



**UNIVERSIDADE FEDERAL DO CEARÁ**  
**CAMPUS DE QUIXADÁ**  
**CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES**

**DAVI OLIVEIRA LOPES**

**ANÁLISE DA CONFORMIDADE DOS REQUISITOS DE PRIVACIDADE DAS  
STARTUPS INCUBADAS NA UFC, DE ACORDO COM A LGPD**

**QUIXADÁ**

**2022**

DAVI OLIVEIRA LOPES

ANÁLISE DA CONFORMIDADE DOS REQUISITOS DE PRIVACIDADE DAS STARTUPS  
INCUBADAS NA UFC, DE ACORDO COM A LGPD

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. Michel Sales Bonfim

Coorientadora: Ma. Maria Simone Mendes Nunes

QUIXADÁ

2022

Dados Internacionais de Catalogação na Publicação  
Universidade Federal do Ceará  
Biblioteca Universitária  
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

L851a Lopes, Davi Oliveira.  
Análise da conformidade dos requisitos de privacidade das Startups incubadas na UFC, de acordo com a LGPD / Davi Oliveira Lopes. – 2022.  
64 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2022.

Orientação: Prof. Dr. Michel Sales Bonfim.

Coorientação: Profa. Ma. Maria Simone Mendes Nunes.

1. Privacidade. 2. Lei Geral de Proteção de Dados Pessoais. 3. Conformidade. I. Título.

CDD 004.6

---

DAVI OLIVEIRA LOPES

ANÁLISE DA CONFORMIDADE DOS REQUISITOS DE PRIVACIDADE DAS STARTUPS  
INCUBADAS NA UFC, DE ACORDO COM A LGPD

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Aprovada em: \_\_\_\_/\_\_\_\_/\_\_\_\_

BANCA EXAMINADORA

---

Prof. Dr. Michel Sales Bonfim (Orientador)  
Universidade Federal do Ceará (UFC)

---

Ma. Maria Simone Mendes Nunes (Coorientadora)  
Universidade Federal do Ceará (UFC)

---

Prof. Ma. Roberta Dutra de Andrade  
Universidade Federal do Ceará (UFC)

---

Prof. Me. Roberto Cabral Rabêlo Filho  
Universidade Federal do Ceará (UFC)

Aos meus pais, por nunca terem medido esforços para me proporcionar um ensino de qualidade durante todo o meu período escolar.

## **AGRADECIMENTOS**

Em primeiro lugar a Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Ao meu orientador e co-orientadora, que me conduziram para elaborar este trabalho sempre com paciência, dedicação e disponibilidade para compartilhar todos os seus vastos conhecimentos.

Aos meus pais e irmã, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

A minha noiva Clara, pelo companheirismo, pela cumplicidade e pelo apoio em todos os momentos delicados da minha vida, você estava lá para me auxiliar e mostrar como agir em meio a tantas diversidades, obrigado por tanto.

Aos amigos que fiz no decorrer desta caminhada e ao meu grupo "Lembre-se BUCUM = 136" que foi peça chave para a resolução de diversas adversidades e contribuiu também para os momentos de descontração durante todo o período do curso, obrigado Alan Cristian, Jamerson, Rafael e Rafaely.

Ao meu amigo Randel, por ter me ajudado inúmeras vezes e sempre disposto a ajudar mesmo em meio a tantos problemas decorrentes dos últimos anos, não mediu esforços para me auxiliar. Obrigado demais!

Obrigado a todos que contribuíram direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado.

“Se você tivesse acreditado na minha brincadeira de dizer verdades, teria ouvido verdades que teimo em dizer brincando.”

(Fred Maia)

## RESUMO

Diante de vários casos de vazamento de dados pessoais nos últimos anos, surgiu a necessidade de elaborar medidas de seguranças para prevenir que informações pessoais dos usuários fossem vazadas e acarretassem prejuízos à integridade dos indivíduos. Por conta disso, foi elaborada a Lei Geral de Proteção de Dados (LGPD), com o intuito de regularizar e fiscalizar as empresas para garantir a proteção dos dados dos usuários em todos os cenários em que os mesmos forem utilizados. Atentando-se a essa problemática, este trabalho tem como objetivo analisar como as *startups* incubadas pela UFC, encontram-se em relação a conformidade dos seus requisitos de privacidade perante à LGPD. Diante disso, foi realizado um estudo da lei e dos requisitos de privacidade, sendo assim possível produzir perguntas que nortearam tanto a LGPD, como os conceitos dos requisitos de privacidade. Dessa forma, as perguntas foram utilizadas como roteiro durante as entrevistas, na etapa de coleta de dados com as *startups* e posteriormente como unidades de contexto, para que fosse possível utilizar o método de análise de conteúdo na visão de Laurence Bardin. Para auxiliar na instrumentalização da pesquisa foi utilizado o *software Iramuteq*, que auxiliou na elaboração de ilustrações, fornecendo também funcionalidades para agregar ainda mais valia às informações da etapa de interpretações dos dados. Foram apresentados pontos de melhoria podendo auxiliar as *startups* a ficarem o máximo em conformidade com a nova lei. Um resultado observado foi que dentre as sete *startups* elegíveis, cinco atingiram o nível esperado de adaptabilidade para com os requisitos de privacidade de acordo com a LGPD, ou seja, dos quatro requisitos de privacidade, que eram também as quatro categorias de análise, as mesmas atingiram o esperado de três requisitos de privacidade, demonstrando que cumprem e procuram se adequar ainda mais às regras que a LGPD orienta. Espera-se que esse estudo seja uma fonte de informações para conhecimento sobre o assunto e uma forma de incentivo para que as *startups* se adequem aos requisitos de privacidade que norteiam a LGPD.

**Palavras-chave:** Privacidade. Lei Geral de Proteção de Dados Pessoais. Conformidade.

## ABSTRACT

Faced with several cases of personal data leakage in recent years, it is fundamental to develop security measures to prevent users' personal information from being leaked and causing damage to the integrity of individuals. Because of this, the General Law of Data Protection (LGPD) was created to regulate and supervise companies to guarantee the protection of users' data in all scenarios in which they are used. Attentive to this problem, this work aims to analyze how the *startups* incubated by the UFC are related to the compliance of their privacy requirements before the LGPD. A law and privacy' study requirements were carried out, thus producing questions that guided both the LGPD and the concepts of privacy requirements. They were used as a *script* during the interviews, in the data collection stage with the *startups*, and later as context units. It was possible to use the content analysis method in the vision of Laurence Bardin. The *software Iramuteq* was used to help in the instrumentalization of the research. It helped in the elaboration of illustrations, also providing functionalities to add even more value to the information in the data interpretation stage. Points for improvement were presented to help the *startups* be as compliant as possible with the new law. One result observed was that among the seven eligible *startups*, five reached the expected level of adaptability to the privacy requirements according to the LGPD, that is, of the four privacy requirements, which were also the four categories of analysis, they reached the expected level of three privacy requirements, emonstrating that They comply and seek to further adapt to the rules that the LGPD guides. It is hoped that this study will be a source of information on the subject and a form of incentive for *startups* to adapt to the privacy requirements that guide the LGPD.

**Keywords:** Privacy. General Personal Data Protection Law. Compliance.

## LISTA DE FIGURAS

Figura 1 – Fluxograma da Análise de Conteúdo .....	24
Figura 2 – Análise estatística sobre o conteúdo relacionado a <i>conformidade</i> .....	34
Figura 3 – Método de <i>Reinert</i> - Divisão dos vocabulários sobre o requisito da <i>conformidade</i> .....	34
Figura 4 – Método de <i>Reinert</i> - Divisão dos vocabulários em um plano cartesiano.....	35
Figura 5 – Análise estatística sobre o conteúdo relacionado a <i>controle de acesso</i> .....	39
Figura 6 – Análise de similitude - Divisão dos temas extraídos dos dados referentes ao requisito de <i>controle de acesso</i> .....	40
Figura 7 – Método de <i>Reinert</i> - Divisão dos vocabulários para o requisito de <i>verificação</i> .....	45
Figura 8 – Análise de similitude - Divisão dos temas extraídos dos dados referente ao requisito de <i>verificação</i> .....	46
Figura 9 – <i>Word cloud</i> de todas as palavras referentes ao requisito de <i>usabilidade</i> .....	50
Figura 10 – Demarcações da palavra “dado”.....	51
Figura 11 – Análise de similitude - Divisão dos temas extraídos dos dados referente ao requisito de <i>usabilidade</i> .....	51
Figura 12 – <i>Word cloud</i> dos principais obstáculos para implementar a LGPD .....	53
Figura 13 – Relação da quantidade de clientes das <i>startups</i> .....	54
Figura 14 – Carta convite para participação de Entrevista .....	62
Figura 15 – Exemplo de um documento do corpus da pesquisa, transcrito e com o processo de demarcação de pontos relevantes.....	63

## LISTA DE TABELAS

Tabela 1 – Análise comparativa entre trabalhos relacionados e este trabalho .....	22
Tabela 2 – Tabela contendo os motivos e quantas <i>startups</i> foram elegíveis para a pesquisa	27
Tabela 3 – Modelo organizatório das categorias de análise - Unidades de Registro (respostas dos entrevistados) e Unidades de Contexto (descrição do que seria analisado de acordo com os conceitos que nortearam à elaboração das perguntas)	30
Tabela 4 – Tabela de percentual atingido do requisito de <i>conformidade</i> .....	31
Tabela 5 – Tabela de percentual atingido do requisito de <i>controle de acesso</i> .....	36
Tabela 6 – Tabela de percentual atingido do requisito de <i>verificação</i> .....	41
Tabela 7 – Tabela de percentual atingido do requisito de <i>usabilidade</i> .....	47

## LISTA DE ABREVIATURAS E SIGLAS

LGPD	<i>Lei Geral de Proteção de Dados</i>
UFC	<i>Universidade Federal do Ceará</i>
GDPR	<i>General Data Protection Regulation</i>
ANPD	<i>Autoridade Nacional de Proteção de Dados</i>
ABNT	<i>Associação Brasileira de Normas Técnicas</i>
TI	<i>Tecnologia da Informação</i>
TFD	<i>Grounded Theory</i>
LGPD4BP	<i>LGPD for Business Process</i>
UFPE	<i>Universidade Federal de Pernambuco</i>
[S]	<i>Representação de fala de uma Startup</i>
2D	<i>Duas Dimensões</i>
DPO	<i>Data Protection Officer</i>

## SUMÁRIO

1	<b>INTRODUÇÃO</b> .....	14
1.1	<b>Objetivos</b> .....	15
2	<b>REFERENCIAL TEÓRICO</b> .....	16
2.1	<b>Privacidade dos Dados</b> .....	16
2.1.1	<i>Requisitos de Privacidade</i> .....	16
2.2	<b>Lei Geral de Proteção de Dados - LGPD</b> .....	17
2.3	<b>ABNT NBR ISO/IEC 27701</b> .....	19
3	<b>TRABALHOS RELACIONADOS</b> .....	20
3.1	<b>Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso</b> .....	20
3.2	<b>Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais</b> .....	20
3.3	<b>Análise de conformidade de processos de negócios em relação a LGPD</b> .	21
3.4	<b>Análise Comparativa</b> .....	22
4	<b>METODOLOGIA</b> .....	23
4.1	<b>Análise de Conteúdo</b> .....	23
4.2	<i>Software de Análise Iramuteq</i> .....	25
4.3	<b>Instrumento de Coleta de Dados</b> .....	26
4.4	<b>Escolha das startups e coleta dos dados</b> .....	26
4.5	<b>Transcrições das Entrevistas</b> .....	28
4.6	<b>Pré-análise</b> .....	28
4.7	<b>Codificação dos dados</b> .....	29
4.7.1	<i>Síntese sobre a elaboração das perguntas orientadas aos requisitos de privacidade</i> .....	29
4.7.2	<i>Processo de categorização</i> .....	30
5	<b>RESULTADOS</b> .....	31
5.1	<b>Análises dos resultados</b> .....	31
5.1.1	<i>Análise das respostas referente a cada categoria de análise</i> .....	31
5.1.1.1	<i>Conformidade</i> .....	31
5.1.1.1.1	<i>Exemplificação com trechos dos respondentes</i> .....	32

5.1.1.1.2	<i>Análises com o software Iramuteq para o requisito de conformidade.....</i>	33
5.1.1.2	<i>Controle de acesso.....</i>	36
5.1.1.2.1	<i>Exemplificação com trechos dos respondentes.....</i>	37
5.1.1.2.2	<i>Análises com o software Iramuteq para o requisito de controle de acesso .....</i>	38
5.1.1.3	<i>Verificação .....</i>	40
5.1.1.3.1	<i>Exemplificação com trechos dos respondentes.....</i>	42
5.1.1.3.2	<i>Análises com o software Iramuteq para o requisito de verificação .....</i>	44
5.1.1.4	<i>Usabilidade.....</i>	46
5.1.1.4.1	<i>Exemplificação com trechos dos respondentes.....</i>	48
5.1.1.4.2	<i>Análises com o software Iramuteq para o requisito de usabilidade .....</i>	49
5.1.2	<b><i>Obstáculos para a conformidade.....</i></b>	52
5.1.2.1	<i>Word Cloud das principais dificuldades de implementação da LGPD.....</i>	52
5.1.2.2	<i>Relação de quantidade de clientes por startup.....</i>	53
5.1.2.3	<i>Pontos de Melhorias .....</i>	54
6	<b>CONSIDERAÇÕES FINAIS .....</b>	56
	<b>REFERÊNCIAS.....</b>	58
	<b>APÊNDICE A–QUESTIONÁRIO UTILIZADO COMO ROTEIRO DURANTE AS ENTREVISTAS .....</b>	60
	<b>APÊNDICE B–CARTA CONVITE ENVIADA PARA AS STARTUPS .</b>	62
	<b>APÊNDICE C–EXEMPLO DE UM DOCUMENTO DO CORPUS DA PESQUISA, TRANSCRITO E COM DEMARCAÇÕES DE PONTOS RELEVANTES .....</b>	63

## 1 INTRODUÇÃO

Devido ao grande crescimento da Internet, várias empresas optaram por adaptar seus canais de interação com os clientes para *websites*, visto que a grande concentração dos seus usuários utilizam com grande frequências suas redes sociais. Além da forma de interação com os clientes, houve a necessidade das organizações inovarem os seus modelos de negócios existentes e implementados.

Exemplos dessa nova possibilidade de modelo de negócio são as denominadas *startups*, as quais são empresas novas e muito inovadoras em qualquer ramo de atuação, onde procuram elaborar modelos de negócios sofisticados sendo escaláveis e repetíveis (FIGUEIRA *et al.*, 2017). Desse modo, as *startups* são organizações que surgiram em meio à várias incertezas e nos mais variados ramos, entretanto trazem em sua essência a inovação para reformular um serviço ou produto, dessa forma buscando impactar o mercado (RIES, 2012).

Contemporaneamente, a *Lei Geral de Proteção de Dados* (LGPD), lei de Nº 13.709, aprovada em 2018 e posta em vigência no mês de agosto de 2020, foi desenvolvida para priorizar e dar ainda mais ênfase à proteção dos dados dos usuários em todos os processos em que são utilizados pelas organizações (BRASIL, 2018). A LGPD veio para garantir a transparência no uso dos dados de pessoas físicas sob qualquer meio, em virtude dos casos em que os usuários foram prejudicados com a exposição dos seus dados pessoais na Internet por meio de ataques cibernéticos (FERNANDES *et al.*, 2021).

