INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
CAMPUS JOÃO PESSOA
DIRETORIA DE ENSINO SUPERIOR
UNIDADE ACADÊMICA DE GESTÃO E NEGÓCIOS
CURSO SUPERIOR DE BACHARELADO EM ADMINISTRAÇÃO

GABRIELLY BEZERRA DOS SANTOS

LGPD: O CASO DA TELLME SCHOOL

João Pessoa
2025

GABRIELLY BEZERRA DOS SANTOS

LGPD: O CASO DA TELLME SCHOOL

Unidade Acadêmica de Gestão e Negócios

TRABALHO DE CONCLUSÃO DE CURSO apresentado ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), curso Superior de Bacharelado em Administração, como requisito institucional para a obtenção do Grau de Bacharel(a) em **ADMINISTRAÇÃO**.

Orientador(a): Caroline Helena Limeira Pimentel Perrusi

JOÃO PESSOA
2025

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Nilo Peçanha do IFPB, *Campus* João Pessoa

S237l Santos, Gabrielly Bezerra dos.

LGPD : o caso da Tellme School / Gabrielly Bezerra dos Santos. – 2025.
52 f. : il.
TCC (Graduação – Curso Superior de Bacharelado em Administração) – Instituto Federal de Educação da Paraíba / Unidade Acadêmica de Gestão e Negócios, 2025.
Orientação: Profª. Carolina Helena Limeira Pimentel Perrusi.

1.Lei geral de proteção de dados (LGPD). 2. Proteção de dados. 3. Conformidade legal. 4. Comunicação organizacional. 5. Estudo de caso. I. Título.

CDU 340.13:004.56(043)

.: Bibliotecária responsável: Lucrecia Camilo de Lima – CRB 15/132

AVALIAÇÃO 37/2025 - CCSBA/UA5/UA/DDE/DG/JP/REITORIA/IFPB

Em 20 de agosto de 2025.

FOLHA DE APROVAÇÃO

GABRIELLY BEZERRA DOS SANTOS

Matrícula 20192460071

LGPD: O CASO DA TELLME SCHOOL

TRABALHO DE CONCLUSÃO DE CURSO apresentado em **20/08/2025** no Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), Curso Superior de Bacharelado em Administração, como requisito institucional para a obtenção do Grau de Bacharel(a) em **ADMINISTRAÇÃO.**

Resultado: APROVADO

João Pessoa, **20** de agosto de 2025.

BANCA EXAMINADORA:

(assinaturas eletrônicas via SUAP)

Caroline Helena Limeira Pimentel Perrusi (IFPB)

Orientador(a)

Giorgione Mendes Ribeiro Junior (IFPB)

Examinador(a) interno(a)

Marcos José de Oliveira Lima Filho (IFPB)

Examinador(a) interno(a)

Documento assinado eletronicamente por:

- **Caroline Helena Limeira Pimentel Perrusi, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 20/08/2025 21:12:37.
- **Giorgione Mendes Ribeiro Junior, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 20/08/2025 21:13:53.
- **Marcos Jose de Oliveira Lima Filho, PROF ENS BAS TEC TECNOLOGICO-SUBSTITUTO**, em 22/08/2025 11:31:10.

Este documento foi emitido pelo SUAP em 20/08/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código 752181
Verificador: df59ebc440
Código de Autenticação:

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter me proporcionado essa experiência e ter me dado forças para concluir, mais esta etapa da minha vida.

A minha orientadora Caroline Helena Limeira Pimentel Perrusi, sou imensamente grata pela orientação, dedicação e paciência ao longo de toda a pesquisa. Suas valiosas contribuições e insights foram fundamentais para o desenvolvimento deste trabalho, e por isso estou profundamente grata.

Aos meus familiares, pelo apoio incondicional, compreensão e por estarem ao meu lado nos momentos de dificuldade. A presença de vocês foi um alicerce essencial para a conclusão deste TCC.

Agradeço também aos profissionais e instituições que, direta ou indiretamente, contribuíram para a realização desta pesquisa. Sem as informações, recursos e incentivos que obtive, este trabalho não teria se concretizado.

Por fim, a todos que, de alguma forma, colaboraram e apoiaram este processo, o meu mais sincero agradecimento. Cada um de vocês teve um papel fundamental nesta realização.

RESUMO

Na atualidade, a preocupação com liberdade, segurança e privacidade dos dados pessoais e empresariais tem aumentado significativamente. É cada vez mais comum que as redes de comunicação divulguem notícias sobre o vazamento de informações corporativas. Isso se deve, em grande parte, à ausência, por muitos anos, de regulamentações que obrigassem as empresas a adotarem medidas rigorosas para proteger esses dados. Diante desse cenário, este estudo tem como objetivo fornecer uma visão geral da Lei Geral de Proteção de Dados (LGPD), analisando sua aplicação na empresa TellMe School. A pesquisa foi conduzida de forma bibliográfica, por meio de estudo de caso, com caráter teórico e empírico, abordagem qualitativa, de caráter exploratório e baseada nos métodos comparativo e empírico, que investigaram percepções, práticas e dificuldades no processo de adequação à LGPD. A autora também participou como respondente do questionário, configurando-se como pesquisadora e respondente participante. Os resultados apontaram diferenças nas percepções entre gestores e colaboradores, revelando que, apesar das iniciativas já aplicadas, o processo de adequação ocorre de forma gradual e ainda carece de integração entre setores e de aplicação efetiva das práticas por toda a organização. Ainda existem fragilidades na comunicação interna, na capacitação da equipe, no acompanhamento das ações e na adoção de tecnologias apropriadas, agravadas pela ausência de suporte técnico especializado. A gestão busca atender às diretrizes da Autoridade Nacional de Proteção de Dados (ANPD) e inclui cláusulas de proteção nos contratos com clientes, demonstrando comprometimento inicial; entretanto, a inexistência de notificações por descumprimento não assegura total conformidade, podendo refletir limitações na fiscalização. Apesar do número reduzido de participantes, característico de estudos de caso em pequenas empresas, as informações coletadas se mostraram consistentes e revelaram avanços, desafios persistentes e pontos críticos no cotidiano organizacional frente à LGPD.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD). Proteção de da
Conformidade legal. Comunicação organizacional. Estudo de caso.

ABSTRACT

Currently, concerns about the freedom, security, and privacy of personal and corporate data have significantly increased. It has become increasingly common for communication networks to report corporate data breaches. This is largely due to the long-standing absence of regulations requiring companies to adopt strict measures to protect such data. In this context, this study aims to provide an overview of the General Data Protection Law (LGPD), analyzing its application within the company TellMe School. The research was conducted through a bibliographic review and case study, with a theoretical and empirical nature, using a qualitative, exploratory approach based on comparative and empirical methods, which investigated perceptions, practices, and challenges in the process of adapting to the LGPD. The author also participated as a respondent to the questionnaire, acting as both researcher and participating respondent. The results revealed differences in perceptions between managers and employees, indicating that, despite the initiatives already implemented, the adaptation process is happening gradually and still lacks integration between departments and effective implementation of practices throughout the organization. There are still weaknesses in internal communication, team training, monitoring of actions, and the adoption of appropriate technologies, worsened by the lack of specialized technical support. The management seeks to comply with the guidelines of the National Data Protection Authority (ANPD) and includes protection clauses in contracts with clients, demonstrating initial commitment; however, the absence of notifications for non-compliance does not ensure full adherence, potentially reflecting limitations in oversight. Despite the small number of participants—characteristic of case studies in small businesses—the data collected proved consistent and revealed progress, ongoing challenges, and critical points in the organization's daily routine with regard to LGPD compliance.

Keywords: General Data Protection Law (LGPD). Data protection. Legal compliance. Organizational communication. Case study.

LISTA DE ABREVIATURAS E SIGLAS

ANPD: Autoridade Nacional de Proteção de Dados
CDC: Código de Defesa do Consumidor
CPF: Cadastro de Pessoas Físicas
DPO: Data Protection Officer
EPP: Empresas de Pequeno Porte
GDPR: General Data Protection Regulation
LGPD: Lei Geral de Proteção de Dados
ME: Microempresa
MEI: Microempreendedor Individual
RIPD: Relatório de Impacto à Proteção de Dados Pessoais
SERPRO: Serviço Federal de Processamento de Dados
VPN: Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

A crescente digitalização das interações sociais e comerciais trouxe desafios inéditos para a proteção de dados pessoais, tornando essencial a criação de normas que garantam a privacidade e a segurança dos indivíduos nesse novo cenário. Antes da publicação da lei geral de proteção de dados pessoais (LGPD), o ordenamento jurídico brasileiro contava com dispositivos como o Código Civil, o Marco Civil da Internet e o Código de Defesa do Consumidor. Apesar dos avanços proporcionados por essas normas, eles mostraram-se insuficientes para atender às necessidades das relações digitais, especialmente no que se refere ao tratamento de dados pessoais, evidenciando a necessidade de um regulamento mais específico e abrangente.

Nesse contexto, a LGPD (Lei nº 13.709/2018) foi sancionada em 2018 e entrou em vigor em 2020, inspirada em regulamentações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A LGPD tem como objetivo central garantir a transparência no uso de dados pessoais, estabelecendo regras claras sobre a coleta, armazenamento, tratamento e compartilhamento dessas informações, além de assegurar direitos fundamentais aos titulares dos dados. Para isso, a lei define princípios como a necessidade, a finalidade e a adequação no tratamento dos dados, além de impor obrigações às empresas e prever sanções administrativas em caso de descumprimento.

Embora a LGPD se aplique a todas as organizações que realizam o tratamento de dados pessoais, independentemente do porte ou segmento. *Startups* e pequenas empresas enfrentam desafios particulares na adaptação à legislação. Muitas dessas empresas possuem recursos limitados, o que pode dificultar a implementação de medidas de conformidade, a adoção de políticas internas de segurança da informação e a realização de avaliações de impacto à proteção de dados. Além disso, o desconhecimento das exigências da LGPD pode expor essas empresas a riscos jurídicos e financeiros, incluindo sanções, perda de credibilidade e impactos negativos no relacionamento com clientes e parceiros.

Diante dessa realidade, este trabalho tem como objetivo geral analisar as mudanças decorrentes da vigência da LGPD nas atividades administrativas de uma empresa de desenvolvimento de software em João Pessoa, utilizando a TellMe School como estudo de caso. A escolha da empresa justifica-se pelo fato de que a autora trabalha atualmente na organização, o que permitiu maior acesso às informações

internas e possibilitou sua participação como respondente dos questionários aplicados. Os objetivos específicos incluem apresentar um panorama geral da LGPD, identificar os desafios enfrentados no ambiente de trabalho das organizações após a implementação da lei, e comparar a percepção dos colaboradores e gestores sobre as mudanças na gestão de processos com a vigência da LGPD.

A pesquisa foi conduzida entre janeiro e julho de 2025, por meio de análise documental, aplicação de questionários estruturados e observação direta, possibilitando identificar barreiras práticas à conformidade com a LGPD e avaliar as adaptações necessárias nos processos internos da organização. A TellMe School foi escolhida como objeto de estudo por ser a instituição onde a autora atua profissionalmente, o que possibilitou acesso direto às informações e dados necessários para a pesquisa, além de se enquadrar adequadamente na proposta do estudo. O tema foi escolhido pela relevância da proteção de dados no cenário atual e pelos desafios enfrentados por pequenas empresas e startups no processo de adequação à LGPD, de modo a contribuir para o debate sobre o tema e oferecer orientações práticas a outras organizações que enfrentam desafios semelhantes. Nesse sentido, busca-se responder à questão-problema: quais as mudanças nas atividades administrativas decorrentes da vigência da LGPD?

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Analisar as mudanças decorrentes da vigência da LGPD nas atividades administrativas de uma empresa de desenvolvimento de software em João Pessoa.

