositivos legais e dos princípios estruturantes da LGPD. Para as PMEs de tecnologia, a conformidade com a LGPD traz uma série de desafios, principalmente devido às limitações de recursos e à complexidade das exigências regulatórias. No entanto, a pesquisa também apontou que a conformidade pode resultar em benefícios significativos, como o aumento da confiança dos clientes, a melhoria da reputação da empresa e a abertura de novas oportunidades de negócios. A adoção de práticas robustas de governança de dados, a implementação de medidas de segurança adequadas e a educação contínua dos funcionários são estratégias fundamentais para alcançar esses benefícios.

Considerando os princípios estabelecidos no Art. 6º da LGPD — como finalidade, adequação, necessidade, transparência e responsabilização — observou-se que apenas 12,5% das empresas afirmam possuir políticas completas e bem divulgadas sobre proteção de dados. Essa constatação reforça o alerta feito por autores como Mendes (2019) e Wimmer (2020), que destacam a centralidade da transparência como condição para o exercício pleno dos direitos dos titulares e como instrumento essencial de legitimação do tratamento de dados.

Embora 100% das empresas reconheçam a importância da conformidade com a LGPD, apenas 25% relataram ter elaborado o Relatório de Impacto à Proteção de Dados (RIPD), e 37,5% desconhecem essa obrigação. Esse dado vai ao encontro das análises de Bioni (2019), que aponta a complexidade da legislação

como uma barreira significativa para as PMEs, sobretudo na ausência de programas de governança bem estruturados.

A presença do encarregado (DPO), figura prevista no Art. 41 da LGPD e considerada estratégica por autores como Vainzof (2020), ainda é incipiente: 37,5% das empresas não designaram qualquer responsável pela interlocução com a ANPD e os titulares. Isso compromete diretamente a accountability, outro princípio essencial da LGPD, conforme destacam Doneda (2006) e Peck (2020), que defendem a necessidade de uma abordagem proativa, documentada e demonstrável da conformidade.

Os dados também revelam que 62,5% das empresas apontam a falta de tempo como principal desafio, seguida pela ausência de conhecimento técnico-jurídico (50%) e pelas limitações financeiras (25%). Essas dificuldades estruturais e operacionais, embora compreensíveis no contexto das PMEs, indicam que a conformidade ainda está distante de se tornar parte da cultura organizacional, conforme sugerido nos modelos de cultura de privacidade de Siponen e Vance (2014). A conformidade não deve se limitar a práticas formais ou pontuais, mas integrar a lógica de funcionamento dos processos e da tomada de decisão.

Ainda assim, a pesquisa revelou pontos positivos e possibilidades futuras: 50% das empresas já reconhecem a LGPD como uma oportunidade para melhoria de processos, e 75% identificam que a conformidade pode aumentar a confiança dos clientes — elementos alinhados à visão de Valente (2020), que compreende a proteção de dados como diferencial competitivo e base para inovação sustentável.

Em conclusão, a conformidade com a LGPD é essencial para garantir a proteção dos dados pessoais e promover a confiança dos clientes, especialmente no contexto das PMEs de tecnologia. A adaptação às exigências da LGPD não apenas evita penalidades legais, mas também posiciona as PMEs de tecnologia como líderes em proteção de dados, contribuindo para um ambiente de negócios mais seguro, confiável e inovador. Dessa maneira, a LGPD deve ser compreendida não somente como um desafio legal, mas também como uma alavanca para o fortalecimento institucional, a valorização da ética digital e o estímulo à inovação responsável no ecossistema empresarial brasileiro.

Assim, embora sejam reconhecidos os desafios, percebe-se que a adequação à LGPD pode ser um fator de fortalecimento institucional para as PMEs tecnológicas. Para que isso se concretize, é necessário superar a visão da LGPD como mero ônus legal e incorporá-la como um valor estratégico. A construção dessa mudança exige não apenas esforço interno, mas o engajamento de universidades, incubadoras, órgãos reguladores e entidades de apoio, que devem atuar de forma coordenada para fornecer capacitação, modelos acessíveis e suporte técnico contínuo.

