

**UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE ADMINISTRAÇÃO**

REBECA DYANGELLES FONTES SOARES

**ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM ESTUDO DE
CASO EM UMA EMPRESA DE TECNOLOGIA EM ARACAJU/SE**

São Cristovão/SE

2023

REBECA DYANGELLES FONTES SOARES

**ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM ESTUDO DE
CASO EM UMA EMPRESA DE TECNOLOGIA EM ARACAJU/SE**

Trabalho de Conclusão de Curso (TCC) apresentado ao Departamento de Administração do Centro de Ciências Sociais Aplicadas da Universidade Federal de Sergipe (UFS), como requisito parcial para a obtenção do título de Bacharel em Administração, em cumprimento às Normas regulamentadas pela Resolução nº 69/2012/CONEPE

Orientador(a): Prof.^a Dr.^a Rosangela Sarmiento Silva

São Cristóvão/SE

2023

REBECA DYANGELLES FONTES SOARES

**ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM ESTUDO DE
CASO EM UMA EMPRESA DE TECNOLOGIA EM ARACAJU/SE**

Trabalho de Conclusão de Curso (TCC) apresentado ao Departamento de Administração do Centro de Ciências Sociais Aplicadas da Universidade Federal de Sergipe (UFS), como requisito parcial para a obtenção do título de Bacharel em Administração, em cumprimento às Normas regulamentadas pela Resolução nº 69/2012/CONEPE

Trabalho defendido e aprovado em 30 de janeiro de 2023.

BANCA EXAMINADORA

Prof.^a Dr.^a Rosangela Sarmiento Silva (Orientador)

Universidade Federal de Sergipe

Prof. Dr. Cláudio Márcio Campos de Mendonça (Membro Interno)

Universidade Federal de Sergipe

Profa. Dra. Thaís Ettinger Oliveira Salgado (Membro Interno)

Universidade Federal de Sergipe

*Tudo tem o seu tempo determinado, e há tempo
para todo o propósito debaixo do céu.
Bíblia Sagrada*

RESUMO

O presente estudo teve como objetivo analisar o modelo de adequação à Lei Geral de Proteção de Dados realizada em uma empresa que presta serviços de tecnologia corporativa no estado de Sergipe por uma empresa de consultoria especializada em *compliance* à LGPD. Para tanto, buscou-se analisar minuciosamente cada um dos processos realizados nas etapas de adequação, bem como a percepção dos sócios e colaboradores para, posteriormente, submeter o modelo à ferramenta “Diagnóstico e Índice de Maturidade de Privacidade para adequação à Lei Geral de Proteção de Dados”, disponibilizada no sítio do governo federal brasileiro. Como método de pesquisa foi utilizado o estudo de caso único. A pesquisa é caracterizada como qualitativa exploratória descritiva. Os instrumentos de pesquisa utilizados foram: entrevistas, análise documental e análise bibliográfica acerca do tema proposto. Os resultados comprovaram a eficiência do modelo de adequação à LGPD aplicado na empresa foco deste estudo através do elevado índice obtido na ferramenta anteriormente citada. Ademais, percebeu-se a relevância da etapa de análise de eficiência no processo de adequação de uma empresa à Lei Geral de Proteção de Dados Pessoais.

Palavras – chave: Adequação. *Compliance*. Índice. LGPD.

ABSTRACT

The present study aimed to analyze the adaptation model to the General Data Protection Law carried out in a company that provides corporate technology services in the state of Sergipe by a consulting company specialized in compliance with the LGPD. To this end, we sought to analyze in detail each of the processes carried out in the adaptation stages, as well as the perception of the partners and collaborators, to subsequently submit the model to the tool “Diagnosis and Privacy Maturity Index for adaptation to the General Law of Protection de Dados”, available on the website of the Brazilian federal government. As a research method, the single case study was used. The research is characterized as descriptive exploratory qualitative. The research instruments used were: interviews, documental analysis and bibliographical analysis about the proposed theme. The results proved the efficiency of the adaptation model to the LGPD applied in the company that was the focus of this study through the high index obtained in the previously mentioned tool. Furthermore, the relevance of the efficiency analysis stage in the process of adapting a company to the General Law for the Protection of Personal Data was noticed.

Keywords: Adequacy. Compliance. Index. GDPR.

LISTA DE ABREVIATURAS E SIGLAS

TIC	Tecnologias de Informação e Comunicação
LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	General Data Protection Regulation
RIPD	Relatório de Impacto a Proteção de Dados
UE	União Europeia

LISTA DE QUADROS

Quadro 1 - Diferenças entre a LGPD e GDPR	19
Quadro 2 - Obrigações	22
Quadro 3 - Etapas para Elaboração do RIPD	23
Quadro 4 - Protocolo de pesquisa	27
Quadro 5 - Processo de adequação.....	28
Quadro 6 – Questionário	29
Quadro 7 - RIPD	38
Quadro 8 - Identificação e Nível de Riscos	39
Quadro 9 - Medidas de Tratamento de Riscos	40
Quadro 10 - Escala de classificação de nível de adequação	42
Quadro 11 - Definições por escala de nível de adoção	42
Quadro 12 - Respostas inseridas para a validação da adequação.....	43
Quadro 13 - Avaliação do nível de adequação.....	45
Quadro 14 - Relação entre Dimensões e Ações de Adequação à LGPD	46

LISTA DE FIGURAS

Figura 1 - Modelo Teórico-Empírico	25
Figura 2 - Questão aberta.	32
Figura 3 - Armazenamento em nuvem.....	33
Figura 4 - Fluxo de Tratamento de Dados Pessoais dos Clientes	36
Figura 5 - Fluxo de Tratamento de Dados Pessoais dos Colaboradores	37

SUMÁRIO

1 INTRODUÇÃO	11
1.1 JUSTIFICATIVA.....	12
1.2 PROBLEMA DE PESQUISA	12
1.3 OBJETIVOS DE PESQUISA	13
2 REFERENCIAL TEÓRICO	13
2.1. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC)	13
2.2. TRANSFORMAÇÃO DIGITAL	14
2.3. SEGURANÇA DA INFORMAÇÃO	16
2.4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)	18
3. PROCEDIMENTOS METODOLÓGICOS	24
3.1. DELINEAMENTO DA PESQUISA	24
3.2. CASO SELECIONADO	25
3.3 UNIDADES DE ANÁLISE E SUJEITOS DA PESQUISA	25
3.4 INSTRUMENTO DA PESQUISA	26
3.5 COLETA DE DADOS	26
3.6 PROTOCOLO DO ESTUDO DE CASO E CONFIABILIDADE	26
3.7 ANÁLISE E INTERPRETAÇÃO DOS DADOS	27
4. PROCESSO DE ADEQUAÇÃO	27
4.1. DESCRIÇÃO DO PROCESSO DE ADEQUAÇÃO	28
4.1.1. Contratação	28
4.1.2. 1º Ato.....	29
4.1.3 2º Ato.....	29
4.1.4. 3º Ato.....	41
4.1.5. 4º Ato.....	41
4.1.6 5º Ato.....	41
5. ANÁLISE DO PROCESSO	42
6. SÍNTESE DOS PRINCIPAIS RESULTADOS	46
7. CONCLUSÃO	47
<u>REFERÊNCIAS</u>	49

1 INTRODUÇÃO

O uso irrestrito e indiscriminado dos dados pessoais tem levado as Tecnologias de Informação e Comunicação (TIC) a exercer uma grande influência na formação de opinião e tomada de decisão das pessoas, as quais necessariamente desconhecem ou sequer autorizaram essa manipulação de dados (HARARI, 2018).

Nesta realidade, a Lei Geral de Proteção de Dados Pessoais - Lei Nº 13.709, de 14 de agosto de 2018 (LGPD) trouxe mudanças aos processos organizacionais das empresas brasileiras. Baseada na General Data Protection Regulation (GDPR), a LGPD tem como objetivo garantir maior segurança aos titulares de dados, que são os mais atingidos em meio a essa era de ratificação das coisas. Sendo assim, a lei exige uma nova cultura organizacional e adequação aos seus parâmetros.

A LGPD estabelece uma cultura de proteção de dados, algo que seja essencialmente disseminado na sociedade, que possa envolver todo o processo de concepção de dados e que produza uma adequação a longo prazo. O intuito real é assegurar maior segurança aos titulares de dados, que se encontram fragilizados em meio a essa era tecnológica com a utilização demasiada de suas informações pessoais (IRAMINA, 2020).

Em Sergipe, com vista a adequar o Estado à LGPD, o governo instituiu a Política Estadual de Proteção de Dados Pessoais através do Decreto nº 40.006, a fim de estabelecer conjunto de diretrizes, projetos, ações e metas estratégicas, para a adequação dos atos de tratamento de dados pessoais realizados no âmbito da administração pública estadual direta e indireta do Poder Executivo (SERGIPE, 2021).

As medidas que devem ser tomadas por todas as empresas e órgãos públicos vão, dentre outras, desde garantir a segurança dos dados, quanto a pseudonimização ou anonimização dos dados para auxiliar na redução dos riscos para os titulares (GOMES, 2019). Assim, é importante que se esteja atento à necessidade imediata à adequação dos processos organizacionais no cumprimento da LGPD, garantindo uma maior segurança e transparência para os titulares dos dados e, sobretudo, minimizando os riscos de sofrer sanções previstas na referida lei.

Como conclui Gomes (2019), notadamente há uma significativa necessidade na mudança de cultura, assim como a adequação às normas que uma nova lei apresenta, e estes não acontecem de uma hora para outra. Também, mesmo com o término das atividades de adequação da empresa à uma legislação com tão pouco tempo tanto de vigência quanto de conclusão como é a LGPD, conseguir

fazer uma análise de eficiência do trabalho realizado representa um diferencial desejado a qualquer organização.

1.1 JUSTIFICATIVA

Grandes mudanças sociais vêm sendo provocadas pelo avanço tecnológico, mas a conscientização da sociedade dos efeitos do desenvolvimento ocorre de forma lenta e as adaptações necessárias não acontecem com o mesmo ritmo (HARRARI, 2018).

A transformação digital, caracterizada pela aplicação das TIC, é uma adequação das empresas à economia digital, que já era uma tendência e foi muito fomentada na pandemia do novo coronavírus. Contudo, apesar do intento em dispor de um relacionamento mais personalizado e fiel ao perfil do cliente, observa-se uma dificuldade para que o cidadão possa saber se as empresas observam o princípio constitucional da privacidade no uso dos seus dados pessoais.

A LGPD estabelece princípios e bases legais (LGPD, 2018), assim como a obrigatoriedade da adequação. No entanto, não há a definição e nem deve ser o objetivo da legislação especificar como devem ser realizadas as atividades e quais seriam boas práticas a serem adotadas, inclusive porque a natureza distinta e a condição atual de investimento de cada empresa devem exigir adoção de modelos distintos e de forma gradativa. Assim, é preciso pesquisar e identificar quais as melhores estratégias para uma determinada empresa.

A adequação das empresas em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da organização. Contudo, apenas a realização da adequação pode não ser garantia de conformidade à referida lei. É importante que haja um processo de análise para validar o nível de sucesso alcançado através das medidas propostas e se, de fato, a aplicação destas medidas foi suficiente para certificar a empresa ao *compliance* à LGPD.

Face ao exposto, este estudo de caso tem suma importância para o entendimento da referida lei, da responsabilidade das empresas brasileiras, das etapas necessárias para a adequação de uma empresa à LGPD e, principalmente, da garantia de conformidade das organizações à Lei Geral de Proteção de Dados, bem como para servir de base para outros estudos e pesquisas sobre este tema.

1.2 PROBLEMA DE PESQUISA

Qual o nível de adequação alcançado por um modelo de processo de conformidade à LGPD em uma empresa de Tecnologia no estado de Sergipe?

1.3 OBJETIVOS DE PESQUISA

Analisar um modelo de processo de adequação à Lei Geral de Proteção de Dados implementado em uma empresa de Tecnologia.

Tem-se ainda os seguintes objetivos específicos:

- Descrever as etapas do processo de adequação à LGPD utilizado pela empresa;
- Evidenciar os resultados alcançados pelo processo de adequação à LGPD;
- Submeter os resultados a uma ferramenta de diagnóstico de nível de maturidade à LGPD.