1.1.2 Objetivos Específicos

- Apresentar um panorama geral da Lei Geral de Proteção de Dados (LGPD);
- Identificar os desafios enfrentados no ambiente de trabalho das organizações após a implementação da LGPD;
- Comparar a percepção dos colaboradores e gestores sobre mudanças na gestão de processos com a vigência da LGPD.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 PANORAMA GERAL DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 14 de agosto de 2018 e publicada sob o nº 13.709/2018, estabelece regras para o tratamento de dados pessoais coletados no Brasil. Seu principal objetivo é assegurar a liberdade, a privacidade e a segurança dos dados dos indivíduos.

Assim como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD passou a exigir mudanças significativas na forma como as empresas gerenciam informações pessoais. O artigo 2º da LGPD apresenta os fundamentos que justificam sua criação e aplicação, buscando equilibrar os direitos individuais com o desenvolvimento econômico. Entre esses fundamentos, destaca-se o respeito à privacidade e à autodeterminação informativa, assegurando que cada pessoa tenha controle sobre seus próprios dados. Além disso, a lei reforça a importância da liberdade de expressão, de informação, de comunicação e de opinião, bem como da inviolabilidade da intimidade, da honra e da imagem dos cidadãos. A LGPD também reconhece o papel da proteção de dados no estímulo à inovação, ao desenvolvimento econômico e tecnológico, e à livre iniciativa e concorrência, sem deixar de lado a defesa do consumidor. Por fim, ela se ancora na promoção dos direitos humanos, da dignidade da pessoa natural e do pleno exercício da cidadania.

A LGPD, portanto, constitui um marco legal para a proteção de dados no Brasil, exigindo adaptações por parte de pessoas jurídicas, tanto públicas quanto privadas, que realizam o tratamento de dados pessoais. De acordo com a definição legal, dados pessoais são todas as informações relacionadas a uma pessoa natural identificada ou identificável, como nome, cadastro de pessoa física (CPF), endereço, e-mail e número de telefone. Quando tratados sem os devidos cuidados, esses dados podem comprometer a privacidade e os direitos fundamentais dos cidadãos. Com isso, é importante destacar que a LGPD define o termo "tratamento" no artigo 5º, inciso X:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Dessa forma, entende-se que o tratamento de dados compreende qualquer operação realizada com dados pessoais. Portanto, todas as atividades que envolvem o uso dessas informações estão sujeitas à aplicação da LGPD. A legislação exige que esse tratamento seja realizado de forma clara e transparente, mediante o consentimento explícito do titular.

O consentimento é um requisito essencial para o tratamento de dados pessoais, devendo ser fornecido de maneira expressa e inequívoca, conforme o artigo 7º, inciso I, da lei. Além da exigência genérica, a lei também é explícita em casos específicos, tais como: o artigo 11, inciso I, trata especificamente dos dados sensíveis, como origem racial, convicções religiosas e dados de saúde; e o, artigo 14, inciso I, que trata dos dados de crianças e adolescentes, ambos exigindo consentimento explícito para sua coleta e uso, determinando, no último caso, que o consentimento deve ser dado de forma específica por pelo menos um dos responsáveis legais. Em todos os casos, o consentimento deve ser fornecido por escrito ou por outro meio que comprove claramente a manifestação de vontade do titular.

Contudo, seguindo o artigo 7º, a LGPD prevê exceções em que o tratamento de dados pode ser realizado sem consentimento, conforme descrito nos incisos II a X:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento do consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> (BRASIL, 2018, art. 7º)

Ao analisar os impactos trazidos pela criação da LGPD, observa-se que sua aplicação prática envolve princípios fundamentais que orientam todo o tratamento de dados pessoais. Nesse sentido, Patrícia Peck Pinheiro (2021, p. 18) ressalta que a legislação deve estar sempre baseada na boa-fé, observando a compatibilidade do tratamento com as finalidades previamente informadas ao titular, a limitação do uso dos dados ao mínimo necessário, além da exigência de transparência. A autora destaca, ainda, que tais princípios devem ser acompanhados da adoção de medidas técnicas e administrativas adequadas para garantir a proteção efetiva dos dados pessoais.

Dessa forma, a aplicação prática da Lei LGPD, especialmente no contexto empresarial, deve ser orientada pelos princípios estabelecidos no artigo 6º da referida lei, os quais funcionam como diretrizes fundamentais para o tratamento de dados pessoais. Princípios como os da finalidade, adequação, necessidade, transparência, segurança e responsabilização não apenas reforçam a obrigatoriedade do consentimento e das bases legais, como também exigem que as organizações implementem políticas e procedimentos administrativos claros e coerentes com essas diretrizes. Isso implica que, além de obter o consentimento dos titulares, as empresas devem demonstrar, por meio de práticas concretas, que tratam os dados de maneira adequada, segura e ética, assegurando o direito à privacidade e à autodeterminação informativa. A boa-fé no tratamento torna-se, assim, pilar essencial para garantir a conformidade com a LGPD, exigindo adaptação na rotina empresarial, nos sistemas tecnológicos e na cultura organizacional.

Nesse mesmo sentido, Patrícia Peck Pinheiro destaca que a LGPD busca estimular a aplicação de seus dispositivos em caráter preventivo, por meio da imputação de sanções administrativas que exigem dos agentes responsáveis maior atenção à garantia da segurança das informações utilizadas. Assim, a lei não se limita a punir, mas pretende fomentar uma cultura organizacional de proteção de dados pessoais, vinculada à responsabilidade e à governança (PINHEIRO, 2020, p. 130).

A necessidade de adequação não se restringe à modificação de processos internos, mas envolve também o entendimento técnico da legislação. É justamente para apoiar esse processo e garantir o equilíbrio entre proteção e viabilidade operacional que a atuação da Autoridade Nacional de Proteção de Dados (ANPD) se torna essencial.

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia federal, criada pela Lei Geral de Proteção de Dados (LGPD) com o objetivo de assegurar a proteção da privacidade e dos dados pessoais no Brasil. Como autarquia, a ANPD possui autonomia administrativa e financeira, permitindo atuar de forma independente na regulamentação, fiscalização e orientação sobre o cumprimento da LGPD, garantindo que organizações públicas e privadas adotem práticas adequadas no tratamento de dados pessoais.

Entre suas atribuições destacam-se a criação de diretrizes para a aplicação da lei, a fiscalização das práticas de tratamento de dados pessoais e a imposição de sanções, como advertências e multas, nos casos de descumprimento. Além disso, a ANPD exerce um papel educativo, orientando tanto as organizações quanto os cidadãos sobre seus direitos e deveres em relação à proteção de dados. O órgão também é responsável por receber e investigar denúncias de violação de dados pessoais, promovendo a transparência e fortalecendo a confiança no sistema nacional de proteção de dados.

Nesse sentido, destaca-se ainda a atuação do Serviço Federal de Processamento de Dados (Serpro), principal empresa pública de serviços de tecnologia da informação do país. O Serpro disponibiliza, em seu site institucional, um questionário com dez perguntas que auxiliam na avaliação do nível de conformidade das empresas com a LGPD (SERPRO, 2019d).

No contexto das *startups* e empresas de pequeno porte, essa conciliação representa um desafio adicional, exigindo a adoção de práticas eficientes de governança de dados, que envolvem a definição de políticas, processos e controles para gerenciar, proteger e utilizar as informações de forma estratégica. A adoção dessas práticas deve ocorrer de maneira a não comprometer a capacidade de inovação e a rápida adaptação ao mercado, características essenciais dessas organizações.

A LGPD estabelece diretrizes claras para o tratamento ético e seguro dos dados pessoais, sua implementação prática impõe desafios significativos, especialmente para empresas com recursos limitados ou sem experiência prévia com normas de proteção de dados. Dessa maneira, além do desafio financeiro, a LGPD impõe diversos desafios às empresas, especialmente a inclusão de novas obrigações que muitas vezes estão fora da rotina dessas organizações.

Esses obstáculos podem comprometer a capacidade de adoção eficaz das medidas de proteção de dados exigidas pela lei, impactando diretamente as operações e o potencial de crescimento dessas empresas.

Dessa forma, fica evidente que a lei visa conciliar a responsabilidade no uso dos dados com o crescimento empresarial, criando um ambiente de maior confiança entre organizações e clientes

2.2 REPERCUSSÕES DA LGPD NO COTIDIANO DAS PESSOAS JURÍDICAS

Dentre as dificuldades enfrentadas pelas empresas destaca-se, sobretudo, a falta de orientações claras sobre as obrigações legais, algo comum quando uma nova legislação entra em vigor. Nesse cenário, torna-se fundamental a contratação de profissionais especializados, não apenas para a execução das atividades previstas na lei, mas também para oferecer suporte e orientação desde as etapas iniciais de adequação.

Conforme destaca o portal Legale Educacional, “a adequação à LGPD exige mudanças estruturais e operacionais para garantir que todos os processos relacionados a dados pessoais estejam em conformidade com a lei […]. É necessário garantir que o consentimento do titular seja obtido de maneira clara e transparente [...], além de armazenar os dados com segurança, seguindo boas práticas de proteção contra acessos indevidos, vazamentos e usos indevidos”.(LEGALE EDUCACIONAL, 2025).

Com o objetivo de proteger a privacidade dos indivíduos, a LGPD impõe às organizações a necessidade de se adequarem a novas regras relacionadas à coleta, armazenamento e uso de dados pessoais. Embora essas exigências se apliquem a todas as entidades, independentemente do porte econômico, os desafios tendem a ser mais significativos para microempreendedores individuais (MEI), microempresas (ME) e empresas de pequeno porte (EPP), especialmente no que se refere à estruturação de processos administrativos e à implementação de medidas técnicas e organizacionais adequadas.

Muitas micro e pequenas empresas não possuem a experiência ou o preparo necessário para lidar com as complexidades dessa legislação, que representou uma novidade no ordenamento jurídico brasileiro. Assim, o risco de não conformidade pode

resultar em sanções severas, como multas e até mesmo a suspensão das atividades de tratamento de dados, comprometendo a continuidade dos serviços prestados.

Diante do processo de aplicação e adequação à LGPD, é possível identificar alguns impactos relevantes no cotidiano das organizações, especialmente para micro e pequenas empresas, que enfrentam maiores dificuldades nesse processo. Esses impactos refletem a análise realizada nesta pesquisa, fundamentada na legislação e em materiais de orientação, como o Guia de Orientação da ANPD (2021).

Entre os principais impactos, destacam-se:

Alterações na coleta e armazenamento de dados: Nos processos administrativos, muitas empresas lidam com grandes volumes de dados pessoais, e a LGPD exige que esses dados sejam coletados de forma clara e com o consentimento do titular. Ou seja, antes de coletar qualquer dado, a empresa precisa colher o termo de consentimento bem como informar ao cliente sobre o uso que será feito dessas informações. Isso muda a forma como as empresas operam, pois antes o processo de coleta era mais simples, sem tanta explicação e disponibilidade de tempo dos clientes.

Conformidade organizacional e impactos nas decisões administrativas: A LGPD impõe mudanças significativas na forma como os dados pessoais são utilizados nas decisões e processos internos. Muitas organizações, tradicionalmente, recorrem ao uso de dados para otimizar fluxos de trabalho, elaborar estratégias de marketing ou aprimorar o atendimento ao cliente. No entanto, com a nova legislação, o uso dessas informações passa a ser restrito às finalidades previamente informadas e autorizadas pelos titulares. Isso obriga as empresas a revisarem suas práticas administrativas, adequando sistemas, rotinas e políticas internas para garantir a conformidade com os princípios da transparência, necessidade e finalidade previstos na lei.