É notório que nos últimos anos ocorreram vários casos de vazamento de dados pessoais na internet, agravando ainda mais a preocupação de todas as empresas que assemelhavam-se na utilização do mesmo modelo de negócio ou, simplesmente, continham em suas bases de dados, informações e dados sensíveis de seus usuários (MIRANDA, 2019).

Em 2019, foi amplamente divulgado o caso de um aplicativo de celular que gerava uma imagem do usuário envelhecida e que após isto armazenava a imagem no seu banco de dados (MIRANDA, 2019). Evidenciado por Miranda (2019), foram levantados diversos questionamentos acerca da finalidade do armazenamento dessas imagens pelo aplicativo, um deles sendo: será que estas fotografias realmente foram, (ou serão) deletadas do banco de dados após um determinado tempo? É uma questão sem resposta, onde não há, ainda, dados que dimensionem a real problemática.

Perante o exposto, surgiu a seguinte problemática: será que as *startups* incubadas na *Universidade Federal do Ceará* (UFC) estão adaptando os requisitos de privacidade dos dados

em consonância com a LGPD?

Existem trabalhos que buscam avaliar como as corporações estão se adaptando ao novo cenário imposto pela LGPD, como o de Rojas e Medeiros (2021) e Costa Júnior (2020). No cenário das *startups* incubadas pela UFC e em que os estudos utilizaram a abordagem da Análise de Conteúdo para extrair informações acerca dos dados coletados, não foram encontrados estudos relativos a essa questão.

## 1.1 Objetivos

O objetivo geral deste trabalho é analisar a conformidade das *startups* incubadas na UFC em relação aos requisitos de privacidade da Lei Geral de Proteção de Dados (LGPD) e propor pontos de melhorias.

Os objetivos específicos são:

- a) Definir as métricas de análise de conformidade do uso da LGPD;
- b) Coletar informações sobre o uso de dados feito pelas *startups* incubadas na UFC;
- c) Discutir os dados encontrados e propor boas práticas da LGPD;

O restante deste trabalho está organizado da seguinte maneira. No Capítulo 2, são apresentados os principais conceitos para o desenvolvimento deste trabalho, que são: Privacidade dos Dados, Lei Geral de Proteção de Dados (LGPD), a norma da ABNT NBR ISO/IEC 27701, a técnica da Análise de Conteúdo e o *software* Iramuteq para analisar e gerar ilustrações das informações. No Capítulo 3, realiza-se a apresentação e discussão dos trabalhos relacionados, com suas semelhanças e diferenças ao trabalho aqui proposto. No Capítulo 4, a metodologia a ser empregada para o desenvolvimento deste trabalho é explicada; e, por fim, no Capítulo 5, são apresentados os resultados deste trabalho.

## 2 REFERENCIAL TEÓRICO

Nesta seção, iremos abordar os principais conceitos utilizados e discorrer a respeito da nova *Lei Geral de Proteção de Dados* (LGPD). Através de uma explicação rápida e objetiva, é realizada uma abordagem informacional do que se trata a LGPD e também são apresentados os conceitos que fundamentam a metodologia da análise que foi realizada no trabalho.

### 2.1 Privacidade dos Dados

A privacidade é um termo que, após vários casos de vazamento de dados pessoais na internet, foi extremamente investigada em diversas áreas (ALVES; NEVES, 2021). A privacidade é o direito de determinar quem pode usufruir dos dados pessoais, com qual finalidade estes dados serão utilizados e como irão ser manipulados, ou seja, como estes dados serão compartilhados a terceiros (KALLONIATIS *et al.*, 2008).

Através de um estudo realizado por Anthony Samy (2017), o mesmo classifica as categorias de privacidade como sendo: conformidade, controle de acesso, verificação e usabilidade. Dessa maneira, para que possa ter como base o que são requisitos de privacidade na compreensão dos usuários, podem ser analisados os quatro conceitos citados, para, assim, compreender a perspectiva de privacidade apresentada pelo autor e também como assegurar a privacidade dos seus dados.

Na subseção 2.1.1 é discorrido a respeito de cada conceito na visão proposta por Anthony Samy (2017).

#### 2.1.1 Requisitos de Privacidade

A definição do primeiro conceito de privacidade na perspectiva de *conformidade* está diretamente ligada à questões legislativas. Isso significa que qualquer utilização de dados deve obter requisitos de privacidade com base na legislação de proteção.

A privacidade na perspectiva do controle de acesso, normalmente tende a ser uma tarefa muito delicada e problemática, pois envolve etapas de segurança como validação e permissões de acesso, dentre outros. Dessa maneira, esta categoria tem como objetivo controlar quais e a quem os dados devem ser informados (ANTHONY SAMY *et al.*, 2017).

Por outro lado, na privacidade na perspectiva de verificação, o autor Anthony Samy (2017) reforça que o objetivo dessa categoria é aplicar métodos convencionais de segurança para

verificar se os requisitos de privacidade mais fundamentais estão adequados e funcionais nas aplicações, contribuindo para aumentar a confiabilidade do sistema.

Por fim, a privacidade na perspectiva de usabilidade está interligada à concepção de como os usuários utilizam-se de suas informações nas bases de dados. Observando também, por quais motivos, arquitetam até mesmo formas de violarem a privacidade de outros indivíduos nas redes sociais. Portanto, esta categoria é vista na visão comportamental de como os usuários usufruem dos dados e como elaborar requisitos de privacidade de maneira a proteger a privacidade de todos os usuários (ANTHONY SAMY *et al.*, 2017).

Portanto, o presente trabalho utilizou os conceitos de privacidade dos dados e requisitos de privacidade, com base do que é a privacidade na prática e como ela será preservada durante e após o desenvolvimento da pesquisa deste trabalho.

## **2.2 Lei Geral de Proteção de Dados - LGPD**

Segundo Miranda (2019), "Novas tecnologias disruptivas aliadas com uma maior dependência desta evolução, geram e disponibilizam uma grande quantidade de dados, que são utilizados no processo de tomadas de decisão". Em decorrência desse cenário e vários casos de vazamentos de dados pessoais na Internet, surge a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018).

Vários aplicativos que oferecem algum tipo de serviço, esperam como moeda de troca, pelo menos, algum dado para utilizar em seus canais de marketing de vendas ou atrelado ao seu objetivo na sua estratégia de negócio, como afirma (MIRANDA, 2019): "Nada na Internet é realmente grátis".

Diante disto, visando minimizar e fornecer a garantia de privacidade e integridade das informações pessoais, a lei de Nº 13.709, nominada Lei Geral de Proteção de Dados (LGPD), foi elaborada no ano de 2018 e no mês de agosto de 2020 posta em vigência no Brasil, influenciada pela lei *General Data Protection Regulation* (GDPR) (GENERAL, 2019), já em vigência desde de 2018.

Os principais pontos abordados pela nova lei visam aplicar regras e punições na maneira como instituições e empresas, no setor público ou privado, tratam os dados pessoais dos usuários, considerando os seguintes processos: coleta, manuseio, revisão das informações que os próprios titulares dos dados solicitarem, conforme consta no Art. 20º da lei (BRASIL, 2018), e o descarte apropriado dos dados, visando proteger tanto as pessoas naturais quanto as pessoas

jurídicas.

Para a LGPD, informação pessoal refere-se à informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018). São enfatizados 3 tipos de dados (BRASIL, 2018):

1. Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
2. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, etc;
3. Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Como a GDPR foi usada como base para a criação da LGPD, é notório que muitas normas tenham semelhanças, todavia, existem também algumas diferenças entre as leis e, especificamente, na maneira como definem alguns tipos de dados. A GDPR define dados criminais como dados sensíveis e evidencia uma segurança redobrada para esse tipo de dados em especial (GENERAL, 2019). A LGPD acrescenta o dado anonimizado aos tipos de dados pessoais. Este tipo de dado se caracteriza por não identificar o usuário, tanto no âmbito do uso nos processos internos das empresas, e nem mesmo a quem este dado pertence, ou seja, o titular.

A LGPD definiu os principais responsáveis pelo manuseio, processamento e comunicação entre os titulares dos dados e os órgãos fiscalizadores, através de 4 títulos:

1. Titular: pessoa natural a quem se refere os dados pessoais que são objetos de tratamento;
2. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
3. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
4. Encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

Dessa forma, todos os processos que necessitam de manuseio dos dados dos usuários, passaram a ser designados para uma pessoa específica podendo ser manuseados e, quais são, as principais responsabilidades que este encarregado terá acerca do processo de manuseio e tratamento dos dados coletados e armazenados. Desta forma, os dados dos titulares podem ser

acompanhados e assegurados, demonstrando que estão obtendo o devido cuidado em todos os processos de utilização.

É importante destacar que foi criado um órgão oficial exclusivamente para aplicar e fiscalizar as empresas que armazenam e estão entrando em conformidade com a nova lei, denominado *Autoridade Nacional de Proteção de Dados* (ANPD) <sup>1</sup>.

### 2.3 ABNT NBR ISO/IEC 27701

A norma da *Associação Brasileira de Normas Técnicas* (ABNT) denominada ABNT NBR ISO/IEC 27701 – Técnicas de segurança: Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes, foi lançada no último mês do ano de 2019, voltada para auxiliar na privacidade da informação. A mesma foi elaborada pelo Comitê Brasileiro de Computadores Processamento de Dados (ABNT/CB-021).

A ABNT NBR ISO/IEC 27701 pode auxiliar as organizações a realizar o tratamento dos dados com as questões de privacidade, evitando casos de uso indevido dos dados pessoais (FARIAS, 2019). Dessa forma, esta norma se enquadra como um auxílio para as empresas, na definição de seus requisitos de privacidade sem o uso inadequado dos dados pessoais dos titulares.

Farias Júnior (2019) enfatiza ainda que a norma ABNT NBR ISO/IEC 27701 tem como foco os requisitos de privacidade de um Sistema de Gestão da Privacidade da Informação (SGPI) e está baseada na conexão e no *compliance*, tanto da norma ABNT NBR ISO/IEC 27001 e na própria ABNT NBR ISO/IEC 27701, levando em consideração a proteção da privacidade dos dados dos titulares.

Portanto, este trabalho usou como base a norma ABNT NBR ISO/IEC 27701 para elaborar os pontos de melhoria dos requisitos de privacidade de acordo a LGPD, para que, dessa maneira, podendo auxiliar as *startups* incubadas na UFC a tomarem decisões que estejam adequadas ao que a LGPD orienta.

---

<sup>1</sup> <https://www.gov.br/anpd/pt-br>

### 3 TRABALHOS RELACIONADOS

Nesta seção, alguns trabalhos relacionados com o projeto proposto neste trabalho estão apresentados, demonstrando pontos semelhantes e diferentes acerca deste projeto.

#### 3.1 Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso

Em Alves e Neves (2021), foi realizado um estudo de caso em uma organização do poder judiciário estadual não especificada, no qual foi notada uma dificuldade dos analistas de requisitos na criação de normas de privacidade que não fossem de difícil compreensão pelos profissionais de *Tecnologia da Informação* (TI).

O objetivo do trabalho foi elaborar uma proposta de requisitos de privacidade para apoiar a definição de requisitos alinhados com a LGPD. Dessa maneira, foram realizadas entrevistas com cinco analistas de requisitos de privacidade da organização pública estudada. Foram feitos relatos de dificuldades no processo de interpretação da nova lei e nas mudanças da rotina de trabalho, a fim de adequar os novos sistemas e os sistemas legados com a legislação em vigência.

As principais diferenças entre o trabalho de Alves e Neves (2021) e o apresentado neste estudo é que este utilizou um questionário para obter as respostas acerca dos requisitos de privacidade durante uma entrevista com os gestores das startups incubadas na UFC, ao passo que no de Alves e Neves (2021), foi realizado uma entrevista com alguns analistas de privacidade da organização pública em estudo, e com as respostas obtidas foi construída a proposta de melhoria. A orientação gerada foi adequada ao software interno do órgão, o sistema Nísia. A técnica de análise utilizada no trabalho de Alves e Neves (2021) foi a Teoria Fundamentada nos Dados, do inglês *Grounded Theory* (TFD). Todavia, este trabalho utilizou a técnica da Análise de Conteúdo para realizar a análise dos dados advindos através das entrevistas, onde a aplicabilidade da técnica foi no cenário específico das *startups* atuantes na UFC.

#### 3.2 Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais

O trabalho apresentado por Rojas e Medeiros (2021) buscou verificar como a LGPD vem sendo encarada pelas instituições de ensino, especificamente, o Instituto Federal, acerca da

adaptação das diretrizes de uso dos dados pessoais em concordância com a LGPD.

Para verificar como está o andamento no quesito de adequação dos procedimentos para a LGPD, foi elaborado um questionário de treze perguntas, as quais foram respondidas pela equipe de TI do Instituto Federal, quando estavam sendo entrevistados pelo autor. Notou-se que a instituição ainda está no estágio inicial de adaptação da lei e que existem diversos termos e questões da própria LGPD que não são bem definidas, ocasionando em uma grande dificuldade dos gestores na adequação da LGPD.

As principais diferenças entre o trabalho de Rojas e Medeiros (2021) e o apresentado aqui é que o mesmo focou nas instituições de ensino e buscou analisar a adaptação da lei no cenário acadêmico, ao passo que este trabalho buscou analisar o cenário das *startups* incubadas nas UFC. As semelhanças com o presente projeto é o uso da técnica de coleta dos dados usando entrevistas para elaborar boas práticas de adequação a LGPD.

### **3.3 Análise de conformidade de processos de negócios em relação a LGPD**

Em Costa Júnior (2020), foi elaborado um método denominado *LGPD for Business Process* (LGPD4BP) que propôs auxiliar as instituições a adaptarem os seus processos de negócios à LGPD. O método é composto por um questionário de avaliação e um método de modelagem que contém um catálogo de padrões que modelam todos os processos internos de maneira a estarem de acordo com a LGPD.

O objetivo do trabalho foi propor uma solução que abordasse técnicas de conformidade que as empresas pudessem utilizar e conseqüentemente atingirem a conformação de seus processos de negócio à LGPD. Para que fosse atingido o objetivo, foi realizado um estudo de caso aplicando o método na *Universidade Federal de Pernambuco* (UFPE) e validado por uma turma de discentes do programa de pós-graduação que aplicou a estratégia e em seguida respondeu o questionário acerca das dificuldades encontradas no decorrer do estudo de caso e também as facilidades do processo de adaptabilidade do método.

As principais diferenças entre o trabalho de Costa Júnior (2020) e este, é que não foi elaborado um método de adequação dos processos de negócio das corporações, todavia, realizou uma análise de cunho avaliativo, onde é analisado a norma da ABNT NBR ISO/IEC 27701 para auxiliar na elaboração de pontos de melhoria nos requisitos de privacidades das *startups* perante a LGPD, verificando como elas estão adequando os seus requisitos de privacidade.

### 3.4 Análise Comparativa

Para uma melhor compreensão das diferenças e semelhanças dos trabalhos apresentados anteriormente, na Tabela 1, são apresentadas as diferentes abordagens de cada trabalho em relação a este, contribuindo para evidenciar a amplitude de suas diferenças.