2 REFERENCIAL TEÓRICO

Este capítulo trata do referencial teórico do estudo de caso proposto. Nele será discutido sobre as tecnologias da informação e comunicação (TIC), a transformação digital, a segurança da informação e os detalhes a respeito dos fundamentos, princípios e bases legais previstas para o tratamento de dados pessoais, bem como as funções da tríade principal estabelecida pela LGPD: encarregado de dados, operador e o controlador. O capítulo encerra discutindo sobre o Relatório de Impacto a Proteção de Dados (RIPD), o qual será utilizado para o estudo de caso deste trabalho.

2.1. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

Notadamente, as TIC representam um tema muito pesquisado, com vasta literatura, inclusive pela característica disruptiva da sua aplicação, quer seja na sociedade, quer seja nas empresas. As TIC hoje representam o que a eletricidade foi na segunda revolução industrial (CASTELLS, 2013). Em uma síntese histórica, as TIC assumiram o protagonismo da terceira revolução industrial, principalmente a partir 1960, a partir do uso da programação digital de sistemas de automação.

As TIC estão fundamentadas em 4 componentes (REZENDE; ABREU 2013): hardware, software, internet e banco de dados. Adicionalmente, mesmo não sendo uma tecnologia, os autores referem-se ao termo *peopleware* para inserir as pessoas no referido contexto tecnológico, pois entendem que através delas é que se consegue ter funcionalidade e utilidade. Os sistemas tecnológicos são socialmente produzidos, indica (CASTELLS 2013). A junção das TIC e *peopleware* forma os sistemas computacionais (LAUDON; LAUDON, 2014).

No advento da terceira revolução industrial imposta pelas TIC, a principal atividade consistia em fazer o processamento de grandes massas de dados em informação, ou seja, atuava na cadeira de transformação inicial do sistema de informação. O computador era uma máquina de processar dados, pessoais ou não, em informação e transmiti-los com agilidade entre emissor e receptor através da internet.

Para uma abordagem mais atual pelo bom emprego das TIC nas empresas, tem-se que os sistemas computacionais passaram a atuar no patamar mais elevado do sistema de informação que é compreender a informação e sua aplicabilidade a partir de contextos, possibilitando o computador analisar e alcançar o nível de conhecimento (PASQUINI, 2020). Consequentemente, foi acrescido às TIC seu papel tecnológico na sociedade. Esse novo contexto será amplamente discutido na seção seguinte deste trabalho.

Anteriormente a evolução das TIC de interação com pessoas e empresa, Alcides; Abreu (2013) já destacavam que os ganhos com a rapidez e precisão da aplicação das TIC no contexto organizacional exige análise de custos, benefícios, riscos e, dentre outros, o respeito à legislação vigente. Assim sendo, a promulgação de leis relacionadas a modo de operação e uso de sistemas de informações por TIC representará sempre um requisito obrigatório de análise e pesquisa, a fim de que construam e mantenham seus sistemas computacionais legalizados.

2.2. TRANSFORMAÇÃO DIGITAL

Ademais entender que a transformação digital se trata da aplicação das TIC nas organizações, Rogers (2016) especifica que se trata de estratégia e de novas formas de pensar. Um outro conceito é que, cada vez mais, as organizações estão explorando novas tecnologias digitais que podem gerar transformações em suas operações, métodos de gestão e cultura (SINGH; HESS, 2017). Dessa forma, novas oportunidades de capitalização foram associadas à era da economia digital (UNO, 2016). Independentemente do modelo de negócio, os sistemas de informação são prioritariamente desenvolvidos a partir do uso ampliado de mecanismos digitais baseados nos sistemas computacionais.

O contexto histórico da transformação digital está diretamente relacionado à revolução industrial que as empresas estão inseridas, atualmente denominada de “Revolução 4.0” onde os computadores deixaram apenas de transformar dados em informação ou conhecimento, mas também de que as máquinas pudessem expressar comportamentos cujos aspectos cognitivos fossem similares ao do ser humano em que pessoas pudessem interagir com inteligências artificiais. Adicionalmente,

tem-se o estabelecimento de novos espaços cyber físicos e a internet das coisas que influenciam quase que diariamente as relações de comércio e relacionamento entre as pessoas e as empresas (PASQUINI, 2020). Podemos citar que, anteriormente, algoritmos estavam restritos aos discos rígidos dos computadores; porém, agora eles estão “presentes” também os espaços físicos e com interação constante e direta.

Apesar do cenário favorável atinente à transformação digital, deve-se ressaltar que a busca da experiência mais personalizada desejada pelo cliente inclui, dentre outros, identificar e relacionar suas características e preferências de maneira profunda e rápida, fazendo com que os avanços tecnológicos afetem diretamente as relações sociais (PINHEIRO, 2021). Com isso, o capitalismo de vigilância, além da obscuridade dos algoritmos que definem a lógica dos softwares, tem sido uma realidade que torna as pessoas vulneráveis a serem influenciadas através de variado e irrestrito tratamento dos seus dados (ZUBOFF, 2020). À medida em que os computadores avançaram nos sistemas de informação, tendo como aliado a capacidade da inteligência artificial e a rapidez algorítmica, o aprendizado alcançado do *peopleware* (Laudon; Laudon, 2014), os sistemas computacionais passaram a inferir na vida pessoal.

Um exemplo expressivo mundialmente conhecido e que alertou governos e sociedades em geral foi o escândalo da “Cambridge Analytica” em que dados de milhões de usuários de uma rede social foram adquiridos para fins de beneficiar a eleição política de um presidente de um país de grande influência para o mundo. Os dados obtidos oportunizaram percepções de um diferencial competitivo alcançados após as análises dos dados. Em razão disso, o processo decisório no marketing se tornou mais assertivo, e através disso, foi possível a criação de campanhas competitivas, eficazes e com probabilidades de sucesso muito mais altas (AGUIAR, 2021).

Logicamente que os avanços técnicos e científicos aplicados e que possibilitaram o progresso da sociedade através da transformação digital não devem ser restringidos ou mesmo desconsiderados, inclusive porque já se discute novos termos para uma geração sucessória de revolução industrial denominada de Revolução 5.0, cujo objetivo de usar tecnologias digitais e habilidades humanas para promover inclusão, sustentabilidade e equidade (SOTT; BAUM; BENDER, 2021).

O bem-estar do cidadão e por uma sociedade com melhores perspectivas de existência e relacionamento é louvável e deve ser fomentado. Contudo, o bem social envolve obrigatoriamente o zelo pelo cumprimento de questões éticas e legais. Por exemplo, o 5o, inciso X, da Constituição

Federal de 1988 deixa claro que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. A transformação digital não está acima das legislações, muito pelo contrário, podemos considerar que a sinergia com a privacidade será mais uma contribuição para que a sociedade esteja mais assegurada para usufruir da próxima revolução.

Desta forma, é necessário considerar como uma boa prática a ser implantada nas empresas a disponibilidade de um recurso tanto interno, voltado para os fluxos organizacionais, quanto externos – para divulgação aos clientes e à sociedade em geral, inclusive governos, para deixar claro como faz uso dos dados pessoais e procura observar as questões éticas e legais relacionado ao estabelecimento e manutenção da privacidade de dado pessoal. Ainda nesta seção será discutido como a lei brasileira de privacidade de dados, denominada de Lei Geral de Proteção de Dados – LGPD.

2.3. SEGURANÇA DA INFORMAÇÃO

Com a expansão de comércio e negócios eletrônicos, baseados no contexto da nova economia, ações maliciosas de roubo de adulteração de informações passaram ser recorrentes através da internet, ameaçando a continuidade das empresas. Teve início então as medidas protetivas de segurança da informação.

A segurança da informação transcende a tecnologia, e rotineiramente sugere novos paradigmas organizacionais (SÊMOLA, 2014). Ela consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade), bem como é autêntica (integridade). Estes três elementos: confidencialidade, integridade e disponibilidade, formam a tríade da segurança da informação (SÊMOLA, 2014), que é a base dos conceitos e práticas relacionados à gestão da segurança da informação.

Adicionalmente, de acordo com Fernandes (2010), quatro outras propriedades são associadas à tríade: autenticação, autorização, identificação e não repúdio (este último, também denominado de irretratabilidade). Atuando em conjunto, estes sete elementos fundamentam a gestão da segurança da informação no intento de proteger dados, sistemas e processos.

- Autenticação: propriedade de garantir a fonte e o teor da informação.
- Autorização: propriedade de permitir ou negar o acesso.
- Identificação: propriedade de registrar algo ou alguém no sistema.

- Não repúdio: propriedade de garantir ao autor sua respectiva responsabilidade pelo que fez.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ABNT 27002, 2013, p. 16). Kozen *et al* (2012) dizem que se a organização está fazendo uso de normas de segurança da informação, ela já está seguindo as diretrizes dos processos de gestão da segurança da informação, o que a possibilita de ser reconhecida pela adoção de boas práticas em gestão da segurança da informação.

A ABNT, adicionalmente à norma 27005, dispõe de um conjunto de normas que compõe a “Família 27000” que busca dar subsídios a implantação do Sistema de Gestão de Segurança da Informação (SI), sendo as principais identificadas como 27001 – referente aos requisitos de implantação; a 27002 com boas práticas relacionadas à norma 27001; e a 27005 que trata da normativa para a realização da gestão de riscos. Portanto, essas normas não são concorrentes, mas sim complementares e apoiam a implantação e manutenção do SGSI.

Com a publicação da LGPD, a ABNT acrescentou uma nova norma à Família 27000 com foco na implantação de um Sistema de Gestão da Privacidade da Informação (SGPI), que apresenta medidas adicionais que devem ser implementadas nas normas 27001 e 27002 para o cumprimento da privacidade de dados (ABNT 27701, 2020).

Para garantir êxito de que as questões relacionadas à segurança da informação sejam atendidas de forma satisfatória, as empresas têm aperfeiçoado e modificado, ao longo do tempo, seus modelos para desenvolvimento e uso dos sistemas computacionais; mas há dificuldades para sua plena implantação, uma vez que a facilidade de uso e a segurança caminham sempre em sentidos opostos (SÊMOLA, 2014). Através de políticas, que envolve planos de conscientização, as empresas buscam estabelecer uma cultura que contemple uma rotina segura às informações.

Do ponto de vista tecnológico, os mecanismos de proteção comumente implementados nas TIC dar implantação de medidas protetivas da segurança da informação são:

- Criptografia;
- Assinatura digital;
- Controle de acesso;
- Certificados digitais; e

- Auditoria.

Convém ressaltar que a ênfase da segurança da informação está diretamente relacionada à informação; portanto, sem referência por exemplo a cumprir os requisitos legais da LGPD, cujo ponto focal está nos dados da pessoa natural. A partir do conceito de sistemas de informação, dados e informação são fundamentalmente elementos distintos (LAUDON; LAUDON, 2014), apesar de interligados pela atividade de processamento.

2.4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Com a globalização e o desenvolvimento de novas tecnologias desenvolve uma competição cada vez mais voraz entre as empresas, desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes. As empresas e até o estado estão cada vez vulneráveis a espionagem ou de ataques de Hackers como evidenciado as divulgações de áudios de empresas e dos principais poderes do Brasil (RAPOSÔ, 2019, p. 2).

Harari (2015) afirma que para evitar a concentração de riqueza e poder nas mãos de uma pequena elite, a solução é regulamentar e controlar a propriedade de dados, inclusive para coibir a atuação e defender as pessoas do capitalismo de vigilância.

A LGPD (Lei Nº 13.709/2018) tem como objetivo principal a proteção aos direitos de liberdade de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei também se direciona à padronização de regulamentos práticos para promover a proteção de dados pessoais de todo cidadão brasileiro, tendo por base o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UE).

A UE também considera a proteção de dados pessoais um direito de todos os cidadãos do país, haja vista que leis relacionadas à proteção de dados já existiam desde 1995, porém eram muito antigas e não correspondiam com o cenário tecnológico da atualidade. Foi a partir deste princípio que o GDPR foi criado, requerendo que empresas e organizações de qualquer porte ou área de atuação sigam regras para coletar, processar, compartilhar e resguardar dados pessoais. Contudo, mesmo sendo baseada na GDPR, a LGPD tem suas diferenças e particularidades as quais estão dispostas no Quadro 1.