Mudanças na governança e conformidade: A LGPD também exige que as empresas criem regras internas para proteger os dados pessoais. Isso inclui nomear uma pessoa responsável por garantir que a empresa siga a lei e que os dados sejam tratados com segurança. De acordo com o artigo 5º da LGPD, essa pessoa é denominada encarregada pelo tratamento de dados pessoais, também conhecido como DPO (Data Protection Officer). O encarregado é o profissional indicado pelo controlador – agente que toma as decisões sobre o tratamento dos dados – para atuar como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade

Nacional de Proteção de Dados (ANPD). Além do encarregado, a legislação também define os papéis do operador, responsável por tratar os dados em nome do controlador, e dos próprios agentes de tratamento, que compreendem tanto o controlador quanto o operador. A definição clara dessas funções é essencial para assegurar a responsabilidade, a transparência e a segurança no tratamento de dados dentro das organizações. Assim, a nomeação do encarregado não é apenas uma formalidade, mas parte fundamental da estrutura de governança exigida pela LGPD, contribuindo para a conformidade legal e para a proteção dos direitos dos titulares.

Nesse contexto, é fundamental compreender os papéis estabelecidos pela LGPD: o controlador é quem toma as decisões sobre o tratamento dos dados pessoais; o operador é quem realiza o tratamento em nome do controlador; e o encarregado (DPO) é o responsável por intermediar a comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Esses papéis devem estar bem definidos dentro da organização, a fim de evitar o uso indevido de informações pessoais.

Além disso, dados que antes ficavam disponíveis a todos os colaboradores podem, agora, ter seu acesso limitado conforme o nível de autorização de cada função. Essa restrição pode ser implementada diretamente nos sistemas internos da empresa, assegurando que apenas os profissionais responsáveis e devidamente autorizados possam acessar determinadas informações sensíveis.

Treinamento dos funcionários: Para garantir que todos na empresa sigam as novas regras, é essencial que todos os funcionários compreendam não apenas a importância da privacidade, mas também como suas atividades diárias podem impactar a conformidade da empresa. O treinamento deve abordar conceitos-chave da LGPD, boas práticas no tratamento de dados e protocolos de segurança da informação. Para facilitar a assimilação e padronizar os procedimentos, é recomendável a utilização de fluxogramas e materiais visuais que ilustram o caminho correto a ser seguido em situações específicas, como o atendimento de solicitações dos titulares ou o encaminhamento de incidentes de segurança.

Apesar dos desafios, a aplicação da LGPD no ambiente corporativo também representa uma oportunidade para a melhoria das práticas de gestão de dados. Ao promover maior transparência e responsabilidade, a conformidade com a legislação pode aumentar a confiança dos clientes e parceiros, conferindo às empresas um diferencial competitivo no mercado.

Ao tratar das medidas técnicas para a proteção dos dados, a Lei Geral de Proteção de Dados (2018) é clara em seu artigo 46, dispõe que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

Além disso, o artigo 50 da mesma legislação orienta que os agentes de tratamento estabeleçam regras de boas práticas e de governança, definindo procedimentos internos, normas de segurança, padrões técnicos, medidas educativas, mecanismos de supervisão e mitigação de riscos. Tais medidas devem ser compatíveis com a natureza das operações de tratamento e com o porte da organização (BRASIL, 2018).

Dessa forma, destaca-se a importância do engajamento da alta direção das empresas na implementação das diretrizes da LGPD. A atuação proativa da liderança na criação e manutenção de uma cultura organizacional orientada à proteção de dados é fundamental para o cumprimento efetivo da lei. A responsabilidade não recai apenas sobre setores técnicos ou jurídicos, mas envolve toda a estrutura organizacional, sendo indispensável que os gestores promovam ações de conscientização, treinamento e fiscalização contínua.

Nesse contexto, os colaboradores também desempenham um papel essencial. Ao participarem da estrutura de governança de dados, eles contribuem para a proteção das informações e para a segurança jurídica da empresa. Conforme Nicolau Olivieri (2020), "a nova legislação de proteção de dados deve, sim e positivamente, ser aplicada no âmbito do contrato de trabalho", uma vez que o artigo 4º da LGPD, ao tratar das exceções à sua aplicação, não exclui as relações de trabalho de seu escopo.

Sob a perspectiva do Direito do Trabalho, a jurista Vólia Bomfim Cassar (2018, p. 67) reforça que “a maior característica do Direito do Trabalho é a proteção do trabalhador”. Tal entendimento se conecta diretamente com os princípios da LGPD, os quais visam assegurar a privacidade e a autodeterminação informativa, garantindo que o trabalhador seja informado, treinado e protegido contra riscos relacionados ao uso indevido de seus dados pessoais no ambiente corporativo.

Ademais, deve-se considerar também o princípio da preservação da empresa, que é igualmente relevante no contexto da proteção de dados. Ao adotar práticas compatíveis com a LGPD, o empregador protege não apenas os dados dos titulares,

mas também a integridade, a reputação e a continuidade operacional da própria organização. O descumprimento da legislação pode acarretar sanções administrativas, perda de confiança do mercado e prejuízos financeiros, comprometendo a sustentabilidade do negócio.

Importante mencionar que a Lei Geral de Proteção de Dados (LGPD) altera procedimentos e determina punições para quem não entre em conformidade com as regras, ou seja, responsabiliza as empresas que não realizam o que foi proposto. Com o propósito de garantir a proteção dos dados pessoais, as principais sanções estão descritas nos artigos 52 e seguintes da LGPD, e variam de acordo com a gravidade da infração, a reincidência e a atitude da organização.

Segundo a Autoridade Nacional de Proteção de Dados (ANPD), essas penalidades podem variar desde advertências até multas que podem atingir o teto de R$50 milhões por infração. A aplicação das sanções levará em consideração critérios como a gravidade da infração, reincidência, boa-fé da organização, grau do dano causado, vantagem obtida, condição econômica do infrator, entre outros (BRASIL, 2018).

Portanto, a legislação visa garantir que as empresas cumpram requisitos de proteção de dados pessoais, e a ANPD pode aplicar essas penalidades de forma proporcional à infração cometida, considerando o contexto e as circunstâncias do caso. Essas penalidades têm o objetivo de reforçar a importância de proteger os dados pessoais, mas, ao mesmo tempo, a adaptação à lei pode ser vista como uma oportunidade para as empresas se destacarem, melhorando sua posição no mercado e conquistando a confiança dos consumidores. Por isso, é fundamental que as organizações adotem boas práticas de segurança e governança de dados para garantir a conformidade com a lei.

Acima disso, o comprometimento da direção com a LGPD deve refletir-se em uma política organizacional ampla e eficaz, capaz de proteger os direitos dos trabalhadores e, simultaneamente, resguardar os interesses estratégicos da empresa.

2.3 RECOMENDAÇÕES PRÁTICAS DA ANPD

Como já citado, a Autoridade Nacional de Proteção de Dados (ANPD) elaborou um Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, com o objetivo de orientar os agentes de tratamento de dados nas

organizações, especialmente aquelas de menor porte, auxiliando-as no processo de adequação à LGPD (ANPD, 2021). Entre as ações recomendadas, destacam-se:

Adequação gradual: Recomenda-se que as empresas adotem uma abordagem progressiva na implementação das medidas de proteção de dados. Isso significa que não é necessário implementar todas as exigências de forma imediata, mas sim conforme a capacidade da organização e a complexidade das atividades de tratamento de dados.

Simplificação de processos: A orientação é simplificação das obrigações e procedimentos relativos à proteção de dados, tornando-os mais acessíveis às micro e pequenas empresas. Entre as medidas propostas estão a elaboração de formulários, checklists e outros instrumentos práticos que auxiliem no cumprimento da LGPD.

Treinamento e conscientização: é importante que as empresas promovam treinamentos e ações educativas sobre proteção de dados entre os colaboradores, mesmo que em menor escala, a fim de garantir que todos compreendam a importância da privacidade e da segurança da informação.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD) simplificado: Prevê-se a possibilidade de elaboração de uma versão simplificada do RIPD, para os agentes de tratamento, especialmente nos casos em que o tratamento de dados envolve riscos menos significativos aos direitos dos titulares.

Adoção de medidas de segurança proporcionais: As organizações devem implementar mecanismos de segurança compatíveis com a sua realidade e proporção do risco envolvido. Entre essas medidas estão o uso de controles de acesso, criptografia, realização de backups e demais práticas que assegurem a integridade e confidencialidade dos dados pessoais.

Facilidade na comunicação com os titulares: Recomenda-se ainda que sejam estabelecidos canais de atendimento simples e acessíveis, que permitam aos titulares exercerem seus direitos, tais como acesso, correção, exclusão ou portabilidade dos dados pessoais.

É importante esclarecer que essas recomendações têm como uma de suas finalidades principais facilitar a adequação das empresas de pequeno porte à LGPD. Levando em consideração suas limitações operacionais e financeiras, mas sem comprometer a efetividade na proteção dos dados pessoais tratados (ANPD, 2021).

Em 27 de janeiro de 2022, a ANPD aprovou o regulamento de aplicação da Lei nº 13.709/2018 (LGPD) voltado aos agentes de tratamento de pequeno porte, por

meio da Resolução CD/ANPD nº 2 (ANPD, 2022). Essa resolução, em seu artigo 2º, define quem são considerados agentes de pequeno porte: microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado (inclusive sem fins lucrativos) e pessoas naturais que realizam tratamento de dados pessoais, desde que não exerçam atividades de alto risco ou em larga escala. O regulamento também prevê exigências simplificadas e um modelo facilitado para o registro das operações de tratamento de dados pessoais, conforme previsto na LGPD.

Nesse contexto, entende-se que os agentes de tratamento de pequeno porte devem implementar algumas medidas administrativas e técnicas fundamentais e indispensáveis, considerando os requisitos mínimos de segurança da informação para proteger os dados pessoais. Além disso, devem avaliar o nível de risco à privacidade dos titulares dos dados e a realidade do agente e do tratamento realizado.

Portanto, o ideal é implementar um conjunto de soluções técnicas voltadas para a proteção dos pilares de segurança. É fundamental que haja um diálogo entre os gestores das empresas, a equipe de tecnologia da informação e os responsáveis pela segurança da informação, a fim de implementar medidas que atendam adequadamente às necessidades, seja com soluções pagas ou com softwares de código aberto, como:

Software de *antivírus*: Que é uma ferramenta destinada a proteger os dispositivos dos usuários, como computadores e celulares, contra *malwares* indesejados. A instalação de um *software* desse tipo é essencial, considerando os diversos meios de infecção, como pela internet ou por mídias removíveis.

Rede Privada Virtual (*VPN – Virtual Private Network*): Trata-se de uma ferramenta que possibilita o acesso remoto de qualquer lugar com conexão à internet. Ela garante que o usuário consiga acessar dados de forma segura e criptografada, não importando onde estejam. Sem a utilização de uma *VPN*, diversas vulnerabilidades na rede poderiam ser exploradas por *hacker*s, resultando em invasões e interceptações de dados.

Backups: são cópias de segurança de arquivos e sistemas, que garantem proteção contra a perda ou danos aos dados, seja por causas acidentais, como desastres naturais, ou por ações deliberadas, como ataques de *hackers*.

Considerando as orientações apresentadas pela ANPD e as práticas recomendadas para a adequação à LGPD, fica evidente que as empresas, principalmente as de pequeno porte, precisam estar atentas à forma como lidam com

os dados pessoais em seu dia a dia. É preciso compreender a importância de implementar medidas de segurança, treinamentos e processos internos que contribuam para o tratamento adequado das informações.

Com base nessa fundamentação teórica, esta pesquisa terá como foco analisar como uma empresa de pequeno porte do setor de desenvolvimento de software na cidade de João Pessoa realiza o tratamento dos dados pessoais, identificando possíveis falhas e sugerindo melhorias que contribuam para a proteção dessas informações e, consequentemente, para a segurança e a sustentabilidade da própria organização.

3 METODOLOGIA DA PESQUISA

Este estudo é caracterizado como uma pesquisa aplicada, pois se baseia na coleta de fenômenos que acontecem na realidade em questão (PRAÇA, 2015, p. 75). O objetivo principal da pesquisa é analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) nas atividades administrativas de uma empresa de desenvolvimento de software em João Pessoa, tendo como a TellMe School.

A escolha da TellMe School como objeto de estudo justifica-se pelo fato de que a autora trabalha atualmente na empresa, o que possibilitou maior acesso às informações internas e facilitou o processo de coleta de dados. Além de conduzir a pesquisa, a mesma também participou como respondente do questionário, assumindo a condição de pesquisadora e respondente participante.

