Computação em nuvem – Um estudo empírico exploratório sobre as determinantes da preocupação com a proteção de dados.

José Filipe da Silva Guimarães Arade de Macedo

Dissertação de Mestrado

Mestrado em Assessoria e Administração

Porto - 2015

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTUTITO POLITÉCNICO DO PORTO

Computação em nuvem – Um estudo empírico exploratório sobre as determinantes da preocupação com a proteção de dados.

José Filipe da Silva Guimarães Arade de Macedo

Dissertação de Mestrado apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Assessoria e Administração, sobre orientação de Mestre Paulo Gonçalves e Doutora Anabela Mesquita.

Esta versão contém as críticas e sugestões dos elementos do júri

Porto - 2015

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

Resumo

Objetivo – O objetivo geral deste trabalho, é a medição da influência de várias variáveis sobre a preocupação do consumidor para com a proteção dos seus dados, concretamente, segurança e a privacidade destes.

Metodologia – Realizou-se um estudo empírico em Portugal, de cariz exploratório, tendo-se recorrido a um instrumento de medida adequado, ao qual, se conseguiu obter uma amostra válida de 255 respondentes. Para além da normal caracterização da amostra, realizou-se uma análise descritiva dos resultados, bem como, uma análise de inferência estatística, a qual, permitiu testar hipóteses e um modelo teórico. Estas hipóteses foram testadas através da correlação de *Spearman*.

Resultados - Os resultados obtidos permitem confirmar que a atitude do consumidor e a sua preocupação com a proteção dos seus dados é, de facto, influenciada por determinadas variáveis, concretamente, a preocupação com as limitações da tecnologia *cloud*, o nível de confiança para com o fornecedor de serviços e a importância dos direitos de proteção de dados pessoais. Conseguiu-se validar um modelo fatorial explicativo da influência destas variáveis sobre a preocupação com a utilização indevida de dados.

Limitações/implicações – Os resultados obtidos carecem de ser analisados com toda a precaução, não podendo ser objeto de generalização, dado ter sido utilizada uma amostra de conveniência. O facto de esta não ter sido estratificada, a nível nacional, exige, tambem, precaução na análise de resultados obtidos. A ausência de trabalhos e estudos homólogos teve algumas implicações na discussão dos resultados. Este estudo suscita a existência de implicações teóricas, académicas e praticas empresariais.

Originalidade/valor – Este estudo constitui um tema atual e relevante, a nível académico, social e empresarial, onde ainda existe uma escassez de literatura e trabalhos, especialmente, em Portugal. Neste trabalho conseguiu-se conceber um modelo teórico que permitiu analisar interessantes relações entre os constructos utilizados, sobretudo, sobre o nível de preocupação, do utilizador da *cloud*.

Palavras-chave:

Computação em Nuvem; Privacidade e Segurança; Riscos e Benefícios; Modelo

Abstract

Purpose – The general purpose of this work was to measure the influence of various variables over the consumer's concern about the protection of his data, specifically, their security and privacy.

Methodology – We carried out an empirical study in Portugal, exploratory in nature, with recourse to an appropriate measurement instrument, which enabled the attainment of a valid sample of 255 respondents. Apart from the normal sample characterization, we carried out a descriptive analysis of the results as well as an analysis of statistical inference, which allowed for hypotheses testing and a theoretical model. These hypotheses were tested by *Spearman* correlation.

Results – The obtained results confirm that the consumer's attitude and its concern about the protection of his data is in fact influenced by certain variables, in particular, concern about the limitations of cloud technology, the level of trust towards the service provider and the importance of personal data protection rights. We were able to validate an explanatory factorial model of the influence of these variables over the concern about the misuse of data.

Limitations/implications – The results require cautioned analysis and can't be generalized, as a convenience sample was used. The fact that this sample hasn't been stratified, at national level, also calls for caution in the analysis of the obtained results. The lack of similar work and studies had some implications in the discussion of results. This study raises the existence of theoretical, academic and business practices implications.

Originality/value – This study constitutes a current and relevant issue at an academic, social and business level, where there is still a shortage of literature and work, especially in Portugal. In this work it was possible to design a theoretical model that allowed us to analyze interesting relationships between the used constructs, mainly, about the level of concern of a *cloud* user.

Key words:

Computação em Nuvem; Privacidade e Segurança; Riscos e Benefícios; Modelo

Agradecimentos

À minha família, por terem possibilitado e acreditado neste meu percurso, bem como, pela motivação prestada em todos os momentos.

Aos professores, orientadores, Mestre Paulo Gonçalves e Doutora Anabela Sarmento, por todo o apoio, instrução e disponibilidade.

Aos restantes professores e colegas de Mestrado, pela influência que tiveram no meu desenvolvimento pessoal e académico.

Por fim, uma palavra de apreço para todos os que contribuíram para esta investigação, em especial, as pessoas que ajudaram no pré teste do questionário e aquelas que responderam a este.

Lista de Abreviaturas

AICPA	*American Institute of Certified Public Accountants*
API	*Application Programing Interface*
ARPANET	*Advanced Research Projects Agency Network*
AWS	*Amazon Web Services*
CEO	*Chief Executive Officer*
CICA	*Canadian Institute of Chartered Accountants*
CRM	*Costumer Relationship Management*
CSA	*Cloud Security Alliance*
DDoS	*Distributed Denial of Service*
DGEEC	Direção Geral de Estatísticas da Educação e Ciência
DGES	Direção Geral do Ensino Superior
DoS	*Denial of Service*
EC2	*Elastic Compute Cloud*
EUA	Estados Unidos da America
GAPP	*Generally Accepted Privacy Principles*
IaaS	*Infrastructure as a Service*
ICO	*Information Comissioners Office*
IoT	*Internet of Things*
ISACA	*Information Systems Audit and Control Association*
ISP	*Internet Service Provider*
KMO	*Kaiser-Meyer-Olkin*
NIST	*National Institute of Standards and Technology*

OS	*Operating System*
PaaS	*Platform as a Service*
PC	*Personal Computer*
S3	*Simple Storage Service*
SaaS	*Software as a Service*
SLA	*Service Level Agreement*
SPSS	*Statistical Package for the Social Science*
TAM	*Technology Acceptance Model*
TI	*Tecnologias de Informação*
UE	União Europeia

Índice

PARTE II

ESTUDO EMPÍRICO

Índice de Tabelas

Índice de Figuras

Introdução

Contextualização

A ideia de computação em nuvem nasce nos anos 60, com Joseph Carl Robnett Licklider e a sua conceptualização de *Intergalactic Computer Network*, a qual, aparece pela primeira vez num memorando enviado aos seus colegas (Licklider, 1963). Um pouco mais tarde, em 1969, Licklider é responsável por possibilitar o desenvolvimento do projeto ARPANET[1], que vinha como que dar forma à sua visão sobre a possibilidade de todas as pessoas no mundo estarem interconectadas e poderem aceder a programas e informação em qualquer sítio, a partir de qualquer local.

A partir de 2000 há um grande impulso da tecnologia *cloud*, pelo simples facto de que as empresas se aperceberem que "as suas maiores aquisições em TI estavam regularmente paradas e só eram totalmente aproveitadas em picos de necessidade . . . o que fez com que investigadores começassem a questionar-se como melhor alavancar este latente poder de processamento" (Halpert, 2011, p. 2).

Assim, foi apenas uma questão de tempo, evolução tecnológica e a aposta das empresas, como a Salesforce, Amazon, IBM, Eucalyptos, Microsoft e Google, para que a tecnologia *cloud* fosse evoluindo e sendo implementada.

Surge, então, agora, a "computação em nuvem", como um "novo" termo no mundo das tecnologias, assinalando o advento de um novo paradigma de computação (Vaquero, Rodero-Merino, Caceres & Lindner, 2009).

É a nova geração de computação e, quem sabe, aquela que venha mudar o mundo, para um onde todos os utilizadores possam ter tudo que precisam na nuvem. É o natural próximo passo na evolução tecnológica, como um serviço *on-demand*[2]. No entanto, não é uma tecnologia perfeita e livre de riscos, tal como não é algo que apareceu agora, existindo desde a invenção do *e-mail* (Mirzaei, 2008).

A computação em nuvem é o termo que descreve, tanto a plataforma, como o tipo de aplicação. Como plataforma, ela fornece, configura e reconfigura servidores, sejam eles máquinas físicas ou virtuais. Como tipo de aplicação, descreve aplicações que são disponibilizadas através da internet, pelos enormes centros de dados e os seus servidores, que são utilizados para alojar, processar, executar e disponibilizar tais aplicações, dados e serviços (Boss, Malladi, Quan, Legregni & Hall, 2007)

A *cloud* é uma metáfora para a internet e é a abstração de uma complexa infraestrutura. Esta tecnologia difere e sobrepõem-se, ao tradicional paradigma de computação, pela sua

[1] *Advanced Reseach Projects Agency Network* (ARPANET) - Projeto do Departamento de Defesa dos Estados Unidos da América – Primeira rede com comutação de pacotes de dados – Percursor da internet.
[2] Algo disponível a pedido, a qualquer momento.

escalabilidade, abstração, economias de escala e serviços dinamicamente configuráveis (Foster, Zhao, Raicu, Lu, 2008).

Uma explicação da *cloud*, em termos simples, pode ser dada como um conjunto de recursos computacionais que são disponibilizados e rapidamente acedidos, através da internet, estando sempre disponíveis para uso. Recursos esses que pertencem a um fornecedor de serviços, que os agrupa numa enorme coleção de recursos para servir todos os utilizadores, sendo aqueles são automática e rapidamente configurados e disponibilizados ao consumidor, de forma mensurada e de acordo com o que este necessita a todo o momento, fazendo com que nunca falte poder de computação ao utilizador, mas, também, com que existam sempre recursos disponíveis para os outros utilizadores (Kok, 2010).

Esta tecnologia possibilita aplicações e serviços, desde o "antigo" *e-mail*, às dominantes redes sociais e, ainda, mais recentemente, soluções de produtividade *online,* como o Office 365, serviços de conteúdo multimédia como Netflix, Youtube ou Twitch ou, mesmo, tecnologia de jogos, por *streaming,* como é o caso do serviço Nvidia Grid, ou o caso da consola Xbox One, que já tem a correr jogos em que grande parte das tarefas computacionais mais exaustivas, são executadas na sua *cloud,* ao invés de na consola do consumidor.

No entanto, apesar dos seus benefícios, a tecnologia de computação em nuvem tem os seus desafios e problemas, com questões de segurança e privacidade servindo de "bandeira" a esses desafios. Numa entrevista cedida e apresentada no trabalho de Martinez (2013), o Diretor da EuroCloud, Andreas Weiss, aponta a enorme importância de segurança e privacidade de dados.

É neste contexto que se insere este estudo, em especial, na análise das questões de segurança e privacidade da tecnologia *cloud*. Como vamos ver, os conceitos de segurança e privacidade são, tanto de foro psicológico, como de natureza física, real e inerente ao funcionamento da tecnologia. Tendo isto em conta, analisa-se e caracterizar-se-á a tecnologia, sendo abordados, também, o conceito de confiança, também ele de foro psicológico e o modelo de aceitação de tecnologia (TAM). Tentar-se-á ver como eles se ligam, com o objetivo de perceber se e como é influenciada a preocupação com proteção/utilização de dados.

Questão de investigação

Numa comunicação de imprensa, da Gartner (2008), esta sumariza bem a realidade que se espera abordar, parcialmente, neste trabalho, transmitindo a ideia que, nos últimos anos, tem havido muito interesse à volta da tecnologia *cloud computing,* aludindo ainda ao facto que, embora se perceba grandes vantagens nesta tecnologia, ainda existem alguns bloqueios à sua adoção.

Alguns autores, como Chen e Zhao (2012) e Loganayagi e Sujatha (2011), complementam e atualizam a ideia supramencionada, referindo que a *cloud* não só veio para ficar, como é a percursora da próxima revolução das tecnologias de informação (TI). Referem ainda que os referidos bloqueios decorrem, entre outros, de preocupações com a segurança e a privacidade, defendendo, também, que os utilizadores devem compreender o funcionamento da tecnologia, o tratamento e a utilização dos seus dados.