Quadro 1 - Diferenças entre a LGPD e GDPR

	LGPD	GDPR
Implementação	Setembro de 2020	Maio de 2018
Contratação de DPO	Todos os casos	Variável em função do volume, sensibilidade, tramitado por órgão público
Comunicação de vazamentos	Dentro de um “período razoável”	Em até 72h
Penalização	2% da receita, com limite máximo de R\$ 50 milhões	4% da receita anual ou até € 20 milhões
Resposta à solicitação de titulares de dados	Em até 15 dias	Em até 30 dias

Fonte: LGPD (2018).

Segundo Sá (2019), a LGPD é um novo paradigma, pelo fato de estabelecer mudanças na rotina empresarial de gestão de dados pessoais nos meios online e offline, tendo como principal finalidade proteger os direitos fundamentais de liberdade e privacidade em qualquer relacionamento que envolva os dados supracitados. Diante de uma mudança tão grande, causada pela lei, as empresas, que antes tinham total liberdade na coleta de dados, passaram a se ver obrigadas pelas novas regras a seguir um padrão que impede que os dados pessoais sejam tratados de qualquer modo.

Dentro desta perspectiva, a LGPD (2018) traz o conceito de dados pessoais, bem como suas classificações dentro da norma. Os dados são classificados como sensíveis, anonimizados, pessoais, pseudonimizados, nos quais cada um tem seu peso diante da LGPD e devem ser tratados de formas diferentes.

- **Dados pessoais:** São todas informações relacionadas à pessoa natural identificada ou identificável, são as informações básicas de um determinado indivíduo como: nome, sobrenome, endereço de residência, RG, CPF, data de nascimento, e-mail, telefone, nacionalidade, hábitos de consumo, interesses.
- **Dados sensíveis:** dado referente à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Dados anonimizados:** dado referente ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

- **Dados pseudonimizados:** são dados que, sozinhos, não conseguem identificar o titular, mas somados a outras informações torna a ação possível.

As bases legais para a proteção de dados da LGPD têm a finalidade de limitar e inibir a utilização dos dados de formas ilegal, ou seja, impedir que esses dados possam ser utilizados de modo demasiado por organizações para seu próprio benefício e sem o consentimento do titular dos dados. As bases legais são o ponto de partida para as empresas e organizações criarem relações mais justas com o consumidor.

A partir do momento em que a LGPD entrou em vigor, empresas que utilizarem dados pessoais sem uma base legal adequada, tratarão dados de forma ilegal. No artigo 7º da LGPD estão descritas as bases legais para a manipulação dos dados, que são elas:

- Consentimento;
- Obrigação legal ou regulatória;
- Execução de políticas públicas pela administração pública;
- Estudos por órgão de pesquisa;
- Execução de contrato;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiros;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Interesse legítimo;
- Proteção ao crédito.

Também descrito na LGPD estão os fundamentos para a proteção de dados pessoais são eles:

1. Respeito à privacidade;
2. Autodeterminação informativa;
3. Liberdade de expressão, de informação, de comunicação e de opinião;
4. Inviolabilidade da intimidade, da honra e da imagem;

5. Desenvolvimento econômico e tecnológico e a inovação;
6. Livre iniciativa, a livre concorrência e a defesa do consumidor;
7. Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

De acordo com Art. 1º da LGPD, a referida lei se aplica a todo e qualquer tratamento de dados, por qualquer meio, seja realizado por pessoa natural ou pessoa jurídica de direito público ou privado.

A lei exige que as atividades de processamento de dados pessoais obedeçam aos seguintes princípios: objetivo, suficiência, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e contribuição, Art.6 da Lei nº. 13.709 de 14 de agosto de 2018 (BRASIL, 2018).

Segundo o art. 5º, inciso VIII e IX, a LGPD identifica e define como equipe de tratamento de dados os controladores e os operadores. Os agentes têm uma importância imensa na hora do tratamento dos dados, pois eles são responsáveis por definir e observar a segurança, sigilo e forma como os dados pessoais são tratados.

A definição do operador é muito parecida com a do controlador, uma vez que ele também pode ser uma pessoa de direito público ou privado, sendo natural ou jurídica. A distinção é que o operador realiza o tratamento dos dados pessoais por ordem e em nome do controlador (LGPD, 2018).

Conforme a LGPD, é de responsabilidade do controlador a tomada de decisão que remete ao tratamento dos dados pessoais, cabendo ao operador segui-las irrestritamente. Como o operador responde solidariamente em caso de eventuais problemas, ele deve sugerir ou até mesmo negar algum tratamento que represente grandes riscos, por exemplo, de vazamento dos dados. Outras obrigações entre controlador e operador são apresentadas no Quadro 2.

O encarregado é responsável por ser um elo entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD), fazendo a comunicação entre essas partes. Conforme a LGPD, cabe ao controlador indicar e informar seu encarregado.

Quadro 2 - Obrigações

	Controlador	Operador
Limites para tratamento	Tratar dados com base legal definida	Tratar dados conforme propósito definidos pelo controlador
Registro	Registro das atividades	Registro das atividades
Relatório de impacto	Elaborar relatório de impacto	Auxiliar o controlador em alguma necessidade
Incidentes	Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Informar ao controlador casos de incidentes
Boas práticas de segurança	Adotar medidas de segurança, técnicas e administrativas aptas a 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 ou ilícito	Adotar medidas de segurança, técnicas e administrativas aptas a 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 ou ilícito
Programa de governança em privacidade	Implementar Programa de Governança em Privacidade, observadas a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados	Receber e estar ciente do Programa de Governança adotado pelo controlador
Direitos dos titulares	Atender aos direitos dos titulares, encaminhando dúvidas e questionamentos ao encarregado de dados	Atender aos direitos dos titulares, encaminhando dúvidas e questionamentos ao encarregado de dados

Fonte: Maciel (2019)

Ademais, com o objetivo de documentar todo tipo de tratamento de dados feito pelas organizações, bem como apresentar um resumo das atividades de adequação realizadas pelos agentes de tratamento de dados, é construído pelo Controlador de dados pessoais o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Conforme a LGPD (2018), o relatório de impacto pode ser compreendido como um documento que tem por finalidade uma avaliação de impacto que tem como meta: considerar, mapear, planejar, efetuar e acompanhar todos os processos para que estejam de acordo com as leis gerais e setoriais de proteção a dados. Em poucas palavras, o relatório servirá como uma identificação das ações de tratamento de dados de uma empresa, uma vez que ele é normalmente associado como resultado de que a organização está em conformidade com o que é proposto pela LGPD. Onde por meio dessa documentação o controlador saberá quais caminhos seguir e quais medidas devem ser tomadas.

O relatório de impacto não necessariamente é uma ferramenta cujo objetivo principal é apenas atender os processos de conformidade junto a LGPD, mas sim, um documento que avalia os impactos e identifica os riscos. É importante deixar claro que os dados do relatório também podem ser produzidos e utilizados para diversas finalidades, por exemplo: para avaliar o impacto de incidentes de segurança; avaliar o impacto de novas tecnologias; avaliar o impacto de novos produtos que podem gerar riscos aos direitos dos titulares de dados etc.

Para que todos os processos que envolvam tratamento de dados, atuais ou futuros, garantam preservação e atendam aos direitos de seus titulares, o relatório de impacto tem que ser uma ferramenta de governança de dados interiorizada no dia a dia da instituição e não só utilizada durante o processo de conformidade, não como uma simples ferramenta de burocracia, mas sim, um documento que ajuda o agente de tratamento de dados, uma vez que os relatórios de impacto não são usados somente para adequar-se à uma lei. Ressaltando que mesmo os relatórios de proteção de dados sendo novos no Brasil, eles são reflexo da regulamentação da UE em proteção de dados.

Quadro 3 - Etapas para Elaboração do RIPD

ETAPA	ATIVIDADE
Identificar os agentes de tratamento e o encarregado	Identificar quem atua como Operador, Controlador e Encarregado de Dados na organização.
Identificar a necessidade de elaborar o relatório	Identificar e descrever quais as categorias dos titulares que terão seus dados tratados pela organização.
Descrever o tratamento	Identificar e descrever a natureza, o escopo e a finalidade do tratamento de dados pela organização.
Identificar partes relacionadas interessadas consultadas	Identificar e descrever todas as partes consultadas necessárias para a elaboração do relatório.
Descrever necessidade e proporcionalidade	Identificar e relatar a fundamentação legal, as medidas de segurança e as salvaguardas referentes à transferência internacional de dados tratados pela organização.
Identificar e avaliar os riscos	Identificar os riscos referentes ao tratamento de dados pessoais na organização e avaliá-los de acordo com a matriz de risco.
Identificar medidas para tratar os riscos	Indicar medidas com a finalidade de mitigar os riscos referente ao tratamento de dados identificados na organização.
Aprovar o relatório	Apresentação do relatório e aprovação individual de execução das medidas indicadas para tratar os riscos
Manter revisão	Revisar continuamente a evolução da adequação e conformidade da organização e registrar novas sugestões e resultados no relatório.

Fonte: adaptado de Guia (2020)

O relatório de impacto é composto por oito etapas ordenadas sequencialmente, são elas: (i) Identificação dos agentes de tratamento e do encarregado; (ii) Necessidade de elaboração do relatório; (iii) Descrição do tratamento; (iv) Partes interessadas consultadas; (v) Identificação da necessidade e proporcionalidade; (vi) Identificação dos riscos à Proteção de Dados Pessoais; (vii) Medidas para

mitigação dos riscos; (viii) Aprovação do relatório. O Quadro 3 mostra as etapas e respectivas atividades relacionadas à elaboração do relatório.

3. PROCEDIMENTOS METODOLÓGICOS

Este capítulo delineará sobre a metodologia utilizada durante o estudo, desde a definição do método até a análise dos dados, para alcançar o objetivo da pesquisa.

O delineamento refere-se ao planejamento da pesquisa em sua dimensão mais ampla, que envolve tanto a diagramação quanto a previsão de análise e interpretação de coleta de dados. Entre outros aspectos, o delineamento considera o ambiente em que são coletados os dados e as formas de controle das variáveis envolvidas (GIL, 2008, p. 68). Ainda de acordo com GIL (2008), um conhecimento é considerado científico na medida em que são identificadas, as operações mentais e técnicas, que possibilitem a sua averiguação. Esse autor descreve a caracterização da metodologia como um conjunto de procedimentos, intelectuais e técnicos, que atuam em prol do alcance ao conhecimento (GIL, 2008).

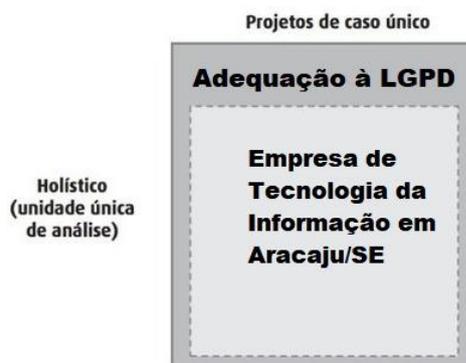
Desta forma, são relatados os procedimentos metodológicos utilizados na pesquisa, com a divisão de partes específicas referentes ao: 1) delineamento da pesquisa; 2) caso selecionado; 3) unidades de análise e sujeitos da pesquisa; 4) instrumento da pesquisa; 5) coleta dados; 6) protocolo do estudo de caso e confiabilidade e 7) análise e interpretação dos dados.

3.1. DELINEAMENTO DA PESQUISA

De acordo com Yin (2015), estudo de caso é um método para investigar um fenômeno contemporâneo (o “caso”) em profundidade e em seu contexto de mundo real. Desta forma, consideramos que a adequação à LGPD se trata do acontecimento recente que obriga as empresas a rever seus processos de tratamento de dados pessoais. Para Schramm (1971), a essência de um estudo de caso é demonstrar, através dos métodos e das etapas, o motivo de uma ou de um conjunto de decisões, e os resultados alcançados através dela.

O presente trabalho trata-se de um estudo de caso único e holístico (YIN, 2015), pois o foco deste estudo foi analisar somente uma empresa e validar o modelo de processo para sua adequação à LGPD considerando seu seguimento mercadológico e suas especificidades organizacionais, através da análise documental de todo o processo de adequação realizado. O modelo teórico da pesquisa ilustrado com mais detalhes na Figura 2 a seguir.