A pesquisa adotou uma abordagem qualitativa, fundamentada em métodos de caráter comparativo e empírico. O método comparativo tem como objetivo identificar semelhanças e diferenças entre as percepções da gestão e dos colaboradores, permitindo a análise das convergências e divergências em relação ao processo de adequação da empresa à LGPD. Já o método empírico pauta-se na observação da realidade e na coleta de dados junto aos sujeitos participantes, possibilitando compreender o fenômeno a partir da experiência concreta. A análise dos resultados, portanto, foi conduzida de forma comparativa, de modo a evidenciar os diferentes pontos de vista no ambiente organizacional.

O universo da pesquisa é composto pela TellMe School, uma startup de tecnologia especializada no desenvolvimento de soluções voltadas para a

comunicação educacional, com foco na interação entre escolas, pais e alunos por meio de plataformas digitais. Fundada há cerca de 12 (doze) anos, a empresa conta atualmente com 10 (dez) colaboradores e 03 (três) gestores e está sediada em João Pessoa, no estado da Paraíba.

A pesquisa foi realizada com a participação de dez colaboradores da TellMe School, atuantes nas áreas de suporte técnico, vendas, administrativo e gestão (três gestores). Os questionários foram aplicados no mês de julho de 2025, por meio da plataforma Google Forms, enviados individualmente por e-mail e respondidos de forma voluntária. Todos os participantes autorizaram o uso das informações exclusivamente para fins acadêmicos.

Para a coleta de dados, foram elaborados dois questionários estruturados. O primeiro, direcionado à gestão, continha 15 (quinze) perguntas, enquanto o segundo, destinado à equipe operacional, apresentou 11 (onze) perguntas. Ambos os instrumentos com questões fechadas e abertas, possibilitando tanto a obtenção de dados objetivos quanto a coleta de percepções subjetivas sobre as práticas adotadas e os desafios enfrentados no processo de adequação à LGPD. Os questionários aplicados encontram-se apresentados nos Apêndices 1 e 2 deste trabalho.

4 ANÁLISE DE DADOS

As perguntas aplicadas aos gestores e colaboradores da TellMe School foram elaboradas a partir das recomendações práticas apresentadas pela Autoridade Nacional de Proteção de Dados (ANPD), descritas na seção 2.3 deste trabalho, servindo como referência para a construção do instrumento de coleta de dados e possibilitando relacionar diretamente a percepção dos participantes com as diretrizes propostas pelo órgão regulador.

Considerando que a pesquisa adotou uma abordagem qualitativa, a análise dos dados concentrou-se na interpretação das percepções dos participantes, buscando identificar padrões, convergências e pontos críticos relacionados à adequação da empresa à Lei Geral de Proteção de Dados (LGPD). O foco esteve em compreender, a partir das respostas fornecidas, como a equipe percebe os desafios, as práticas já adotadas e as lacunas existentes no processo de conformidade com a legislação.

As respostas foram analisadas de forma interpretativa, por meio de uma leitura inicial exploratória seguida de uma leitura analítica, visando agrupar as informações por temas recorrentes e destacar as percepções mais relevantes. Esse procedimento permitiu uma melhor compreensão da realidade vivenciada pelos colaboradores, sem a preocupação com dados estatísticos ou quantificação dos resultados.

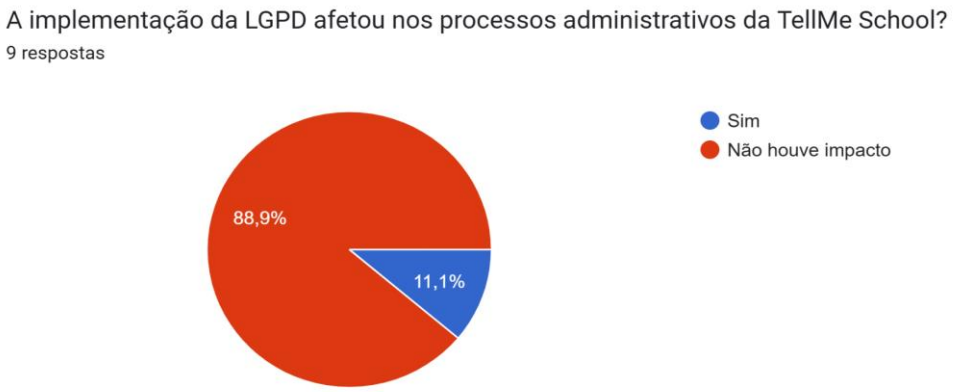
A pesquisa caracteriza-se como bibliográfica, pois foi fundamentada em estudos e publicações já existentes sobre a Lei Geral de Proteção de Dados e seus impactos, fornecendo base teórica para a análise. Também se enquadra como estudo de caso, por analisar em profundidade a realidade específica da empresa TellMe School, permitindo compreender seu contexto, práticas e desafios. Trata-se ainda de uma pesquisa teórica, por buscar interpretar conceitos e diretrizes da legislação, e empírica, por coletar e analisar dados obtidos diretamente com gestores e colaboradores. Essa combinação possibilitou uma visão mais abrangente da cultura organizacional em relação à proteção de dados, evidenciando avanços obtidos e dificuldades que persistem no processo de adequação à legislação vigente.

4.1 O IMPACTO DA LGPD NOS PROCESSOS ADMINISTRATIVOS

A partir da análise dos questionários aplicados aos colaboradores e gestores da TellMe School, foi possível identificar percepções distintas sobre os efeitos da LGPD

nos processos administrativos da empresa. A maior parte dos colaboradores afirmou não ter percebido impactos significativos após a implementação da lei. Cerca de 88,9% responderam que não houve alterações relevantes, enquanto apenas uma pequena parte (11,1%) indicou que houve mudanças, sendo que um dos participantes destacou que os efeitos foram mais notáveis no setor de suporte ao cliente. A seguir, apresenta-se o gráfico correspondente a esses dados.

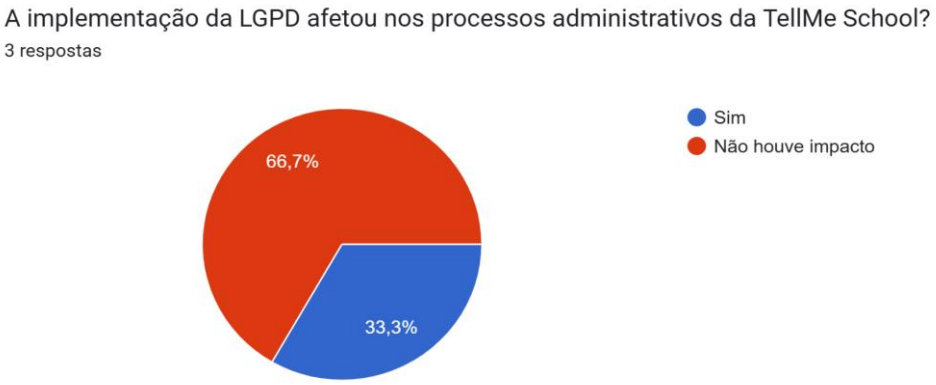
Gráfico 1 – Percepção dos colaboradores sobre alterações nos processos após a LGPD



Fonte: Dados da Pesquisa (2025)

Já do ponto de vista da gestão, 33,3% relataram que a LGPD trouxe mudanças, principalmente em aspectos legais como a revisão de contratos com os clientes e nas funcionalidades dos aplicativos. No entanto, 66,7% consideraram que a lei não causou impacto direto nos processos administrativos. A seguir, apresenta-se o gráfico com a representação desses dados.

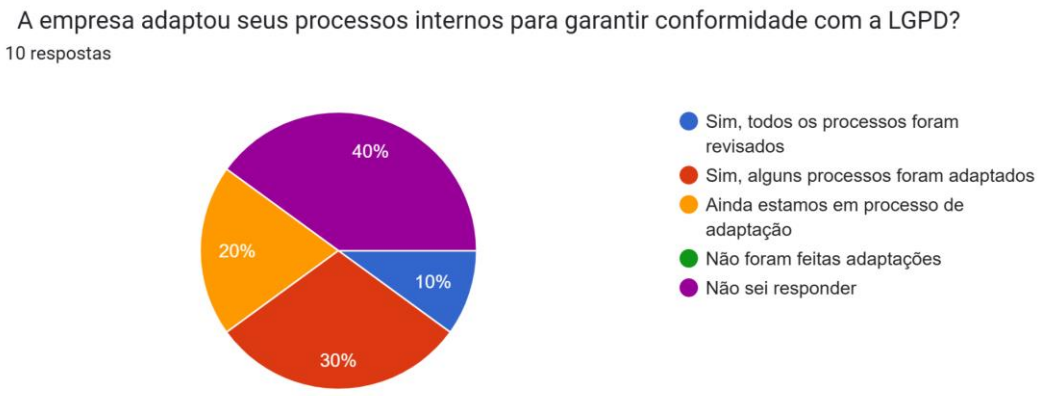
Gráfico 2 – Percepção dos gestores sobre os impactos da LGPD nos processos administrativos



Fonte: Dados da Pesquisa (2025)

Quando questionados sobre as adaptações realizadas para garantir a conformidade com a LGPD, as respostas também revelaram divergências entre os grupos. Todos os gestores afirmaram que os processos internos foram revisados e adaptados. Em contrapartida, entre os colaboradores, apenas 10% disseram que todos os processos foram revisados, enquanto 30% relataram que apenas alguns processos foram modificados. Outros 20% afirmaram que a empresa ainda está em fase de adaptação, e 40% não souberam responder.

Gráfico 3 – Percepção dos colaboradores sobre as adaptações realizadas para garantir a conformidade com a LGPD

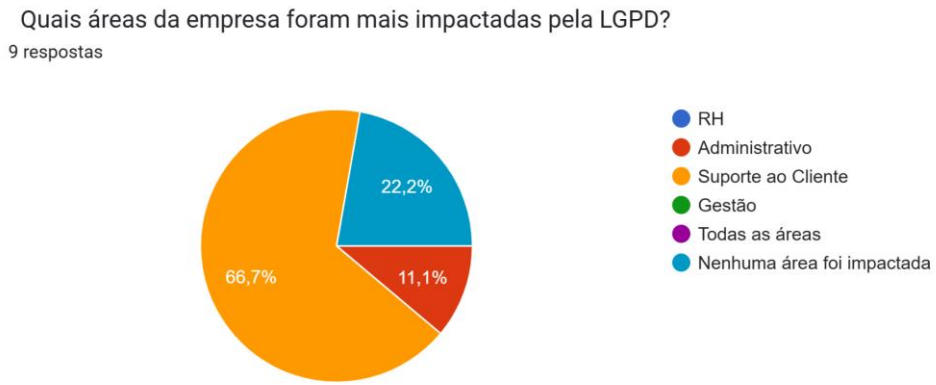


Fonte: Dados da Pesquisa (2025)

Sobre as áreas mais impactadas pela LGPD, tanto colaboradores quanto gestores apontaram o setor de suporte ao cliente como o mais afetado. Entre os

colaboradores, 66,7% destacaram essa área, enquanto 11,1% mencionaram o setor administrativo e 22,2% afirmaram que nenhuma área foi impactada. Os gestores, por sua vez, indicaram que todas as áreas da empresa foram impactadas, com ênfase especial no suporte ao cliente e no setor de desenvolvimento de tecnologia (TI).