O que acaba de ser referido, bem como o que será abordado ao longo deste trabalho, apontam à inegável realidade que a computação em nuvem tem e terá, cada vez mais, um papel preponderante no mundo, seja a nível empresarial ou pessoal. Ora, isto que significa duas coisas. A nível empresarial, uma entidade vai ter que perceber que se não adotar a *cloud* vai ficar para trás e, portanto, tem que estar preparada. A nível pessoal, um indivíduo tem que compreender que seja a nível pessoal, ou a nível laboral, mais cedo ou mais tarde, terá que tomar decisões e, um indivíduo, encontrará a necessidade de utilizar uma solução *cloud,* ou mesmo, a necessidade de avaliar e decidir a adoção e utilização desta a nível laboral.

Neste sentido, é útil verificar se proteção de dados (leia-se segurança e privacidade de dados) é de facto uma preocupação e de que forma pode ser influenciado. Para esta finalidade, definiu-se, como questão geral de investigação a pergunta: será que, nas tecnologias de computação em nuvem, existe alguma relação entre as perceções de segurança, privacidade, conhecimento, confiança e frequência de utilização da tecnologia, que permita antever ou justificar o nível de preocupação, do consumidor, para com a proteção dos seus dados?

Motivação e objetivos

Este trabalho não tem como objetivo abordar este tema de uma perspetiva puramente tecnológica. Não aborda sistemas, infraestrutura ou arquitetura da tecnologia. Não é estudada regulamentação ou casos de estudo e, também, não focará a perspetiva ou modelos de negócio. Aproveitar-se-á de informação relevante, a qual, pode ser mencionada, mas, apenas o necessário para o fluir do trabalho.

Esta dissertação atenta uma objetiva para o utilizador final, o consumidor, embora, seja levemente abordado e algumas vezes mencionados os diferentes papéis de fornecedor, integrador e consumidor. Mais uma vez, tal é feito de forma sucinta e almeja, unicamente, a transmissão de uma imagem mais completa.

Esta dissertação aponta ser um documento informativo, para uma capaz e controlada utilização da tecnologia de computação em nuvem, desenrolando uma investigação com o objetivo geral de medir a influência de várias variáveis sobre a preocupação com questões de segurança e privacidade, no fundo, a preocupação com a proteção de dados.

De acordo com este objetivo, tentar-se-á medir, ainda, um conjunto de fenómenos que permitam delimitar o conceito e campo de estudo, propondo-se para isso as seguintes questões e objetivos:

- descrever a tecnologia de computação em nuvem, bem como, os seus benefícios e desafios;
- abordar conceitos de ligação, como confiança e modelos de aceitação de tecnologias;
- identificar o nível de conhecimento e utilização da tecnologia;
- identificar as principais perceções do consumidor, relativamente à tecnologia;
- identificar se a preocupação com segurança e privacidade de dados é real;
- identificar fatores que influenciem a preocupação com a proteção de dados;

Quanto à motivação em si, existe uma grande vontade de adquirir e criar conhecimentos nesta área. Esta tecnologia vai continuar a evoluir e o seu alcance e predominância vão aumentar, o que significa e, por isso, acredita-se na necessidade de uma melhor compreensão da tecnologia, para uma melhor utilização e evolução da mesma. Assim, a motivação passa por uma tentativa do aumento de conhecimento sobre a tecnologia e sobre os seus utilizadores, esperando-se contribuir para uma evolução, maturação, de ambos. Já do ponto de vista "meramente" académico, a motivação é simples, sendo ela a vontade de criar e expandir conhecimentos.

Metodologia de investigação

Será realizada uma extensiva investigação secundária, utilizando como fontes secundárias, artigos, dissertações, teses, bem como, publicações, *white papers*, e relatórios da indústria e resultante de conferências. Este trabalho traduz uma pesquisa exploratória ou explicativa e descritiva, pretendendo-se uma revisão de literatura capaz de fornecer um enquadramento ao tema, definição de objetivos e definição de metodologia de investigação.

No que diz respeito à anteriormente especificada metodologia de investigação, embora, esta seja abordada no seu devido capítulo, podemos avançar que se optou por uma abordagem empírica quantitativa, por forma a medir-se fenómenos passíveis de análise estatística. Com o objetivo de recolher ainda dados primários, o instrumento escolhido foi um questionário.

Este instrumento seria utilizado para tratamentos estatístico, incluindo, o teste de hipóteses que permitisse responder à questão geral de investigação supramencionada, em, questão de investigação.

Importância do estudo

Utilizando a ferramenta *Google Trends* (2015a; 2015b), observamos que o interesse no tópico de *cloud computing* despoletou em 2007 e 2008, tendo atingido o seu expoente máximo, relativamente à pesquisa de computação em nuvem como indústria, nos anos de 2014 e 2015 (*Google Trends*, 2015a).

Recorrendo à ferramenta *Microsoft Bing Academic Search* encontramos informação congruente. Pode-se observar que é em 2008 que o número de publicações e citações, sobre *cloud computing*, começam a crescer notoriamente face à norma.

Procurando conhecer a importância da tecnologia de modo mais concreto, aproveitamos alguns valores e previsões da Gartner. Em 2008 a Gartner já previa que computação em nuvem se tornasse "tão influente como o negócio eletrónico" (Gartner[3], 2008), prevendo mais tarde, em 2016, que "o crescimento de computação aumentará, ao ponto de se tornar a maior parte dos gastos em novas TI" (Gartner[4], 2013). Para 2015, prevê que os gastos com TI's e respetivos dispositivos vão aumentar cerca de 2,4% em 2015, atingindo gastos na ordem dos $3,8 triliões. Desta que este aumento se deve grande parte à "adoção de serviços *cloud*" (Gartner[5], 2015c), um crescimento na ordem das centenas de milhares de milhões de dólares.

Tornando ainda mais concreto o crescimento previsto para esta tecnologia, a Sungardas (2014, p. 2) publica mais um estudo da Gartner, onde esta prevê para o período de 2013/2016 uma taxa de crescimento anual de 19,5% para a adoção de serviços de SaaS[6], 27,7% para PaaS[7], 41,3% para IaaS[8] e de 22% para serviços de segurança.

Conforme será mencionado mais à frente, a computação em nuvem começou por ser utilizada em algo tão simples como o correio eletrónico (*e-mail*) e hoje em dia, temos as redes sociais, aplicações de comunicação e serviços de armazenamento completamente proliferadas e como a face mais visível da *cloud*, contudo, estes não são os estágios ou aplicações finais de computação em nuvem.

A verdade é que, segundo um estudo realizado pela Evans Data Corporation, citado e abordado num artigo da Forbes, por Columbus (2015), a *cloud* já domina e vai dominar, cada vez mais, o desenvolvimento da *Internet of Things* [9] (IoT), a qual, é tida como a próxima grande "explosão" na área tecnológica. Esta realidade é fácil de imaginar. Obviamente, temos os telemóveis e os computadores, mas, já temos outros grandes exemplos a serem introduzidos, como as televisões

[3] http://www.gartner.com/newsroom/id/707508
[4] http://www.gartner.com/newsroom/id/2613015
[5] http://www.gartner.com/newsroom/id/2959717
[6] *Software* como um serviço (*Software as a Service* – SaaS)
[7] Plataforma como um serviço (*Platforma as a Service* – PaaS)
[8] Infraestrutura como um serviço (*Infrasctructure as a Service*)
[9] *Internet of Things*: "Proposto desenvolvimento da internet, em que, objetos do quotidiano têm capacidades de conectividade de rede, permitindo-lhes o envio e receção de dados" (Oxford Dictionaries, 2014)

e os eletrodomésticos inteligentes, ou, mais concretamente, os já existentes *smartwatches* dentro dos *wearables*, as crescentes soluções automóveis, como o caso da Tesla, Apple e da Microsoft e a empresa NEST adquirida pela Google, agora parte da Alphabet, que transforma produtos banais, como um detetor de fumo ou alarmes, em aparelhos capazes de aprender e adaptar-se, mantendo uma constante ligação à internet. Este tipo de conectividade gera enormes quantidades de dados e a "computação em nuvem fornece a solução *back-end* para o processamento e computação destes enormes fluxos de dados" (Chao, 2011, p. 1).

Utilizando as palavras da Vice-presidente da Comissão Europeia e responsável pela Agenda Digital Europeia, Neelie Kroes (2014), "a próxima fase da internet será centrada em dados e impulsionada e dirigida pela conetividade. Computação em nuvem*, big data*[10]*, the internet of thing*s . . . para dar o salto de fé para este novo mundo, fiabilidade e confiança são pré-requisitos. Mas, quando nem o telefone da chanceler é sagrado, essa confiança nunca mais pode ser tida como garantia . . . para biliões em todo o mundo, essa confiança está agora perdida.". O que serve como uma boa transição para a resposta da importância deste estudo.

É inegável a importância desta tecnologia. Tal como é inegável a relevância e atualidade deste tema, seja de um ponto de vista pessoal, laboral, empresarial ou académico.

Respondendo à questão, sobre a importância, de um ponto de vista académico, a verdade é que, os trabalhos semelhantes que existem são quase exclusivamente de natureza puramente técnica, orientados à vertente empresarial e com estudos de análise descritiva simples. Outros, são extremamente focados numa única vertente ou aplicação da tecnologia, "sofrendo" da mesma simplicidade de estudo. Isto significa que existe uma limitação e lacunas nesta área de conhecimentos.

Este estudo genérico da tecnologia, de natureza não técnica, focado mais no lado do consumidor final, procura analisar as vertentes de privacidade e segurança, utilizando uma análise mais completa, perante uma clara lacuna de literatura e estudo em geral e, no caso nacional, em particular. Deste modo, procuramos contribuir, assim, para o estender do conhecimento existente nesta área e contexto português.

Organização do documento

Esta dissertação é composta por uma introdução geral e sete capítulos que serão divididos em três partes, cada uma com os seus respetivos capítulos. Está em causa estabelecer uma estrutura "para responder à exigência de clareza da exposição" e que "conterá os seguintes elementos" (Correia e Mesquita, 2013, p. 12): a) Introdução/enunciado do problema; b) revisão

[10] Big Data: "Ativos de informação de alto volume, alta velocidade e de alta variedade, que exigem formas inovadoras e de baixo custo de processamento de informação" (Gartner, 2015b)

de literatura; c) metodologia do estudo; d) apresentação e análise dos resultados do estudo; e) conclusões, recomendações e propostas de trabalho futuro;

Na introdução geral, será contextualizado o tema em estudo, apresentando a motivação e a importância do estudo, bem como, a questão geral de investigação e objetivos do mesmo.

No primeiro capítulo faz-se a revisão de literatura, relativa à definição da tecnologia *cloud*. Concretamente, abordar-se-á a história de como surge e se sedimenta a tecnologia, a definição da tecnologia e a caracterização da mesma (i.e., características chave, modelos de serviço e modelos de implementação).

No segundo capítulo faz-se uma revisão de literatura, onde se introduz as características da tecnologia que a distinguem, positivamente, das demais, funcionando como impulsionadores da sua adoção. Ou seja, abordar-se-á os benefícios da tecnologia de um ponto de vista concreto e técnico, embora de forma básica, servindo como complemento ao capítulo um para uma compreensão da tecnologia.

No terceiro capítulo faz-se uma revisão de literatura, onde serão introduzidos aquelas que são tidas como os principais inconvenientes, desvantagens ou limites da tecnologia. Esta introdução será feita de forma e com intuito semelhante à do capítulo dois.

No quarto capítulo terminamos a revisão de literatura. Após se obter, nos primeiros três capítulos, uma noção da tecnologia de computação em nuvem e o seu funcionamento, parte-se agora para o "afunilar" do tema e para as questões, sobre as quais se desenvolverá o estudo empírico. Neste capítulo, serão abordadas e apontadas, de forma concreta, as questões que ameaçam a privacidade e segurança dos nossos dados no ambiente *cloud*, bem como, conceitos importantes, como confiança e o modelo de adoção de tecnologias.