Figura 1 - Modelo Teórico-Empírico



Fonte: Adaptado de Yin (2015)

Além disso, é caracterizada como uma pesquisa qualitativa exploratória descritiva, pois a característica mais importante dessa pesquisa é a necessidade de se conhecer um fato ou fenômeno ainda pouco explorado, que, no caso, é a validade do processo de adequação à LGPD dentro da realidade organizacional do objeto de estudo.

3.2.CASO SELECIONADO

O objeto de estudo é uma empresa que presta serviços referentes a tecnologias da informação e comunicação corporativas, situada na cidade de Aracaju/SE, que, através de uma consultoria, havia realizado a adequação à LGPD em setembro de 2021. A pesquisa iniciou-se em maio de 2022 e foi finalizada em novembro do mesmo ano. A referida empresa atua há 22 anos no mercado sergipano e conta com dois sócios e doze colaboradores, dentre os quais, dez estão ligados diretamente à área de operação de sistemas e tecnologias, enquanto os outros dois estão ligados às áreas financeira e pessoal da empresa. Além do tempo de mercado, a qualidade e o preço dos serviços prestados elevam o diferencial competitivo da empresa e a torna uma das principais integradoras em telecomunicações do estado.

3.3 UNIDADES DE ANÁLISE E SUJEITOS DA PESQUISA

As unidades analisadas foram todos os doze colaboradores dos setores pertencentes ao caso selecionado, os quais façam tratamento de dados pessoais, bem como todos os documentos relacionados à adequação à LGPD realizada. Ao todo, doze pessoas foram entrevistadas (oito colaboradores e dois sócios), considerando como critério de participação a presença dos funcionários presentes no período da coleta de dados, excluindo-se apenas os que estiverem ausentes da empresa por algum afastamento (férias, licença etc.) e de aviso prévio.

3.4 INSTRUMENTO DA PESQUISA

Segundo Minayo (2008), a entrevista é a estratégia que mais se utiliza no trabalho de pesquisa. De acordo com Gil (1999), a entrevista é uma forma de interação social, feita através da busca de uma das partes em coletar dados e da colaboração da outra parte em fornecer as informações.

Com o objetivo de conhecer os processos de adequação à LGPD implementados no objeto de estudo, bem como entender quais foram as participações e condutas dos colaboradores durante o processo, foram feitas duas entrevistas abertas e focalizadas a respeito do tema proposto. A primeira entrevista teve como foco as opiniões e percepções dos sócios acerca do que compreendiam sobre a LGPD e sobre a adequação realizada pela empresa de consultoria, enquanto a segunda, buscava as opiniões dos colaboradores da empresa a respeito do mesmo tema. Além disso, foi feita uma análise documental com todos os documentos referentes à adequação realizada na empresa, e, uma pesquisa bibliográfica, com foco na Lei Geral de Proteção de Dados Pessoais e nas principais literaturas que a abrangem.

3.5 COLETA DE DADOS

Os dados representam os mais baixos elementos registrados que resultam de alguma observação, entrevistas, experiência ou situação análoga a um experimento (YIN, 2016).

Nesse sentido, inicialmente, nas dependências da empresa, foi feita uma investigação presencial com os sócios e colaboradores nos setores da empresa sobre os processos de adequação realizados e quais foram as contribuições de cada setor. Posteriormente, foram solicitados todos os documentos físicos e digitais gerados pelo processo de adequação, foram eles: e-mails, formulários e Relatório de Impacto à Proteção de Dados, Política de Privacidade de Dados e contratos ou cláusulas contratuais relativas à LGPD.

3.6 PROTOCOLO DO ESTUDO DE CASO E CONFIABILIDADE

Para Zanelli (2002), a credibilidade de uma pesquisa consiste no uso das teorias conceituais e na adoção de etapas metodológicas criteriosas.

Segundo Luna (1998, p. 736), “o protocolo é uma etapa importante na realização da pesquisa, pois através dos procedimentos contidos nele, é possível reaplicar a pesquisa, ou até mesmo, aplicá-lo em outros estudos que tenham características semelhantes ao primeiro”. O protocolo da pesquisa do presente estudo de caso está disposto no Quadro 4.

Quadro 4 - Protocolo de pesquisa

Item de Protocolo	Resposta
Visão Geral do estudo de caso e finalidade do protocolo	Analisar um modelo de processo de adequação à Lei Geral de Proteção de Dados implementado em uma empresa de Tecnologia.
Procedimentos de coleta de dados	<ol style="list-style-type: none"> 1. Entrevistas; 2. Análise documental.
Questões do estudo de caso	<ol style="list-style-type: none"> 1. Quais são as etapas do processo de adequação à LGPD utilizado pela empresa? 2. Quais foram os resultados alcançados pelo processo de adequação à LGPD? 3. Qual o nível de maturidade à LGPD alcançado pela empresa quando submetida a uma ferramenta de diagnóstico?
Guia para relatório do estudo de caso	<ol style="list-style-type: none"> 1. Antes: Verificar horários adequados para as entrevistas, agendar entrevistas, verificar documentos da empresa a serem analisados. 2. Depois: Verificar se as entrevistas estão adequadas, realizar transcrição, examinar se todos os documentos analisados foram adequados, realizar análises documentais e das entrevistas.

Fonte: Elaborado pela autora com base em Yin (2015).

3.7 ANÁLISE E INTERPRETAÇÃO DOS DADOS

Segundo Gil (2008), a análise e a interpretação dos dados são dois processos que, apesar de serem conceitualmente distintos, estão sempre relacionados. “O objetivo da análise é organizar os dados para o fornecimento de respostas para a investigação, já na interpretação, o objetivo é interrelacionar as respostas a outros conhecimentos já obtidos, a fim de encontrar o sentido mais amplo das respostas” (GIL, 2008, p. 175). A partir de informações extraídas dos meios de coleta de dados utilizados nesta pesquisa, conforme explanado no objeto de pesquisa, foi possível identificar as etapas do processo de adequação à LGPD utilizado pela empresa, bem como avaliar os resultados obtidos após a realização da adequação.

4. PROCESSO DE ADEQUAÇÃO

O presente capítulo tem como propósito atender aos dois primeiros objetivos específicos desta pesquisa, são eles: (i) descrever as etapas do processo de adequação à LGPD utilizado pela empresa; (ii) evidenciar os resultados alcançados pelo processo de adequação à LGPD.

4.1. DESCRIÇÃO DO PROCESSO DE ADEQUAÇÃO

Quadro 5 - Processo de adequação

PROCESSO	ATIVIDADES	ETAPAS	ESTIMATIVA DE TEMPO
Contratação	Assinatura do contrato	Reunião com os sócios para assinatura.	1h
1º Ato	Comunicado institucional	1. E-mail de apresentação. 2. Reunião de Apresentação, Ambientação (LGPD) e Sensibilização. 3. Envio de material completo sobre LGPD.	5 dias
2º Ato	Mapeamento de Dados	1. Envio de formulário via e-mail com prazo máximo de 48h para respostas. 2. Identificação dos dados pessoais tratados. 3. Construção do fluxograma de dados pessoais. 4. Construção do Relatório de Impacto e Proteção aos dados pessoais.	30 dias
3º Ato	Reunião de alinhamento ao <i>Compliance</i> .	Apresentação do RIPD e autorização de medidas propostas.	3 horas
4º Ato	Adoção de medidas já aprovadas	Aplicação efetiva das medidas propostas.	45 dias
5º Ato	Definição do encarregado de dados	Escolha e publicitação do agente encarregado de dados.	1 hora

Fonte: Autora.

Segundo relatado nas entrevistas, a empresa terceirizou a adequação e contratou uma empresa especialista em adequação à Lei Geral de Proteção de Dados. O processo teve início no dia 15 de setembro de 2021, com uma reunião entre os sócios e a empresa contratada, para explanação do método que seria utilizado para realizar a adequação, que foram divididos em cinco atos (processos), conforme descrito no Quadro 5.

4.1.1. Contratação

A reunião de contratação aconteceu no dia 16 de setembro de 2021, no escritório da empresa estudada, com a devida apresentação dos processos, atividades, etapas e estimativa de tempo para a adequação à LGPD, e cumpriu seu tempo estimado de 1 hora. Nesta reunião, foram solicitados os e-mails corporativos de todos os colaboradores da empresa, com a finalidade de enviar o e-mail de apresentação da empresa de consultoria contratada.

4.1.2. 1º Ato

As atividades referentes ao primeiro ato foram iniciadas no dia posterior à reunião de contratação, 16 de setembro de 2021, com o envio do e-mail de apresentação a todos os colaboradores da empresa com a confirmação de leitura comprovada por todos. Logo após, no dia 18 de setembro de 2021, foi enviado de material completo sobre LGPD confeccionado pela empresa de consultoria contratada. Para finalizar este processo (1º ato), nos dias 20 e 21 de setembro de 2021, foram realizadas duas reuniões de apresentação, ambientação e sensibilização à LGPD, a primeira com o setor operacional de TI e a segunda com os setores de Gestão de Pessoas e Financeiro.

4.1.3 2º Ato

As atividades referentes ao segundo ato foram iniciadas no dia 23 de setembro de 2021 com o envio de questionário a respeito dos dados pessoais tratados, que foi enviado via e-mail pela empresa de consultoria contratada para os sócios e colaboradores da empresa, para que respondam de acordo com o seu setor. O questionário foi composto por dez (10) questões, das quais sete (7) são objetivas e três (3) subjetivas, conforme demonstrado no Quadro 2.

Após as 48 horas reservadas para o recebimento de respostas, foram iniciadas as etapas de identificação dos dados pessoais tratados e associação às suas respectivas bases legais para o tratamento dos dados pessoais identificados. Para tais finalidades, foram analisadas as respostas descritas nesta seção.

Quadro 6 – Questionário

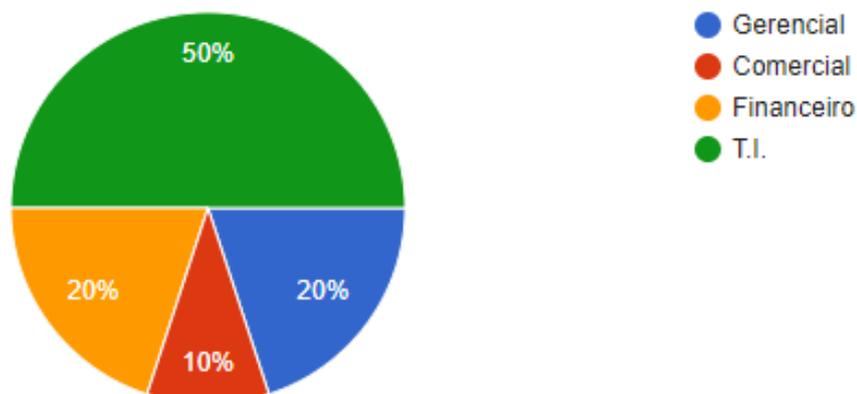
<p>Indique o setor ao qual você faz parte.</p> <p><input type="checkbox"/> Gerencial <input type="checkbox"/> Comercial Financeiro <input type="checkbox"/> TI <input type="checkbox"/> Outro. Citar:</p>
<p>Você sabe o que são dados pessoais?</p> <p><input type="checkbox"/> Sim <input type="checkbox"/> Não</p>
<p>No desempenho da sua atividade, há coleta de algum dado listado abaixo?</p> <p><input type="checkbox"/> Estado civil, identidade, dados de identificação (RG, CPF), imagens (foto)</p> <p><input type="checkbox"/> Vida pessoal (estilo de vida, situação familiar)</p> <p><input type="checkbox"/> Informações econômico- financeiras (receita, situação financeira, situação tributária)</p> <p><input type="checkbox"/> Dados de conexão (IP, logs, etc)</p> <p><input type="checkbox"/> Dados de localização (movimentos, dados de GPS, GSM, etc)</p> <p><input type="checkbox"/> Dados da Seguridade Social e Trabalhista (PIS, PASEP, Seguro desemprego,</p> <p><input type="checkbox"/> Programa de Assistência Social, vínculos trabalhistas, etc)</p> <p><input type="checkbox"/> Dados que revelem origem racial ou étnica</p> <p><input type="checkbox"/> Dados que revelem opiniões políticas</p>