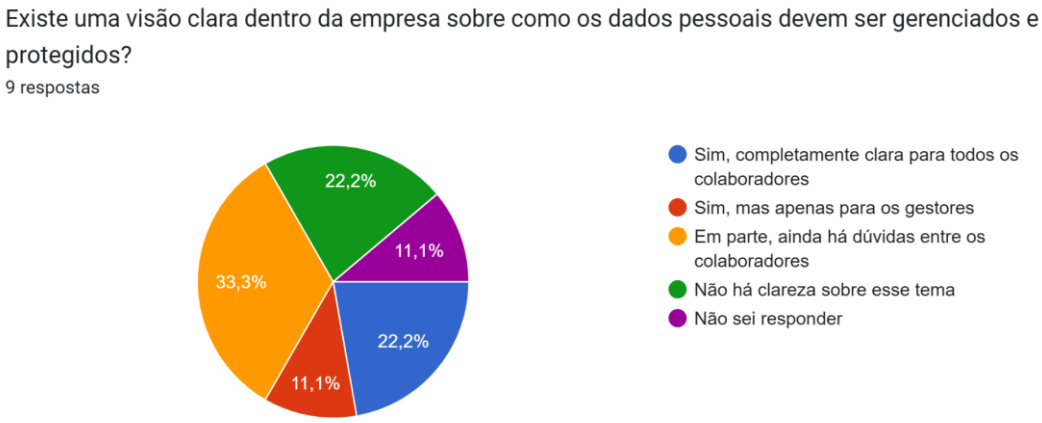
Gráfico 4 – Percepção dos colaboradores sobre quais áreas da empresa foram mais impactadas pela LGPD



Fonte: Dados da Pesquisa (2025)

Por fim, quanto à clareza interna sobre a gestão e proteção de dados pessoais, as respostas novamente apontaram uma diferença de percepção. Enquanto 100% dos gestores afirmaram que há diretrizes claras e bem comunicadas sobre como os dados devem ser tratados, entre os colaboradores apenas 22,2% disseram que esse entendimento é plenamente compartilhado por todos. Outros 33,3% indicaram que o tema ainda gera dúvidas, 22,2% relataram não ter clareza sobre o assunto e 11,1% afirmaram que as orientações são claras apenas para os gestores e 11,1% não souberam responder.

Gráfico 5 – Percepção dos colaboradores sobre a visão clara dentro da empresa sobre como os dados pessoais devem ser gerenciados e protegidos



Fonte: Dados da Pesquisa (2025)

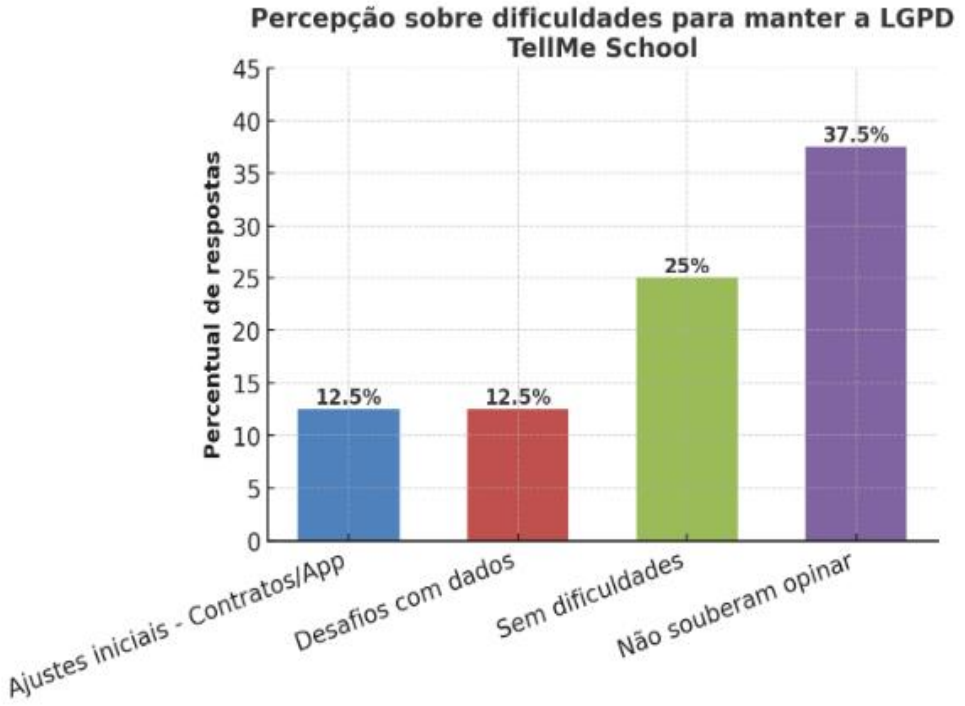
Essas diferenças entre as percepções da equipe e da gestão sugerem que, apesar das iniciativas para atender à LGPD, ainda há desafios relacionados à comunicação interna e ao alinhamento sobre as práticas de proteção de dados na TellMe School. Isso demonstra que, embora as mudanças já tenham sido iniciadas, o processo de adequação ainda está em andamento e requer um esforço contínuo para que a cultura de proteção de dados seja compreendida e aplicada por todos os setores da empresa.

4.2 OS DESAFIOS NA IMPLEMENTAÇÃO DA LGPD

Durante a coleta e análise das respostas dos formulários aplicados à equipe e aos gestores da TellMe School, foi possível observar os principais desafios enfrentados pela organização para se adequar à LGPD.

A análise indica que 12,5% dos colaboradores mencionaram ajustes iniciais em contratos e no aplicativo como os principais pontos de atenção. Outros 12,5% relataram desafios relacionados ao cuidado e tratamento diário dos dados. Já 25% afirmaram que não houve dificuldades relevantes, enquanto 37,5% não souberam opinar ou responder, possivelmente por não terem participado diretamente do processo.

Gráfico 6 – Percepção dos colaboradores sobre se houve dificuldades para manter a LGPD efetivamente implementada nos processos administrativos

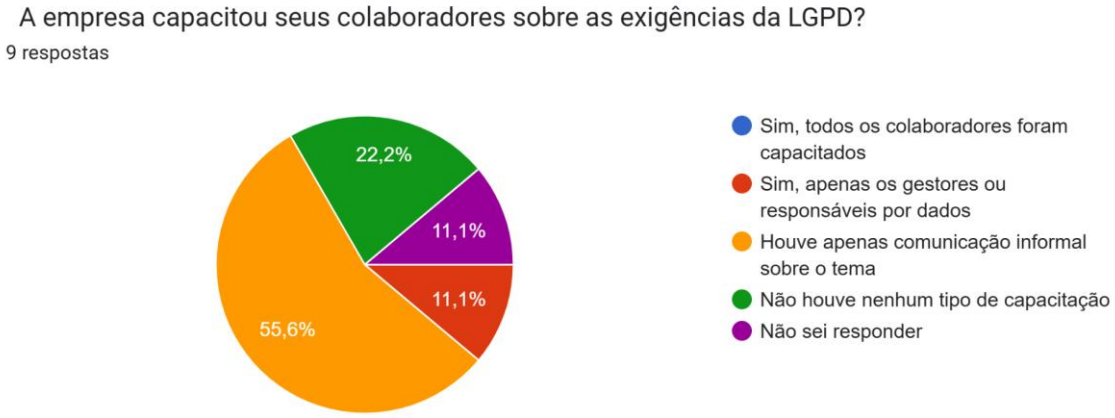


Fonte: Dados da Pesquisa (2025)

Por outro lado, os gestores relataram que não houve nenhuma dificuldade significativa para implementar a LGPD. Essa diferença nas respostas pode indicar que a percepção dos desafios varia entre os níveis da empresa.

Sobre a capacitação dos colaboradores, houve divergência entre os relatos. Enquanto os gestores afirmaram que todos foram capacitados formalmente, 55,6% dos colaboradores relataram que houve apenas comunicação informal sobre o tema. Além disso, 22,2% afirmaram que não houve qualquer tipo de capacitação, 11,1% disseram que apenas os gestores ou responsáveis pelos dados receberam treinamento e outros 11,1% declararam não saber responder. Esses dados evidenciam falhas na comunicação interna e indicam a necessidade de investir em treinamentos estruturados, que alcancem todos os colaboradores de forma clara e consistente.

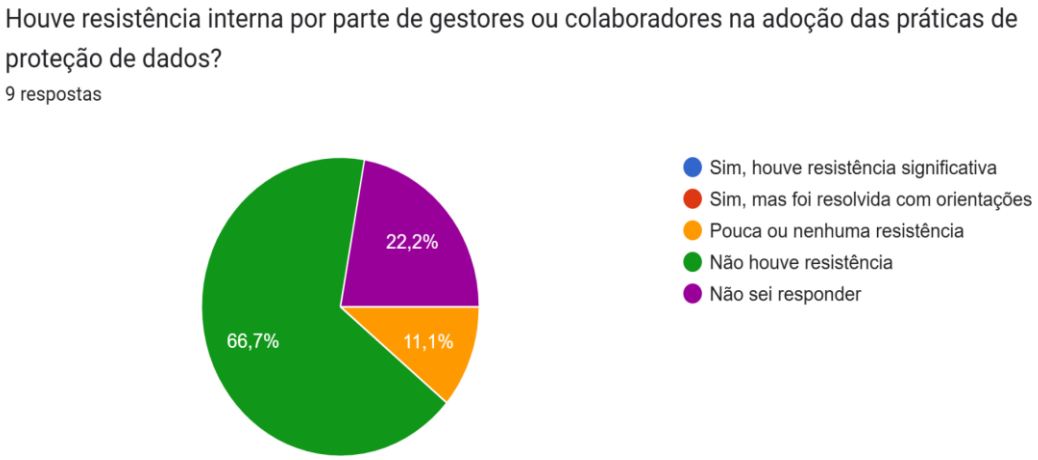
Gráfico 7 – Percepção dos colaboradores sobre a capacitação das exigências da LGPD



Fonte: Dados da Pesquisa (2025)

Em relação à resistência interna para a adoção das práticas exigidas pela LGPD, a maioria dos respondentes (66,7%) afirmou que não houve resistência por parte dos gestores ou colaboradores, indicando uma boa aceitação das mudanças. Por outro lado, 11,1% relataram que houve pouca ou nenhuma resistência, enquanto 22,2% disseram não saber responder. A gestão também afirmou que não percebeu resistência significativa entre os funcionários, reforçando que, mesmo nos poucos casos de resistência inicial, ela foi superada com orientações e acompanhamento adequados.

Gráfico 8 – Percepção dos colaboradores sobre a resistência interna na adoção das práticas de proteção de dados



Fonte: Dados da Pesquisa (2025)

Outro ponto importante é que, segundo todos os gestores, a empresa não contratou serviços técnicos especializados para auxiliar na implementação da LGPD. Isso indica que o processo foi feito de forma interna, o que pode explicar algumas das falhas percebidas pelos colaboradores, especialmente quanto à falta de treinamento formal.

Diante desses dados, percebe-se que, embora a TellMe School tenha feito esforços para se adequar à LGPD, ainda existem desafios a serem superados, principalmente relacionados à comunicação com a equipe, à capacitação e ao acompanhamento das práticas de proteção de dados. A ausência de apoio técnico especializado também pode ter dificultado a adoção de medidas mais completas e eficientes.

4.3 GOVERNANÇA DE DADOS E RISCOS

A governança de dados, no contexto da Lei Geral de Proteção de Dados (LGPD), envolve a adoção de práticas, políticas e estruturas organizacionais que assegurem o uso adequado, seguro e transparente das informações pessoais tratadas pela empresa.

Ao serem questionados sobre a existência de responsáveis formais pelo tratamento de dados (como encarregado, controlador e operador), 50% dos colaboradores indicaram que a empresa não possui pessoas designadas para essas

funções. Outros 40% afirmaram que existem responsáveis, porém sem uma formalização clara. Apenas 10% declararam não saber responder à pergunta. Nenhum colaborador indicou que há responsáveis formalmente designados. Esses dados evidenciam uma fragilidade na estrutura de governança de dados da empresa, sugerindo riscos legais e operacionais, especialmente em caso de incidentes relacionados à proteção de dados pessoais. A seguir, apresenta-se o gráfico correspondente a essas informações.