Tabela 1 – Análise comparativa entre trabalhos relacionados e este trabalho

<b>TRABALHO</b>	<b>MÉTODO DE COLETA DE DADOS</b>	<b>DE PÚBLICO ALVO / DE MERCADO-ALVO</b>	<b>TÉCNICA DE ANÁLISE QUALITATIVA</b>
<b>(ALVES; NEVES, 2021)</b>	Entrevista	Orgão do Poder Judiciário Estadual	Teoria Fundamentada nos Dados - TFD
<b>(ROJAS; MEDEIROS, 2021)</b>	Entrevista	Instituto Federal	Técnica de Revisão Sistemática
<b>(COSTA, 2020)</b>	Questionário	Empresas envolvendo seus processos de negócio	Revisão Literária
<b>Este trabalho</b>	Entrevista	<i>Startups</i> incubadas na UFC	Análise de Conteúdo

Fonte: Elaborado pelo autor (2022).

## 4 METODOLOGIA

Para que os objetivos propostos neste trabalho fossem alcançados, um conjunto de etapas precisou ser seguido, conforme descrito nas próximas seções.

### 4.1 Análise de Conteúdo

Análise de conteúdo é um método utilizado para análises qualitativas, abordando técnicas de análise das comunicações. Para Bardin (2011), análise de conteúdo consiste no conjunto de instrumentos metodológicos cada vez mais sutis, que estão em constante aperfeiçoamento, que se aplicam a “discursos” extremamente diversificados.

Os principais passos da metodologia da análise de conteúdo de acordo com Bardin (2011), são as etapas da: organização, codificação e categorização. Na Figura 1, é apresentado o fluxograma do método de análise de conteúdo.

Na primeira etapa, denominada **pré-análise ou organização**, é feito um levantamento dos dados e da maneira como foram coletados e armazenados, por exemplo: documentos escritos, vídeos, transcrições de entrevistas, etc. Nesta fase de organização é feita uma verificação dos dados e observado o que pode ser considerado útil ou não para alcançar o objetivo da análise.

Na etapa de **codificação**, é importante analisar dois pontos cruciais, sendo eles a unidade de registro e unidade de contexto. **Unidade de registro** é o termo que representa o que será analisado, ou seja, parte do texto que possa ser analisado, podem ser palavras, verbos, conceitos, temas ou temática (BARDIN, 2011).

Já **Unidade de contexto** se caracteriza pela parte onde as unidades de registros estão contidas e qual o contexto em que estão englobadas (BARDIN, 2011). Em um texto pode ser considerado o parágrafo, no qual as unidades de registro foram selecionadas, se for dividido por capítulos, quais capítulos os registros foram marcados, dentre outros.

Dessa forma, o processo de codificação se caracteriza por demarcar palavras/chaves/-conceitos que são as unidades de registro escolhidas para serem submetidas à análise, os quais estão contidas em uma unidade de contexto em que a mesma pode ser previamente selecionada, para que se possa alcançar o objetivo da análise.

Figura 1 – Fluxograma da Análise de Conteúdo



Fonte: Elaborado Via Carreira (2021)

Por fim, o passo de **categorização** é a parte que reúne as informações obtidas da codificação. Nesta fase é observado onde esses dados irão responder a problemática do trabalho, ou seja, a sua análise. Podem ser categorizadas pela frequência de vezes que aparecem, pela semântica, de acordo com os significados dos códigos, sintático, de acordo com a organização

frasal dos códigos, pela lexicografia, de acordo com a organização das palavras contidas no texto, se vem antes ou depois e etc.

Portanto, a utilização da análise de conteúdo para o projeto foi escolhida por auxiliar desde a coleta dos dados até a elaboração dos resultados. Dessa forma, utilizando-se da análise de conteúdo tem-se um passo a passo bem definido e um plano de execução de cada passo, possibilitando atingir os objetivos específicos, contribuindo para a realização do objetivo geral.

#### **4.2 Software de Análise Iramuteq**

O sistema *Iramuteq* é um *software* livre, distribuído sob os termos da licença GNU GPL (v2), sendo a versão utilizada foi a 0.7 *alpha 2-2020*. Não foi encontrado no *site* o desenvolvedor que contribuiu na última atualização do *Iramuteq*. O sistema é uma dentre várias opções de ferramentas que auxiliam para instrumentalizar uma análise qualitativa.

O primeiro motivo para esta ferramenta ter sido escolhida, para auxiliar a elaboração das análises e posteriormente nas inferências sobre as informações obtidas dos dados, é que a mesma tem a capacidade de suportar um grande volume de dados textuais. Sendo assim, sabendo que as respostas de algum entrevistado poderia ser longa e com características de âmbito muito aberto, foi visto a primeira vantagem para uso na pesquisa.

Sobre essa mesma perspectiva, para auxiliar na organização, tendo em vista a possibilidade de uma grande massa de dados textuais, era necessário ter em mente a organização de todo esse conteúdo. Desta maneira, a segunda vantagem para utilizar o *software Iramuteq* foi sua otimização para organizar os volumes de dados (IRAMUTEQ, 2020).

Ainda sobre a perspectiva de organização dos dados, a terceira vantagem foi que o *software Iramuteq* realiza a análise das palavras de um determinado grupo dentro do contexto em que foram citadas, contribuindo para que as unidades de registro estivessem realmente dentro do mesmo contexto em que foram pré-estabelecidas na elaboração das perguntas.

Dentre outras vantagens relevantes para o uso do *software Iramuteq*, podemos citar: o fato de oferecer diversas funcionalidades dentre elas, elaborar figuras, selecionar e contabilizar classes gramaticais e gerar *Word Clouds* que auxiliam na compreensão das informações de maneira visual (IRAMUTEQ, 2020).

Uma desvantagem em se utilizar do *software*, é que se torna necessário entender a estrutura de como são codificados os dados dentro da plataforma. É esperado que se tenha um conhecimento sobre como é executado o processo de inclusão dos dados na ferramenta

de maneira padrão, sendo necessário ser efetuado, de maneira sistemática, cada passo e assim dificultando para que o pesquisador inicialize de fato as análises.

Os tutoriais de instalação <sup>1</sup> e utilização do *software Iramuteq* podem ser encontrados no próprio site da ferramenta <sup>2</sup>.

### 4.3 Instrumento de Coleta de Dados

Para o procedimento de coleta de informações neste trabalho, utilizamos o método de entrevista pois se mostrou a melhor forma de conseguir extrair informações de maneira legítima e que não fosse pré-elaborada, como o método de questionário.

O método de entrevista é uma dentre as várias opções de coleta de dados qualitativos, apresentando vantagens de fornecer oportunidades para motivar e esclarecer o respondente; conceder flexibilidade ao respondente ao definir as sequências e palavras no qual serão apropriadas; ter um controle maior diante a situação, por fim, propiciar uma maior avaliação das respostas, observando o comportamento não verbal do respondente (CASSIANI *et al.*, 1996).

Deste modo, foi elaborado um questionário composto de quatorze perguntas, que podem ser visualizadas no **Apêndice A**. Constituídas, as mesmas foram utilizadas como roteiro para as entrevistas com os responsáveis pelas *startups*. Estas perguntas que foram elaboradas através do estudo da LGPD e de acordo com os requisitos de privacidade estabelecidos através da fundamentação teórica deste trabalho, sendo *conformidade, verificação, controle de acesso e usabilidade*, de acordo com Anthony Samy (2017).

Uma ressalva é que o uso dos dados coletados com as entrevistas, foram previamente autorizadas pelas empresas, pedindo autorização para utilizar os dados apenas para fins acadêmicos e informando apenas o ramo de atividade.

Com o roteiro de perguntas e o método de coleta definidos, foi colocado em prática o passo de seleção e coleta das informações das *startups*.

### 4.4 Escolha das *startups* e coleta dos dados

Para obter as informações das *startups* incubadas pela UFC, foi necessário listar todas as que fossem elegíveis para a pesquisa, observando alguns pré-requisitos para participação. Com isso, o primeiro seria a *startup* ter coletado dados dos usuários/clientes ou, de acordo com

<sup>1</sup> <http://www.iramuteq.org/documentation>

<sup>2</sup> <http://www.iramuteq.org/telechargement>

o tipo de estratégia empresarial, haver possibilidade de coleta de dados futuramente.

Através do programa “Empreende UFC” (INOVAÇÃO, 2020), foi possível ter acesso a uma lista de várias *startups* incubadas pela universidade. Dessa maneira, com a obtenção da lista foi possível ter acesso aos canais de interação das *startups*, como *e-mail* e o número de telefone, podendo assim estabelecer o primeiro contato.

Em seguida, foram enviados e-mails explicando o motivo da entrevista e convidando-as para participação na pesquisa. No total, dezenove *startups* estavam na lista. Dentre elas, duas já haviam aceitado participar em convite que foi feito de forma direta através do *WhatsApp* e uma não tinha e-mail válido, mas foi feito contato telefônico. Sendo assim, foi enviada uma carta convite para as outras dezesseis *startups*. A carta convite pode ser visualizada no **Apêndice B**. Finalmente, elegíveis para a entrevista foram detectadas sete *startups*, todas auto-consideradas no ramo de atividade de serviços de tecnologia.

Em suma, doze *startups* deram um retorno sobre a disponibilidade para aceite da entrevista e as sete *startups* restantes, não deram nenhum retorno. Na Tabela 2, é possível visualizar as informações apresentadas acima, bem como o ramo de atividade das *startups*.

Tabela 2 – Tabela contendo os motivos e quantas *startups* foram elegíveis para a pesquisa

<i>Startups</i>	Ramo de Atividade	Deu Retorno?	Aceitou?	Elegíveis?	Motivo
<i>Startup 01</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 02</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 03</i>	Serviço	Sim	—	Não	Encerrou as atividades
<i>Startup 04</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 05</i>	Comércio	Sim	—	Não	Não pretende coletar dados dos usuários
<i>Startup 06</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 07</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 08</i>	Serviço	Sim	—	Não	Fase muito inicial de aplicabilidade da LGPD
<i>Startup 09</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 10</i>	Serviços para Comércio	Sim	—	Não	Não coletará dados dos usuários
<i>Startup 11</i>	Serviço de tecnologia	Sim	Sim	Sim	—
<i>Startup 12</i>	Serviço	Sim	—	Não	Não implementou nada sobre a LGPD
<i>Startup 13</i>	Serviço	Não	—	—	—
<i>Startup 14</i>	Serviços de Tecnologia	Não	—	—	—
<i>Startup 15</i>	Serviço de Consultoria	Não	—	—	—
<i>Startup 16</i>	Serviço	Não	—	—	—
<i>Startup 17</i>	Serviço Ambiental	Não	—	—	—
<i>Startup 18</i>	Serviço	Não	—	—	—
<i>Startup 19</i>	Serviço Tecnologia	Não	—	—	—

Fonte: Elaborado pelo autor (2022).

Das doze *startups*, cinco não se enquadraram por conta do pré-requisito do trabalho e por outros motivos como o encerramento das atividades, não pretensão de coleta de dados de clientes e estarem em uma situação de adaptabilidade com a LGPD muito prematura.

Dessa maneira, para que fosse possível a coleta das respostas dos entrevistados, foi

utilizada a conta do *Google Workspace* do Núcleo de Inovação e Empreendedorismo (Inove) da UFC - Campus de Quixadá, para que assim fossem realizadas as gravações das entrevistas.

Com os dados coletados, foi iniciado o próximo passo do projeto que foram as transcrições das entrevistas.

#### 4.5 Transcrições das Entrevistas

Nesta etapa do trabalho foram realizadas as transcrições das entrevistas. O processo foi desenvolvido de maneira manual, assistindo as entrevistas e anotando as respostas dos entrevistados em um documento editável.

Para que fossem transcritos os principais trechos das entrevistas, foi necessário assistir novamente todas elas e observá-las, uma por uma, onde estes determinados trechos seriam utilizados para compor as unidades de registro. Posteriormente as mesmas foram utilizadas na fase de análise do conteúdo obtido com as reuniões, por conta disso, esta foi a etapa que demandou mais tempo, contudo, contribuiu para uma melhor exploração do material.

#### 4.6 Pré-análise

Nesta fase da pesquisa foi realizada a *leitura flutuante*, caracterizada por estabelecer o contato com os documentos, deixando-se invadir por impressões e orientações (BARDIN, 2011). Após isso, passou-se para a fase de escolha dos textos transcritos para a elaboração do *corpus* da pesquisa, definido como o conjunto de documentos tidos em conta, para que, enfim, pudessem ser submetidos aos procedimentos analíticos (BARDIN, 2011). Através da leitura dos textos, foram encontradas informações sobre as hipóteses da pesquisa, no que se refere à conformidade dos requisitos de privacidade de acordo com a LGPD.

Para que o *corpus* da pesquisa fosse desenvolvido, foi necessário conhecer algumas regras definidas por Bardin (2011), como:

1. **Exaustividade:** nesta parte é preciso ter em conta todos os elementos do *corpus*, ou seja, não pode excluir qualquer elemento por esta ou aquela razão. Foi concluída essa regra na fase de transcrições das entrevistas, onde todas foram revistas, a fim de ter uma melhor exploração dos dados.
2. **Representatividade:** essa etapa leva em conta os documentos selecionados, sendo que os mesmos, devem conter informações relevantes para o universo

da pesquisa. Foi concluída essa regra, após seleção das partes principais das entrevistas após o período de sondagem e transcrições das mesmas.

3. **Homogeneidade:** nesta fase os documentos retidos devem obedecer a critérios precisos de escolha e não apresentar singularidades exorbitantes. Foi concluída essa regra, na medida em que os trechos escolhidos foram selecionados partindo da premissa dos conceitos dos requisitos privacidade, já pré-definidos na elaboração das perguntas.
4. **Pertinência:** neste ponto, os documentos devem ser adequados, no sentido de fonte de informações, para servirem ao objetivo que instiga a análise. Essa regra foi concluída, na medida em que os dados coletados e sondados foram de extrema importância para responder a questão de pesquisa, dessa forma, sendo condizentes aos objetivos.

## 4.7 Codificação dos dados

### 4.7.1 Síntese sobre a elaboração das perguntas orientadas aos requisitos de privacidade

Constituído o *corpus* da pesquisa, passamos para a fase de exploração e codificação dos dados. Nesta etapa da pesquisa os documentos continham as **unidades de registro**, que são unidades de significação codificadas, que foram analisadas dentro das **unidades de contexto**, que são as unidades de compreensão para codificar as unidades de registro (BARDIN, 2011). Dessa forma, este trabalho utilizou as perguntas para centralizar cada resposta, formando as unidades de registro, referentes aos conceitos dos requisitos de privacidade norteando as unidades de contexto.

Por exemplo, a primeira pergunta foi elaborada baseada no primeiro conceito de requisito de privacidade, a *conformidade*. Sendo assim, a resposta obtida remete ao que o entrevistado iria responder baseado no conceito já pré-estabelecido na elaboração da pergunta. Dessa forma, contribuindo para que a etapa de codificação dos dados e a análise sobre os mesmos fossem mais rápidos, após o longo período de transcrições, revisões das entrevistas e a elaboração do *corpus* da pesquisa.

Um dos documentos que foi transcrito, codificado e demarcado com pontos relevantes utilizados na etapa de interpretação dos dados, pode ser visualizado no **Apêndice C**.

Na próxima subseção é demonstrado como ficou organizado a divisão das categorias

pré-definidas para auxiliar na etapa de análise e interpretação dos dados coletados das entrevistas.

#### 4.7.2 Processo de categorização

O principal objetivo do trabalho é analisar qual é a situação de conformidade dos requisitos de privacidade pelas *startups* incubadas pela UFC. Sabendo disso, as principais **categorias de análise** que foram verificadas remetem diretamente aos requisitos de privacidade. Com isso, os quatro requisitos de privacidade também são as categorias de análises.