<input type="checkbox"/> Dados que revelem crenças religiosas ou losó cas <input type="checkbox"/> Dados revelando associação sindical <input type="checkbox"/> Dados genéticos <input type="checkbox"/> Dados biométricos com o objetivo de identi car exclusivamente uma pessoa singular <input type="checkbox"/> Dados relativos à saúde <input type="checkbox"/> Dados relativos à vida sexual ou orientação sexual de uma pessoa singular Dados relativos a condenações e infrações penais
Além destes, há outros dados pessoais tratados não citados anteriormente? Se existe, relacione-os.
Ao coletar qualquer um dos dados acima especificados, onde são armazenados? <input type="checkbox"/> Google Drive – Nuvem <input type="checkbox"/> OneDrive <input type="checkbox"/> Planilha Excel <input type="checkbox"/> Word <input type="checkbox"/> Documento físico
Além destes, há outros locais de armazenamento não citados anteriormente? Se existe, relacione-os.
Quais setores da empresa possuem acesso aos dados coletados? <input type="checkbox"/> Todos, ou seja, amplo acesso <input type="checkbox"/> Apenas o financeiro <input type="checkbox"/> Apenas o TI <input type="checkbox"/> Apenas a Gerência <input type="checkbox"/> Apenas o Comercial <input type="checkbox"/> Apenas pessoas indicadas.
Há um prazo mínimo para conservação dos dados coletados? <input type="checkbox"/> Não há prazo mínimo <input type="checkbox"/> 01 – 02 anos <input type="checkbox"/> 03 – 05 anos <input type="checkbox"/> 05 – 10 anos <input type="checkbox"/> Acima de 10 anos
Os dados coletados são compartilhados com outra empresa ou pessoa que não se encontra no quadro de funcionários da instituição (estabelecimento)? <input type="checkbox"/> Não <input type="checkbox"/> Sim. Relacione-as:

Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

No Gráfico 1 abaixo, têm-se as respostas referentes à primeira indagação do questionário acerca dos setores dos quais os colaboradores fazem parte, e constata-se que 50% dos respondentes estão alocados na área de operação de sistemas e tecnologias da informação, 20% na área financeira, 20% na área comercial de vendas de serviços e 10% estão atuando na gerência da empresa.

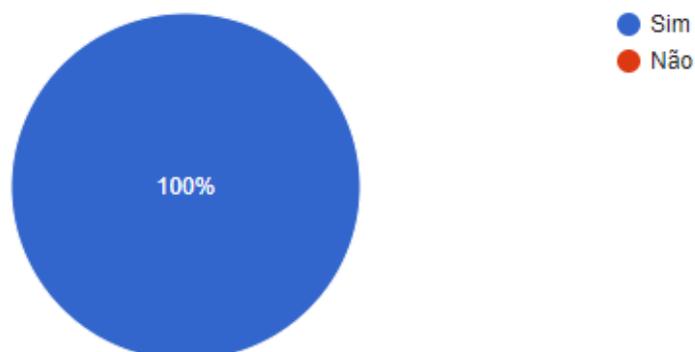
Gráfico 1 - Setor organizacional dos respondentes.



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A questão seguinte foi sobre o conhecimento dos respondentes acerca do que são dados pessoais. E, como demonstrado no Gráfico 2, 100% afirmou possuir esse conhecimento.

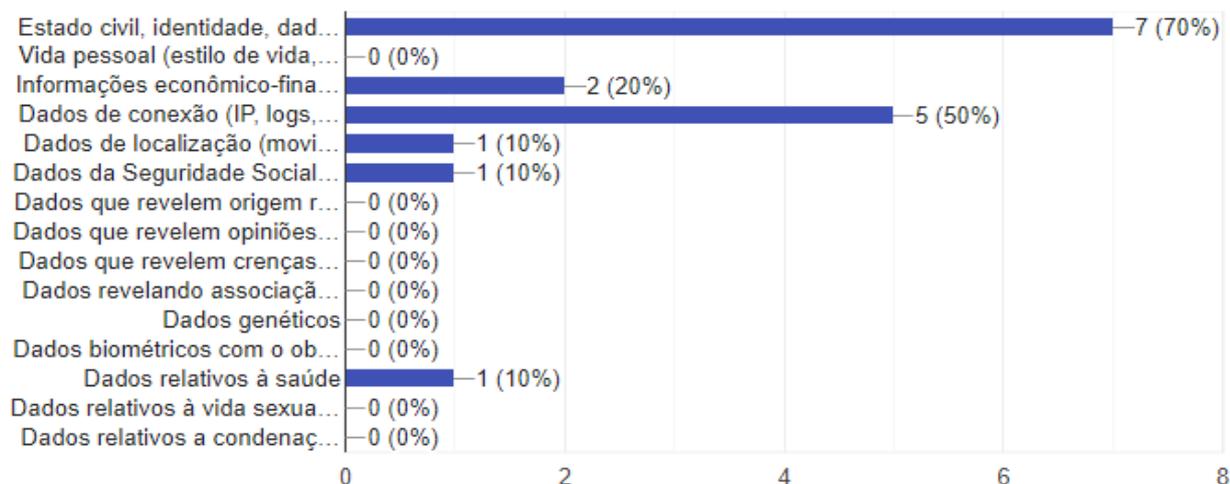
Gráfico 2 – Conhece o que são dados pessoais.



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A questão três coloca em pauta o tipo de dado pessoal tratado pela empresa, onde 70% dos respondentes dizem armazenar informações sobre pessoa natural, o que inclui informações que podem identificar o indivíduo. Os demais, com 20% das respostas, obtiveram-se o armazenamento de informações econômicas, em seguida, com 10% cada, dados de localização, seguridade social e por fim, dados referentes à saúde dos indivíduos, conforme disposto no Gráfico 3.

Gráfico 3 – Tipos de dados pessoais tratados.



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

Na quarta pergunta é indagado se, além dos dados citados anteriormente, havia outros dados tratados pela área de atuação da empresa, e, como disposto na Figura 2, 30% dos respondentes informaram que não, 60% responderam citando dados pessoais que já estavam descritos na pergunta anterior e apenas 10% informaram que, além dos dados citados na questão três, também havia o armazenamento de ligações no serviço de Call Center oferecido pela referida empresa.

Figura 2 - Questão aberta.

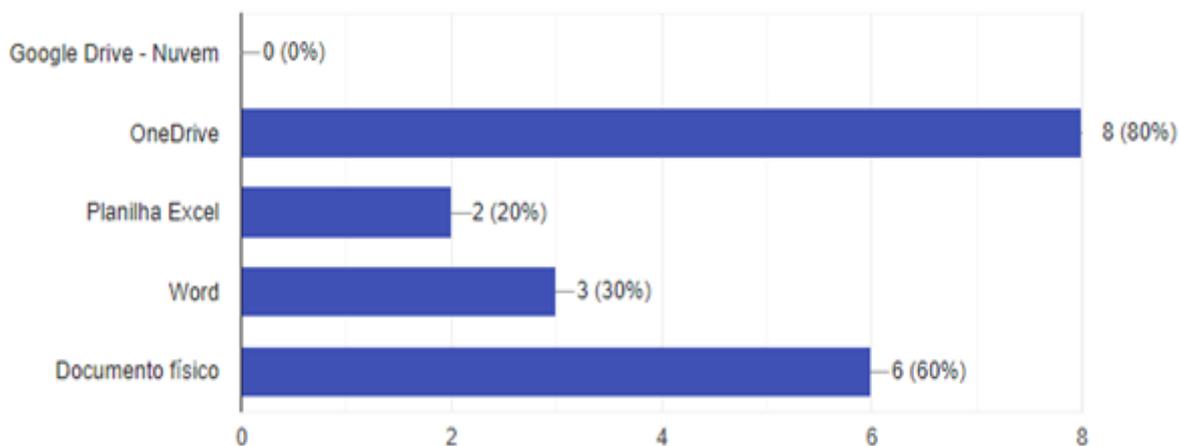
Não
Dados das empresas que fechamos contratos ou propostas. Dados dos cartões cnpj das empresas.
Relatório e gravação de ligações entrantes e saíntes (PABX ou serviço Call Center).
CNPJ, informações sobre setor e permissão de usuários dentro da rede
Nao
NÃO
dados bancarios
Contratos sociais
endereço, contato telefonico

Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A questão cinco, que permite múltipla escolha, investiga onde são armazenados os dados pessoais coletados pela empresa, onde 80% afirmaram armazenar no OneDrive, tecnologia de armazenamento em nuvem, 20% respondeu armazenar em Planilha Excel, 30% no editor de textos

Microsoft Word e, por fim, 60% dos respondentes disseram armazenar os dados em documentos físicos, conforme disposto no Gráfico 4.

Gráfico 4 - Dispositivos das TIC.



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A sexta questão, semelhantemente à quarta, é indagado se, além destes, havia outros locais de armazenamento dos dados pessoais coletados não citados anteriormente, e, conforme a Figura 3, apenas 16% responderam que havia, citando armazenamento em disco rígido e em formato PDF. Os outros 84% responderam que não.

Figura 3 - Armazenamento em nuvem

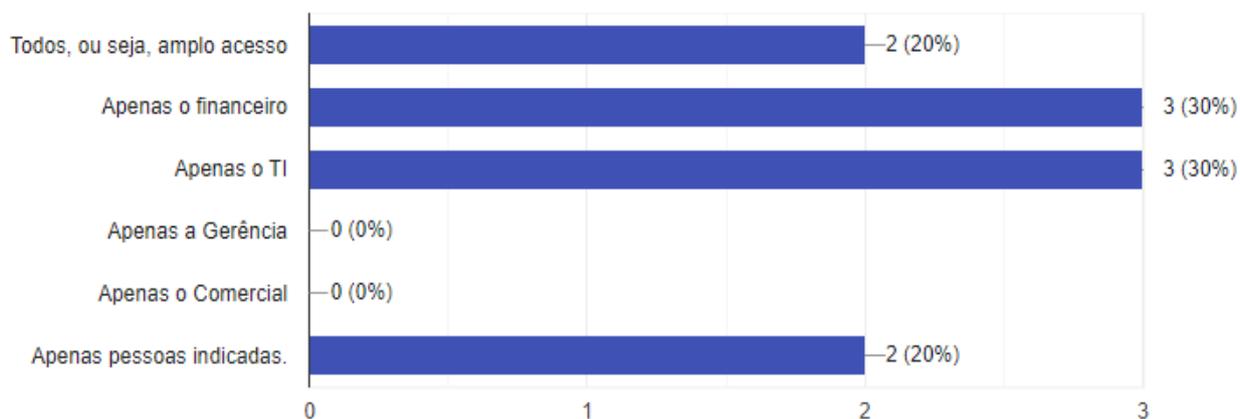
não
Não
Não.
nenhum
Nao
NÃO
No dispositivo local de armazenamento (disco rígido)
Documentos em PDF , guardados em pasta no notebook

Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

Na sétima questão foi questionado quais setores da empresa possuíam acesso aos dados pessoais coletados, e, as alternativas “apenas o setor financeiro” e “apenas o setor de T.I.” obtiveram,

cada uma, 30% do resultado, enquanto as alternativas “todos, ou seja, amplo acesso” e “apenas pessoas indicadas” tiveram 20% das respostas, cada uma, conforme Gráfico 5.

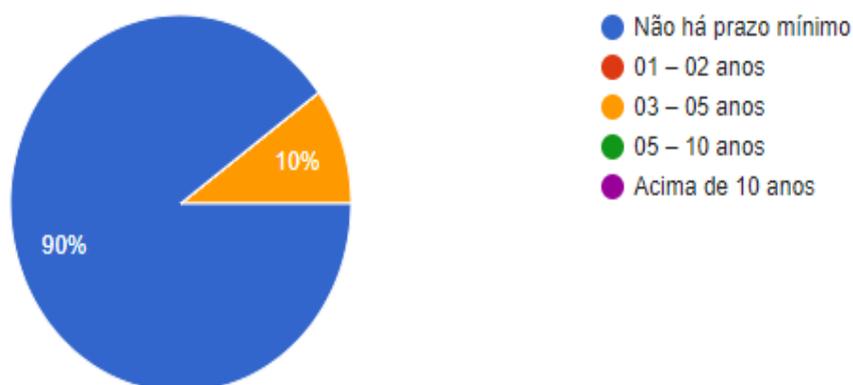
Gráfico 5 - Acesso aos dados pessoais



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A questão oito indaga aos respondentes se há um prazo mínimo para a conservação dos dados pessoais coletados pela empresa, independente do setor, e, como disposto no Gráfico 6, 90% deles responderam que não há prazo mínimo e apenas 10% informaram que os dados permanecem na empresa entre 3 e 5 anos.