Gráfico 9 – Percepção dos colaboradores sobre a capacitação das exigências da LGPD

Fonte: Dados da Pesquisa (2025)

Em relação às medidas preventivas para evitar vazamentos de dados, tanto colaboradores quanto gestores mencionaram práticas importantes, como cláusulas contratuais com orientações claras sobre o uso e compartilhamento de informações, orientações éticas no ambiente de trabalho e o uso de logins individuais para acesso aos sistemas. No entanto, muitas dessas ações ainda são informais e não estão documentadas em políticas internas, o que dificulta o controle e o monitoramento eficaz dos riscos. Mesmo com boas intenções e práticas culturais presentes na rotina da empresa, a ausência de políticas estruturadas e de treinamentos contínuos enfraquece a capacidade da organização de prevenir falhas humanas e incidentes de segurança.

No que se refere ao uso de tecnologias para garantir a segurança e a conformidade com a LGPD, houve uma diferença de percepção entre a gestão e a equipe. Enquanto 100% da gestão afirmou que a empresa utiliza diversas ferramentas específicas, como antivírus, VPN e backups. Enquanto apenas 30% dos colaboradores afirmaram que a empresa utiliza diversas ferramentas específicas, a maior parte (60%) indicou que apenas soluções básicas são utilizadas, o que pode apontar para uma falha na comunicação interna ou no conhecimento técnico de quais ferramentas estão implementadas. Além disso, 10% dos respondentes disseram não saber responder, o que reforça a necessidade de uma governança de dados mais transparente, com comunicação clara em todos os níveis da organização.

Por fim, observa-se que a gestão da TellMe School tenta seguir as recomendações da Autoridade Nacional de Proteção de Dados ANPD e inclui cláusulas de proteção de dados nos contratos com clientes, o que demonstra um esforço inicial de conformidade com a LGPD e os resultados indicam uma preocupação crescente com a proteção de dados e a adoção gradual de medidas para atender à legislação

Ainda há desafios relacionados à definição de responsabilidades, ao uso de tecnologias adequadas e à capacitação da equipe e a ausência de notificações por descumprimento da LGPD não garante total conformidade, podendo refletir também uma fiscalização limitada.

Sendo assim, embora o número de participantes seja reduzido, o que é característico em estudos de caso com empresas de pequeno porte, o material analisado demonstrou riqueza de conteúdo. As respostas ofereceram subsídios valiosos para identificar aspectos críticos do cotidiano organizacional frente à LGPD, incluindo a percepção sobre o nível de conhecimento da equipe, os procedimentos adotados e os pontos de atenção que ainda demandam ajustes ou maior sensibilização.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar os desafios enfrentados pela TellMe School na adequação à Lei Geral de Proteção de Dados (LGPD). Através de uma abordagem qualitativa, buscou-se compreender como gestores e colaboradores percebem e vivenciam a aplicação da LGPD no cotidiano da organização.

Os resultados mostraram que, embora a empresa tenha iniciado ações importantes, como ajustes contratuais e atenção ao atendimento ao cliente, ainda existem fragilidades. A principal delas é a falta de capacitação formal da equipe e a ausência de definição clara de responsabilidades no tratamento de dados. Também se observou divergência entre a visão da gestão e dos colaboradores quanto ao nível de preparo da equipe, o que aponta falhas na comunicação interna.

Com base nesses resultados, conclui-se que a TellMe School demonstra um esforço inicial na adequação à LGPD, mas ainda precisa avançar na formalização de suas práticas, especialmente na definição de papéis, capacitação contínua e na adoção de políticas internas documentadas.

Como recomendação prática, sugere-se a contratação de um profissional especializado em proteção de dados. Entretanto, considerando que essa medida pode representar custos elevados para empresas de pequeno porte, recomenda-se como alternativa preliminar a capacitação da equipe por meio de cursos específicos no qual a empresa pode encontrar na internet ou, ainda, a designação de um colaborador para receber treinamento e assumir essa função, em conformidade com as orientações da Autoridade Nacional de Proteção de Dados (ANPD).

Além dessas medidas, destaca-se a importância da implementação de um regimento interno sobre proteção de dados, no qual os colaboradores deverão declarar que leram, compreenderam e estão cientes de todos os seus termos, responsabilizando-se pelo tratamento adequado das informações com as quais lidam. Como contribuição deste trabalho, foi incluído no Anexo 1 um exemplo de regimento interno que a empresa pode adotar (INTUIX, 2025). Para reforçar o engajamento e confirmar a leitura do regulamento, a empresa também pode promover treinamentos dinâmicos, como quiz via plataformas interativas (por exemplo, o Kahoot), com premiação aos melhores respondentes, a fim de incentivar a participação e motivar a equipe.

Recomenda-se, ainda, que tanto a revisão contratual com clientes quanto a adoção de boas práticas de governança de dados pelos colaboradores sejam consideradas medidas indispensáveis para garantir a proteção das informações. Nesse sentido, a adequação à LGPD vai além da conformidade legal, representando um fator essencial para assegurar a confiança de clientes e parceiros, além de fortalecer a credibilidade da organização perante a sociedade. A proteção dos dados pessoais, quando incorporada de maneira estratégica, contribui para relações mais transparentes e seguras, consolidando a empresa como agente comprometido com a ética e a responsabilidade no tratamento das informações.

Entre as limitações deste estudo, destaca-se o número reduzido de participantes, o que é característico de estudos de caso em empresas de pequeno porte. Ainda assim, os dados coletados foram suficientes para alcançar o objetivo proposto, que foi de analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) nas atividades administrativas da TellMe School.

Para pesquisas futuras, sugere-se ampliar o número de participantes, incluir a visão de clientes ou parceiros da empresa, e realizar análises comparativas com outras startups ou empresas da mesma área. Essas abordagens podem oferecer uma compreensão mais ampla sobre os desafios e estratégias de adequação à LGPD no setor de tecnologia educacional.

Por fim, a pesquisa reforça que, mesmo diante de limitações estruturais, é possível construir um caminho sólido de conformidade com a LGPD por meio de planejamento, capacitação e engajamento organizacional. Investir na cultura de proteção de dados é essencial para fortalecer a imagem da empresa, reduzir riscos legais e garantir a confiança dos clientes e da sociedade.

REFERÊNCIAS

ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. **Autoridade Nacional de Proteção de Dados, Brasília**, v. 1, n. 1, p. 1-21, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf . Acesso em 03 jan. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), para agentes de tratamento de pequeno porte. *Diário Oficial da União: seção 1*, Brasília, DF, 28 jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 2 jul. 2025.

BRASIL, Lei n.13.709 de 14 de agosto de 2018. **Lei geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em 14 maio 2025.

CASSAR, Vólia Bonfim. **Resumo de Direito do Trabalho** 6ºed. rev,atual e ampl Rio de janeiro: Forense; São Paulo: Método, 2018. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2017;001099616 . Acesso em 14 maio 2025.

INTUIX. **Regimento interno de proteção de dados**. Disponível em: https://intuix.com.br/. Acesso em: 11 maio 2025.

LEGALE EDUCACIONAL. **Como a LGPD impacta as empresas?.** Disponível em: https://legale.com.br/blog/como-a-lgpd-impacta-as-empresas/?utm_source=chatgpt.com . Acesso em: 22 ago. 2025.

OLIVIERI, Nicolau. **LGPD e sua necessária adequação às relações de trabalho**, Disponível em:https://www.jusbrasil.com.br/artigos/lgpd-e-sua-necessaria-adequacao-as-relacoes-de-trabalho/762654576 . Acesso em 14 maio 2025.

PINHEIRO, Patrícia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD).** São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 22 ago. 2025.

PRAÇA, S.; GARCIA. **Metodologia da pesquisa científica**: organização estrutural e os desafios para redigir o trabalho de conclusão. Disponível em: http://uniesp.edu.br/sites/_biblioteca/revistas/20170627112856.pdf . Acesso em: 20 jan. 2025.

SERPRO. **LGPD: a versão brasileira do regulamento europeu**. 2019a. Disponível em:https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais . Acesso em 15 jan. 2025.

TRISTÃO, Gabriela Rodrigues et al. **Lei Geral de Proteção de Dados:** desafios técnicos enfrentados por microempresas e empresas de pequeno porte. In: FatecSeg-Congresso de Segurança da Informação. 2021. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/4 . Acesso em 21 nov. 2024.

APÊNDICE

APÊNDICE 1: Pesquisa Qualitativa- Questionário online aplicado aos gestores

Sobre os impactos da LGPD na empresa - TellMe School

Este questionário está sendo aplicado exclusivamente para fins de estudo acadêmico e deve ser respondido pela gestão da empresa. Todas as respostas serão tratadas com total sigilo e anonimato. Agradecemos sua colaboração!

Sobre o Impacto da LGPD nos Processos Administrativos

A gestão da empresa conhece a Lei Geral de Proteção de Dados (LGPD)?

- ◯ Sim, possui conhecimento completo
- ◯ Sim, possui conhecimento básico
- ◯ Conhecimento superficial ou limitado
- ◯ Não conhece a lei
- ◯ Não sei responder

A implementação da LGPD afetou nos processos administrativos da TellMe School?

- ◯ Sim
- ◯ Não houve impacto

Caso tenha respondido afirmativamente à questão anterior, por favor, descreva as dificuldades enfrentadas

Sua resposta

A empresa adaptou seus processos internos para garantir conformidade com a LGPD?

- ◯ Sim, todos os processos foram revisados e adaptados
- ◯ Sim, apenas os processos mais críticos foram modificados
- ◯ A adaptação ainda está em andamento
- ◯ Não foram feitas adaptações
- ◯ Não sei responder

Quais áreas da empresa foram diretamente afetadas pela LGPD?

- ◯ RH
- ◯ Administrativo/Financeiro
- ◯ Suporte ao cliente
- ◯ Gestão
- ◯ Todas as áreas
- ◯ Nenhuma área foi afetada
- ◯ Não sei responder

Caso tenha mais de uma área impactada, por favor, descreva as áreas.

Sua resposta

Existe uma visão clara dentro da empresa sobre como os dados pessoais devem ser gerenciados e protegidos?

- ◯ Sim, há diretrizes claras e bem comunicadas a todos
- ◯ Sim, mas apenas entre os gestores
- ◯ Ainda existem dúvidas sobre esse tema
- ◯ Não há clareza sobre como gerenciar dados pessoais
- ◯ Não sei responder

Sobre os Desafios na Implementação da LGPD

A empresa já contratou serviço técnico especializado para adequação à LGPD?

- ◯ Sim, contratou uma consultoria ou empresa especializada
- ◯ Sim, mas apenas apoio jurídico ou informal
- ◯ Não contratou nenhum serviço especializado
- ◯ Não sei responder

A TellMe School enfrentou dificuldades relevantes para manter a LGPD efetivamente implementada em seus processos administrativos?
Em caso positivo, quais foram as dificuldades?