No quinto capítulo entramos na parte do estudo empírico, onde é descrita a metodologia de investigação, o que significa a apresentação da formulação de hipóteses, o tipo de pesquisa, a amostra e a construção do instrumento de recolha de dados primários, bem como, as técnicas de análise de dados que foram utilizadas.

No sexto capítulo apresentam-se e analisam-se os resultados obtidos. Caracteriza-se a amostra, analisa-se a validade fatorial e analisa-se a fiabilidade e consistência interna das escalas propostas. É, ainda, feita uma análise descritiva e de inferência estatística dos resultados, onde se apresenta a comprovação, ou não, das hipóteses formuladas e, por fim, apresenta-se o modelo obtido procura explicar os fatores que influenciam a preocupação com a proteção dos nossos dados.

No sétimo capítulo são apresentadas as conclusões deste estudo, o que se conseguiu comprovar, possíveis implicações, bem como, as apresentadas propostas e ideias para investigações futuras relativas a este tema.

Na figura 1 pode-se observar a estrutura do presente trabalho.

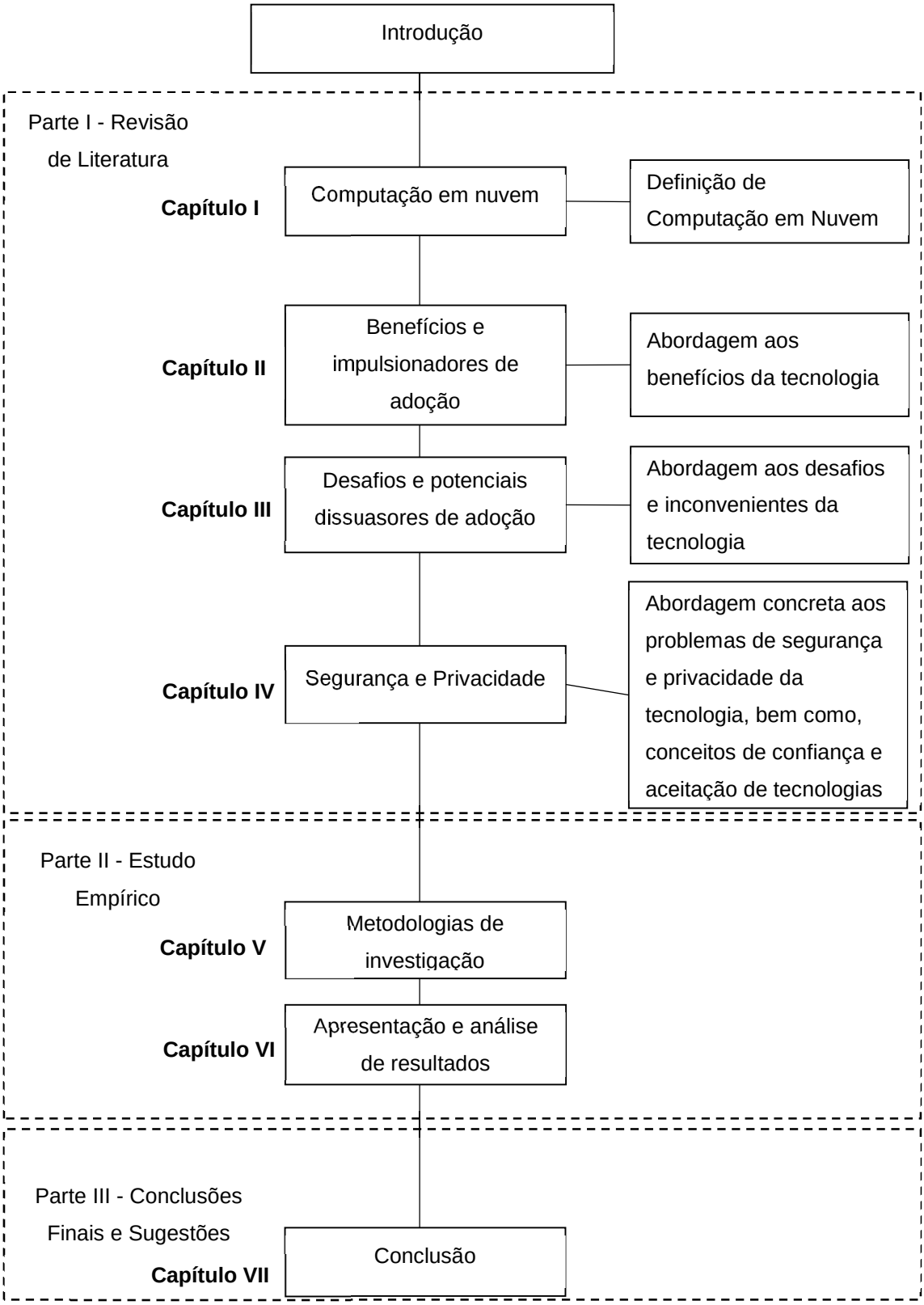

Figura 1 – Estrutura e organização do documento.

Fonte: elaboração própria.

Capítulo I – Computação em nuvem

1.1 - Introdução

Neste capítulo apresenta-se um enquadramento teórico essencial para a compreensão da restante revisão de literatura e estudo, fornecendo-se a compreensão básica do funcionamento da tecnologia de computação em nuvem.

Este capítulo começa com a introdução à definição, mais aceite e abrangente, da tecnologia. Posteriormente, expande-se o estudo dessa definição, abordando os seus conteúdos. Assim, são analisadas as principais características da computação em nuvem, bem como, os seus modelos de fornecimento de serviço e modelos de implementação.

No final do capítulo, é apresentada uma conclusão, sob a forma de sumula e esquematização daquilo que foi abordado servindo também como breve ligação ao capítulo seguinte.

1.2 - Definição *cloud*

Tentar apresentar uma definição completamente abrangente, para o termo *cloud computing (*computação em nuvem*),* parece ser algo impossível. Isto, porque esta será sempre moldada pelas características da área de ação, *software*, serviço e plataformas onde e por quem esta tecnologia é utilizada. Ao mesmo tempo, a tecnologia computação em nuvem continua a evoluir, por si só, e através de novas aplicações que continuam a surgir. No entanto, constatamos que a definição mais utilizada e aceite é aquela que é fornecida pelo *National Institute of Standards and Technology* (NIST). Sendo a conceção base mais, generalizadamente, aceite, é dela que este trabalho vai partir.

O NIST define *cloud computing* como "um modelo que possibilita o acesso por rede, de forma ubíqua, conveniente e sob pedido, a um conjunto partilhado de recursos computacionais configuráveis (e.g. redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente providos e libertados, com mínimo esforço de gestão e interação com o fornecedor de serviço. Este modelo *cloud* é composto por cinco características essenciais, três modelos de serviços e quatro modelos de implementação.” (Mell & Grance, 2011, p. 2).

Continuando sob a definição de computação em nuvem de Mell & Grance (2011, pp. 2-4), apresenta-se de seguida as características chave, os modelos de serviço e os modelos de implementação *cloud.*

1.2.1 - Características chave

Os autores supramencionados definem cinco principais características, que refletem o funcionamento da tecnologia e que irão refletir as suas vantagens e desafios. Assim, as características são as que se seguem.

Auto-serviço *on-demand* - O consumidor pode, unilateralmente e sem qualquer tipo de interação com os respetivos fornecedores de serviços, prover recursos computacionais. (e.g. tempo de servidor ou capacidade de armazenamento).

Amplo acesso por rede – Os recursos sãos disponibilizados por rede e acedidos através de mecanismos *standard*, o que promove a sua utilização por diversificados tipos de plataformas (e.g. telemóveis, *tablets*, portáteis e desktops).

Agrupamento de recursos - Os recursos computacionais do fornecedor são agrupados para servir múltiplos consumidores, através de um modelo multi-inquilino em que os diferentes recursos, físicos e virtuais, são atribuídos e reatribuídos de acordo com a procura/necessidade do consumidor (e.g. largura de banda, processamento e armazenamento de dados). Há uma sensação de independência geográfica, no sentido em que o consumidor, normalmente, não tem qualquer controlo ou conhecimento sobre a localização exata dos recursos que está a utilizar, podendo ter apenas uma ideia mais abstrata/geral como o país.

Elasticidade rápida - Os recursos podem ser providos e libertados de forma elástica. Em alguns casos isto pode, mesmo, acontecer automaticamente, por forma a manter recursos livres, possibilitando uma rápida correspondência à procura/necessidade por parte dos consumidores. Assim, para o normal consumidor, os recursos disponíveis aparentam ser ilimitados, podendo ser utilizados a qualquer momento (e.g. *website* que num determinado momento tem um enorme aumento de acessos).

Serviços mensurados - Os sistemas *cloud* controlam e otimizam, automaticamente, a utilização de recursos, alavancando mensurações abstratas de capacidades e utilização adequada de um dado serviço. (e.g. armazenamento, processamento, largura de banda, contas de utilizador ativas). A utilização de recursos pode ser monitorizada, controlada e reportada, fornecendo informação transparente sobre referido serviço ao fornecedor e ao consumidor. (Mell & Grance, 2011, p. 2)

1.2.2 - Modelos de serviço

Relativamente aos modelos de serviço, é importante ter a noção do que é infraestrutura *cloud.* Esta denominação é dada a um coletivo de recursos, conceptualmente organizados numa camada física, sobre a qual assenta uma camada abstrata, que possibilita as cinco, previamente mencionadas, características de computação em nuvem. A camada física consiste no *hardware,* tipicamente servidores e componentes de rede, funcionando como a base, através da qual, a camada de abstração, o *software*, é implementada (Mell & Grance, 2011).

Os modelos de serviço são os que se apresentam de seguida.

> Software como um serviço (*SaaS*) - Capacidade provida ao consumidor para utilizar *software* do fornecedor de serviços que corre numa infraestrutura *cloud*. As aplicações são acessíveis através de diferentes dispositivos por interfaces *thin*, como um *internet browser* (e.g. *e-mail*), ou, interface de programa. O consumidor não gere nem controla a infraestrutura base da *cloud*, o que inclui a rede de computadores, sistemas operativos, armazenamento e, salvo especificas exceções de configuração, nem mesmo capacidades individuais do programa.
>
> Plataforma como um serviço (*PaaS*) - Capacidade provida ao consumidor para implantar e executar aplicações, na infraestrutura *cloud*, criadas ou adquiridas pelo consumidor e . . . suportadas pelo fornecedor. O consumidor não gere nem controla a infraestrutura base da *cloud*, o que inclui a rede de computadores, sistemas operativos, armazenamento e, salvo especificas exceções de configuração, nem mesmo capacidades individuais do programa.
>
> Infraestrutura como um serviço (*IaaS*) - Capacidade provida ao consumidor para utilizar recursos de processamento, armazenamento, rede e outros, onde o consumidor pode implementar e executar qualquer *software*, o que pode inclui sistemas operativos e aplicações. O utilizador não controla nem gere a infraestrutura base da *cloud,* mas, tem controlo sobre sistemas operativos, armazenamento e aplicações ou até, possivelmente, controlo limitado sobre componentes de rede específicos (e.g. *firewalls*). (Mell & Grance, 2011, pp. 2-3)

1.2.3 - Modelos de implementação

Por fim, temos os modelos de implementação, os tipos de *cloud* no que toca à localização física do seu *hardware*, quem tem acesso e qual o nível de acesso e controlo. Assim, de seguida serão apresentados e definidos referidos modelos.

> *Cloud* privada - A infraestrutura *cloud* é provida para o uso exclusivo de uma única organização, composta pelos seus constituintes (e.g. unidades de negócio). Pode ser da propriedade, gerida e operacionalizada pela própria organização, por uma terceira entidade ou por ambos e pode existir dentro ou fora das instalações da organização.
>
> *Cloud* comunidade - A infraestrutura *cloud* é provida para o uso exclusivo de uma comunidade específica de consumidores de diferentes organizações com objetivos semelhantes (e.g. missão, requisitos de segurança, politicas e considerações de observância). Pode ser da propriedade, gerida e operacionalizada pela própria organização, por uma ou mais organizações da comunidade, por terceira entidade ou uma combinação de ambos e pode existir dentro ou fora das instalações da organização.