Gráfico 6 - Conservação dos dados

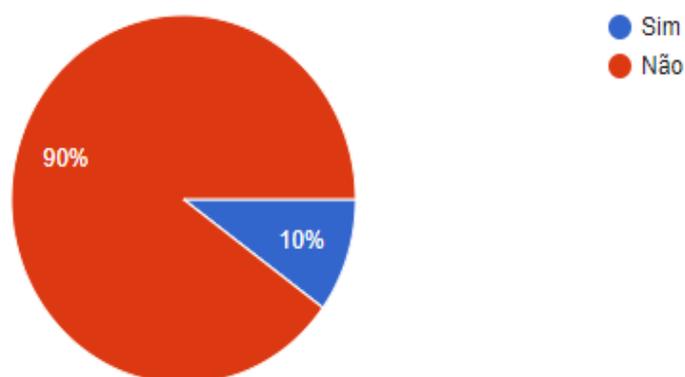


Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A nona questão trata acerca do compartilhamento de dados pessoais coletados pela referida empresa com outras pessoas físicas ou jurídicas, se há ou não este compartilhamento. E, como

demonstrado pelo Gráfico 7, apenas 10% dos respondentes afirmaram que sim, há compartilhamento de dados pessoais com pessoas externas à empresa, enquanto 90% responderam que não há.

Gráfico 7 - Compartilhamento de dados



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

A décima e última questão utiliza a questão anterior como base e questiona aos 10% que responderam que há compartilhamento de dados pessoais com agentes externos à organização quais são as empresas e/ou pessoas que recebem dados pessoais compartilhados pela referida empresa. O único(a) respondente desta questão informou que há compartilhamento com o escritório responsável pela contabilidade da empresa em questão.

A partir das respostas obtidas através do questionário, foi possível iniciar a segunda atividade do processo, que é identificar os dados pessoais tratados pelo objeto de pesquisa e dividi-los em duas categorias com descrições individuais. A primeira categoria é o tratamento de dados pessoais dos clientes, abrangidos em duas classificações:

- Informações de identificação pessoal: Nome, endereço residencial, estado civil e telefone;
- Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG do cliente.

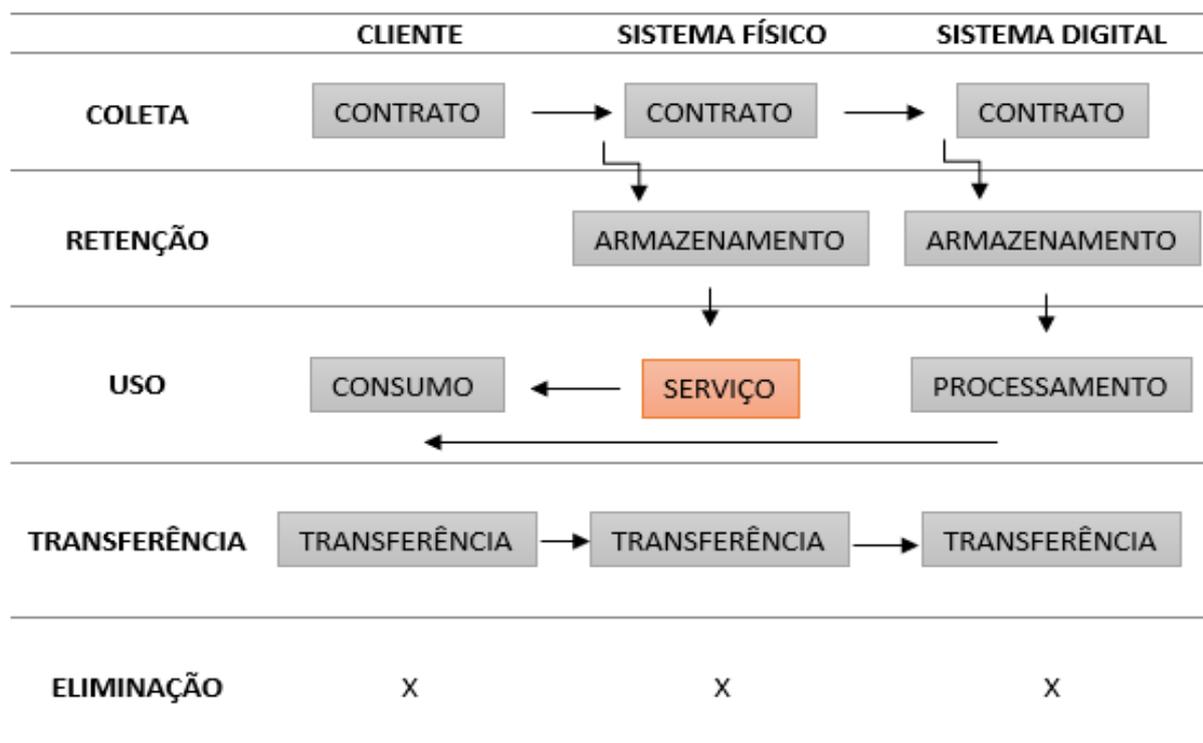
A segunda categoria se trata do tratamento dos dados dos colaboradores da empresa estudada, abrangidos nas seguintes classificações:

- Informações de identificação pessoal: Nome, endereço residencial, estado civil e telefone;

- Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG do cliente;
- Dados da Seguridade Social e Trabalhista: PIS, PASEP, Seguro desemprego, Programa de Assistência Social e vínculos trabalhistas;
- Dados relacionados à saúde: exames ASO.

A terceira atividade do 2º ato compreende a construção dos fluxogramas dos dados pessoais. Novamente, pelo fato de a empresa realizar tratamento de dados pessoais em duas categorias, clientes e colaboradores, foi necessário que a empresa de consultoria criasse um fluxograma para cada uma delas. O primeiro deles foi referente à categoria dos clientes. Nesta, os dados pessoais são coletados mediante assinatura contratual, sendo o próprio titular de dados a fonte. Os dados são, automaticamente, transferidos e armazenados nas instalações digitais do sistema da empresa e, também no acervo de documentos, no setor pessoal/financeiro. Esse fluxo de tratamento de dados é demonstrado na Figura 4.

Figura 4 - Fluxo de Tratamento de Dados Pessoais dos Clientes



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

Legenda figura fluxo de dados:

CONTRATO: Documento de prestação de serviço assinado.

SISTEMA FÍSICO – Contrato impresso físico.

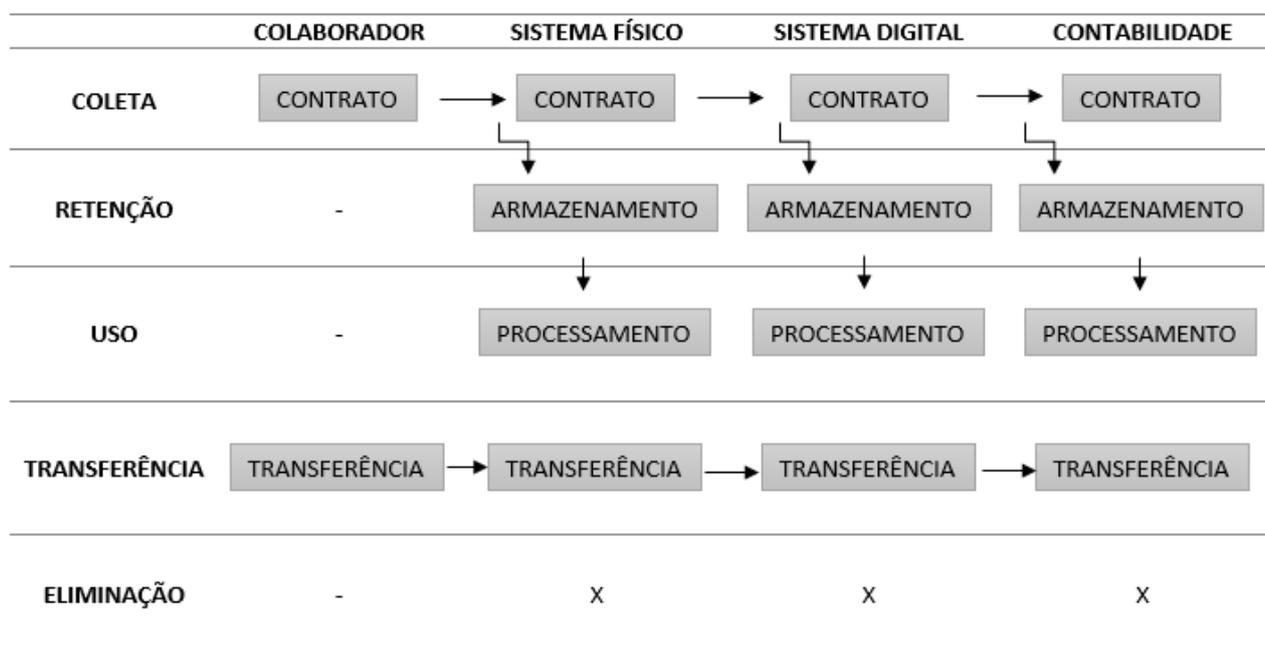
SISTEMA DIGITAL – Contrato no formato digital.

CONTABILIDADE – Empresa contratada para ser responsável pela contabilidade da empresa estudada.

Após o serviço prestado, o contrato não prevê a eliminação total de dados dos clientes dos sistemas digital e físico, logo, serão mantidos armazenados durante a duração do contrato firmado entre a empresa e o cliente e por até uma quantidade razoável de tempo para fins de possíveis solicitações judiciais. Este período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção.

O segundo fluxograma é referente ao fluxo de dados observado na categoria dos colaboradores da empresa estudada. Nesta, os dados pessoais são coletados mediante contratação. Os dados são automaticamente transferidos e armazenados nas instalações digitais do sistema da empresa estudada e, também no acervo de documentos da empresa, no setor pessoal/financeiro. A fonte de dados nesta categoria é o próprio colaborador mediante apresentação de documentos (originais e cópias) e assinatura de contrato. Esse fluxo de tratamento de dados é demonstrado pela Figura 5.

Figura 5 - Fluxo de Tratamento de Dados Pessoais dos Colaboradores



Fonte: Relatório de Impacto à Proteção a Dados Pessoais (2021).

Legenda figura fluxo de dados:

CONTRATO: Documento de contratação assinado.

SISTEMA FÍSICO – Contrato impresso físico.

SISTEMA DIGITAL – Contrato no formato digital.

CONTABILIDADE – Empresa contratada para ser responsável pela contabilidade da empresa estudada.