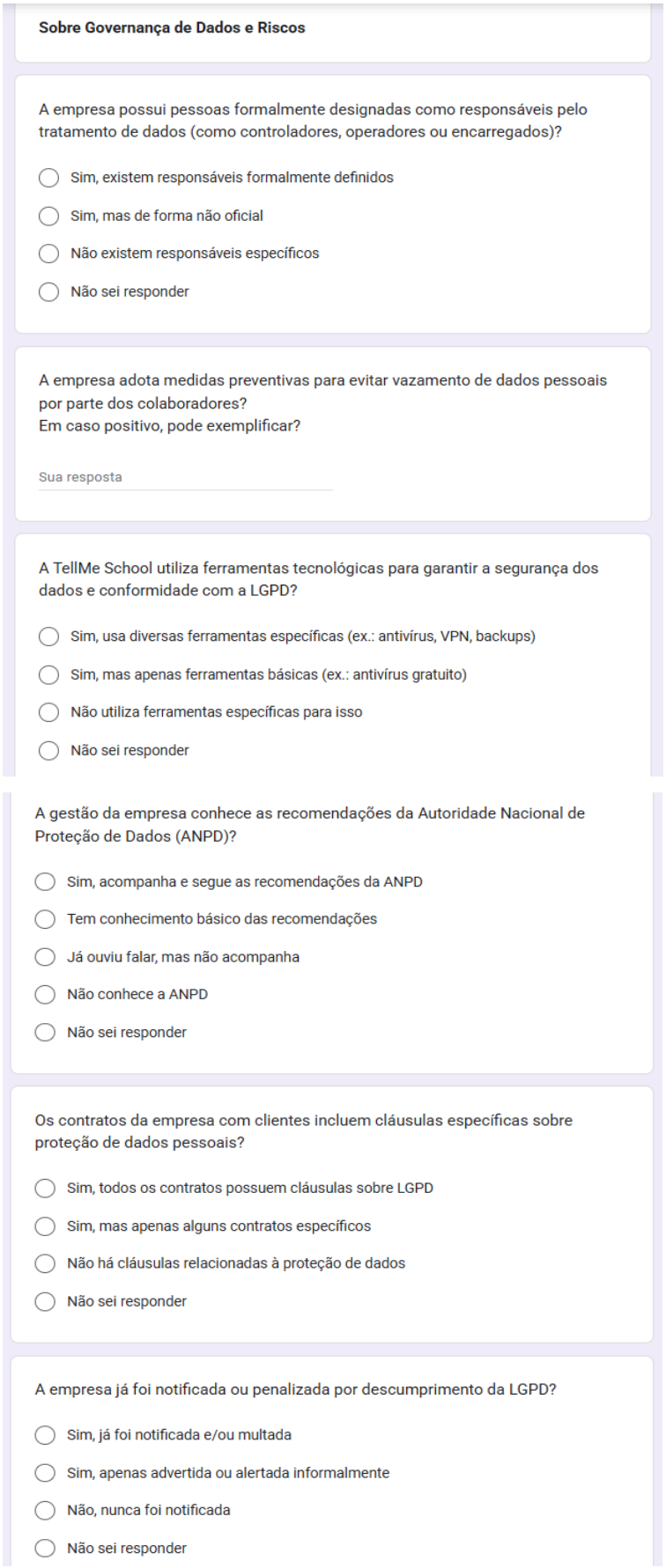
Sua resposta

A empresa capacitou seus colaboradores quanto às exigências da LGPD?

- ◯ Sim, todos foram capacitados formalmente
- ◯ Sim, mas apenas os responsáveis pelas áreas de dados
- ◯ Houve apenas orientação informal
- ◯ Não houve nenhuma capacitação
- ◯ Não sei responder

Houve resistência interna por parte dos colaboradores para adotar as práticas de proteção de dados?

- ◯ Sim, houve bastante resistência
- ◯ Sim, mas foi superada com orientação
- ◯ Pouca resistência
- ◯ Nenhuma resistência
- ◯ Não sei responder



Sobre Governança de Dados e Riscos

A empresa possui pessoas formalmente designadas como responsáveis pelo tratamento de dados (como controladores, operadores ou encarregados)?

- ◯ Sim, existem responsáveis formalmente definidos
- ◯ Sim, mas de forma não oficial
- ◯ Não existem responsáveis específicos
- ◯ Não sei responder

A empresa adota medidas preventivas para evitar vazamento de dados pessoais por parte dos colaboradores?
Em caso positivo, pode exemplificar?

Sua resposta

A TellMe School utiliza ferramentas tecnológicas para garantir a segurança dos dados e conformidade com a LGPD?

- ◯ Sim, usa diversas ferramentas específicas (ex.: antivírus, VPN, backups)
- ◯ Sim, mas apenas ferramentas básicas (ex.: antivírus gratuito)
- ◯ Não utiliza ferramentas específicas para isso
- ◯ Não sei responder

A gestão da empresa conhece as recomendações da Autoridade Nacional de Proteção de Dados (ANPD)?

- ◯ Sim, acompanha e segue as recomendações da ANPD
- ◯ Tem conhecimento básico das recomendações
- ◯ Já ouviu falar, mas não acompanha
- ◯ Não conhece a ANPD
- ◯ Não sei responder

Os contratos da empresa com clientes incluem cláusulas específicas sobre proteção de dados pessoais?

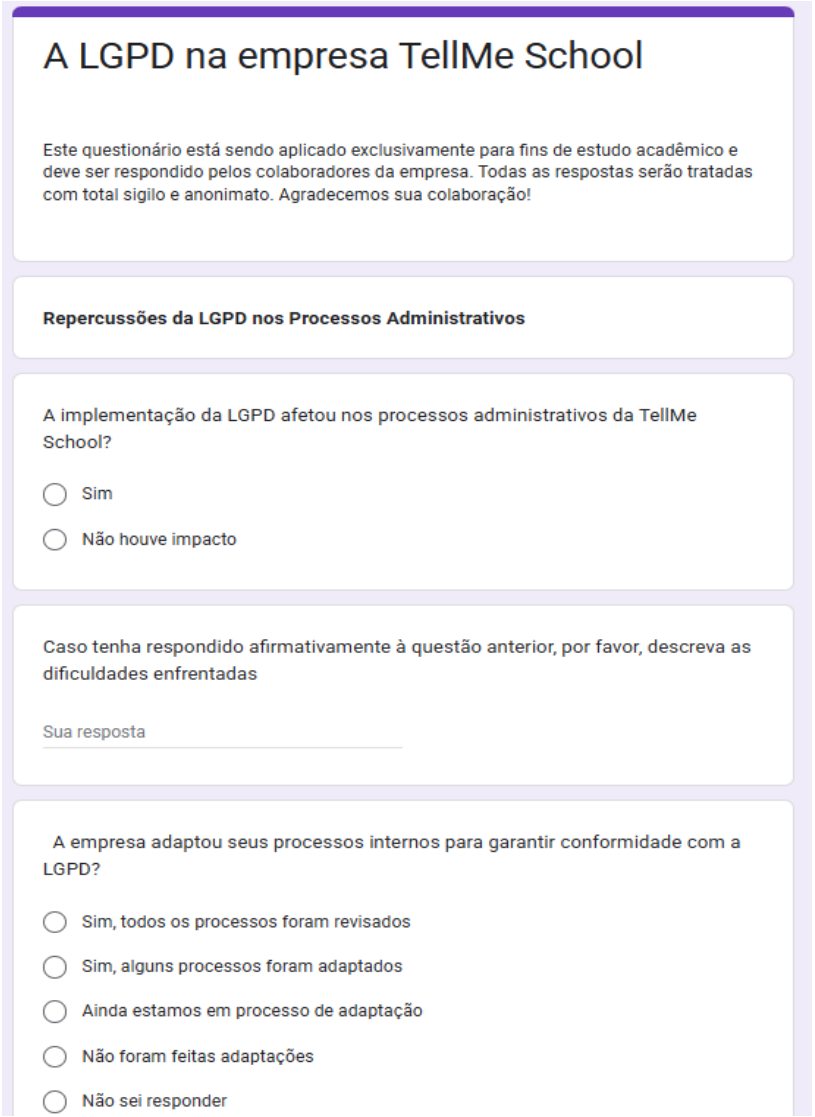
- ◯ Sim, todos os contratos possuem cláusulas sobre LGPD
- ◯ Sim, mas apenas alguns contratos específicos
- ◯ Não há cláusulas relacionadas à proteção de dados
- ◯ Não sei responder

A empresa já foi notificada ou penalizada por descumprimento da LGPD?

- ◯ Sim, já foi notificada e/ou multada
- ◯ Sim, apenas advertida ou alertada informalmente
- ◯ Não, nunca foi notificada
- ◯ Não sei responder

Fonte: Elaboração Própria (2025).

APÊNDICE 2: Pesquisa Qualitativa- Questionário online aplicado aos colaboradores.



A LGPD na empresa TellMe School

Este questionário está sendo aplicado exclusivamente para fins de estudo acadêmico e deve ser respondido pelos colaboradores da empresa. Todas as respostas serão tratadas com total sigilo e anonimato. Agradecemos sua colaboração!

Repercussões da LGPD nos Processos Administrativos

A implementação da LGPD afetou nos processos administrativos da TellMe School?

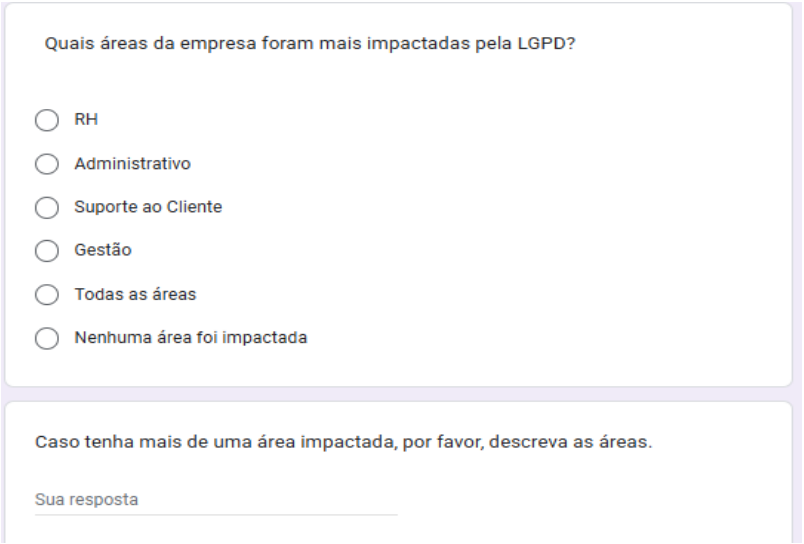
- ◯ Sim
- ◯ Não houve impacto

Caso tenha respondido afirmativamente à questão anterior, por favor, descreva as dificuldades enfrentadas

Sua resposta

A empresa adaptou seus processos internos para garantir conformidade com a LGPD?

- ◯ Sim, todos os processos foram revisados
- ◯ Sim, alguns processos foram adaptados
- ◯ Ainda estamos em processo de adaptação
- ◯ Não foram feitas adaptações
- ◯ Não sei responder



Quais áreas da empresa foram mais impactadas pela LGPD?

- ◯ RH
- ◯ Administrativo
- ◯ Suporte ao Cliente
- ◯ Gestão
- ◯ Todas as áreas
- ◯ Nenhuma área foi impactada

Caso tenha mais de uma área impactada, por favor, descreva as áreas.

Sua resposta

Existe uma visão clara dentro da empresa sobre como os dados pessoais devem ser gerenciados e protegidos?

- ◯ Sim, completamente clara para todos os colaboradores
- ◯ Sim, mas apenas para os gestores
- ◯ Em parte, ainda há dúvidas entre os colaboradores
- ◯ Não há clareza sobre esse tema
- ◯ Não sei responder

Sobre os Desafios na Implementação da LGPD

A TellMe School enfrentou dificuldades relevantes para manter a LGPD efetivamente implementada em seus processos administrativos?
Em caso positivo, quais foram as dificuldades?

Sua resposta

A empresa capacitou seus colaboradores sobre as exigências da LGPD?

- ◯ Sim, todos os colaboradores foram capacitados
- ◯ Sim, apenas os gestores ou responsáveis por dados
- ◯ Houve apenas comunicação informal sobre o tema
- ◯ Não houve nenhum tipo de capacitação
- ◯ Não sei responder

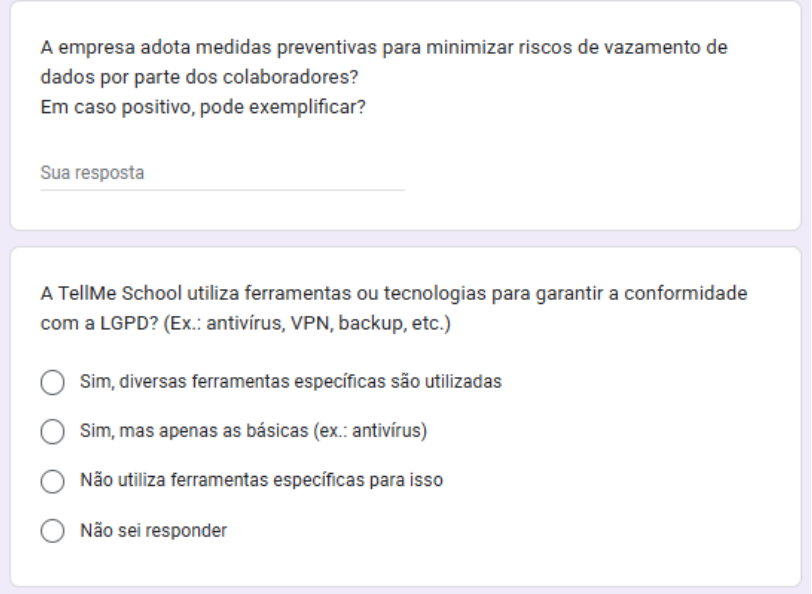
Houve resistência interna por parte de gestores ou colaboradores na adoção das práticas de proteção de dados?