Cloud pública - A infraestrutura *cloud* é provida para o livre uso do público em geral. Pode ser da propriedade, gerida e operada por entidade de negócios, académica, governamental ou uma combinação destes. Esta infraestrutura existe nas instalações do fornecedor de serviços *cloud*.

Cloud hibrida - A infraestrutura *cloud* é composta por duas, ou mais, infraestruturas *cloud* distintas (privada, comunidade ou pública) que, embora existam e se mantenham como entidades singulares, são unidas por tecnologias que permitem a portabilidade[11] de dados e aplicações (e.g. *cloud bursting* para gestão de equilíbrio de carga entre *clouds*). (Mell & Grance, 2011, p. 3)

1.3 - Conclusão

Este curto capítulo serviu para uma melhor compreensão da tecnologia de computação em nuvem, as suas características base e funcionamento. Em suma, tentando pôr a teoria abordada em termos mais comuns e numa ideia mais clara, computação em nuvem refere-se a um conjunto de recursos computacionais que existem fora do nosso dispositivo e que pertencem a um fornecedor de serviços. Recursos esses que estão sempre disponíveis, são partilhados por diversos utilizadores para as mais diferentes tarefas e aos quais, acedemos através da internet, sem necessidade de interagirmos com referido fornecedor, visto que esses recursos se configuram de forma automática para corresponder às atividades e necessidades do consumidor de forma instantânea. Esses recursos estão em constante mensuração e avaliação, por forma a fornecer exatamente aquilo que o consumidor necessita, mantendo a maior quantidade possível de recursos livres, por forma a estarem disponíveis para satisfazer, a todo o momento, as necessidades do maior número possível de utilizadores. Os recursos utilizados pelo consumidor podem ser sobre a forma de *software* e/ou *hardware* e podem advir de uma infraestrutura privada, de comunidade ou institucional, pública ou híbrida.

Na figura que se segue fica esquematizado aquilo que se abordou neste capítulo.

[11] Capacidade de tratar e migrar dados e aplicações, entre diferentes fornecedores e/ou ambientes *cloud*.

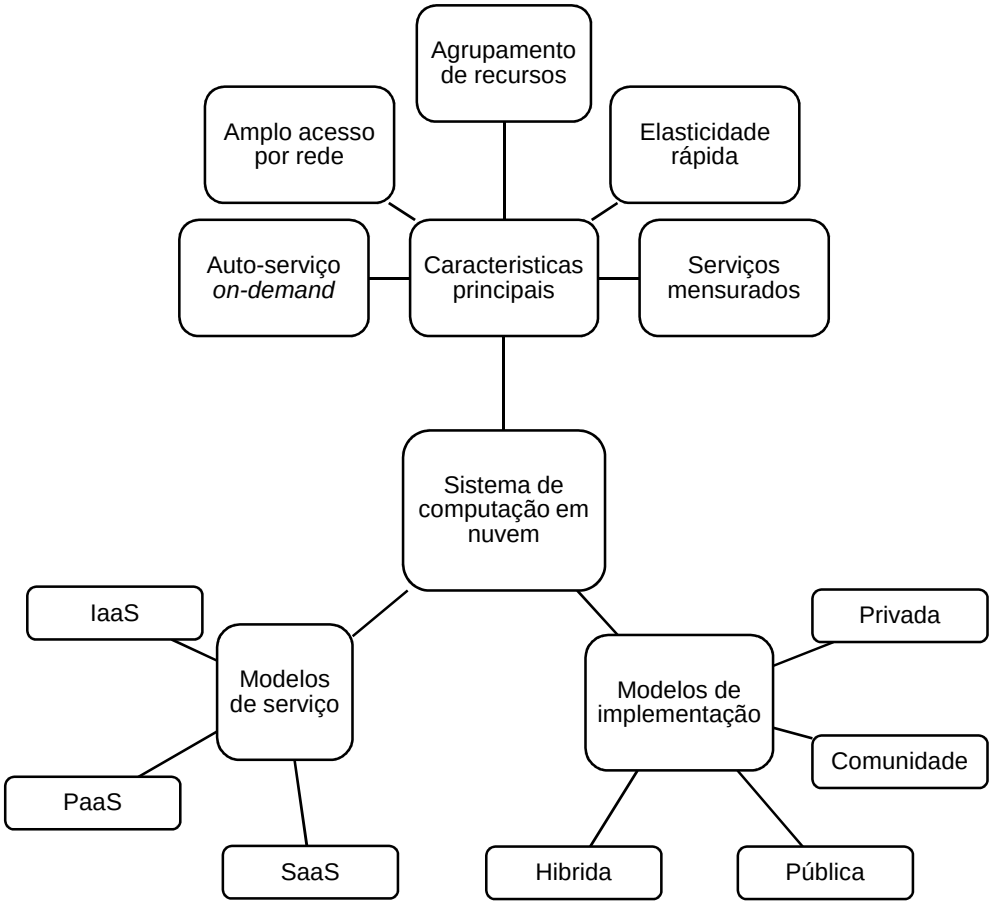

Figura 2 – Esquematização da definição e funcionamento base de computação em nuvem.

Fonte: adaptação própria da teoria abordada.

Apesar de todos os capítulos serem uma sequência natural de constante explanação do que foi previamente abordado, este primeiro, embora curto, é fulcral, pois, é a partir destas características e modelos de serviço e implementação que, se vai extrair e explicar os temas seguintes.

Capitulo II – Benefícios e impulsionadores de adoção

2.1 - Introdução

Neste segundo capitulo inicia-se uma revisão de literatura mais profunda, mas, assente nos princípios base aprendidos no capítulo anterior.

A partir da definição e caracterização de computação em nuvem, partimos, agora, para a abordagem às principais vantagens da tecnologia de computação em nuvem face às soluções tradicionais.

Conforme vamos abordando os conceitos, espera-se não apenas transmitir e explicar os benefícios da *cloud*, mas, também, deixar claro e dar uma concreta noção de que estes advêm da forma como a *cloud* funciona e é utilizada.

Para além dos principais benefícios, no final será apresentada uma breve conclusão e esquematização do que será aqui abordado.

2.2 - Benefícios

Intimamente ligados às, já abordadas, características chave de computação em nuvem, Armbrust et al., (2009), Armbrust et al., (2010), Halpert (2011), Kundra (2011), Macias e Thomas (2011a), Macias e Thomas (2011b), Mattoon, Hensle e Baty (2011), Takai (2012) e McKendrick (2013) identificam e apresentam similarmente os principais benefícios da tecnologia de computação em nuvem, que é o que será apresentado de seguida.

Quaisquer citações relevantes ou ideias complementares destes ou outros trabalhos serão devidamente introduzidas e referenciadas no seguimento das ideias dos autores supramencionados e apresentadas, daqui em diante.

2.2.1 - Elasticidade, escalabilidade e agilidade

A elasticidade e a escalabilidade são conceptualmente semelhantes, diferenciando-se por considerações temporais e funcionais, tendo origem na característica, previamente abordada, de elasticidade, que nos remete para eficiência da correspondência entre a procura e a oferta de recursos (Herbst, Kounev & Reussner, 2013).

A elasticidade prende-se com a capacidade de adaptação, no momento, às alterações de carga de trabalho, à capacidade de prover e desprover recursos, escalando rapidamente a capacidade do serviço, para que, “a todo o momento e tanto quanto possível, os recursos disponíveis correspondam à procura” (Herbst et al. 2013, p. 24). Isto é útil para situações em que um serviço se depara com um pico de utilização. Exemplificando, um *site* de internet, que tem um número de acessos, mensais, na ordem das centenas e que está configurado e preparado para tal. Se num determinado momento se depara com um considerável excedente de acessos, em

simultâneo, o mais normal seria que o acesso e a navegação nesse *site* se tornassem, devido à congestão, condicionado, lento ou mesmo impraticável. O serviço poderia ser mesmo interrompido. A referida elasticidade atua, aumentando as capacidades do serviço por forma a impedir ou pelo menos atenuar estes efeitos.

A escalabilidade é uma outra forma de correspondência à procura, concretamente, procura planeada. É a "capacidade que o sistema tem de suster um aumento de carga de trabalho, através da utilização de recursos adicionais" (Herbst et al. 2013, p.25), atempadamente provisionados, embora, o oposto também seja possível. É o poder que o consumidor tem para adquirir apenas os recursos que precisa (Bhisikar, 2011; Comissão Europeia, 2012a; Liang, 2012; Gorelik, 2013). Para melhor perceção damos o exemplo de um utilizador que tem uma conta de armazenamento *cloud,* com uma determinada capacidade, que, embora, seja suficiente no seu quotidiano, durante um período de tempo não o vai ser. O utilizador pode adquirir, permanente ou temporariamente, mais espaço de armazenamento. A situação inversa, é, também, possível, o que torna claro os benefícios para uma organização, em que pode, mantendo o exemplo, obter mais armazenamento de forma granular e proporcional à evolução das necessidades da empresa.

A agilidade remete-nos para a velocidade e facilidade com que estas duas situações são implementadas. Se no caso de elasticidade parece algo óbvio, dada a velocidade em que os necessários processos autónomos decorrem, o mesmo é verdade no caso da escalabilidade, onde a diferença comparativa com uma solução não *cloud* é mais concreta, mais facilmente visualizada. Acima de tudo, a aquisição de recursos dá-se sem as necessidades temporais de adquirir e instalar *hardware* e *software*, sendo que, a própria interação entre consumidor e fornecedor é mínima ou nula (Macias & Thomas, 2011a; Liang, 2012).

2.2.2 - Multi-inquilino

A tecnologia *cloud* tem, inerentemente, vários inquilinos, "até as *clouds* privadas, que correm a carga de trabalho de uma única empresa, possuem múltiplos inquilinos, sejam cargas de trabalho ou utilizadores individuais." (Halpert, 2011, p. 3). Passando para um novo exemplo. Como senhorio, eu posso fornecer uma casa a cada inquilino ou, neste caso de arquitetura multi-inquilino, eu posso fornecer, a cada inquilino, o acesso a uma unidade de uma única casa.

Em linguagem informática isto traduz-se como um "modo de operação do *software,* onde múltiplas e independentes instâncias de uma ou múltiplas aplicações operam num ambiente partilhado. As instâncias (inquilinos) estão isoladas logicamente, mas, integrados fisicamente" (Gartner[12], 2015a). Um exemplo mais concreto é o de armazenamento na *cloud*. Utilizar um serviço de armazenamento não significa que, do lado do fornecedor, esteja um disco apenas

[12] http://www.gartner.com/it-glossary/multitenancy

para uma pessoa. O que existe são autênticos campos de servidores, conjuntos de recursos, que são agrupados e despoletados para satisfazer uma necessidade.

2.2.3 - Economia

Este benefício advém principalmente das características de elasticidade e agrupamento de recursos e pode ser facilmente compreendida nas ideias seguintes.

Embora seja um beneficio, tanto para fornecedores de serviço, como para o consumidor, é mais fácil visualizar o benefício do lado do fornecedor, que, "ao alavancar uma infraestrutura partilhada e economias de escala[13], consegue rendimentos exponenciais, o que faz da computação em nuvem um modelo de negócio irresistível" (Kundra, 2011, p. 2). O fornecedor de serviços não produz uma solução para cada cliente, há um conjunto de recursos que se configuram as vezes e das formas necessárias para fornecer determinada solução num determinado momento e, também, por isso, é muito mais prático e rentável construir centros de dados de grandes dimensões do que um de pequenas dimensões. O mesmo se aplica à aquisição de recursos como eletricidade, rede e armazenamento, que ficam tanto mais baratos quanto maior o volume de compra.

Este efeito das economias de escala permite uma redução de custos que é transmitido e beneficiado, pelos consumidores, empresariais ou pessoais, visto que, torna desde logo os serviços mais baratos. Ao mesmo tempo, de acordo com os benefícios da *cloud*, os consumidores podem "medir e pagar apenas pelos recursos de TI que consomem, aumentar ou diminuir a sua utilização para igualar às necessidades e constrangimentos orçamentais . . . Recursos necessários . . . podem ser provisionados mais rapidamente e com mínimo *overhead* [14] . . ." (Kundra, 2011, p. 2).