Na Tabela 3, é demonstrado como ficou organizado as categorias de análise, unidades de registro, unidades de contexto e a categoria de contexto.

Tabela 3 – Modelo organizatório das categorias de análise - Unidades de Registro (respostas dos entrevistados) e Unidades de Contexto (descrição do que seria analisado de acordo com os conceitos que norteariam à elaboração das perguntas)

CATEGORIA DE CONTEXTO: Conformidade dos Requisitos de Privacidade		
Categorias de Análise	Unidades de Registro	Unidades de Contexto
Conformidade	Respostas das perguntas sobre Conformidade	Conformidade, esta definição está diretamente ligada a questões legislativas, ou seja, para qualquer utilização dos dados, sejam eles utilizados em aplicações web, softwares ou qualquer forma de usar os dados, precisam estar de acordo com uma legislação de proteção dos dados. Com isso, obtendo requisitos de privacidade baseados na lei (ANTHONY-SAMY et al., 2017)
Controle de Acesso	Respostas das perguntas sobre Controle de acesso	Para controle de acesso, normalmente tende a ser uma tarefa muito delicada e problemática, pois envolve etapas de segurança como validação de acesso, permissões de acesso e etc. Dessa maneira, esta categoria tem como objetivo controlar quais e a quem os dados poderão serem informados (ANTHONY-SAMY et al., 2017).
Verificação	Respostas das perguntas sobre Verificação	Para verificação, o autor reforça que o objetivo dessa categoria é aplicar métodos convencionais de segurança para verificar se os requisitos de privacidade mais fundamentais estão adequados e funcionais nas aplicações, contribuindo para aumentar a confiabilidade do sistema (ANTHONY-SAMY et al., 2017).
Usabilidade	Respostas das perguntas sobre Usabilidade	Usabilidade, está interligada a concepção de como os usuários utilizam-se dos dados e por quais motivos, adentrando em um aspecto mais amplo, arquitetam até mesmo formas de violarem a privacidade de outros indivíduos nas redes sociais (ANTHONY-SAMY et al., 2017).

Fonte: Elaborado pelo autor (2022).

Após isso, foi iniciado o processo do tratamento e interpretações acerca dos resultados.

## 5 RESULTADOS

### 5.1 Análises dos resultados

Nesta etapa, foi iniciada a fase de análise sobre o material coletado e explorado. De acordo com Bardin (2011), se todas as operações da pré-análise forem convenientemente concluídas, a fase de análise, nada mais é, que a aplicação das decisões tomadas.

#### 5.1.1 Análise das respostas referente a cada categoria de análise

Considerando que as perguntas foram elaboradas dentro do conceito dos requisitos de privacidade mostrados na fundamentação teórica deste trabalho e as mesmas foram explicadas na fase de síntese da concepção das perguntas, abaixo encontram-se as análises realizadas sobre cada conceito que norteava as perguntas e as interpretações dos resultados com o auxílio do *software Iramuteq*.

##### 5.1.1.1 Conformidade

As perguntas **um, cinco, seis, oito e dez** tratavam a respeito do requisito de privacidade da *conformidade*, sendo a pergunta oito baseada em dois requisitos de privacidade: *conformidade e usabilidade*. O conceito de *conformidade* refere-se aos processos legislativos para com dados dos usuários, observando a maneira como são ou seriam utilizados para serviços de *software*, prospecção de negócio, estratégias de *marketing*, dentre outros, assim, estando alinhado com o que a LGPD orienta. Na Tabela 4 é apresentado o que foi analisado e extraído dos dados fornecidos pelos entrevistados.

Tabela 4 – Tabela de percentual atingido do requisito de *conformidade*

Perguntas =>	1	5	6	8	10	SOMA TOTAL (%)
<b>Startup 01</b>	20%	20%	20%	20%	20%	<b>100%</b>
<b>Startup 02</b>	20%	—	20%	20%	20%	<b>80%</b>
<b>Startup 04</b>	20%	20%	—	20%	20%	<b>80%</b>
<b>Startup 06</b>	20%	20%	20%	—	20%	<b>80%</b>
<b>Startup 07</b>	20%	20%	20%	20%	—	<b>80%</b>
<b>Startup 09</b>	—	20%	20%	—	—	<b>40%</b>
<b>Startup 11</b>	—	—	20%	—	20%	<b>40%</b>
<b>% ESPERADO</b>	<b>60%</b>					

Fonte: Elaborado pelo autor (2022).

Para essa categoria foi escolhido o percentual de 60% como sendo o valor esperado, baseado no fato de que as *startups* já tinham dados de usuários ou pretendiam coletar dados dos mesmos. Dessa forma, compreendendo que as mesmas já deveriam estar em conformidade com pelos menos 60% do que era investigado pelas perguntas, caso estivessem, era atribuído o valor de 20%, sendo esse valor escolhido baseado na quantidade de perguntas, ou seja, cinco perguntas representavam 100%, logo uma pergunta que atingia o esperado, representava 20% do total.

Através das unidades de registro, inclusas nas unidades de contexto, neste caso, a *conformidade*, foi possível observar que dentre as sete *startups* elegíveis, cinco *startups*, representando aproximadamente 70% das *startups* selecionáveis, atingiram o percentual mínimo estabelecido e demonstram que estão cientes, analisam e cumprem este requisito de privacidade, de acordo com o que a LGPD orienta.

Já sobre outra perspectiva, as duas *startups* que representam os 30% restantes, não tiveram o cuidado e o processo de antecipação para cumprir o que era investigado através das perguntas, ou seja, das cinco perguntas, ambas as *startups* responderam apenas duas perguntas, representando 40% do total, demonstrando através do conteúdo das respostas que não tiveram o cuidado para com os dados dos usuários ou realizaram ações preventivas para com os mesmos.

#### 5.1.1.1.1 Exemplificação com trechos dos respondentes

Conforme informado anteriormente, para os aspectos que demonstraram a ciência e a preocupação por parte das *startups* que representam 70% da amostra, podem ser evidenciados nos quatros trechos das entrevistas, a seguir.

Maneira escolhida para demonstrar a *Representação de fala de uma Startup* ([S]):

[S1]: “O nosso medo era dá certo, ter tração e crescer **mas por algum motivo de descuido legal nosso, a gente perder credibilidade no mercado ou fechar o negócio. Por conta disso, sempre tivemos bastante cuidado, desde o começo nos preparamos bastante.**”

[S2]: “A gente interpreta de maneira muito natural. Salvo não me engano a nossa startup é posterior a lei, então ela começou a funcionar a partir do momento em que a lei já existia, **então para a gente foi bem natural, não tivemos nenhuma preocupação em expor nenhum dado sigiloso, em fugir do que a lei está definindo, até por que já era premissa que era para seguir essa lei desde do começo.**”

[S2]: “Olha eu acho que a gente segue isso aí à risca. Como eu tinha dito, os dados relativos aos titulares são diminutos, só pegamos o que realmente necessita em base de

*relação contratual, por exemplo, devemos pegar por padrão dados plenamente justificáveis para o contrato e fora disso os dados bancários para pagamento, mas aí usando o sistema de pagamentos não precisamos guardá-los, no frigor dos laudos, os dados pessoais que vamos ter deles serão os dados exclusivamente necessários ao regime contratual, somente.”*

*[S4]: “Hoje nossa startup, trabalha com alguns consultores. Não sofremos mudanças na concepção do nosso serviço, não nas questões burocráticas a respeito da LGPD por que iniciamos a empresa já sabendo e buscando se adaptar a lei.”*

Referente as duas *startups* que não atingiram a expectativa para o requisito de *conformidade*, podem ser evidenciados nos dois seguintes trechos de entrevistas:

*[S9]: “No momento não é a prioridade, a gente tem muitas outras coisas para resolver até chegar essa parte de proteção de dados, muitas coisas de design, do produto em si.”*

*[S11]: “Bem, é até um pouco diferente porque eu ainda não entendi como implantar esse aspecto do “privacy by design”. Como essa lei diz que devemos ter uma privacidade dos dados antes de implementar qualquer coisa de tecnologia, eu ainda não sei como implementar isso já que a etapa de obtenção de dados seria através de tecnologia também.”*

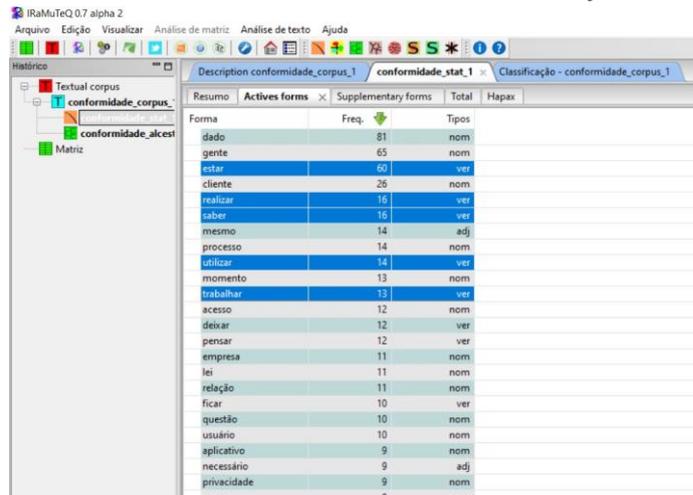
#### 5.1.1.1.2 Análises com o *software Iramuteq* para o requisito de *conformidade*

Com o auxílio do *software Iramuteq* para instrumentalizar as análises sobre dos dados coletados, foram utilizadas algumas ferramentas que são fornecidas pelo sistema. Dessa forma, ficando ainda mais compreensível as interpretações de maneira visual.

Os motivos pelos quais foram utilizadas as funcionalidades de análise estatísticas e o método de *Reinert* do *software Iramuteq* para verificar o conteúdo sobre *conformidade*, foram por motivos visuais e por melhor intrumetalização dos dados. Por conta disso, é possível observar que foram utilizadas diferentes análises nesta etapa de uso do *software Iramuteq*.

Na Figura 2, é possível observar uma análise estatística fornecida pelo *software Iramuteq*. Através do *software* é possível verificar os verbos que obtiveram o maior número de frequência.

Figura 2 – Análise estatística sobre o conteúdo relacionado a *conformidade*

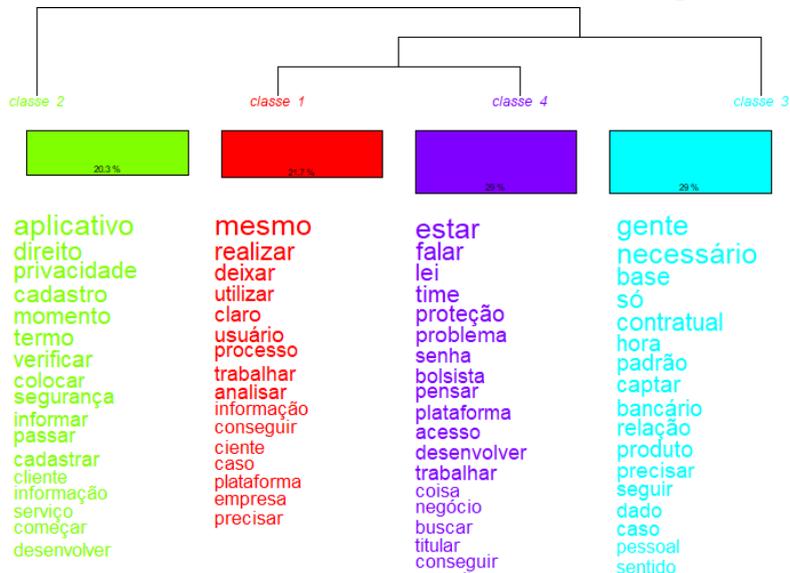


Fonte: Elaborado pelo autor (2022).

A Figura 2 demonstra uma seleção de verbos que mais obtiveram ocorrências para o requisito de *conformidade*. Os verbos “estar”, “realizar”, “saber”, “utilizar” e “trabalhar” foram os mais utilizados pelos entrevistados na medida em que os mesmos estavam discorrendo sobre o requisito de *conformidade*, através das perguntas. As ocorrências foram de, respectivamente, 60, 16, 16, 14 e 13.

Utilizando uma funcionalidade inclusa no *software Iramuteq*, denominada Método de *Reinert*, foi possível visualizar os diferentes vocabulários, denominadas como classes pelo sistema *Iramuteq*, referentes aos dados, demonstrando a proximidade entre os mesmos. Na Figura 3, é possível verificar uma ilustração dos vocabulários e as palavras inclusas em seu respectivo grupo.

Figura 3 – Método de *Reinert* - Divisão dos vocabulários sobre o requisito da *conformidade*

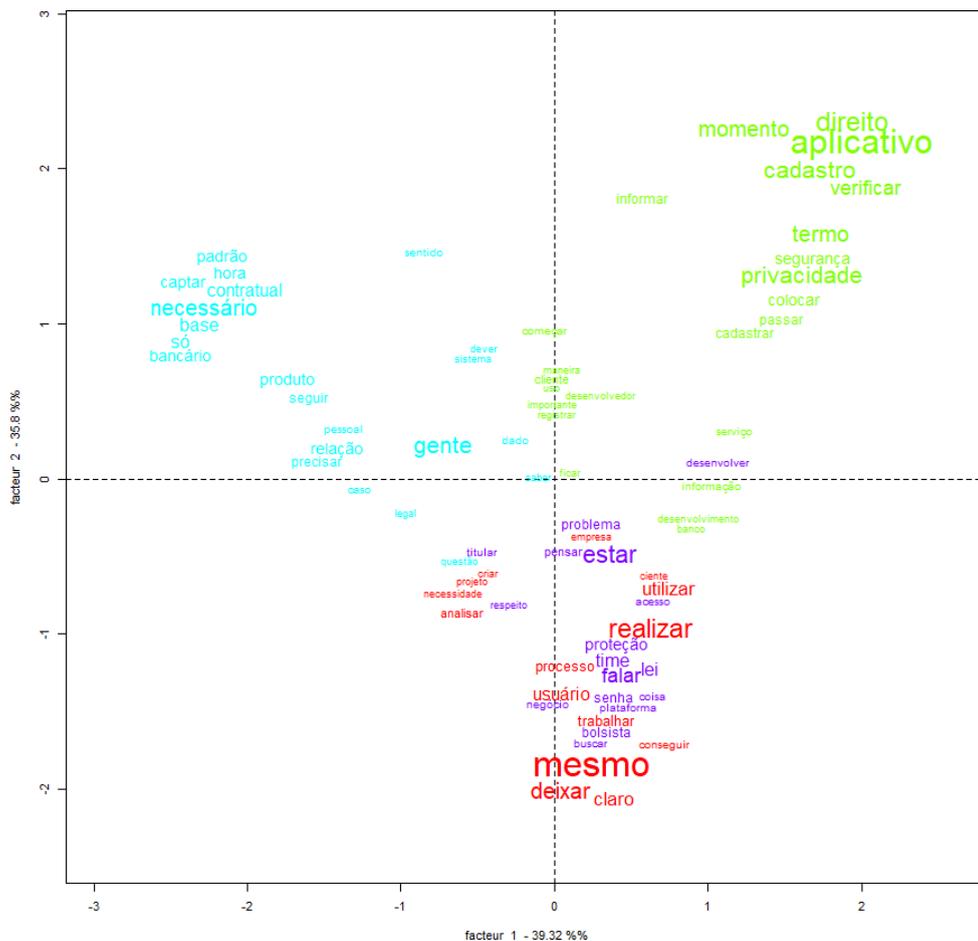


Fonte: Elaborado via Iramuteq (2022).