Quadro 7 - RIPD

SEÇÃO	RESPOSTA
Identificar os agentes de tratamento de dados	- Controlador: empresa de tecnologia estudada; - Operador: colaboradores da empresa de tecnologia estudada; - Encarregado de Dados: não há.
Identificar a necessidade de elaborar o relatório	A empresa de tecnologia da informação estudada realizará tratamento de dados pessoais e dados pessoais sensíveis, por isto, faz-se necessário a elaboração do RIPD.
Dados pessoais dos clientes	Informações de identificação pessoal: Nome, endereço residencial, estado civil e telefone; Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG do cliente.
Dados pessoais dos colaboradores	Informações de identificação pessoal: Nome, endereço residencial, estado civil e telefone; Informações de identificação atribuídas por instituições governamentais: CPF, RG e órgão expedidor do RG do cliente; Dados da Seguridade Social e Trabalhista: PIS, PASEP, Seguro desemprego, Programa de Assistência Social e vínculos trabalhistas; Dados relacionados à saúde: exames ASO.
Identificar partes interessadas consultadas	- Colaboradores de todos os setores - Consultoria jurídica especializada contratada - Gerentes da empresa estudada - Empresa de consultoria especializada em LGPD
Descrever necessidade e proporcionalidade	A necessidade de elaboração do RIPD, no caso da empresa estudada, está fundamentada na hipótese legal para tratamento de dados pessoais é o art. 7º, V da LGPD: “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”. E para isto, a empresa estudada fez a contratação dos serviços de adequação à LGPD e de Encarregado de Dados de uma empresa especializada. Para assegurar os direitos dos titulares de dados, a empresa estudada disponibilizou e-mail e telefone como meios de contato para que os titulares dos dados pessoais possam demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações.
Identificar e avaliar os riscos	Descrição no Quadro 5
Identificar medidas para tratar os riscos	Descrição no Quadro 6
Aprovar o relatório	A responsabilidade da aprovação da execução das medidas descritas para cada risco identificado é da empresa estudada, que leva em consideração o nível do risco identificado e a possibilidade de execução individual de cada uma das medidas. Neste caso, a empresa estudada aprovou a execução imediata de todas medidas propostas e, ao final, tornou-se completamente adequada à Lei Geral de Proteção de Dados Pessoais.
Manter revisão	A empresa especializada contratada pela empresa de tecnologia estudada, na função de Encarregado de Dados Pessoais, tem a responsabilidade de manter o RIPD atualizado após revisões programadas do andamento dos processos organizacionais após a adequação. Bem como, de manter a empresa estudada atualizada em relação a mudanças ou novas solicitações da legislação vigente. Até o presente momento, ocorreram duas reuniões de alinhamento entre a empresa estudada e a empresa de consultoria especializada, que serviram para acompanhar e atestar a manutenção das boas práticas de <i>compliance</i> em LGPD.

Fonte: Relatório de Impacto à Proteção aos Dados Pessoais (2021)

Após a construção dos fluxogramas, iniciou-se a quarta e última etapa deste processo: construção do Relatório de Impacto à Proteção aos Dados Pessoais (RIPD). Para nortear as atividades

a serem desenvolvidas em cada prevista para construir um RIPD, foi utilizado o modelo proposto pelo Ministério da Economia (BRASIL, 2020), disponível na seção de “Demais guias operacionais do Departamento de Privacidade e Segurança da Informação”, o que orienta a elaboração de documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação. Os Quadros 7, 8 e 9 expõem os resultados do RIPD construído pela empresa de consultoria contratada acerca da empresa de tecnologia estudada.

Quadro 8 - Identificação e Nível de Riscos

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Coleção excessiva.	10	15	150
R02	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R03	Informação insuficiente sobre a finalidade do tratamento.	15	15	225
R04	Perda.	15	15	225
R05	Retenção prolongada de dados pessoais sem necessidade.	15	15	225
R06	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R07	Inexistência de uma Política de Privacidade de Dados no site.	15	15	225
R08	Inexistência de cláusulas contratuais no que se refere à adequação da empresa à LGPD.	15	15	225

Fonte: Relatório de Impacto à Proteção de Dados Pessoais (2021).

Quadro 9 - Medidas de Tratamento de Riscos

Risco	Medida(s)	Efeito sobre o Risco ¹	Risco Residual ²			Medida(s) ³ Aprovada(s)
			P	I	Nível (P x I)	
R01 – Coleção excessiva	Fazer lista de dados pessoais mínimos necessários para o formulário.	Evitar	0	10	0	APROVADA
R02 – Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	Manter os dados bem protegidos e restringir ao máximo o acesso de pessoas a eles.	Reduzir	5	10	50	APROVADA
R03 – Informação insuficiente sobre a finalidade do tratamento	Deixar todas as finalidades do tratamento dos dados pessoais bem explícitas no contrato firmado.	Evitar	0	10	0	APROVADA
R04 – Perda.	Manter o backup sempre atualizado.	Reduzir	10	10	100	APROVADA
R05 - Retenção prolongada de dados pessoais sem necessidade.	Controle e fiscalização dos processos ao longo do tempo.	Reduzir	5	10	50	APROVADA
R06 - Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	Solicitar em todos os novos contratos a autorização do tratamento dos dados pessoais mediante apresentação de finalidade e, entrar em contato com os clientes de contratos já firmados para solicitar autorização do tratamento de todos os dados pessoais já retidos, também mediante apresentação de finalidade.	Reduzir	5	10	50	APROVADA

R07 - Inexistência de uma Política de Privacidade de Dados no site.	Criação de uma Política de Privacidade de Dados e disponibilizá-la no site informando a utilização de cookies e solicitando a autorização para o tratamento, bem como, disponibilizar contato via e-mail e telefone do encarregado de dados pessoais da empresa.	Evitar	0	10	0	APROVADA
R08 - Inexistência de cláusulas contratuais no que se refere à adequação da empresa à LGPD.	Implementação de cláusula contratual em todos os contratos de prestação de serviços da empresa.	Reduzir	5	15	75	APROVADA

Fonte: Relatório de Impacto à Proteção aos Dados Pessoais (2021).

4.1.4. 3º Ato

O terceiro ato corresponde à Reunião de Alinhamento ao *Compliance*, cujo objetivo é que a empresa de consultoria contratada apresente o RIPD e, com ele, todas as medidas propostas para a adequação geral à LGPD. A responsabilidade da aprovação da execução das medidas descritas para cada risco identificado é da empresa estudada, que leva em consideração o nível do risco identificado e a possibilidade de execução individual de cada uma das medidas. Neste caso, a empresa estudada aprovou a execução imediata de todas medidas propostas e, após essa reunião, ocorrida no dia 25 de outubro de 2021, foram instauradas todas as medidas propostas pela empresa de consultoria.

4.1.5. 4º Ato

Nos 45 dias seguintes à Reunião de Alinhamento ao *Compliance*, do dia 26 de outubro ao dia 10 de dezembro de 2021, foram implementadas todas as medidas propostas no Relatório de Impacto à Proteção de Dados Pessoais que foram identificadas na seção “Medidas de Tratamento de Riscos”.

4.1.6 5º Ato

No dia 15 de dezembro de 2021, ocorreu o quinto e último ato, com uma reunião para discutir os resultados e fazer a escolha do Encarregado de Dados. A empresa de consultoria responsável pela adequação apresentou uma proposta para assumir a atividade de Encarregado de Dados, tornando-se responsável pela intermediação entre a Autoridade Nacional de Proteção de Dados (ANPD), os titulares de dados e a empresa estudada, conforme os postulados legais.

5. ANÁLISE DO PROCESSO

Este capítulo tem o objetivo de atender o terceiro e último objetivo específico desta pesquisa, que é submeter os resultados a uma ferramenta de diagnóstico de nível de maturidade à LGPD. Para essa finalidade, foi utilizada a ferramenta “Diagnóstico e Índice de Maturidade de Privacidade para adequação à Lei Geral de Proteção de Dados – LGPD” disponibilizada no sítio do governo federal brasileiro através do Ministério da Gestão e Inovação em Serviços Públicos.

O procedimento é o preenchimento de um formulário eletrônico realizado pela autora da pesquisa com informações referentes às análises documentais de processos e resultados alcançados na adequação, trazendo subsídio para formalização e cálculo de um índice de acordo com o Quadro 10:

Quadro 10 - Escala de classificação de nível de adequação

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Fonte: BRASIL, 2022.

Para subsidiar o correto preenchimento das questões do formulário de diagnóstico, cada questão formulada apresenta dispõe de uma referência baseada na LGPD e/ou em normas e pode ser respondida com as opções, as quais são dispostas no Quadro 11.

Quadro 11 - Definições por escala de nível de adoção

Nível de adoção aplicada	Definição	Exemplos
Não adota	A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la.	A organização sabe da necessidade de adotar a prática de elaborar “uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais”, mas não tomou ainda qualquer decisão no sentido de formalizar sua adoção.
Iniciou plano para adotar	A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares etc).	Para adotar a prática de elaborar “uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais”, a organização elaborou plano de ação formal que estabelece as atividades, cronograma e responsáveis relativos à elaboração da política.
Adota parcialmente	A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento	A prática apresentada é “o órgão já realizou um inventário dos serviços que tratam dados pessoais”. A organização, por sua vez, executa o processo de inventários dos dados pessoais

	realizado; ou a prática não é executada uniformemente em toda a organização.	apenas para alguns serviços, ou o processo não é executado por todas as suas unidades.
Adota integralmente	A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.	Para atender à prática “o órgão já realizou um inventário dos serviços que tratam dados pessoais”, a organização possui e executa um processo de inventário dos serviços que tratam dados pessoais utilizados em todas as suas unidades, ainda que o processo não esteja formalmente instituído como norma de cumprimento obrigatório.

Fonte: BRASIL, 2022.

Por se tratar de uma ferramenta para fins de administração pública é solicitada a identificação do órgão ou autarquia federal. Neste caso, foi utilizada a opção “OUTROS” no campo do órgão, seguido do CNPJ da empresa de tecnologia da informação. Nos campos de e-mail e nome de contato foi cadastrado o da autora deste trabalho. No Quadro 12 estão dispostas as respostas apontadas para os itens solicitados na ferramenta de diagnóstico.

Quadro 12 - Respostas inseridas para a validação da adequação

Item	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
Governança				
1 - As partes envolvidas com a implementação da LGPD realizaram a leitura do Guia de Boas Práticas sobre a Lei Geral de Proteção de Dados (LGPD) produzido pela Secretaria de Governo Digital?				X
2 - O órgão já realizou um planejamento do seu Programa Institucional de Privacidade de Dados?				X
3 - O órgão desenvolveu um plano de comunicação interno do Programa Institucional de Privacidade de Dados?				X
4 - O órgão já realizou a indicação de um encarregado com conhecimento e experiência suficientes e autonomia para implementar a LGPD?				X
5 - O órgão disponibilizou para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?				X
6 - O órgão designou os líderes responsáveis por cada frente de atuação no tratamento dos dados?				X
7 - Foram definidos indicadores que serão utilizados para medir os resultados do Programa Institucional de Privacidade de Dados?	X			
8 - O órgão elaborou Relatório de Impacto à Privacidade de Dados Pessoais - RIPD?				X
9 - O RIPD foi elaborado com base nas orientações da seção 2.5 e Anexo I do Guia de Boas Práticas LGPD?				X
10 - A(s) área(s) envolvidas com tratamento de dados participou(aram) de algum treinamento relacionado com o tema de proteção de dados pessoais?			X	
Conformidade legal e respeito aos princípios				

11 - O órgão, dentro dos limites de suas competências legais, implementou ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais dos cidadãos e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada?				X
12 - O órgão realizou um mapeamento entre os dados processados e a competência legal/finalidade para a qual eles são necessários?				X
13 - O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD estão sendo respeitados durante o desenvolvimento de serviços que tratarão dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?			X	
14 - Os princípios da LGPD são aplicados a todo tratamento de dados pessoais realizados pelo órgão, tanto para clientes dos serviços públicos fornecidos quanto servidores, funcionários e/ou colaboradores da instituição?				X
15 - O órgão conscientizou a(s) área(s) envolvida(s) com tratamento de dados pessoais que a administração pública pode efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas para entrega de serviços públicos e que nesses casos não precisará colher o consentimento do titular dos dados?				X
16 - O órgão, ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas, dá publicidade sobre a finalidade e a forma como o dado será tratado?				X
17 - O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado?				X
Transparência e direitos do titular				
18 - A identidade e as informações de contato do encarregado foram divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?				X
19 - O órgão comunica internamente os objetivos do Programa Institucional de Privacidade de Dados?			X	
20 - O órgão elaborou uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados e revisou as Políticas de Privacidade já existentes?				X
21 - As Políticas de Privacidade dos serviços são elaboradas em linguagem simples e acessível?				X
Rastreabilidade				
22 - O órgão já realizou um inventário dos serviços que tratam dados pessoais?			X	
23 - O órgão já realizou uma classificação dos dados tratados entre dados pessoais e dados pessoais sensíveis?				X
24 - O órgão mantém rastreabilidade dos dados do titular seja em formato eletrônico ou físico (papel)?				X
Adequação de contratos e de relações com parceiros				

25 - O órgão já realizou uma adequação dos instrumentos convocatórios que estão sendo elaborados?				X
26 - O órgão já realizou uma revisão dos contratos em vigência para adequá-los à Lei Geral de Proteção de Dados?				X
Segurança da Informação				X
27 - O órgão efetivamente implementou os controles de segurança para os riscos identificados no Relatório de Impacto à Proteção dos Dados Pessoais?				X
28 - O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?				X
29 - O órgão gera evidências para comprovar que tomou medidas de segurança para proteger os dados pessoais contra ameaças externas e internas?				X
30 - Medidas de segurança são planejadas desde a fase de concepção do produto ou do serviço até a sua execução (Security by Design)?				X
Violações de dados				
31 - O órgão estabeleceu um processo de comunicação das possíveis violações de dados pessoais?				X
32 - O órgão realiza uma gestão de incidentes para tratar possíveis violações dos dados de forma efetiva?				X
33 - O órgão fornece um canal para recebimento de denúncias e de alertas de ocorrências de irregularidades, como denúncias de possíveis vazamento de dados e falhas de segurança?				X

Fonte: Brasil, 2022.