Concretamente, trata-se de um novo nível de eficiência de utilização de recursos que resultam em, cada vez menos, gastos (Bhisikar, 2011; Kundra, 2011 & Liang, 2012). O facto de deixar de ser necessário o investimento próprio para a aquisição, posse, administração e manutenção de *hardware* e *software*, capazes de originar soluções semelhantes às obtidas por um fornecedor de serviços *cloud,* cria uma alteração de paradigma, de custos de investimento para custos operacionais e isto abre portas a uma nova realidade, em que o consumidor tem acesso a soluções de alta performance que, em condições normais de investimento, posse, administração e manutenção, não teria (Cellary & Strykowski, 2009; Pokharel & Park, 2009; Bhisikar, 2011; Elbadawi, 2011; Chandrasekaran & Kapoor, 2011; Zissis & Lekkas, 2011; Comissão Europeia, 2012a)

[13] Conceito aplicado a uma situação em que o preço por unidade para produzir um determinado bem, diminui à medida que o ´numero de peças produzidas aumenta (Proteste)
[14] Custos operacionais, como por exemplo, eletricidade, custos laborais com pessoas, etc.

Isto é facilmente percebido com um simples caso exemplificativo. Um consumidor empresarial faz uma compra de uma aplicação que pode ser partilhada por vários utilizadores, ao invés de adquirir uma para cada utilizador. Pode escalar a compra de recursos, como armazenamento *cloud*, às reais necessidades da empresa, aumentando conforme a atividade da empresa cresce ou em momentos de elevada carga de trabalho, ou, no oposto, diminuindo em alturas de férias, o que torna desnecessária, a situação de ter de realizar grandes investimentos, como na compra de servidores, baseados apenas em expectativas e que depois podem não ser suficientes ou, inversamente, até ficarem sem uso. Com isto, poupa, também, nos custos de manutenção e de administração que estariam inerentes à posse física de referidos servidores.

2.2.4 - Abstração

Uma das mais significativas alterações no paradigma da computação é a de abstração, entre os modelos de serviço e o lado operacional que os suporta. Ou seja, por exemplo, um consumidor de *SaaS* vai interagir com a aplicação em si, mas, mantém-se isolado quanto ao lado operacional do serviço, não interagindo com o sistema operativo nem com o *hardware* da *cloud*.

Isto é extremamente importante, porque, "permite que organizações, que não têm as proficiências de administração de sistemas nem as instalações de computação necessárias, consigam utilizar aplicações empresárias hospedadas por outros" (Halpert, 2011, p. 3).

2.2.5 – *On-demand*

Talvez o benefício mais concreto e mais lógico, seja, também, o mais esquecido, talvez por estar implícito e ubíquo na tecnologia, sendo mesmo uma das principais e abordada característica da tecnologia. Salvaguardando a situação de falhas de acesso ao serviço, a serem abordadas de seguida, a *cloud* está sempre presente e sempre disponível, eliminando restrições espaciais e temporais, de *hardware* e *software,* possibilitando a aquisição, acesso e término de serviços a qualquer momento, em qualquer lugar, através de uma opulência de dispositivos computacionais.

2.2.6 - Portabilidade *cloud bursting*

A capacidade de portar uma aplicação de entre diferentes ambientes *cloud* possibilita algo extremamente útil e denomina-se de *cloud bursting.* Quando uma organização adota uma *cloud* híbrida, para correr uma aplicação, beneficia das vantagens de ambas (Krikos, 2010, pp. 60-75)

Cloud bursting traduz uma situação em que "uma organização pode correr uma aplicação, com carga de trabalho estável, numa *cloud* privada, mas, quando ocorre um pique de carga de trabalho . . . eles podem irromper para uma *cloud* pública, utilizando os seus recursos e devolvendo-os quando já não são necessários" (Demarest & Wang, 2010).

2.3 - Conclusão

Basicamente, aquilo que conseguimos concluir é que os principais benefícios da tecnologia advêm, diretamente, das características que definem a tecnologia. Isto parece algo normal e lógico, mas, é interessante e útil existir uma correspondência tão direta.

É útil de um ponto de vista de abstração conceptual, para uma crescente compreensão da tecnologia e, extremamente, interessante dado o que se abordará e concluirá no capitulo seguinte.

Esta relação tão direta, também nos permite opinar no sentido que, de facto, a computação em nuvem marca uma clara mudança de paradigma no que toca a tecnologias. Isto porque não estamos a falar de uma maneira diferente de operar, mas, sim, na adoção de algo cuja sua natureza, por si só, é diferente o suficiente para expandir drasticamente as nossas capacidades, bem como, abrir caminho a novas possibilidades. De resto, esta é a ideia que transparece ao longo deste trabalho, através dos diversos autores referenciados, especialmente e, de forma mais concreta, os relatórios e previsões da Gartner (2008), Gartner (2013) e Gartner (2015c), que apontam para que a *cloud* esteja em crescente implementação e sirva de base para o futuro.

Sumariando os benefícios abordados, a *cloud* oferece-nos o acesso a uma maior e imensa quantidade de recursos computacionais de forma extremamente controlada e autónoma. Recursos esses que aumentam exponencialmente a capacidade de processamento de dados do utilizador, e/ou que aumentam as soluções e serviços disponíveis. Tudo isto com uma mínima barreira de entrada, visto que o funcionamento da tecnologia permite a sua utilização por consumidores sem grande proficiência tecnológica e a nível económico, os custos de adesão, são, reduzidos ou nulos e os custos da sua contínua subscrição são, extremamente, pequenos dado o funcionamento da tecnologia e economias de escala.

Na figura que se segue, apresenta-se, novamente, a esquematização da tecnologia, com o acréscimo do que foi abordado neste capítulo, apresentando as relações mais diretas entre os benefícios e características de computação em nuvem.

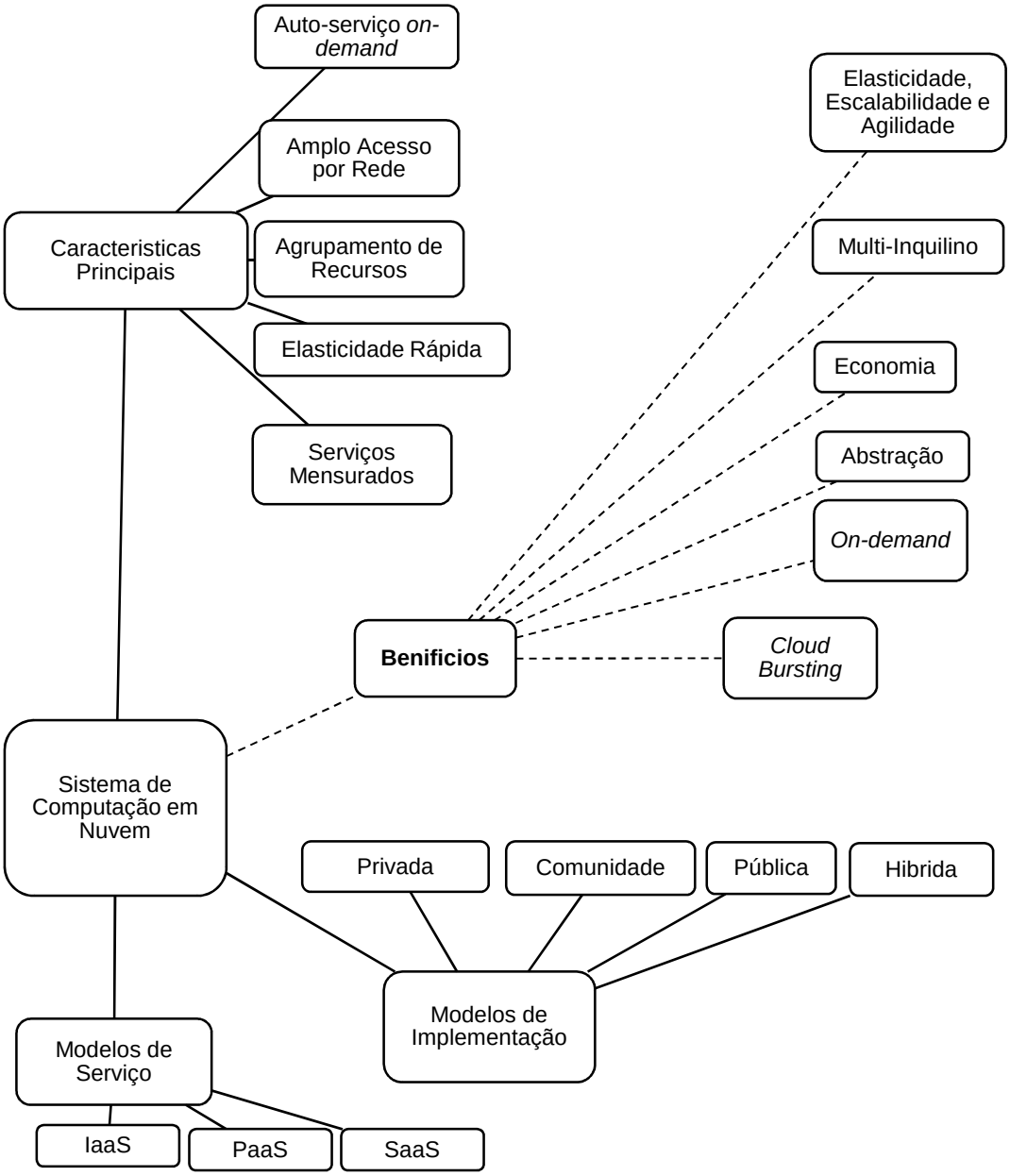

Figura 3 – Esquematização de benefícios e relação com tópicos de capítulo I.

Fonte: adaptação própria da literatura abordada.

Capítulo III – Desafios e potenciais dissuasores de adoção

3.1 - Introdução

Neste terceiro capítulo continua-se a revisão de literatura, de forma similar ao capítulo anterior.

A partir da definição e caracterização de computação em nuvem, identificamos, agora, as principais desvantagens e/ou riscos da tecnologia.

Tal como no segundo capítulo, para além de explorar os desafios inerentes à computação em nuvem, procura-se, também, transmitir a ligação entre estes e as características chave da *cloud*.

Abordados os desafios e riscos, no final será apresentada uma breve conclusão e esquematização do que será aqui abordado, bem como, a sua ligação aos temas anteriores.

3.2 - Desafios

Apesar dos vários e significativos benefícios de computação em nuvem, esta tecnologia não está imune a riscos e desafios.

Ao contrário de soluções tradicionais, num ambiente de computação em nuvem, o consumidor perde algum controlo sobre os seus dados e sobre os recursos tecnológicos utilizados. Por acréscimo, a forma como a tecnologia funciona e a forma como é implementada pelos fornecedores abrem portas a outros desafios, de natureza, também, de controlo, mas, igualmente, problemas de localização dos dados, o que implica questões de legislação e regulamentação, o que por sua vez gera mais preocupações de segurança e privacidade.

De seguida abordam-se os trabalhos de Mather, Kumaraswamy e Latif (2009), Barnatt (2010), Dialogic (2010), Halpert (2011), Macias e Thomas (2011), Badger, Grance, Patt-Corner e Voas (2012), Takai (2012) e T-Systems (2012) Badger et al. (2012), os quais, identificam as principais barreiras à adoção da *cloud*.

Quaisquer citações ou ideias complementares de outros trabalhos serão devidamente introduzidas e referenciadas no seguimento das ideias dos autores supramencionados e apresentadas daqui em diante.

3.3 - Fiabilidade *cloud*

A fiabilidade “remete-nos para a probabilidade de um sistema fornecer, dentro de definidos parâmetros temporais e funcionais, um serviço livre de falhas” (Badger et al. 2012, pp. 8-2) e é um dos importantes dissuasores, sendo necessária uma constante evolução nesta área (Takai, 2012). Para a *cloud* a fiabilidade advém de quatro componentes individuais, identificados por

Badger et al. (2012): 1) recursos de *hardware* e *software* oferecidos pelo fornecedor; 2) pessoas do lado do fornecedor (funcionários); 3) conetividade com os serviços contratados; 4) pessoas do lado do consumidor (utilizadores).