Composta por quatro classes de vocabulários, de onde a classe dois deriva a classe três, e a classe três origina as classes de vocábulos um e quatro. Dessa forma, é possível observar que o termo “aplicativo” da classe dois, tem ligação com o termo “base” referente a base de dados, onde se encontra localizado na classe três e o mesmo tem ligação com o termo “proteção” da classe quatro e “usuário” da classe um. Sendo assim, demonstrando que todas as classes revelam que os termos estavam próximos, reafirmando as interpretações sobre o requisito de privacidade da *conformidade*.

Com a representação da próxima figura, é possível observar que a classe três está mais próxima à classe dois, ficando assim mais próximas em relação aos seus contextos. As classes um e quatro estão em intersecção, ficando mesclados os contextos de ambas. Na Figura 4, é demonstrado os vocabulários em um plano cartesiano em *Duas Dimensões (2D)*, mostrando as palavras e suas proximidades uma com as outras.

Figura 4 – Método de *Reinert* - Divisão dos vocabulários em um plano cartesiano



Fonte: Elaborado via Iramuteq (2022).

Através das cores das classes demonstradas na Figura 3, é possível observar como as palavras estão distribuídas sobre o plano cartesiano, verificando que as mesmas encontram-se o mais próximos das sentenças que tem uma lógica de contexto, como por exemplo, as palavras “aplicativo” e “privacidade”, localizados no quadrante superior direito, estarem mais próximas em sentido de significado e contexto dos termos “necessário” e “sistema” localizados no quadrante superior esquerdo.

#### 5.1.1.2 Controle de acesso

As perguntas **três e quatro** tratavam a respeito do requisito de privacidade do *controle de acesso*. O conceito de *controle de acesso*, que norteava as perguntas acima, referia-se aos processos delicados e muita das vezes problemáticos, acerca de permissões de acesso, validações de acesso e outros. O objetivo desse requisito é controlar quem tem acesso, quais são esses acessos e a quem poderia ser informado esses dados (ANTHONY SAMY *et al.*, 2017).

Na Tabela 5, é apresentado o que foi analisado e extraído dos dados fornecidos pelos entrevistados.

Tabela 5 – Tabela de percentual atingido do requisito de *controle de acesso*

<b>Perguntas =&gt;</b>	<b>3</b>	<b>4</b>	<b>SOMA TOTAL (%)</b>
<b><i>Startup 01</i></b>	50%	50%	<b>100%</b>
<b><i>Startup 02</i></b>	—	50%	<b>50%</b>
<b><i>Startup 04</i></b>	50%	50%	<b>100%</b>
<b><i>Startup 06</i></b>	50%	—	<b>50%</b>
<b><i>Startup 07</i></b>	50%	50%	<b>100%</b>
<b><i>Startup 09</i></b>	—	50%	<b>50%</b>
<b><i>Startup 11</i></b>	50%	—	<b>50%</b>
<b>% ESPERADO</b>			<b>50%</b>

Fonte: Elaborado pelo autor (2022).

Para essa categoria foi escolhido o percentual de 50% como sendo o valor esperado para ser alcançado, baseado que as *startups* já tinham dados de usuários ou pretendiam coletar dados dos mesmos. Dessa forma, compreendendo que as mesmas já deveriam está em conformidade com pelos menos este percentual para os processos que envolvem o *controle de acesso* referentes aos dados dos usuários, caso estivessem, era atribuído o valor de 50%, sendo esse valor escolhido baseado na quantidade de perguntas, ou seja, duas perguntas representavam 100%,

logo uma pergunta que atingia o esperado, representava 50% do total.

Através das unidades de registro, observadas nas unidades de contexto, neste caso a *controle de acesso*, foi possível observar que dentre as sete *startups* elegíveis, três *startups*, representando aproximadamente 42%, estão cientes, se preocuparam com esse requisito desde da sua concepção como empresa e cumprem este requisito de privacidade, de acordo com o que a LGPD orienta.

As quatro *startups*, representando os 58%, tomando para efeito de comparação o tempo de empresa de uma delas, no qual era relativamente maior que as outras três *startups*, onde ambas estavam no mesmo cenário dos 58%, somente atingiu o mínimo de expectativa para esta categoria, que seria de pelo menos 50%. Para esse cenário, era esperado que as mesmas já analisassem uma melhor maneira de realizar a comunicação com os clientes ou ter a disponibilidade de criar um relatório para informar acerca de possíveis mudanças provenientes da própria LGPD para os seus usuários. Em suma, as quatro *startups* apenas atingiram o percentual médio do que era esperado.

#### 5.1.1.2.1 Exemplificação com trechos dos respondentes

Os trechos abaixo são referentes as *startups* que estão cumprindo e analisaram esse requisito desde sua concepção, demonstrando o devido cuidado com o *controle de acesso* aos dados de seus usuários.

[S1]: *“Temos os termos de uso e as políticas de privacidade. Então, isso também foi uma das primeiras coisas que nos preocupamos em fazer e sempre alinhado com o suporte jurídico, para realmente o nosso documento ter um peso legal e ter vigência legal. Então quando o cliente fecha com a gente, ele está ciente assim como qualquer outra plataforma de quais são os nossos interesses com os dados dele. Portanto, além de ter isso muito claro, a gente nunca agiu de má fé, em relação aos dados, nunca compartilhamos dados, nunca tentamos tratar eles com segundas intenções e etc.”*

[S4]: *“Deixamos claro nos termos de uso e nas políticas de privacidade. As nossas políticas de privacidade e os termos de uso foram elaboradas pensando justamente na questão da utilização dos dados do aplicativo, onde estão listadas e onde deixamos claro todas as informações sobre a utilização dos dados.”*

[S7]: *“Não existe manipulação por terceiros. Hoje na nossa estrutura, não cedemos os dados dos nossos clientes para nenhum terceiro, não se tem nenhuma plataforma,*

***nenhuma empresa vinculada conosco que manipule os dados dos clientes então por isso não acontecer, não precisamos comunicar, entendo dessa forma.***”

Referente às 4 *startups* que compreendiam os 58%, abaixo encontra-se os trechos onde é possível observar, principalmente a *startup* com mais tempo de atuação do que as demais, evidenciando que não tinha ainda nada definido sobre essa questão.

[S2]: ***“Ainda não, inclusive vou até anotar aqui para colocar no nosso ponto de discussão.”***

[S6]: ***“Relatório não, ainda não, mas é uma preocupação para médio prazo.”***

[S9]: ***“Não existe esse meio de comunicação agora, mas ele vai existir provavelmente. A partir do momento que a gente fica aberto a receber reclamações, a receber dúvidas que o usuário tenha sobre a plataforma ou sobre o serviço ou qualquer coisa, ele pode está se informando sobre o que tá acontecendo com seus dados. Eu não sei se faz sentido isso o que eu tô falando, isso aí é realmente aplicado dessa forma, mas é o que eu acredito que seja possível.”***

[S11]: ***“Não, no momento ainda não.”***

[S11]: ***“Ainda não mas vai ser implantado assim que conseguirmos desenvolver.”***

#### 5.1.1.2.2 Análises com o *software Iramuteq* para o requisito de *controle de acesso*

Na Figura 5, é demonstrado uma seleção dos verbos que mais obtiveram ocorrências para o requisito de *controle de acesso*. Os verbos “estar”, “informar”, “acreditar”, “entender” e “existir” foram os mais utilizados durante o período em que os entrevistados estavam discorrendo sobre o requisito de *controle de acesso*. As ocorrências foram de, respectivamente, 8, 7, 4, 3 e 3.

O motivo pelo qual foram utilizadas as funcionalidades de análise estatísticas e a análise de similitude do *software Iramuteq* para verificar o conteúdo sobre *controle de acesso*, foram por motivos visuais e por melhor intrumentalização dos dados acerca de demonstrar que os verbos reafirmavam as interpretações. Por conta disso, é possível observar que foram utilizadas diferentes análises nesta etapa de uso do *software Iramuteq*.

Figura 5 – Análise estatística sobre o conteúdo relacionado a *controle de acesso*

Forma	Freq.	Tipos
dado	14	nom
cliente	10	nom
estar	8	ver
termo	8	nom
gente	7	nom
informar	7	ver
pagamento	6	nom
uso	5	nom
acreditar	4	ver
comunicação	4	nom
plataforma	4	nom
politico	4	adj
privacidade	4	nom
terceiro	4	nom
banco	3	nom
claro	3	adj
coisa	3	nom
entender	3	ver
existir	3	ver
ficar	3	ver
forma	3	nom

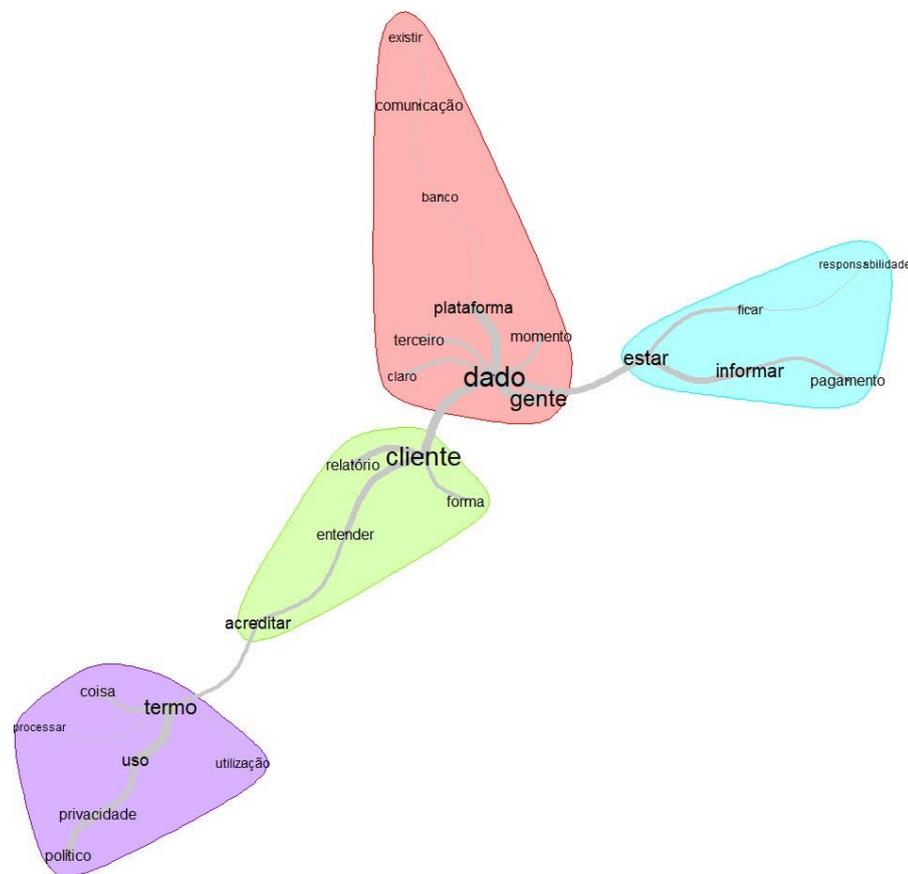
Fonte: Elaborado pelo autor (2022).

Nesta perspectiva, é possível verificar que o verbo “informar” é o segundo dentre os mais utilizados, demonstrando que as *startups* 01, 04 e 07, que atingiram o máximo para esta categoria de análise, observam a importância de informar acerca do controle de acesso aos dados dos seus usuários.

Utilizando a funcionalidade de análise de similitude, é possível compreender de maneira visual, como é feita a construção dos temas mais importantes, mostrando as sentenças próximas e distantes uma das demais, de acordo com a maior ocorrência das palavras. Com isso, a sentença que mais mencionada consiste o principal “nó” que origina os demais temas relevantes, como por exemplo as palavras “dado” e “cliente”, onde pode ser observado e demonstrado como os dados exemplificam e reafirmam o que foi discorrido acerca das respostas das *startups*.

Na Figura 6, é representada a análise de similitude sobre os dados referentes ao requisito de *controle de acesso*. Através desta análise é possível notar os principais temas no *corpus* textual, postos em análise para o requisito de *controle de acesso*.

Figura 6 – Análise de similitude - Divisão dos temas extraídos dos dados referentes ao requisito de *controle de acesso*



Fonte: Elaborado via Iramuteq (2022).

### 5.1.1.3 Verificação

As perguntas **sete, nove, onze e doze** tratavam a respeito do requisito de privacidade da *verificação*. A pergunta **onze** foi formulada baseada em dois requisitos de privacidade, sendo *verificação e usabilidade*. O conceito de *verificação* que era associado aos processos convencionais de segurança sobre os dados dos usuários, tais como controle de vazamentos de dados, verificações da confiabilidade dos sistemas que armazenavam os dados sensíveis, controle de versões de códigos, backups e outros (ANTHONY SAMY *et al.*, 2017). O objetivo desse requisito é verificar se as funções básicas e fundamentais para a segurança dos dados estavam sendo analisadas ou praticadas pelas *startups*.

Na Tabela 6, é apresentado o que foi analisado e extraído dos dados referentes ao requisito de privacidade de *verificação* fornecidos pelos entrevistados. Através disso, é possível visualizar a distribuição dos percentuais atingidos para esta categoria.

Tabela 6 – Tabela de percentual atingido do requisito de *verificação*

<b>Perguntas =&gt;</b>	<b>7</b>	<b>9</b>	<b>11</b>	<b>12</b>	<b>SOMA TOTAL (%)</b>
<b><i>Startup 01</i></b>	25%	——	25%	25%	<b>75%</b>
<b><i>Startup 02</i></b>	25%	25%	25%	25%	<b>100%</b>
<b><i>Startup 04</i></b>	25%	——	25%	25%	<b>75%</b>
<b><i>Startup 06</i></b>	——	——	25%	25%	<b>50%</b>
<b><i>Startup 07</i></b>	25%	25%	25%	25%	<b>100%</b>
<b><i>Startup 09</i></b>	25%	——	——	——	<b>25%</b>
<b><i>Startup 11</i></b>	25%	——	25%	25%	<b>75%</b>
<b>% ESPERADO</b>				<b>50%</b>	

Fonte: Elaborado pelo autor (2022).

Para essa categoria foi escolhido o percentual de 50% como sendo o valor esperado para ser alcançado, baseado no fato de que as *startups* já tinham dados de usuários ou pretendiam coletar dados dos mesmos. Dessa forma, compreendendo que as mesmas já deveriam está em conformidade com pelos menos este percentual referente aos processos básicos de segurança sobre os dados, caso estivessem, era atribuído o valor de 25%, sendo esse valor escolhido baseado na quantidade de perguntas, ou seja, quatro perguntas representavam 100%, logo uma pergunta que atingia o esperado, representava 25% do total.

Através das unidades de registro, inclusas nas unidades de contexto, neste caso a *verificação*, foi possível observar que dentre as sete *startups* elegíveis, duas *startups*, representando aproximadamente 30%, atingiram o máximo esperado, mostrando que estão cientes, analisam e cumprem este requisito de privacidade, de acordo com o que a LGPD orienta. Nesta mesma interpretação, atingindo 75% do esperado, três *startups*, representando aproximadamente 40%, cumprem acima do expectável demonstrando em parte o cuidado com os dados dos clientes, porém deixando a desejar no âmbito de ter um plano de contingência para vazamentos dos dados. Nesse caso, nenhuma das três já integravam alguma maneira de inibir o vazamento dos dados de maneira preservativa.