Como indicações para estudos futuros, sugere-se a realização das análises aqui propostas em outros tipos e portes de organizações, a fim de que possam ser compreendidos os diferentes desafios, bem como as práticas de adequação à LDGP em empresas de outras naturezas, o que oferece a possibilidade de compreender com profundidade outros contextos e a construção de panoramas comparativos. Além disso, indica-se também o acompanhamento das empresas aqui relatadas, realizando-se novos estudos com o decorrer do tempo no próprio centro alvo desta pesquisa de campo, a fim de que seja possível obter uma visão não somente circunstancial, mas igualmente longitudinal deste processo, uma vez que ele é compreendido como algo que ocorre paralelamente à mudanças essenciais no âmbito da cultura organizacional e, desta forma, requer tempo para sua efetiva realização.

Por fim, é fundamental pontuar as limitações desta pesquisa para a correta interpretação de seus resultados. O estudo se concentrou em um recorte específico — pequenas e médias empresas de tecnologia vinculadas ao ecossistema do CRITT/UFJF — com uma amostra não probabilística e de tamanho reduzido. Dessa forma, os achados aqui apresentados, embora relevantes para o contexto analisado, não permitem generalizações estatísticas para o universo mais amplo de PMEs no Brasil. Reconhecer tais delimitações não invalida as contribuições do trabalho, mas as contextualiza, reforçando a importância das sugestões de estudos futuros para a construção de um conhecimento mais abrangente sobre o tema.

ABSTRACT

The digital transformation of recent decades has intensified the use of personal data, making it a strategic asset in economic and social spheres, while also raising concerns about privacy and information security. In response, Brazil enacted the General Data Protection Law (LGPD) in 2018, which came into effect in 2020. The law aims to regulate data processing and ensure transparency, security, and respect for citizens' rights. For small and medium-sized technology enterprises (SMEs), compliance with the LGPD presents significant challenges, given their heavy reliance on data and limited technical and financial resources. However, legal compliance can also serve as a strategic opportunity to strengthen reputation, increase market trust, and adopt more sustainable governance practices. This study analyzes the impact of the LGPD on SMEs incubated by the CRITT/UFJF (Regional Center for Innovation and Technology Transfer at the Federal University of Juiz de Fora). It investigates how these companies interpret and apply the law's principles, what technical and administrative measures have been implemented to ensure data security, and what internal and external benefits are being perceived through compliance. The research also explores how responsible data management can drive innovation. The goal is to contribute to the academic debate and offer practical solutions for a sector still adapting to this new legal framework.

Keywords: Personal Data; Data Protection; Brazilian General Data Protection Law (LGPD); Small and Medium-Sized Enterprises (SMEs); Digital Transformation; Information Security.

REFERÊNCIAS

AMARAL, D. A. R.; RIBEIRO, F. F. **Gestão e governança de dados:** promovendo dados como ativo de valor nas empresas. São Paulo: Novatec Editora, 2017.

BARBIERI, C. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Brasport, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. São Paulo: Editora Revista dos Tribunais, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 15 de janeiro de 2025

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 24 de maio de 2025

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FERNANDES, A. A.; ABREU, V. F. de. **Implantando a governança de TI: da estratégia à gestão de processos e serviços**. 4. ed. Rio de Janeiro: Brasport, 2016.

MENDES, Laura Schertel. **Privacidade e proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Editora Revista dos Tribunais, 2019.

PECK, Patricia. **Direito digital aplicado 5.0**. São Paulo: Saraiva, 2020.

SIPONEN, M.; VANCE, A. **Building an awareness-centered information security policy compliance model**. *Industrial Management & Data Systems*, v. 114, n. 4, p. 715–731, 2014.

UNIVERSIDADE FEDERAL DE JUIZ DE FORA. *Centro Regional de Inovação e Transferência de Tecnologia – CRITT*. Disponível em: <https://www2.ufjf.br/critt/>. Acesso em: 10 jun. 2025.

VAINZOF, Rony. **Comentários à Lei Geral de Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2020.

VALENTE, Mariana. **Proteção de dados no Brasil: a Lei Geral de Proteção de Dados (LGPD) comentada**. São Paulo: Thomson Reuters Brasil, 2020.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 1998.

WIMMER, Miriam. **Proteção de dados pessoais: fundamentos teóricos e práticos**. São Paulo: Saraiva, 2020.