Tendo em conta estas componentes, percebe-se que fiabilidade é algo de difícil mensuração. Em primeiro lugar, mesmo que se consiga medir a fiabilidade de cada uma componente, a partir do momento em que agrupamos componentes, estamos a aumentar os pontos de falha complicando qualquer tipo de previsão. Em segundo lugar temos o contexto. Mesmo para o *hardware* onde se consegue, com alguma facilidade atribuir mensurações de fiabilidade, a verdade é que estas medidas são realizadas em contextos específicos. Na *cloud* há uma mistura de recursos, mistura de contextos, o que vem mais uma vez complicar qualquer tipo de previsão (Badger et al. 2012).

3.3.1 - Dependência de rede

Segundo os trabalhos de Badger et al. (2012) e Gorelik (2013), podemos retirar as seguintes noções.

A ubiquidade da *cloud* é algo extremamente importante, mas, não tem utilidade quando não temos uma ligação à internet e, infelizmente, ainda, existem sérias limitações no acesso à internet. Uma organização deverá ter, em condições normais, acesso constate à internet, mas, um consumidor individual tem limitações básicas de acesso à rede, como por exemplo, o andar de metro (subterrâneo) ou de avião. Mesmo, quando temos ligação de internet ativa, os serviços que corremos estarão dependentes da qualidade desta.

Ao mesmo tempo, o facto de os serviços correrem via internet, deixando os nossos dados de estar unicamente no nosso equipamento, estando disponíveis pela rede, significa que estão suscetíveis de serem intercetados, embora, existam camadas de proteção, como encriptação de dados em trânsito. A comunicação por rede, também, expõe as aplicações a erros que não aconteceriam em ambientes normais.

Um aspeto fundamental, quando falamos de ligações de rede, é a latência. Quando a nossa ligação à internet está degradada, ou simplesmente não é suficientemente capaz, ocorre um fenómeno a que associamos ao conceito de latência[15], que é afetada, concretamente, por congestionamento da ligação, erros de configuração ou outras falhas processuais, devendo, por isso, ser algo a ter conta, pois, o utilizador pode ter necessidades específicas. Outro fator a ter em conta e que afeta, severamente, as latências obtidas, é a distância, em termos geográficos, entre o utilizador e o centro de dados do fornecedor de serviços, algo, que, tambem está, normalmente, fora do controlo do utilizador (Gorelik, 2013).

[15] Latência – "Atraso de tempo que um sistema demora a processar um pedido . . . é o tempo que demora uma mensagem a viajar até ao fornecedor, mais o tempo que a resposta demora a ser recebida pelo consumidor" (Badger et al. 2012, p. 8-1)

Pode não parecer algo problemático e há soluções de mitigação, mas, alta latência, não se traduz apenas numa experiencia mais lenta, embora, a simples lentidão possa tornar uma ferramenta em algo inútil. Mas, há muitas aplicações que simplesmente não têm grande tolerância para variações nos tempos de resposta, tornando-se simplesmente impossível a continuação de utilização ou, mesmo, o simples acesso ao serviço (Badger et al. 2012).

Temos que compreender que quase todos os *inputs* e acessos à informação têm ou acrescentam latência. O próprio funcionamento da *cloud,* nomeadamente a "virtualização e tecnologias de supervisão acresçam latência à performance da aplicação" (Krikos, 2010, p. 60).

A partir de dada altura a latência total pode ser insuportável.

3.3.2 - Disponibilidade

Mencionada como um fator benéfico e característico da *cloud*, deve-se compreender que a disponibilidade de serviços pode ser severamente afetada, no sentido em que o fornecedor de serviços pode, em determinadas situações, ser incapaz de manter o serviço a correr (totalmente ou parcialmente com decréscimo de usabilidade e/ou qualidade) e disponível para os seus utilizadores. A partilha de infraestrutura entre consumidores, que possibilita economias de escala, significa que, se o sistema for pressionado ou mesmo abusado, as repercussões negativas serão sentidas por todos os que utilizem esses recursos, afetando a performance ou mesmo a disponibilidade do sistema (Muiknck-Hughes, 2011; Martínez, 2013; Gorelik, 2013).

Um único utilizador pode, especialmente, se tiver intenções, concretamente, nefárias, conseguir impactar a experiencia ou acesso, de outros utilizadores, consumindo o máximo de recursos possíveis. Como os recursos são partilhados, se um utilizador estiver a criar uma carga de trabalho de tal magnitude, para além das especificações de utilizador singular, a performance do serviço obtida pelos outros utilizadores, ligados a esses recursos, vai ser inferior (Muiknck-Hughes, 2011). Como exemplo, se um utilizador executar vários programas no seu computador pessoal (*Personal Computer* - PC), por cada programa extra a correr, a performance do PC será inferior para cada um desses programas. Se for mais longe e correr aplicações que são criadas, especificamente, para *stressar* um sistema, como *benchmarks* de performance, mais facilmente se consegue sobrecarregar o computador. O mesmo princípio aplica-se ao ambiente *cloud*, com as agravantes da tecnologia, como facto de ser algo multi-inquilino.

Como abordado, embora os recursos *cloud* pareçam ilimitados, não o são e, num ambiente *cloud*, pode-se dar uma situação semelhante aquela, supramencionada, do utilizador com o seu PC, onde, a diferença e o enfase estará no número de pessoas a utilizar referido computador. Se os recursos da *cloud* estão a ser todos utilizados, os restantes utilizadores não têm recursos para aceder.

Um exemplo, abusivo e nefário, deste deste tipo de situação são os *DoS* ou *DDoS*, ou seja, ataques em que um, ou mais, utilizadores tiram total partido da elasticidade da *cloud* para atacar

uma maior quantidade de utilizadores, ou mesmo organizações. Na prática, estes utilizadores apontam ao seu alvo, direta ou indiretamente, saturando a rede e/ou recursos computacionais do alvo (Muiknck-Hughes, 2011). Como exemplo, vejamos: 1) há não muito tempo, a aplicação *Skype* tinha uma vulnerabilidade que permitia a visualização do IP do utilizador, possibilitando o ataque por parte de outros utilizadores, almejavam esse IP e o utilizador via-se incapaz de realizar as mais simples tarefas, porque, a sua largura de banda e/ou o seu *hardware* estavam a ser *stressados* por uma fonte externa; 2) do lado do fornecedor, os *DoS* são facilmente combatidos, existindo então os *DDoS*; o conceito mantem-se, mas, o ataque é lançado a partir de vários dispositivos e ligações de internet, o que designamos de *botnet*[16]; o alvo são os vários recursos *cloud* de uma organização e quando bem-sucedidos, temos a indisponibilidade generalizada de um serviço, como por exemplo, quando a rede de jogos *Playstation Network* ou *Xbox Live*, ficam indisponíveis para várias regiões ou mesmo para o mundo inteiro.

Apesar de esta ser a origem, mais comum, deste problema, facilmente se compreende que para além da sob utilização de recursos, há outros fatores que podem afetar a disponibilidade de serviços. Interrupções de serviços podem, também, acontecer quando os recursos estão inoperáveis, seja derivado de problemas físicos, como avarias, tecnológicos, causas naturais ou até provocados pelo homem (que não a situação do exemplo supramencionado). Como exemplo explicativo, em 2007, devido a um transformador danificado, a *Rackspace* teve uma falha de serviço, que durou 36 horas (Halpert, 2011).

Ainda assim, cada vez mais, e como no caso de ataques, as organizações tomam medidas para evitar este tipo de situações. O grande problema é no caso de remoção de *hardware* por motivos fora do controle. Exemplo disto, como na *cloud,* especificamente na virtualização, há uma partilha de recursos, isto significa que vários utilizadores podem ver a sua informação confiscada devido a práticas ilegais de um único utilizador. Quando se confisca a informação do ator da atividade ilegal, não se confisca apenas a sua informação, mas sim, a plataforma (os recursos) onde ela está, confiscando os recursos de outros.

Ainda assim, há algumas soluções para evitar uma total perda de acesso aos nossos dados. Num cenário simplista, em que um utilizador guarda os seus documentos na *cloud*, já há serviços, como *OneDrive* e *Google Drive*, que permitem a instalação da respetiva aplicação no PC, mantendo os documentos sincronizados entre *cloud* e o computador, disponíveis em ambos. Ou seja, é um sistema de redundância simples, semelhante ao que fornecedores de serviço utilizam. A ideia base, para não perder acesso a dados, é ter esses dados armazenados em vários locais, embora nem sempre seja possível ou pratico.

[16] *Botnet* "é a designação dada a uma "coleção de PCs infetados e controlados, remotamente, por um agressor" (Fisher, 2013). Ou seja, um PC infetado por *malware* torna-se um *bot* sob controlo do agressor e, ao infetar vários PCs, o agressor cria uma rede de *bots,* ou seja, uma *botnet*.

3.4.1 - Risco de continuidade de operações

Ao contrário do que acontece quando se está a utilizar recursos internos, ao utilizarmos recursos *cloud*, se o fornecedor deixar de suportar um serviço, ou se, simplesmente, deixar de existir, visto que o risco de encerramento de negócio é normal em qualquer industria, o consumidor pode-se ver numa situação precária, dada esta dependência para com os recursos do fornecedor. Quanto mais sensíveis e dependentes, até de calendário, forem as suas necessidades, o consumidor incorre em crescentes despesas (Badger et al. 2012).

3.4.2 - Recobro de desastre

Como extensão ao ponto anterior, apesar de economia ser um benefício apontado, tanto a fornecedores, como consumidores, há custos que nem sempre são lembrados e, embora, também se aplique a consumidores para uso pessoal, é a nível organizacional que mais se podem fazer sentir.

Cada vez mais, as organizações têm uma presença ininterrupta e precisam de um funcionamento 24 horas por dia, o que quer dizer que, as suas aplicações e soluções são tão críticas "que devem estar disponíveis para suportar operações 24 horas por dia, 7 dias por semana" (Mather et al. 2009, p. 31). No entanto, e para além das situações focadas em "Disponibilidade", não se está livre de imprevistos, os quais, podem ir, desde algo, tão simples como 1 minuto de falha de energia, ou, como exemplo da *Rackspace*, até falhas catastróficas como desastres naturais, roubo de *hardware* ou percalços eletrónicos, para os quais tem que haver planeamento e documentação de soluções rapidamente executáveis.

Mesmo para o caso de um consumidor final, em caso de falha, este fica, na prática, sem recursos, despendendo tempo e dinheiro por cada minuto que passa e, por isso, o consumidor deve identificar e ter em consideração qual a sua tolerância à frequência e duração de situações de perda de serviços. O consumidor deve ter uma noção de a partir de quando é que começa a ter impacto no seu negocio, quais os possíveis danos e tentar precaver-se junto do fornecedor. Isto de um ponto de vista mais empresarial, mas, um consumidor privado, deverá ter semelhantes considerações, quanto mais não seja, porque está a pagar por um serviço que se espera interrupto, ou quase, havendo sempre, no mínimo, a consideração dos custos contínuos de subscrição de serviços (Badger et al. 2012)

Os fornecedores de serviço devem ter mecanismos de combate a este tipo de situações e devem fornecer, detalhadamente, esses mecanismos e "quanto tempo é necessário para que os serviços sejam totalmente restaurados" (Kok, 2013, p. 15)

Ao mesmo tempo, o fornecedor tem que ter em conta que existem SLAs[17] que, em caso de incumprimento, podem incorrer em custos adicionais. O consumidor deve procurar o máximo de garantias possíveis, o que pode significar maiores custos. Em paralelo, o fornecedor deve fornecer o máximo de garantias e seguros a nível de "suporte, recobro de desastres, modificação de aplicações e perda de dados" (Mather et al. 2009, p. 32), sendo que, estes necessários seguros e recursos, testes e planeamento, significam custos adicionais, embora o fornecedor os vá mitigar ao cobrar esta segurança ao seu consumidor (Gorelik, 2013). Esta mitigação, para prevenir a perda de dados e percalços eletrónicos, consegue-se pondo-se em prática soluções de redundância, replicação e diversidade, o que significa mais recursos, mais cargas de trabalho e, mesmo, maior presença geográfica, sendo este último importante para replicar dados em diferentes localizações para prevenir algo, como, desastres naturais.