Após o preenchimento das perguntas solicitadas na ferramenta de diagnóstico é possível observar no Quadro 13 a avaliação do nível de adequação da empresa, com índices que variam entre 0 e 1. Os resultados do objeto de estudo apontaram as dimensões Governança, Conformidade Legal e Respeito aos Princípios, Transparência e Direitos do Titular, e Rastreabilidade com índices 0,89, 0,92, 0,89 e 0,83, respectivamente, e as dimensões Adequação de Contratos e de Relações com Parceiros, Segurança da Informação e Violações de Dados com índice 1, nota máxima. A média aritmética dos índices individuais resulta no índice geral, chamado Índice da Adequação à LGPD, o qual obteve a nota 0,93 e foi classificado como “Aprimorado”.

Quadro 13 - Avaliação do nível de adequação

Dimensões	Índice	Nível
1 - Dimensão Governança	0.89	
2 - Dimensão Conformidade legal e respeito aos princípios	0.92	
3 - Dimensão Transparência e direitos do titular	0.89	
4 - Dimensão Rastreabilidade	0.83	
5 - Dimensão Adequação de contratos e de relações com parceiros	1	
6 - Dimensão Segurança da Informação	1	
7 - Dimensão Violações de Dados	1	
Índice da Adequação à LGPD	0.93	Aprimorado

Fonte: Brasil, 2022.

6. SÍNTESE DOS PRINCIPAIS RESULTADOS

Com base na análise do Diagnóstico de maturidade de privacidade para adequação à LGPD, o Quadro 14 faz uma síntese dos resultados obtidos em relação à adequação à LGPD da empresa foco deste estudo. É possível observar no referido quadro que há uma relação entre as dimensões avaliadas no diagnóstico e as ações de adequação à LGPD realizadas, e através desta relação, pode-se constatar a eficiência do modelo de adequação à LGPD adotado pela empresa estudada, pois todas as Dimensões avaliadas foram atendidas por ações de adequação e obtiveram índices satisfatórios. Os resultados alcançados nas Dimensões “Governança”, “Conformidade Legal e Respeito aos Princípios” e “Adequação de Contratos e Relações com Parceiros” corroboram com os estudos de Sá (2019), quando o autor diz que a LGPD promove mudanças na rotina empresarial para proteger os direitos fundamentais de liberdade e privacidade dos titulares de dados. Já nas Dimensões “Rastreabilidade”, “Segurança da Informação” e “Violação de Dados”, os resultados alcançados atestam a eficiência das medidas protetivas da Segurança da Informação propostas nos estudos de Semôla (2014), quando o autor discorre sobre confidencialidade, integridade e disponibilidade, os três elementos que compõe a tríade da Segurança da Informação.

Quadro 14 - Relação entre Dimensões e Ações de Adequação à LGPD

DIMENSÕES DO DIAGNÓSTICO DE MATURIDADE DE PRIVACIDADE PARA ADEQUAÇÃO À LGPD	QUESTÕES DO DIAGNÓSTICO DE MATURIDADE DE PRIVACIDADE PARA ADEQUAÇÃO À LGPD	ATOS DO PROCESSO DE ADEQUAÇÃO À LGPD	AÇÕES REALIZADAS PARA ADEQUAÇÃO À LGPD
GOVERNANÇA	1ª a 10ª	1º, 2º e 3º Ato	Comunicados institucionais, Mapeamento de Dados e Reuniões de Compliance.
CONFORMIDADE LEGAL E RESPEITO AOS PRINCÍPIOS	11ª a 17ª	1º, 2º, 3º, 4º e 5º Ato	Todas as ações.
TRANSPARÊNCIA E DIREITOS DO TITULAR	18ª a 21ª	4º e 5º Ato	Solicitação de dados mínimos para a finalidade estabelecida e solicitação de autorização de tratamento a antigos e novos clientes.
RASTREABILIDADE	22ª a 24ª	2º Ato	Identificação e classificação de dados pessoais e dados pessoais sensíveis e Documentação física e digital de todos os dados pessoais tratados.

ADEQUAÇÃO DE CONTRATOS E RELAÇÕES COM PARCEIROS	25ª e 26ª	4º Ato	Implementação de cláusula contratual sobre as responsabilidades inerentes a ambas as partes.
SEGURANÇA DA INFORMAÇÃO	27ª a 30ª	4º e 5º Ato	Atualização de backup e criação de Política de Privacidade de Dados.
VIOLAÇÕES DE DADOS	31ª a 33ª	5º Ato	Contratação de uma empresa especializada para atuar como Encarregado de Dados.

Fonte: Elaborado pela autora com base no Diagnóstico de Maturidade de Privacidade para Adequação à LGPD.

Portanto, de acordo com a Lei nº 13.709/2018 e do Decreto nº 40.006 com a Política Estadual de Proteção de Dados Pessoais é correto dizer que a empresa objeto de estudo da presente pesquisa, após a realização de todos os atos do método avaliado e durante o período de duração da pesquisa, encontra-se em plena conformidade à Lei Geral de Proteção de Dados Pessoais.

7. CONCLUSÃO

São incontestáveis os benefícios advindos da transformação digital, seja nas relações sociais e/ou comerciais. Todavia, o uso ampliado e indiscriminado de dados pessoais, a rigor, tem demonstrado ser muito mais voltado para o bem do capital, além da influência que se é exercida nas pessoas sem o seu prévio conhecimento e/ou consentimento. Em síntese, há uma manipulação do indivíduo.

Uma regulamentação que possa exercer uma influência direta e contundente deve vir dos governos. A Lei Geral de Proteção de Dados Pessoais vem então exercer o seu papel de tal finalidade aqui no Brasil.

Na realização deste estudo de caso, percebeu-se que a análise dos processos é uma etapa relevante em razão de trazer segurança para a empresa que está em seus passos finais ou já concluídos de adequação.

A ferramenta de diagnóstico utilizado apresentou ser um instrumento norteador e ampliado da LGPD. Sendo esta disponibilizado pelo Governo Federal, a quem também tem a função de fiscalização através da Autoridade Nacional de Proteção de Dados (ANPD), propicia uma maior seguridade à empresa.

O objeto de estudo desta pesquisa apresentou um nível aprimorado de adequação, o que reflete que o modelo adotado pela empresa de consultoria alcançou quase que em sua totalidade os requisitos legais.

A experiência vivenciada permitiu uma percepção sobre os desafios que permeiam a adequação, principalmente por ser um assunto de incipiente tanto de conhecimento quanto de experiência de implantação.

REFERÊNCIAS

- ABNT ISO 27002. (2013). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR/ISO/IEC 27002:2013** tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação.
- BRASIL. **Relatório de Impacto a Proteção de Dados Pessoais**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx. 2020.
- CASTELLS, Manuel. **A Galáxia da Internet**. Rio de Janeiro: Zahar, 2003.
- GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. Editora Atlas SA, 2008.
- GIL, Carlos, A. **Como Elaborar Projetos de Pesquisa**. 6ª edição. São Paulo, Atlas, 2017.
- VOSS, C.; TSIKRIKTSIS, N.; FROHLICH, M. **Case research in operations management**. *International Journal Of Operations & Production Management*, v. 22, n. 2, p. 195-219, 2002.
- GOMES. **Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD: Uma breve análise da sua definição e papel na LGPD**. Maria Cecília Oliveira Gomes. Revista da AASP, n. 144. 2019.
- GUMMESSON, E. **Case study research and network theory: birds of a feather**. *Qualitative Research in Organizations and Management. An International Journal*, v. 2, n. 3, p. 226-248, 2007.
- GUIA. **Guia De Boas Práticas Lei Geral de Proteção de Dados (LGPD)**. [S. l.: s. n.], 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia_lgpd.pdf.
- HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.
- IRAMINA, Aline. **RGPD v. LGPD: Adoção Estratégica Da Abordagem Responsiva Na Elaboração Da Lei Geral De Proteção De Dados Do Brasil e Do Regulamento Geral De Proteção De Dados Da União Europeia**. *Revista de Direito, Estado e Telecomunicações*, v. 12, n. 2, 2020.
- LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação**. 11. ed. Rio de Janeiro: Pearson, 2014.
- LIMA, Victor Henrique Pereira. **LGPD análise dos impactos da implementação em ambientes corporativos: Estudo de caso**. Pontifícia Universidade Católica de Goiás - Escola de Ciências Exatas e da Computação. Graduação em Ciência Da Computação. 2020.
- LUNA, B. F. **Seqüência Básica na Elaboração de Protocolos de Pesquisa**. *Revista Arq. Bras. Cardiol.*, v. 71, n. 6, p. 735-740, 1998.

MACIEL, Rafael Fernandes. **Manual prático sobre a Lei geral de proteção de dados pessoais (Lei nº 13.709/2018)**. 1ª ed. Goiânia: RM Digital Education. 2019. E-book. Acesso restrito via Minha Biblioteca.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento**. 11 ed. São Paulo: Hucitec, 2008

OLIVEIRA, Izabel Vitorino. **A quinta revolução da inteligência artificial**.

PANEK, Lin Cristina. **Lei geral de proteção de dados Nº 13.709/2018: Uma análise dos principais aspectos e do conceito de privacidade na sociedade informacional**. Universidade Federal do Paraná. 2019. EM 11º CONGRESSO DE INICIAÇÃO CIENTÍFICA E TECNOLÓGICA DO IFSP. Disponível em:
<http://ocs.ifsp.edu.br/index.php/conict/xiconict/paper/viewPaper/7259>. 2020

PASQUINI, Nilton César. **Revoluções industriais: uma abordagem conceitual**. Revista Tecnológica da Fatec Americana. v. 8 n. 01 (2020). Disponível em:
<https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/235>. 2020.

RAPÔSO CFL, et al. **LGPD-Lei geral de proteção de dados pessoais em tecnologia da informação**. Rev. Revisão Sistemática. 2019; 4(19): 14-18.

REZENDE, Dênis Alcides. ABREU, Aline França de. **Tecnologia da Informação: aplicada aos sistemas de informação empresariais**. 9ª Ed. São Paulo: Altas, 2013.

ROGERS, D. L. **The Digital Transformation Playbook: Rethink your Business for the Digital Age**. New York: Columbia University Press, 2016

Schramm, W. (1971). **Notes on case studies of instructional media projects**. Working paper, the Academy For Educational Development, Washington, DC.

SERGIPE. **Decreto Nº 40.006, de 5 de outubro de 2021**. Diário Oficial do Estado de Sergipe - Nº 28.766 Aracaju/Sergipe. Disponível em:

https://s3-sa-east-1.amazonaws.com/diariospdf/_2021/10/06/diario_executivo_estado_sergipe/4233/a426285e740d64b23ab6eae2703ea130/diarioOficial.pdf.

SINGH, A., & HESS, T. How Chief Digital Officers Promote the Digital Transformation of their Companies. MIS Quarterly Executive, 16(1), 1–17, 2017.

UNO. A transformação digital. Desenvolvendo Ideias na LLORENTE & CUENCA. 2016. Disponível em: <<http://www.revista-com.br/wp-content/uploads/2>> Acesso em 03/09/2019.

YIN, Robert K. **Estudo de Caso: Planejamento e Métodos**. 5ª Edição. Porto Alegre: Bookman, 2015

YIN, R. K. **Pesquisa qualitativa do início ao fim**. Porto Alegre: Penso, 2016. Tradução: Daniel Bueno.

ZANELLI, J. C. **Pesquisa qualitativa em estudos da gestão de pessoas.** Estudos da Psicologia, n. 7, p. 79-88, 2002.