- ◯ Sim, houve resistência significativa
- ◯ Sim, mas foi resolvida com orientações
- ◯ Pouca ou nenhuma resistência
- ◯ Não houve resistência
- ◯ Não sei responder

Sobre Governança de Dados e Riscos

A empresa possui pessoas designadas formalmente como responsáveis pelo tratamento de dados (como encarregado, controlador e operador)?

- ◯ Sim, temos responsáveis formalmente designados
- ◯ Sim, mas sem formalização clara
- ◯ Não há pessoas designadas para essas funções
- ◯ Não sei responder



Fonte: Elaboração Própria (2025).

ANEXOS

Anexo 1: Exemplo de regimento interno para se implementar na TellMe School com os colaboradores - POLÍTICA INTERNA DE PROTEÇÃO DE DADOS.

INTUIX
SMART CERTIFICATIONS

POLÍTICA INTERNA DE PROTEÇÃO DE DADOS

1. Definições

Para fins de cumprimento da Lei Geral de Proteção de Dados nº 13.709/18, de acordo com o Capítulo 1 "Disposições Preliminares", o art. 5º especifica as principais informações determinantes:

Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Dado pessoal sensível: qualquer dado pessoal que contenha informação sobre:

- Origem racial ou étnica.
- Convicção religiosa.
- Opinião política.
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político.
- Saúde.
- Vida sexual.
- Genética ou biometria.

Titular: Pessoa natural (física) a quem se referem os dados. Tratamento: qualquer operação com os dados pessoais, incluindo armazenamento.

Consentimento: manifestação livre e inequívoca pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade específica.

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. São operadores os empregados, prestadores de serviço e demais parceiros que participam do tratamento de dados pessoais dentro da empresa.

Controlador: pessoa física ou jurídica, de direito público ou privado, que administra e toma decisões sobre o tratamento de dados pessoais.

Agentes de tratamento: o controlador e o operador.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Encarregado de Dados (DPO): pessoa indicada pelo controlador para ser responsável pela comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANDP).

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

2. Objetivo da política interna de proteção de dados

A organização deve orientar a todos os membros acerca das boas práticas em proteção de dados pessoais, visando conformidade com a Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais.

3. Contexto da LGPD

A Lei Geral de Proteção de Dados foi aprovada em 2018, com o objetivo de trazer ao ordenamento jurídico brasileiro uma preocupação que já tem lugar em todos os países desenvolvidos: a proteção de dados pessoais. No mundo todo, a legislação de proteção a dados de pessoas naturais é um instrumento necessário para garantir maior segurança jurídica e o respeito aos direitos humanos fundamentais. Assim sendo, a conformidade com tais leis tem sido um fator importante internamente.

4. Princípios da LGPD

São os princípios norteadores da Lei Geral de Proteção de Dados e, também, os desta política interna:

Adequação: o tratamento dos dados tem que ser compatível com a finalidade informada ao titular.

Necessidade: o tratamento deve ser limitado ao mínimo necessário para atingir a finalidade proposta.

Livre acesso: os titulares têm o direito de acessar a qualquer tempo as informações referentes ao tratamento que seus dados recebem.

Qualidade dos dados: o tratamento dos dados deve mantê-los exatos, claros, relevantes e atualizados, sem discrepâncias ou distorções.

Transparência: o tratamento dos dados deve ser explicado aos titulares de maneira transparente e acessível, observado o segredo comercial e industrial necessário.

Segurança: os dados pessoais devem ser protegidos pelo controlador, para que não sejam perdidos, alterados, destruídos ou acessados indevidamente.

Prevenção: cabe ao controlador tomar medidas para prevenir danos provenientes do tratamento de dados pessoais.

Não discriminação: o tratamento de dados pessoais não deve ser realizado com finalidades discriminatórias, ilícitas ou abusivas.

Responsabilização e prestação de contas: demonstração, aos titulares, das medidas utilizadas para garantir conformidade com a Lei Geral de Proteção de Dados Pessoais.

5. Responsabilidade compartilhada

A responsabilidade pelo correto tratamento dos dados pessoais é compartilhada entre todos que atuam como controladores e operadores, sendo fundamental a cooperação de todos para que a empresa esteja sempre em conformidade com a lei, oferecendo segurança a todos os titulares de dados pessoais sob seu controle.

Nos termos dos art. 42 e seguintes da Lei Geral de Proteção de Dados nº 13.709/18, o operador de dados pessoais que descumprir as diretrizes lícitas de proteção de dados do controlador responderá como se também fosse controlador dos dados em questão, estando assim sujeito à responsabilidade civil, administrativa e criminal sobre o tratamento inadequado dos dados.

Segundo art. 23 da mesma Lei, a violação de segredos da organização, concepção que inclui dados pessoais sob seu controle, poderá a critério exclusivo da Direção ser motivo para embasar a

demissão por justa causa de colaboradores ou a rescisão de contrato de prestadores de serviços envolvidos na violação, sem prejuízo das ações de regresso cabíveis judicialmente.

6. Tratamento dos dados pessoais

O tratamento de dados deve seguir os princípios definidos nesta política, devendo ser estritamente voltado às finalidades às quais as coletas dos dados se destinam, respeitando os princípios desta política e os critérios de compartilhamento e de segurança das informações.

Os dados pessoais devem ser manipulados apenas por pessoas que precisem lidar com eles. Assim, reduzem-se os riscos de falhas humanas propiciando um vazamento ou uso inadequado da informação. Para garantia, é necessário dividir os dados por setores e por responsabilidades específicas dentro de cada setor. Assim se saberá em cada situação quem são os operadores dos dados e os riscos de um incidente na segurança da informação diminuem.

Para garantir este tratamento setorizado dos dados, cada acesso ao banco de dados da empresa é individual e intransferível. Assim, somente pessoas autorizadas poderão ter acesso.

O mero acesso e/ou a utilização indevida de quaisquer dados pessoais armazenados ou processados pela empresa são terminantemente proibidos, sob pena de demissão por justa causa (ou rescisão do contrato de prestação de serviços e/ou fornecimento), sem prejuízo da responsabilização cível e criminal cabível em âmbito judiciário do infrator.

7. Critérios de coleta dos dados pessoais.

As informações referentes a pessoas físicas somente devem ser coletadas na medida da necessidade para a prestação de serviços e/ou fornecimento. Em todas as hipóteses é devido o consentimento para o tratamento dos dados, que deverá ser obtido em conformidade com a Lei Geral de Proteção de Dados nº 13.709/18.

O consentimento é requerido ao solicitar os dados aos titulares, quando necessário, através do aceite no campo apropriado do sistema ou mediante e-mail resposta à solicitação.

8. Critérios de armazenagem dos dados pessoais.

Quanto à armazenagem, devem seguir as seguintes diretrizes:

Quando armazenados fisicamente: os dados devem ficar em local protegido, fora do alcance de outras pessoas que não são expressamente autorizadas a acessá-los.

Quando armazenados digitalmente: devem ficar em pasta protegida por criptografia e restrição de acesso por senha pessoal.

Eventuais cópias de dados pessoais somente devem ser feitas em caso de necessidade para cumprimento da finalidade proposta ao tratamento, todas as cópias devem ser administradas internamente e protegidas para que não ocorra vazamento de dados.

9. Critérios de compartilhamento interno de dados pessoais.

Os dados pessoais somente podem ser compartilhados com pessoas cuja função dentro da empresa exija que elas tenham acesso. Por exemplo: dados referentes a saúde ocupacional, como atestados médicos, exames admissionais e outros, só podem ser compartilhados dentro da empresa com pessoas responsáveis pelo tratamento dessas informações, como o responsável pelo RH. Não podendo ser compartilhados com alguém da área técnica que não precise ter acesso a esses dados para o cumprimento de suas funções.

10. Critérios de compartilhamento externo de dados pessoais.

O compartilhamento de dados pessoais com pessoas ou entidades externas à empresa deve ser restrito ao mínimo necessário para a execução dos contratos e prestações de serviços e/ou fornecimentos, que os titulares estão envolvidos, incluindo o cumprimento de obrigações legais. Mesmo quando o tratamento envolver diretamente a prestação de serviços e/ou o fornecimento, o consentimento para este tratamento e compartilhamento deverá ter sido previamente obtido.

11. Critérios de eliminação dos dados pessoais.

Quando atingida a finalidade do tratamento dos dados pessoais e o armazenamento, para satisfazer quaisquer exigências legais, for desnecessário, estes deverão ser devidamente eliminados física e digitalmente. O titular deve ser comunicado desta eliminação nos casos em que ela se dê de maneira diversa à prevista no termo de consentimento aplicável.

12. Prestação de informações e transparência.

Os operadores de dados pessoais deverão prover todas as informações requeridas pelos titulares acerca do tratamento de seus dados pessoais, respeitando o direito da empresa de manter sigilo comercial quando cabível. A finalidade do tratamento deve ser sempre evidenciada e transparente.

Quando houver solicitação da prestação de informações sobre os dados pessoais pelo titular destes, os operadores deverão informar ao Encarregado da Proteção de Dados Pessoais sobre a solicitação e então prestar as informações solicitadas ao titular.

13. Encarregado da Proteção de Dados Pessoais (DPO).

O encarregado da proteção de dados pessoais DPO é a pessoa responsável, nos termos da Lei Geral de Proteção Dados nº 13.709/18, pela comunicação com os titulares.

São atribuições do encarregado: verificar os riscos existentes, apontar as medidas corretivas e avaliar periodicamente a segurança de dados pessoais dentro da empresa, devendo também realizar eventuais comunicações necessárias com os titulares ou com o poder público.

Quaisquer questionamentos que surgirem no dia a dia da empresa acerca da proteção de dados pessoais devem ser levados ao encarregado para que este possa orientar de imediato o operador ou buscar junto às entidades especializadas uma orientação adequada ao questionamento levantado.

14. Relatório de Impacto à Proteção de Dados Pessoais.

O Encarregado da Proteção de Dados Pessoais manterá relatório de avaliação de riscos e impactos à proteção de dados pessoais, por meio dele, as medidas necessárias à segurança da informação de dados pessoais poderão ser estruturadas, implementadas e avaliadas.

Quando necessário é realizada a elaboração de um relatório de impacto e o encarregado de dados ficará responsável por informar os riscos e procedimentos necessários quando ocorre o vazamento de dados.

Fonte: INTUIX (2025)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus João Pessoa - Código INEP: 25096850
Av. Primeiro de Maio, 720, Jaguaribe, CEP 58015-435, João Pessoa (PB)
CNPJ: 10.783.898/0002-56 - Telefone: (83) 3612.1200

Documento Digitalizado Ostensivo (Público)

Entrega Versão Final TCC - Gabrielly Bezerra dos Santos

Assunto:	Entrega Versão Final TCC - Gabrielly Bezerra dos Santos
Assinado por:	Gabrielly Santos
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Gabrielly Bezerra dos Santos**, **ALUNO (20192460071) DE BACHARELADO EM ADMINISTRAÇÃO - JOÃO PESSOA**, em 29/08/2025 12:12:16.

Este documento foi armazenado no SUAP em 29/08/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1590573
Código de Autenticação: f847c9ef51