Isto abre uma dificuldade de planeamento, também, para o consumidor. Deve-se procurar economias de escala e o não ter todos os dados e tarefas concentrados num só serviço pode parecer mais seguro, mas, se cada serviço implicar custos de segurança adicional, é possível que se atinjam tais custos que, economias de escala signifiquem e exijam a concentração e combinação de dados e serviços. Mais uma vez há que frisar que, embora seja uma situação mais concreta a nível empresarial, um consumidor privado pode e deve ter comportamentos semelhantes.

3.4.3 - Avaliação de acordos de nível de serviço

Com base em trabalhos como o de Muijnck-Hughs (2011), Shimba (2010) e Gorelick (2013) a par dos outros trabalhos referidos no início do capítulo, podemos dizer que os *SLAs* são, na essência, um contrato de prestação de serviços e, como tal, deve ser o mais *standard* possível, com o simples objetivo de ser facilmente comparado e avaliado pelo consumidor.

Embora devam ser ajustados à tecnologia, quanto menos os contratos forem moldados pelo conteúdo, serviço e fornecedor, passando e seguindo cada vez mais um modelo com termos, normalização e valores métricos comparáveis, tornar-se-ia algo facilmente comparável. Ou seja, com as devidas salvaguardas, os contratos deverão tornar-se o mais *standard* possível, para uma mais fácil e rápida comparação entre serviços e fornecedores serviços.

Esta estandardização permitiria uma melhor escolha de fornecedores e serviços, reduzindo, também, os custos monetários e de mão-de-obra inerentes à análise e escolha de soluções, especialmente, na situação de escolha de serviços menos eficientes, tendo em conta as necessidades do consumidor.

[17] Acordo de Nível de Serviço (*Service Level Agreement – SLA)* – É um acordo negocial entre ambas as partes, fornecedor e utilizador, onde é descrito o serviço contratado, metas, níveis e responsabilidades das partes.

Ou seja, a não estandardização de SLA's é um problema, mas, ao mesmo tempo, é uma boa forma de mitigação de riscos. Perceba-se, que, o consumidor individual não tem tanto esta possibilidade, visto que, o seu "poder" limita-se, quase, a uma opção única de aceitação ou não aceitação de termos, mas, tem sempre alguma capacidade negocial. No entanto, esta é uma das situações que corresponde mais ao consumidor empresarial, que, pode-se assegurar, contratualmente, contra muitos ou todos os desafios/problemas da *cloud*, pelo menos, de um ponto de vista monetário.

3.4.4 - Portabilidade de cargas de trabalho e interoperabilidade de fornecedores - *standards*

De acordo com os trabalhos referidos no início do capítulo, especialmente Badger et al. (2012) e, conforme, a ótima síntese realizada no guia da *Cloud Security Alliance* (2011), podemos proceder à caracterização deste desafio para a utilização da *cloud*.

Como previamente abordado, uma característica, benefício e impulsionador da *cloud,* é a portabilidade de dados, mas, existe um fator muito importante, ainda não mencionado. Adotar uma determinada solução *cloud* não pode significar uma eterna dependência para com determinados serviços, aplicações ou equipamentos, muito menos de fornecedores.

Inicialmente pode não parecer um problema, mas, ao movermo-nos para a *cloud* temos de mover para lá as nossas tarefas, aplicações e/ou dados e "interoperabilidade não é uma particular valência da computação em nuvem de hoje em dia" (Krikos, 2010, p. 59). Se, por algum motivo, quisermos voltar atrás, podemos retirar essas tarefas, aplicações e/ou dados da *cloud* e voltar a implanta-las na nossa infraestrutura. Tal é praticável e o fornecedor pode oferecer tal capacidade, mas, o problema põe-se quando o que desejamos é mudar de fornecedor. A portabilidade de dados assenta em interfaces e formato de dados e aqui é que se torna complicado. Há bastante consenso e *standards*, por isso, em situações tradicionais, como o armazenamento, os *standards* estão presentes e consegue-se a portabilidade, mas o mesmo não acontece com soluções mais complexas. Interoperabilidade está refém da capacidade de gerir aplicações, independentemente, do fornecedor ou da infraestrutura, mas, as *clouds* são construídas para e em diferentes infraestruturas com diferentes APIs[18] (Krikos, 2010). Um exemplo comum, remete-nos para os sistemas IaaS, que, **"**expõem detalhes de baixo nível (*low-level*), como interfaces de dispositivos, o que significa que qualquer falha de alinhamento entre dispositivos é um obstáculo." (Badger et al. 2012, pp. 8-5).

A situação complica-se, ainda mais, quanto mais nos afastamos de um simples aluguer de recursos físicos. Num campo mais abstrato, como permissões de utilização de um determinado programa, torna-se difícil traduzir a situação através dos standards existentes o que pode impedir a portabilidade entre fornecedores. Por tudo ser muito específico a cada fornecedor, incluindo as

[18] Interface de programação de aplicação (*Application Program Interface* – API) – Conjunto de protocolos, rotinas e ferramentas para a codificação/programação de aplicações de *software*.

definições de recursos, torna-se necessária a criação e a imposição de novos *standards*. Alguns, como DMT09 (*Open Virtualization Formant*[19]) e SNI10 (*Cloud Data Management Interface*[20]), já existem, mas, continuam a existir problemas. Por um lado, precisam de continuar a serem desenvolvidos para melhorar a sua eficácia e, acima de tudo, para reduzir os custos de interoperabilidade entre fornecedores. Isto não é fácil, tendo em conta a rápida evolução da tecnologia. As inovações e a necessidade estão sempre "adiantadas" à regulamentação e à criação de *standards*. A adaptação estará sempre ligeiramente atrasada. (Badger et al, 2012)

Tendo tudo isto em conta, há ainda mais um problema que daqui decorre. É mais uma situação em que se levantam questões de segurança. Um exemplo muito claro é a alteração de fornecedor de serviços. Para que a transferência de serviços entre diferentes fornecedores seja possível, quando é possível, o fornecedor atual tem de ceder ao fornecedor destino, credenciais de acesso válidas.

3.5 - Observância e governança

Mais uma vez, de acordo com os trabalhos indicados no início do capítulo e recorrendo, também, às definições por Badger et al. (2012), procedemos à abordagem dos temas e subtemas de observância e governança.

Como abordado e como é natural, o fornecedor quer controlar os seus bens, mas, o consumidor também o quer. Complicando a situação, por vezes, existe, ainda, uma terceira entidade, os integradores, que subscrevem a um ou mais serviços de um ou mais fornecedores por forma a oferecerem um outro serviço ao consumidor final e obviamente, este integrador, também, quer controlar os seus bens. Isto levanta questões de direitos de propriedade sobre dados e o dever de garantir observância de leis e regulamentação.

Segundo Badger et al. (2012), embora o fornecedor esteja na melhor posição para garantir e fazer cumprir toda a jurisdição e regulamentação que se aplique aos dados, na verdade, a responsabilidade final está do lado do utilizador, que acaba por ser a entidade com menor conhecimento e controlo sobre os dados, sobre como e onde estes estão a ser armazenados. Ou seja, questões de privacidade, segurança e controlo dos nossos dados complicam-se com a introdução da entidade "integradores", levantando-se, ainda, outros problemas, conforme se abordará de seguida.

[19] *Standard* livre relativo à utilização e distribuição de recursos virtuais, referindo-se geralmente ao correr *software* em máquinas virtuais (VM)
[20] Interface de aplicação para a criação, recuperação, atualização e o apagar de elementos em ambiente *cloud*

3.5.1 - Localização de dados – requisitos políticos e legais

A complicar esta situação levanta-se um outro problema. O fornecedor, integrador e consumidor não estão, necessariamente, localizados nos mesmos países ou regiões. Aliás, os próprios recursos *cloud* e mesmo os dados, a informação em si, podem, também, ter uma localização completamente diferente. Isto é relevante porque diferentes países e regiões possuem e aplicam diferentes regulamentações, relativamente ao tratamento de dados.

Em computação em nuvem há uma variável que consiste sobre "onde residem os dados, onde são processados e onde são acedidos" (Mather, Kumaraswamy & Latif, 2009), sendo que, diferentes regulamentações se podem aplicar. Isto significa que a tecnologia *cloud* infringe e submete-se ao "reino" e restrições da política, o que por si só levanta outros problemas. Tal como a internet, para atingir toda a sua potencialidade e funcionar sobre conceitos de liberdade e igualdade, a *cloud* precisa de se libertar destes constrangimentos políticos. Existem claros e recentes exemplos sobre o pior que a politica, especialmente diferentes políticas, podem fazer à *cloud,* ou mesmo à internet como um todo. Vejamos mais exemplos: 1) numa leitura de artigos de Granick (2013) ou TheVerge (2013) vemos uma situação preocupante que conjuga, como referido, tudo o que de mal pode acontecer com a mistura de política e tecnologia; Nos EUA, possibilitado e assente no *Patriot Act (Section 215)* e *FISA Amendments Act (Section 702),* a NSA criou vários projetos e ferramentas, sendo o mais conhecido *PRISM*, através das quais a agência coleciona dados eletrónicos privados dos utilizadores; Fá-lo, com base na regulamentação, de forma "legal", mas, sem o devido processo, visto que os chamados *FISA Courts* (tribunais), funcionam com o representante da *NSA* e juiz, mas, sem qualquer oposição, sendo que, a parte que melhor simboliza o problema mencionado, é que o foco é posto nos utilizadores que não os dos EUA e tal é possível porque os recursos *cloud* e dados estão lá; Com esta regulamentação, a *NSA* obtém informação diretamente, por exemplo, pela interceção de dados, nos cabos de internet que atravessam os oceanos, ou indiretamente, exercendo o seu poder ao exigir os dados às empresas fornecedoras de serviços; Tendo em conta que sobre esta alçada estão empresas como Verizon, Sprint, Apple, Facebook, Google e Microsoft, as quais são responsáveis por quase a totalidade de trafego de dados, estas práticas são extremamente nefastas, levantando graves problemas de segurança e privacidade.; 2) outra situação nos EUA remete-nos para o debate da neutralidade da internet[21], que tem sofrido graves reveses, estando mesmo posta em causa, devido, mais uma vez a regulamentações e decisões judiciais que se encontram num sentido completamente oposto ao Europeu; Temos como grande exemplo a situação da Netflix, que se viu forçada a pagar ao *ISP* Comcast, para que os seus serviços não fossem propositadamente degradados. A Netflix cria e transmite conteúdos (i.e. filmes e series) via internet; Estes serviços utilizam muita largura de banda e a Comcast, apesar dos seus clientes pagaram por acesso à internet e por larguras de banda suficientes, decidiu identificar

[21] Net neutrality – Principio que significa que o "trafego deve ser tratado equitativamente, sem descriminação, restrições ou interferências, independentemente do emissor, recetor, tipo, conteúdo, dispositivo, serviço ou aplicação. (Vera, Ernst, Andersdotter & Trautmann, 2014, pp 1)

este tipo de trafego e reduzir a sua qualidade por não se sentir na obrigação de suportar este tipo específico de trafego, porque não o tinha em mente quando vendeu aos seus clientes ligações e serviços que o conseguem suportar; Esta prática de identificação e descriminação de tipo de dados vai completamente contra ao conceito de neutralidade de redes, mas, é permitida e tem início, numa polémica decisão de um tribunal federal dos EUA, que decretou que a FFC "não tem autoridade para forçar fornecedores de serviços de internet a manter as suas redes abertas a todas as formas de conteúdo" (Kang, 2010); Desde então, a Comcast e outras grandes empresas, também, de telecomunicações, têm-se vindo a sobrepor à FCC e neutralidade de redes, chegando ao ponto da Netflix, ver-se obrigada a fornecer recursos de rede e a pagar uma "tarifa" à Comcast, para que os seus serviços deixassem de ser altamente degradados, por forma a conseguir continuar o seu negócio.