Sobre outra perspectiva, uma *startup*, representando aproximadamente 15%, atingiu o mínimo esperado para os processos básicos de segurança, neste caso 50%, demonstrando que cumpre o necessário, sendo a formalização de término de tratamento dos dados e monitoração de possíveis vulnerabilidades. Nesse ponto de vista, para a mesma era mais importante não deixar as tarefas de rotina ficarem sobrecarregadas, com isso, deixando de lado a prevenção dos dados, mesmo diante de algum problema de segurança que poderia surgir futuramente.

Por fim, uma única *startup*, representando aproximadamente 15%, alcançou apenas 25% do que era analisado pelas perguntas, aproximando-se do mínimo esperado para os processos básicos de verificação e prevenção da segurança sobre os dados. Com isso, a mesma não conseguiu atingir o esperado para os processos de contingência de vazamento de dados, sobre a protocolização acerca da eliminação dos dados dos usuários após o seu término de uso e não possuindo uma verificação de possíveis vulnerabilidades, mesmo que não tivesse uma equipe especializada para esta determinada função, não tinha também um colaborador da equipe de desenvolvimento, para verificar os processos de segurança.

#### 5.1.1.3.1 Exemplificação com trechos dos respondentes

Os seguintes trechos são as falas das duas *startups* que atingiram o máximo esperado, as quais cumprem e analisam os processos básicos de segurança como pré-requisito, ficando ordenadas com as normas de privacidade, dessa forma alinhadas com o que a LGPD orienta.

[S2]: **“Sim, a gente tem um processo de atualização, até mesmo por que todos os nossos bancos de dados ficam na nuvem, não temos nenhum servidor próprio ou servidor alugado, é todo na Amazon AWS, e a tanto a Amazon tem esse processo de garantia de não deixar obsoleto o sistema de banco de dados, mas também esse compromisso.”**

[S2]: **“Temos esse mapeamento sim, principalmente os dados mais sigilosos, a gente tem muito bem mapeados, como o CPF para relação contratual ou algum dado bancário que a gente possa vir a ter para o sistema de pagamentos, os demais dados como nome completo para título de contratação e identificação, é muito simples a gente expressar para o titular, isso aí está bem definido nas nossas regras de negócios a função de cada um.”**

[S7]: **“Usamos os servidores do Google, então não temos problemas com isso. Também temos contrato com a Amazon AWS. Se importamos com as versões do npm, registrados no npm, mas em relação ao versionamento do banco de dados, não temos esse problema por que terceirizamos esse serviço com essas plataformas SaaS.”**

[S7]: **“Cara, sim. Por que como utilizamos essas soluções de armazenamento dos dados nas plataformas do Google e Amazon, elas próprias nos protegem desses ataques e como não trazemos dados sensíveis dos usuários, não ficamos inseguros a respeito de vazamento de dados.”**

Os seguintes trechos são referentes às falas das três *startups* que atingiram 75% do esperado para o requisito de *verificação*, ficando apenas com uma das quatro perguntas, sem

atingir o desejado. Exclusivamente para essa representação, foram utilizadas as perguntas 07, 09 e 12 para demonstrar o que foi interpretado.

Referente as perguntas 07, 09 e 12, respectivamente, da *startup* 01:

[S1]: *“Os nossos bancos de dados estão todos na nuvem, então facilita muito a questão de segurança e não temos problemas de perder o acesso à máquina. Por conta disso, não temos essa rotina de tratamento de verificação das versões do banco de dados porque a própria plataforma da nuvem faz esse trabalho pela gente.”*

[S1]: *“Não temos um plano para isso.”*

[S1]: *“Esta pessoa é o nosso CPO que cuida desse processo de verificação das vulnerabilidades técnicas por que essa questão está diretamente relacionado com a estrutura do nosso produto, e como é a especialidade dele, então ele está à frente.”*

Referente as perguntas 07, 09 e 12, respectivamente, da *startup* 04:

[S4]: *“Por enquanto estamos realizando de maneira manual e no momento passa um determinado período, por exemplo três meses, solicitamos atualização de dados para os clientes. Atualizando o banco, no caso do conteúdo do banco e atualização da plataforma ocorre em um determinado período de tempo, para poder melhorar a questão de segurança das informações.”*

[S4]: *“Nós estamos adequando isso e estudando para poder melhorar para esse quesito.”*

[S4]: *“Hoje nós temos a nossa equipe da parte desenvolvimento, por enquanto eles que estão cuidando também da parte da segurança. Estamos buscando sempre melhorar nessa parte da segurança dos clientes.”*

Referente as perguntas 07, 09 e 12, respectivamente, da *startup* 11:

[S11]: *“Não ainda não, por que a gente não desenvolveu o nosso banco de dados e as conexões da API com o servidor do Firebase ainda. Mas assim que terminar, vamos realizar. Então não teremos problemas em relação a isso.”*

[S11]: *“Não, não foi planejado nada ainda.”*

[S11]: *“Não temos uma equipe formada para isso, cada um ficou responsável com áreas distintas e só coube a uma pessoa para verificar isso, que no caso sou eu.”*

Os seguintes trechos são referentes às falas da única *startup* que atingiu o mínimo esperado para o requisito de verificação.

[S6]: *“Para esse momento não, porque como nós estamos iniciando agora, nós*

*estamos criando agora a ferramenta, e a preocupação é quando começar a rodar, aí é o momento em que a gente vai começar trabalhar em políticas de segurança.”*

*[S6]: “Eu acho que até te respondi sobre, é porque é uma coisa muito complicada excluir dados dentro de um banco, porque ela pode parar a aplicação inteira. Portanto, dentro da própria plataforma quando o usuário ele pede desligamento, a gente vai notificar e perguntar: você está solicitando desligamento? a partir de agora seus dados não estão mais sendo utilizados para meio de vendas, comunicação e etc. Tudo através da plataforma vale ressaltar.”*

E por fim, os trechos da única *startup*, que não atingiu o mínimo esperado (50%) para os processos básicos de verificação e prevenção da segurança sobre os dados.

*[S9]: “Também não temos.”*

*[S9]: “Não sabia disso, realmente não sabia disso. Eu não tinha pensado nisso, por que normalmente a gente só se cadastra, a parte de se desvincular ele é não é tanto analisado.”*

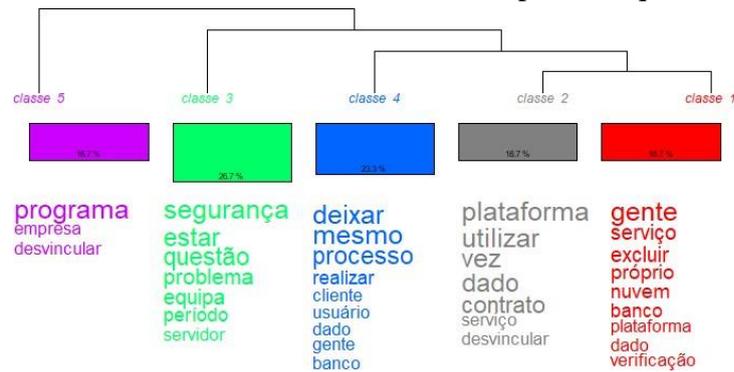
*[S9]: “Não temos no momento, pode ter, mas no momento não temos.”*

#### 5.1.1.3.2 Análises com o *software Iramuteq* para o requisito de *verificação*

O motivo pelo qual foram utilizadas as funcionalidades do método de *Reinert* e a análise de similitude do *software Iramuteq* para verificar o conteúdo sobre *verificação*, foram por motivos visuais, pois a análise estatística não se mostrava melhor que os métodos citados acima. Por conta disso, é possível observar que foram utilizadas diferentes análises nesta etapa de uso do *software Iramuteq*.

Na Figura 7, foi utilizado do Método de *Reinert*, demonstrando a classificação dos vocabulários para a categoria de análise de *verificação*. Através dessa funcionalidade foi possível observar que palavras “empresa” da classe cinco, tem conexão com o vocábulo “segurança” da classe quatro, sendo esta que contendo as palavras “realizar” e “banco” obtendo ligação direta com as palavras “contrato” e “dados” pertencentes à classe dois e, por fim, a palavra “serviço” da classe dois com ligação a sentença “nuvem” da classe um, referindo aos serviços de armazenamento de dados na nuvem.

Figura 7 – Método de *Reinert* - Divisão dos vocabulários para o requisito de *verificação*



Fonte: Elaborado via Iramuteq (2022).

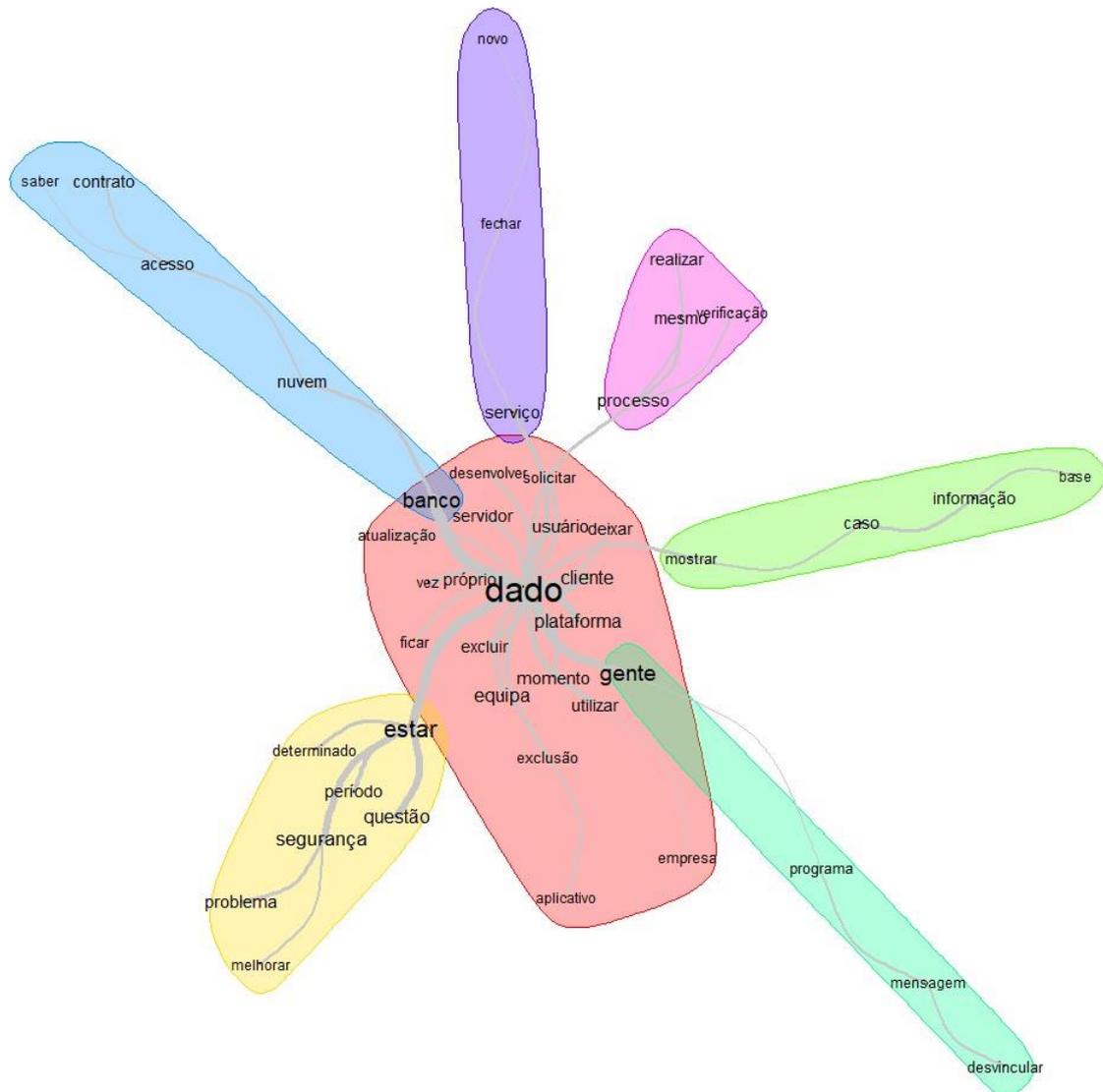
Para o requisito de *verificação*, foram encontradas cinco classes de vocabulários, sendo que a classe cinco originou a classe três, que por sua vez originou a classe quatro, que originou as classes um e dois.

Observando de maneira mais ampla, foi possível verificar que as *startups* dois e sete obtiveram uma melhor compreensão dos processos básicos de segurança, onde as mesmas atingiram o máximo esperado para as perguntas de cunho avaliativo sobre o requisito de *verificação*. Desta forma, ao realizar as análises com o *software Iramuteq*, foi possível observar que todas as sentenças acerca do requisito de *verificação*, estavam direcionadas com um vocábulo específico, demonstrando que as palavras da classe cinco desencadeavam sobre a classe três, sendo esta a que originou as demais classes. Sendo assim, reforçando o que as interpretações demonstraram acerca das respostas das *startups* sobre o requisito de *verificação*. Com isso, atestando para que os processos que envolvem a adaptabilidade dos métodos básicos de segurança estavam ou caminhavam para a conformidade com o que a LGPD orienta.

Na Figura 8, utilizando a análise de similitude sobre os dados referentes ao requisito de *verificação*, foi verificado que as palavras que se assemelhavam em relação ao contexto, estão divididas e separadas pelos termos que obtiveram maior ocorrência, que neste caso foram as palavras “dado”, “processo”, “banco”, “serviço”, “estar” e “gente”. É possível compreender que a palavra “dado” se refere aos dados dos usuários, contendo várias sentenças pertencentes ao mesmo contexto, como os processos de “exclusão” e “atualização”, o verbo “solicitar”, “desenvolver”, “utilizar”, “empresa”, “aplicativo” e “servidor”, onde as mesmas estão reunidas no maior conjunto desta análise concernente a *verificação*. Sendo assim, mostrando que a maioria,

cerca de aproximadamente 85% das *startups*, estava, pelo menos, analisando os processos fundamentais de segurança. Isto pode ser visto nas exemplificações com trechos das respostas dos entrevistados na seção 5.1.1.3.1.

Figura 8 – Análise de similitude - Divisão dos temas extraídos dos dados referente ao requisito de *verificação*



Fonte: Elaborado via Iramuteq (2022).

#### 5.1.1.4 Usabilidade

As perguntas **dois**, **oito e onze** tratavam a respeito do requisito de privacidade da *usabilidade*. Vale ressaltar que, além de usabilidade, as perguntas **oito e onze** também foram baseadas nos requisitos de *conformidade* e *verificação*, respectivamente. O conceito de

*usabilidade* foca nos processos de como os usuários utilizam-se dos seus dados, presentes nas plataformas das *startups*, e por quais motivos os mesmos poderiam arquitetar meios de prejudicar a privacidade de outros usuários. Dessa maneira, o objetivo desse requisito é observar a visão comportamental de como os usuários desfrutam dos dados (ANTHONY SAMY *et al.*, 2017).

Através das unidades de registro, inclusas nas unidades de contexto, neste caso a *usabilidade*, foi possível observar que dentre as sete *startups* elegíveis, seis delas, representando aproximadamente 85%, atingiram o esperado para esta categoria, sendo notório que estão cientes acerca da fácil comunicação por partes dos usuários para solicitarem alguma atualização de seus dados nas bases de dados das *startups*. Da mesma maneira, analisaram isso previamente, obtendo a ciência sobre a prontidão para atender estas requisições dos usuários, promovendo uma melhor qualidade de serviço, do mesmo modo que cumprem este requisito de privacidade, de acordo com o que a LGPD orienta. Na Tabela 7, é apresentado o que foi analisado e extraído dos dados fornecidos pelos entrevistados.

Sob outra perspectiva, apenas uma única *startup*, representando aproximadamente 15%, atingiu o percentual mínimo esperado (66,66%), demonstrando que compreende a importância de atender as solicitações dos usuários, referentes aos seus dados e da mesma maneira que é de conhecimento da mesma, a importância do mapeamento dos dados para uma eventual explicação, para compreender qual finalidade aqueles dados estão ou serão utilizados pela organização. Porém, sobre a fase de eliminação dos dados foi o ponto em que ficou mais a desejar, demonstrando novamente que a respondente também não atingiu o esperado para este quesito acerca dos processos de *verificação* referentes aos procedimentos básicos de segurança sobre os dados dos usuários.

Tabela 7 – Tabela de percentual atingido do requisito de *usabilidade*

<b>Perguntas =&gt;</b>	<b>2</b>	<b>8</b>	<b>11</b>	<b>SOMA TOTAL (%)</b>
<b><i>Startup 01</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b><i>Startup 02</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b><i>Startup 04</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b><i>Startup 06</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b><i>Startup 07</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b><i>Startup 09</i></b>	33,33%	33,33%	—	<b>66,66%</b>
<b><i>Startup 11</i></b>	33,33%	33,33%	33,33%	<b>99,99%</b>
<b>% ESPERADO</b>			<b>66,66%</b>	

Fonte: Elaborado pelo autor (2022).

Para essa categoria foi escolhido o percentual de 66,66% como sendo o valor esperado para ser alcançado, com base em que as *startups* já tinham dados de usuários ou pretendiam coletar dados. Dessa forma, compreendendo que já deveriam estar cientes, pelo menos, com este percentual acerca dos processos de *usabilidade* atendendo as solicitações dos usuários sobre os seus dados, caso estivessem, era atribuído o valor de 33,33%, sendo esse valor escolhido baseado na quantidade de perguntas, ou seja, três perguntas representava 100%, logo uma pergunta que atingia o esperado, representava 33,33% do total.

#### 5.1.1.4.1 Exemplificação com trechos dos respondentes

Os seguintes trechos são referentes às falas das seis *startups* que atingiram 85% do esperado para o requisito de *usabilidade*.

[S1]: *“Nunca aconteceu esse tipo de solicitação, mas se acontecer alguma vez, a gente consegue sim fazer, conseguimos excluir, editar ou adicionar nos nossos canais de armazenamento de dados. Então ele pode fazer tanto de forma automática, por exemplo excluir o perfil dele na plataforma ou se esses dados estiverem em algum outro ambiente, que não seja dentro da plataforma, responder algum formulário nosso, ele respondeu alguma outra coisa e que os dados estão em outro canto, ele pode solicitar isso diretamente nos nossos canais de comunicação e a gente faz esse cuidado com os dados, esse tratamento de dados. Se isso acontecer alguma vez, é super tranquilo.”*

[S2]: *“Sim, o usuário uma vez que ele tenha a devida identificação, até deixando claro que a identificação necessária para a gente não ferir a própria lei, garantindo que o usuário titular daquela informação seja o titular de fato, desde de que seja identificado, identificado com documento oficial com foto, e-mail e toda a formalização, ele tem acesso total dos dados deles e dados da produção dele, acesso total e também tem o poder dos dados deles mesmo diante da nossa base, que inclui também a exposição a terceiros, processo esse que a nossa startup não trabalha e nem vende os dados a terceiros.”*

[S4]: *“É possível fazer essa alteração, é muito importante fazer a atualização de dados e a gente até solicita cada um determinado X de meses para fazer essa atualização.”*

[S7]: *“Temos sim, é de fácil comunicação para realizar quaisquer solicitações dos usuários. Nós mesmos, por exemplo podemos apagar os dados no banco de dados, caso uma solicitação de exclusão seja pedida e não seja possível realizar via aplicativo.”*

[S11]: *“Sim, é de fácil comunicação para realizar essas operações.”*

Os seguintes trechos se referem às falas da única *startup* que atingiu 66,66% do esperado para o requisito de *usabilidade*.

[S9]: “*Eu acredito que vai existir, porque eu acho que quando a gente faz, quando a gente vai criar alguns serviços ele tem que ter um tipo de assistência ao consumidor né, ao usuário. Então é uma ponte, não deixa de ser, então acredito que quando a gente vai desenvolver isso ele tem a condição de perguntar sobre os dados dele e tenho direito de saber o que é que tá sendo fornecido.*”

[S9]: “*Não sabia disso, realmente não sabia disso. Não faço ideia de como a pessoa teria acesso para saber dessa informação, poderia ser através de algum canal de comunicação ou uma mensagem de quando ela se desvincula-se do programa poderia aparecer uma mensagem para ela.*”

#### 5.1.1.4.2 Análises com o *software Iramuteq* para o requisito de *usabilidade*

O motivo pelo qual foram utilizadas as funcionalidades de *Word cloud* e a distribuição dos verbos demarcados, observados com o *software Iramuteq* para verificar o conteúdo sobre *usabilidade*, foi por questões visuais e por melhor demonstrar que realmente as *startups* buscavam se adequar os seus recursos para atender as solicitações dos usuários. Por conta disso, é possível observar que foram utilizadas diferentes análises nesta etapa de uso do *software Iramuteq*.

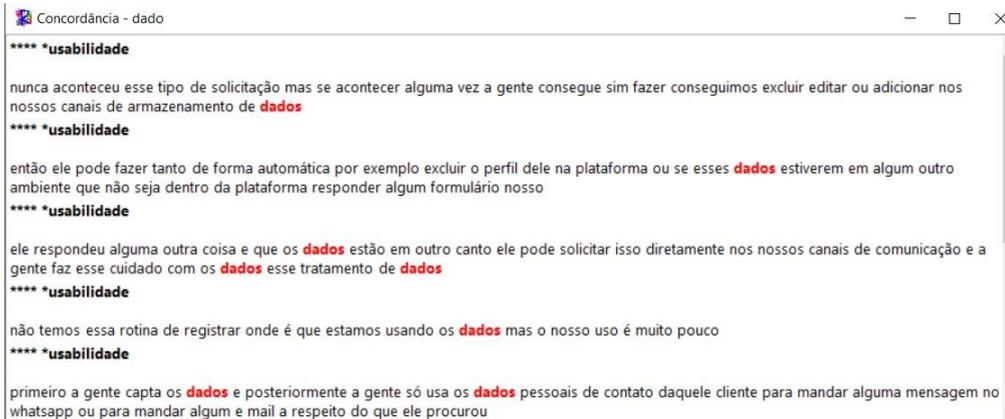
Na Figura 9, foi utilizada a funcionalidade que gera uma nuvem de palavras, do inglês, *Word Cloud*. Com essa função, é possível demonstrar de maneira visual, uma ilustração contendo uma imagem de palavras, onde suas ocorrências para um determinado contexto são demonstradas em uma relação de tamanho, conforme a quantidade de vezes que aparece no conjunto de dados. Ficando, assim, destacado quais palavras predominaram em relação às demais no aglomerado de dados coletados e submetidos à análise.

Observando a Figura 9, é possível identificar as palavras “*dado*” logo de início, sendo até previsível por ser um dos principais pontos das falas de todas as *startups*. Continuando a observar, é possível visualizar as palavras “*gente*” referindo aos colaboradores das instituições, “*cliente*”, referindo aos clientes das *startups*, “*acesso*” referindo ao fácil acesso para os usuários solicitarem as suas informações ou para verificarem alguma informação nas bases de dados das *startups*.

Através da maioria das palavras, é possível identificar uma ação para um deter-



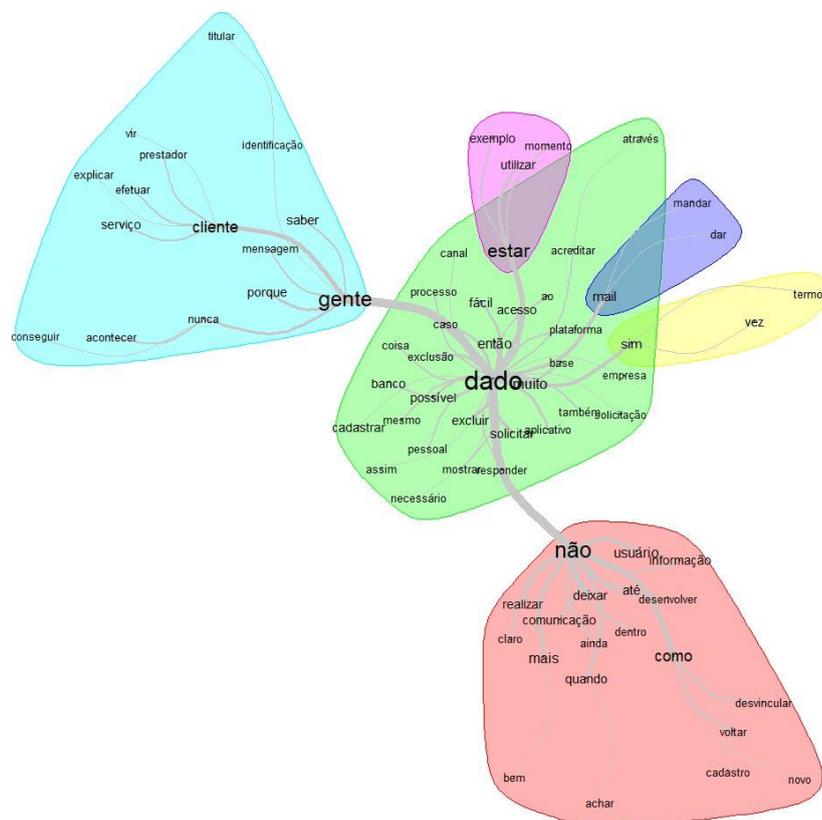
Figura 10 – Demarcações da palavra “dado”



Fonte: Elaborado via Iramuteq (2022).

Na Figura 11, é possível visualizar e compreender as interpretações discorridas anteriormente, demonstrando que, para o requisito de *usabilidade*, é de fácil compreensão e obtenção de várias interpretações, vistas através de uma perspectiva mais investigativa pelo pesquisador, como nas interpretações iniciais da seção 5.1.1.4, tanto como as análises mais profundas, utilizando o *software Iramuteq*.

Figura 11 – Análise de similitude - Divisão dos temas extraídos dos dados referente ao requisito de *usabilidade*



Fonte: Elaborado via Iramuteq (2022).

Utilizando a funcionalidade de análise de similitude, é observado novamente que as palavras “dado”, “gente”, os advérbios “não” e “sim”, o verbo “estar” de onde existem as suas ramificações de seu estado de tempo, e “mail” referente a *e-mail*, formaram os principais temas encontrados pelo *Iramuteq*.

Diante disso, é possível observar que a palavra “dado” que, para a maioria das categorias, ficou com o maior número de ocorrências, sendo extramamente plausível, pois o trabalho buscava analisar a conformidade de dados. Sendo assim, o conjunto do mesmo guarda a maioria das temáticas para o vocábulo “dado”, demonstrando que as suas ramificações estão diretamente relacionadas ao que se faz com estes dados, como “utilizar” que está contido na temática “estar”, no qual a mesma foi originada pelo conjunto de sentenças pertencentes ao agrupamento “dado”.

### 5.1.2 *Obstáculos para a conformidade*

Nesta subseção são apresentadas as principais dificuldades encontradas pelas *startups*. Dessa forma, foram selecionados pontos de melhoria podendo auxiliá-las a ficarem ainda mais adaptadas as regras que a LGPD exige.

Exclusivamente para essas análises, as perguntas treze e quatorze foram utilizadas como parâmetro informacional e informacional/conformidade, respectivamente. Compreendendo como parâmetro informacional da pergunta treze, obter uma relação entre o estado de conformidade da *startup* e a quantidade de clientes, encontrando essa informação na subseção 5.1.2.2. A pergunta quatorze é compreendida como parâmetro informacional/conformidade pois a sua utilização foi para obter as principais dificuldades de implementar a LGPD, assim, norteando também o conceito de *conformidade*, onde essa informação pode ser encontrada na subseção a seguir.

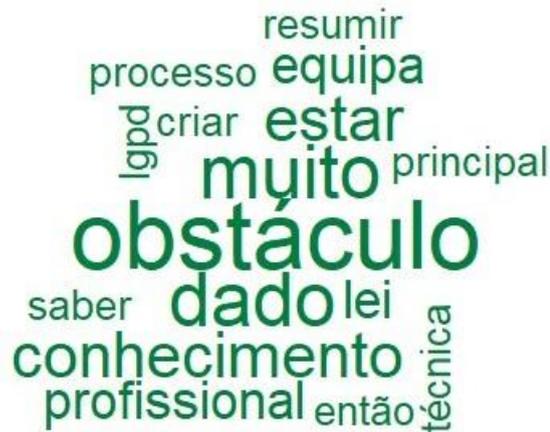
#### 5.1.2.1 *Word Cloud das principais dificuldades de implementação da LGPD*

Para que fosse possível obter uma noção acerca das dificuldades para implementar a LGPD e observando o ponto de vista das *startups*, a **pergunta quatorze** foi construída fornecendo uma visão mais peculiar sobre quais eram os principais obstáculos para se obter a conformidade com a nova lei.

A Figura 12, demonstra através de uma nuvem de palavras, quais foram os principais problemas das *startups* para iniciar a adequação com as regras da LGPD. Desta maneira, fica

claro quais os principais obstáculos para que as mesmas possam ficar o mais adaptadas às regras que a LGPD orienta e exige.

Figura 12 – *Word cloud* dos principais obstáculos para implementar a LGPD



Fonte: Elaborado via Iramuteq (2022).

Nesta perspectiva, as palavras “conhecimento”, “profissional” no que se refere a mão de obra especializada, e “saber” referindo-se a real implementação da lei, foram as sentenças que mais se mostraram relevantes. A falta de conhecimento e mão de obra especializada para pôr em prática o que a LGPD orienta, foram as principais queixas que as mesmas relataram, demonstrando que estão cientes da obrigação de implementação das regras da LGPD, porém a falta de conhecimento sobre a lei acarreta o principal obstáculo.

#### 5.1.2.2 *Relação de quantidade de clientes por startup*

A maioria das *startups* que obtiveram um resultado considerado adequado, também são as mesmas que contém o maior número de clientes em relação as demais, como exemplo as *startups* 01, 04.

Na Figura 13, é possível visualizar com detalhes a quantidade de clientes de cada *startup* e a distribuição em valores de percentual, equivalentes a cada uma sobre o total geral .

Figura 13 – Relação da quantidade de clientes das *startups*



Fonte: Elaborado pelo autor (2022).

### 5.1.2.3 Pontos de Melhorias

Os pontos de melhorias foram selecionados baseados nos principais problemas que surgiram no decorrer da pesquisa, sendo eles de algumas das *startups* elegíveis, principalmente para o requisito de *verificação* e para a compreensão da própria LGPD, visto como um dos principais obstáculos para sua implementação. Todavia, para que todas as *startups* possam melhorar as suas especificações e regras dos seus requisitos de privacidade, foram escolhidas as soluções complementares que estão listadas a seguir:

1. ABNT NBR ISO/IEC 27701 – Técnicas de segurança: Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes;
2. ABNT NBR ISO/IEC 29184:2021;
3. Certificação da ABNT para empresas que buscam adequação à LGPD;

Para o ponto um, utilizando esta norma como um guia para sanar as principais dúvidas pertinentes a compreensão do que a LGPD exige, acaba tornando-se um grande aliado para elaborar, principalmente, os processos de segurança de uma aplicação que armazena dados dos usuários.

Para o ponto dois, a norma NBR ISO/IEC 29184:2021, recentemente elaborada, no dia 25 de junho de 2021, especialmente para a LGPD, é uma boa opção para compreender ainda mais a importância da transparência dos avisos de uso dos dados dos usuários e da obtenção do seu consentimento de maneira clara, evidenciando para qual a finalidade do uso dos seus dados (BLUM, 2022).

Por fim, o ponto três engloba uma ótima opção para conseguir compreender de maneira concreta todos os processos que envolvem à adequação da LGPD, desde dos processos legislativos e englobando também os aspectos de verificação, adentrando em mecanismos de segurança relevantes para as plataformas e base de dados das *startups* (CRIPTOID, 2022). Caso surgir interesse por parte da *startup*, é necessário entrar em contato com o suporte da ABNT, enviando um e-mail para o Setor de Certificação da ABNT <sup>1</sup>, onde serão recebidas mais informações juntamente com os documentos necessários para iniciar o processo de certificação.

---

<sup>1</sup> [certificacao@abnt.org.br](mailto:certificacao@abnt.org.br)

## 6 CONSIDERAÇÕES FINAIS

Com a grande quantidade de dados pessoais contidos nas bases de dados de milhares de instituições, estar em conformidade com a LGPD é extremamente necessário para obtenção do controle, transparência e proteção dos dados pessoais, a fim de que esse grande volume de informações seja amplamente analisado e assegurado de quaisquer violações tanto por terceiros e até mesmo por descuido das próprias organizações. Outrossim, a fiscalização por parte dos órgãos competentes faz-se necessária para reforçar a necessidade da devida prevenção para com as informações obtidas através dos dados dos usuários.

O objetivo deste trabalho foi realizar uma análise de conformidade das *startups* incubadas na UFC, em relação aos requisitos de privacidade de acordo com a nova Lei Geral de Proteção de Dados (LGPD).

Foi realizado um estudo da lei e dos requisitos de privacidade sendo assim possível produzir perguntas que norteavam tanto a LGPD, como os conceitos dos requisitos de privacidade. Dessa forma, os questionamentos foram utilizados como roteiro durante as entrevistas, na etapa de coleta de dados com as *startups* e, posteriormente, como unidades de contexto para que fosse possível utilizar o método de análise de conteúdo na visão de Bardin (2011). Um resultado observado foi que dentre as sete *startups* elegíveis, cinco *startups* atingiram o nível esperado de adaptabilidade para com os requisitos de privacidade de acordo com a LGPD, ou seja, dos quatro requisitos de privacidade, que eram também as quatro categorias de análise, as mesmas atingiram o esperado de três requisitos de privacidade. Dessa forma, demonstrando que cumprem e procuram se adequar ainda mais às regras que a LGPD orienta para que as empresas possam cumprir, contribuindo para uma melhor proteção dos dados dos usuários.

Inicialmente, foi possível detectar que algumas das *startups* demonstraram impressões não verbais muito fortes, principalmente a respeito do desconhecimento de algumas informações básicas da lei, notícias sobre a LGPD e até mesmo do que seria o *Data Protection Officer* (DPO) e a sua importância. A LGPD orienta que as empresas contratem este profissional para tomar os devidos cuidados com os dados de seus usuários, com a função de garantir a conformidade com a lei, aceitando reclamações dos titulares e prestando esclarecimentos e solucionando problemas relativos aos dados dos clientes, dentre outros.

O presente trabalho igualmente o de Rojas e Medeiros (2021) e Alves e Neves (2021), levantou o mesmo ponto de obstáculo para implementar a própria lei, sendo que a dificuldade de compreensão dos termos e questões da própria LGPD, evidenciados por Rojas e Medeiros

que orienta a criação de normas de privacidade que não sejam de difícil compreensão pelos profissionais de Tecnologia da Informação (TI) mostrados, também, por Alves e Neves (2021), foram os principais obstáculos para à adequação à lei e a mesma dificuldade era levantada pela maioria das *startups* que contribuíram para a elaboração deste projeto. Diferentemente do método oferecido por Costa Júnior (2020), este projeto propôs pontos de melhoria para auxiliarem as *startups* a sanar suas dúvidas a respeito da compreensão da própria LGPD, tanto quanto informa uma norma de diretrizes e requisitos para agregarem ainda mais transparência e segurança para as aplicações que elas desenvolveriam. Desta maneira, elevando o discernimento dos processos que envolvem a proteção dos dados até o direito que as próprias *startups* dispõem para analisar a conduta errada de um determinado usuário que pretende denegrir a reputação das mesmas.

Para trabalhos futuros, pode-se verificar se há interferência do tempo de atuação das empresas que serão submetidas à análise. Nesta perspectiva, observando se o tempo de atuação é proporcional perante os resultados e se demonstra limitações durante a fase de codificação e análise dos resultados. Outra métrica que pode ser utilizada é analisar a perspectiva do usuário, através de uma coleta de dados utilizando um formulário, observando se as organizações que estão sendo submetidas a análise, estão cumprindo o esperado à respeito da prevenção dos seus dados e a respeito da prontidão para esclarecer dúvidas e principalmente sobre a transparência no uso de dados.

Espera-se que esse estudo seja uma fonte de informações para conhecimento sobre o assunto e uma forma de incentivo para que as *startups* se adequem aos requisitos de privacidade que norteiam a LGPD.

## REFERÊNCIAS

- ALVES, C.; NEVES, M. **Especificação de requisitos de privacidade em conformidade com a lgpd: resultados de um estudo de caso.** [S. l. : s.n], 2021.
- ANTHONY SAMY, P.; RASHID, A.; CHITCHYAN, R. Privacy requirements: present & future. In: IEEE. **2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS).** [S. l.], 2017. p. 13–22.
- BARDIN, L. **Análise de Conteúdo: a visão de Laurence Bardin.** Edição 70. São Paulo: [s.n], 2011. ISBN 8562938041.
- BLUM, O. **ABNT lança norma sobre avisos de privacidade e obtenção de consentimento.** [S. l. : s.n], 2022. Disponível em: <https://opiceblum.com.br/abnt-lanca-norma-sobre-avisos-de-privacidade-e-obtencao-de-consentimento/>. Acesso em 29 de jan.2022.
- BRASIL. **Lei geral de proteção de dados.** [S. l. : s.n], 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em 14 de jul.2021.
- CASSIANI, S. H. D. B.; CALIRI, M. H. L.; PELÁ, N. T. R. A teoria fundamentada nos dados como abordagem da pesquisa interpretativa. **Revista latino-americana de enfermagem, SciELO Brasil**, v. 4, p. 75–88, 1996.
- COSTA, J. E. A. **Análise de conformidade de processos de negócios em relação a lgpd.** Tese (Doutorado) – Universidade Federal de Pernambuco, 2020.
- CRIPTOID. **ABNT certifica empresas que se adequam à LGPD.** [S. l. : s.n], 2022. Disponível em: <https://cryptoid.com.br/banco-de-noticias/abnt-certifica-empresas-que-se-adequam-a-lgpd/>. Acesso em 01 de fev.2022.
- FARIAS, J. A. **Vem aí a ABNT NBR ISO/IEC 27701.** [S. l. : s.n], 2019. Disponível em: [http://www.abnt.org.br/images/Docspdf/Artigos/Artigo\\_27701.pdf](http://www.abnt.org.br/images/Docspdf/Artigos/Artigo_27701.pdf). Acesso em 20 de ago.2021.
- FERNANDES, M. A. de S.; OLIVEIRA, F. G. de; FERRAZ, F. S.; SILVA, D. A. da; CANEDO, E. D.; JR, R. T. de S. Impactos da lei de proteção de dados (lgpd) brasileira no uso da computação em nuvem. **Revista Ibérica de Sistemas e Tecnologias de Informação, Associação Ibérica de Sistemas e Tecnologias de Informacao**, n. E42, p. 374–385, 2021.
- FIGUEIRA, K. K.; HÖRBE, T. d. A. N.; VARGAS, K. d. F. S.; MACHADO, E. C.; MOURA, G. L. de. Startups: estudo do processo de abertura e gerenciamento. **Revista de Administração da Universidade Federal de Santa Maria**, v. 10, p. 56–71, 2017.
- GENERAL. **Data Protection Regulation: A versão em português (de português).** [S. l. : s.n], 2019. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 03 de ago.2021.
- INOVAÇÃO, C. de Empreendedorismo e. **Programa Empreende UFC.** [S. l. : s.n], 2020. Disponível em: <https://condominio.ufc.br/programaempreendeufc/>. Acesso em 22 de dez.2021.
- IRAMUTEQ, C. G. **Logiciel d’analyse Iramuteq.** [S. l. : s.n], 2022. Disponível em: <http://www.iramuteq.org/>. Acesso em 20 de dez.2021.

KALLONIATIS, C.; KAVAKLI, E.; GRITZALIS, S. Addressing privacy requirements in system design: the pris method. **Requirements Engineering**, Springer, v. 13, n. 3, p. 241–255, 2008.

MIRANDA, M. G. **Lei Geral de Proteção de Dados-LGPD**. [S. l: s.n], 2019.

RIES, E. **A Startup Enxuta**. São Paulo: Leya, 2012. 275 p.

ROJAS, M. A. T.; MEDEIROS, J. K. Avaliação da adequação de instituto federal à lei geral de proteção de dados pessoais. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, [S. l], v. 1, n. 13, 2021.

VIA CARREIRA . **O que é análise de Conteúdo?** Veja o passo a passo do método. [S. l], 2021. Disponível em: <https://viacarreira.com/analise-de-conteudo/>. Acesso em: 18 de jan.2022.

## APÊNDICE A – QUESTIONÁRIO UTILIZADO COMO ROTEIRO DURANTE AS ENTREVISTAS

**Questão 1.** O conceito de "Privacy by Design" está diretamente ligado a LGPD mesmo que não esteja transcrito propriamente na Lei. O termo "Privacy by Design" se refere a idéia de proteger a privacidade do usuários desde a concepção de qualquer sistema de tecnologia da informação ou prática de negócio, ou seja, para essa metodologia a proteção da privacidade seria o ponto de partida para o desenvolvimento de qualquer projeto, sendo incorporada à própria arquitetura técnica dos produtos ou serviços, e, principalmente, incorporada a um padrão de operação da própria organização. Dessa maneira, como a instituição encara essa mudança da metodologia do ponto de vista da concepção do seu produto/serviço?

**Questão 2.** É possível os titulares poderem solicitar uma atualização, exclusão ou consulta de informações pessoais das bases de dados da instituição, desde que estejam de acordo com as regras de utilidade dos serviços ou softwares da empresa e que não seja impedimento para a integridade da instituição?

**Questão 3.** A instituição tem ou está elaborando um relatório informacional para os titulares dos dados, mostrando que os seus dados passarão por algum processamento de utilidade da organização?

**Questão 4.** Existe um modelo de comunicação para informar aos titulares que os seus dados serão ou poderão ser manipulados por terceiros, sem que haja qualquer prejuízo para os mesmos? Justifique a resposta para quaisquer hipóteses.

**Questão 5.** De acordo com LGPD no seu artigo 41, o controlador deverá indicar o encarregado pelo tratamento de dados pessoais, denominado como DPO (Data Protection Officer). Vocês tem previsão de contratar alguém para esse cargo ou há um processo de busca por um profissional para o cargo? Conforme noticiado pelo site Olhar Digital, a Autoridade Nacional de Proteção de Dados (ANPD) abriu uma consulta pública para que fossem revistas algumas regras para startups e pequenas empresas a respeito da obrigatoriedade do DPO para as mesmas. Com a dispensa do cargo, seria necessário a criação de um canal de comunicação entre os titulares dos dados. Nesse sentido, a elaboração desse canal está sendo analisada ou já estava sendo posto em prática?

**Link:** <<https://olhardigital.com.br/2021/08/31/pro/andp-dispensa-dpo-startups-mpes/>>

**Questão 6.** Para que os profissionais de desenvolvimento de software da empresa esteja cientes dos principais requisitos de privacidade que a LGPD orienta, foi iniciado um plano de conscien-

tização para que os mesmos estejam preparados para o desenvolvimento baseado na privacidade dos dados, assim como o conceito de "Privacy by Design" estabelece e que norteia a LGPD?

**Questão 7.** A instituição tem um processo de verificação de atualizações dos softwares do banco de dados para que não se tornem obsoletos, ocasionando problemas de segurança? Justifique a resposta para quaisquer hipóteses.

**Questão 8.** A instituição tem mapeado os dados pessoais utilizados, e tem também registrado onde e como eles estão armazenados e utilizados? Aplica as medidas de proteção adequadas?

**Questão 9.** A instituição tem estruturado um plano de contingência para possíveis vazamentos de dados pessoais? Justifique a resposta para quaisquer hipóteses.

**Questão 10.** O princípio de minimização no regulamento europeu e o princípio da necessidade estabelecido pela LGPD no artigo 6º inciso III, caracteriza-se pela coleta mínima de dados dos titulares afim de que os dados coletados sejam somente utilizados para satisfazer a necessidade da situação ou seja não coletar dados que estejam muito divergentes das demais informações coletadas. Dessa forma, como a startup, dentro dos limites de suas competências legais, implementou ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais, para atingir a finalidade legal desejada?

**Questão 11.** No artigo 16 da LGPD informa a fase de eliminação após o término do tratamento dos dados pessoais. Mediante isto, como a instituição protocola a eliminação dos dados para que o titular esteja ciente da real exclusão das informações?

**Questão 12.** A instituição designou uma equipe que realizará o monitoramento das vulnerabilidades técnicas dos mecanismos que tratam os dados pessoais?

**Questão 13.** Qual a quantidade em média de clientes que a startup possui?

**Questão 14.** Quais os principais obstáculos para implementar a LGPD?

## APÊNDICE B – CARTA CONVITE ENVIADA PARA AS STARTUPS

Figura 14 – Carta convite para participação de Entrevista



### Convite para realização de uma entrevista acadêmica

**Prezada Startup,**

Me chamo Davi Oliveira e sou graduando em Redes de Computadores pela Universidade Federal do Ceará (UFC) no campus de Quixadá.

Estou realizando uma análise qualitativa para o meu TCC que tem por tema: "Análise da conformidade dos requisitos de privacidade das startups incubas na UFC de acordo com a LGPD".

O meu principal objetivo é avaliar como as startups estão encarando e adaptando os requisitos de privacidade a Lei Geral de Proteção de Dados. Com os resultados da pesquisa será elaborado um informativo contendo propostas de pontos de melhorias, auxiliando a instituição o máximo possível dentro de sua realidade a ficar em conformidade a LGPD.

Portanto, preciso realizar uma entrevista para verificar como a startup está encarando essas mudanças e se estão atentas para a importância da conformidade para a prevenção dos dados pessoais dos clientes/usuários que compõe a sua carteira de clientes. Dessa maneira, venho convidar a startup para participar desta pesquisa e assim contribuir para a elaboração e conclusão do meu trabalho.

Como o intuito do trabalho será apenas para fins acadêmicos nenhum dado confidencial que comprometa a instituição será divulgado, principalmente o **nome da instituição não será divulgado, apenas o seu ramo de atuação.**

Desde já agradeço o aceite dessa solicitação e fico imensamente grato pela contribuição acadêmica que a startup contribuirá.

Atenciosamente,

**Davi Oliveira**