Estas preocupações não são boas, nem para os consumidores, nem para os fornecedores e, em última instância, nem para a própria tecnologia, que, para alem de ver a sua adoção reduzida, vê, também, a sua evolução bloqueada. Não podermos ter uma "*cloud* de informação e serviços capazes, da qual possamos chamar a nós ou construir sobre ela, se algo ou alguém estiver, a todo o momento, a manipular os dados em si contidos, ou pior ainda, se algo a estiver a bloquear o seu acesso para alcançar objetivos ocultos" (Mather et al. 2009, p. 34). Mas, na prática, mesmo que ainda longe do ideal, independentemente do país ou região, a verdade é que há diferenças enormes de regulamentação. Enquanto nos EUA temos situações como as acima abordadas, em que nem a FCC consegue estabelecer qualquer tipo de oposição, onde a opinião geral é de que "neutralidade de rede é um morto-vivo. A data de execução ainda não está definida, mas podem ser dias, ou meses" (Ammori[22], 2013), na Europa e apesar de serem necessárias negociações e adoção dos países, a verdade é que, conforme podemos no artigo de Turk (2014) e nas propostas de reforma, por parte da do Parlamento Europeu nele mencionadas e, ainda, tambem, segundo o artigo da Reuters por Chee (2014), a Europa vota a favor da manutenção da neutralidade das redes, declarando efetivamente que todo o trafego de internet deve ser tratado de igual forma, independentemente da fonte ou conteúdo. Mais uma vez, a internet está intimamente ligada à *cloud*, sendo o meio através do qual a *cloud* se concretiza.

Sendo isto algo que interessa especialmente ao consumidor, a verdade é que, cada vez mais, é algo de crescente interesse para os próprios fornecedores. Seja por real interesse ou por pura diferenciação de produto, ainda assim, para os fornecedores, a localização dos dados, mais concretamente, dos centros de dados, interessa principalmente pelos custos económicos inerentes e qualidade de mão-de-obra. Diferentes países e regiões têm diferentes "custos de construção dos centros de dados e custos de energia, proteção e segurança, disponibilidade de força de trabalho instruída, custos de trabalhadores e a qualidade de infraestrutura pública." (Badger et al. 2012, p. 8-6).

[22] http://www.wired.com/2013/11/so-the-internets-about-to-lose-its-net-neutrality/

Em suma, pelo prisma de consumidor, especialmente o consumidor empresarial, deve ter em mente que é o responsável absoluto pelos seus dados e, como tal, deve procurar manter-se informado e, caso seja necessário, exigir garantias que os seus dados estão com conformidade com o que lhes é exigido, apesar de se levantar outra complicação nesse momento. Os fornecedores vêm a implementação e a configuração dos seus sistemas como informação privilegiada/industrial, o que quer dizer que tendem a não fornecer qualquer informação. O que torna excecionalmente importante a existência de jurisdição que responsabilize os fornecedores e proteja os consumidores.

3.6 - Conclusão

Após a revisão de literatura deste capitulo, aquilo que conseguimos concluir é que os principais dissuasores ou desvantagens da tecnologia advêm, quase diretamente, das características que definem a tecnologia. Uma conclusão em tudo semelhante à do capitulo anterior e, igualmente e novamente, útil de um ponto de vista de abstração conceptual, para uma crescente compreensão da tecnologia.

Sumariando, então, a teoria abordada neste capítulo. É verdade, da mesma que para cada característica chave da *cloud*, havia uma correspondência para com um beneficio, uma vantagem, tambem, agora, parece existir uma relação para com desafios. Estes desafios prendem-se com uma ideia “central”, controlo. A partir do momento que os nossos dados entram na *cloud*, o controlo sobre estes torna-se, aproveitando um termo bem presente e relacionado com a tecnologia e abordagem de literatura, mais abstrato. O controlo pode até ser o mesmo, pode até ser total, mas, está sempre dependente do acesso a esses dados e, este conceito de acesso é outro que é fulcral.

Concretizando, os desafios da *cloud,* são, a fiabilidade desta, até que ponto o serviço vai correr sem falhas, tal como, a dependência da rede, que, embora torne a *cloud* em algo ubíquo, essa ubiquidade depende de acesso à rede e em condições capazes para a execução do serviço. Nesta linha de pensamento, temos disponibilidade, como um problema individual, embora relacionado com rede, visto que, mesmo que exista, do lado do consumidor, todas as condições para o acesso ao serviço, o mesmo pode não acontecer do lado do fornecedor de serviços. Num outro “espectro”, temos as questões de observância e governança, que envolvem as questões da localização de dados e onde se agrupo as diferenças e os problemas legais, regulamentares e políticos que afetam a *cloud*. A tecnologia, a sua acessibilidade e evolução, não deveria ser reduzida ou atrasada por este tipo de fatores, nem, muito menos, deveria ser fragmentada a nível igualdade de direitos e circunstâncias, mas, infelizmente, é. Por fim, resultante de todos estes fatores e mais alguns, temos os problemas denominados de fatores económicos. Tudo que foi mencionado, se tiver impacto na qualidade ou capacidade de acesso aos seus dados e serviços, está a custar ao consumidor, especialmente a nível empresarial. Costuma-se dizer que “tempo

é dinheiro” e, neste caso, é verdade. Além dos aspetos já mencionados, existe ainda o risco de continuidade de operações, por parte do fornecedor, as situações de desastre (e.g. desastre natural que destrói um centro de dados) e a dificuldade de portar cargas de trabalho entre fornecedores ou mesmo a capacidade de mudar de fornecedor de serviços. Finalmente, os SLA, por um lado um problema de estandardização que dificulta a comparação entre fornecedores e serviços, por outro, uma capacidade de mitigação de risco.

De seguida faz-se uma nova esquematização do que foi abordado até ao momento, apresentada na figura que se segue.

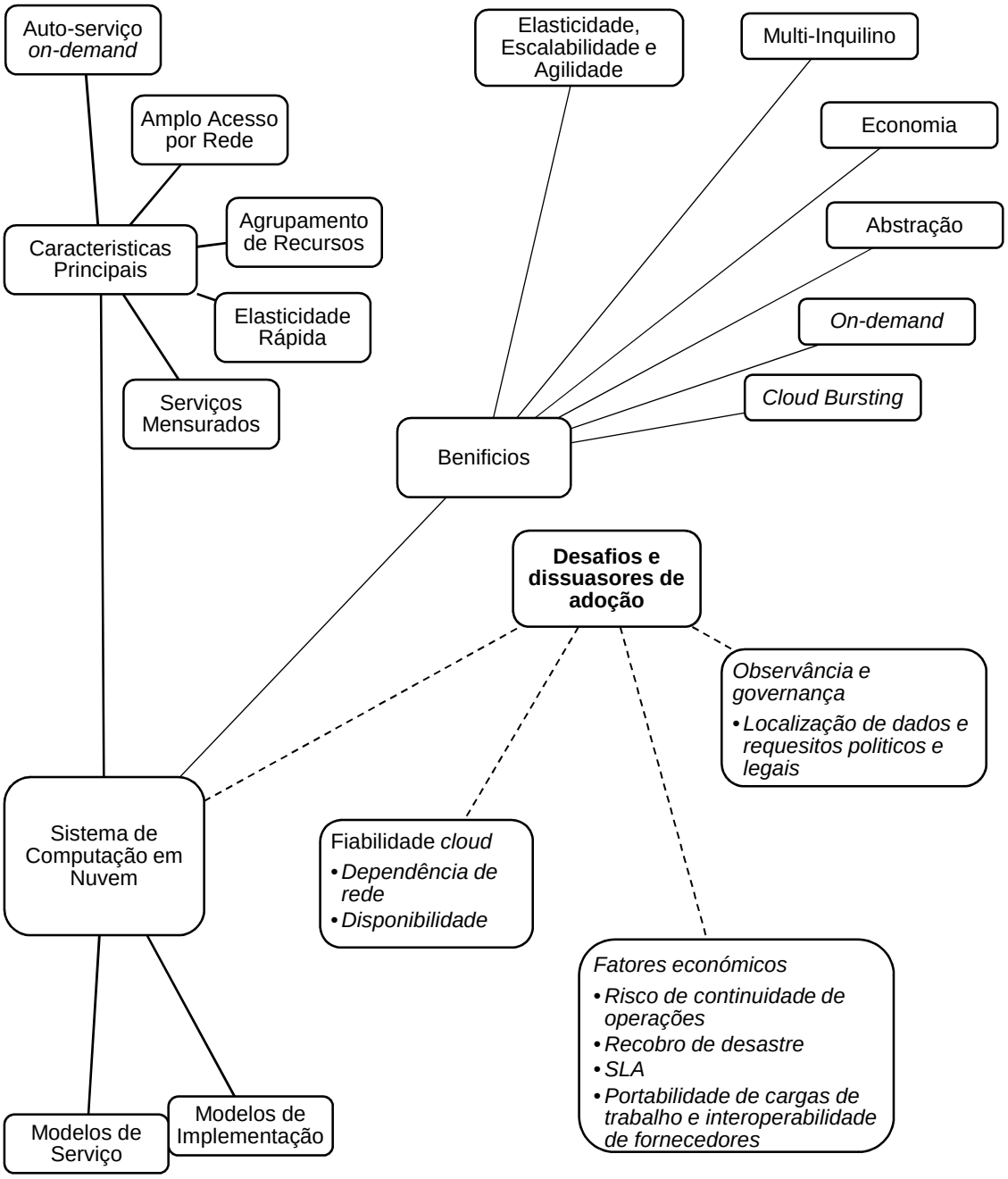

Figura 4 – Esquematização de desafios e dissuasores de adoção em relação com tópicos de capítulo I e II.

Fonte: adaptação própria da literatura abordada.

Capitulo IV – Segurança, privacidade e conceitos relacionados

4.1 - Introdução

Neste quarto capítulo continua-se a revisão de literatura, sendo que, agora, o enfase será mesmo posto na segurança e privacidade, bem como, conceitos relevantes e possivelmente correlacionados.

A abordagem teórica, realizada no capitulo que se segue, será feita como uma sequência natural dos capítulos anteriores, tentando agora, com uma noção mais compreensiva da tecnologia, debruçarmo-nos, concretamente, sobre segurança e privacidade.

Para além das questões, conceitos, de segurança e privacidade, serão, também, abordados outros conceitos e possíveis variáveis do estudo, como confiança, facilidade de utilização percebida, utilidade percebida e, ainda, risco e controlo percebido. Serão, também e à semelhança dos capítulos anteriores, abordados conceitos complementares para uma compreensão do funcionamento da *cloud* e a sua relação com as questões de segurança e privacidade, como, por exemplo, o ciclo de vida de dados e o modelo de aceitação de tecnologia estrutura de pensamento para a elaboração do trabalho.

Completada a abordagem de conceitos e modelos, no final será apresentada uma breve conclusão do que será aqui abordado.

4.2 – Contextualização

Chegados a este ponto, interiorizado o funcionamento da tecnologia e, por isso, com uma melhor capacidade de abstração e compreensão, é, no entanto, útil fazer uma breve contextualização, a qual se segue.

Durante a exploração das características, benefícios e desafios da *cloud*¸ foram várias vezes mencionadas as ideias de privacidade e segurança. De facto, quase tudo que caracteriza esta tecnologia pode originar ou pelo menos associar-se a este tipo de preocupações. Sendo percebidas como as maiores forças dissuasoras de adoção da *cloud*, é, precisamente, nelas se irá focar este próximo capítulo. E, é, realmente, isso que estes dois conceitos representam, desafios. Como qualquer outra posse tangível ou intangível, a informação só está segura quando existe e é acedida apenas pelo proprietário, o que cria a ideia, mais ou menos enraizada, que a privacidade e a segurança de dados na *cloud,* é como um processo de troca contínua, com os enormes benefícios de computação em nuvem. Há uma procura de computação em nuvem porque é desejada e necessária a facilitação de armazenamento, processamento, recuperação

e comunicação de informação e dados, sendo que para tal, é necessário o fluxo destes últimos, desde o momento da sua criação, até ao momento da destruição dos dados que vão sendo acedidos ao longo daquilo que se designa de ciclo de vida de dados, algo posteriormente abordado.

Todas as inovações tecnológicas que atuam nesta área apresentam a mesma troca de praticabilidade e facilidade com algum nível de perda de segurança e privacidade. Na essência, sempre que se adiciona pontos de acesso e tratamento de dados, está-se a adicionar pontos de falha, onde a segurança e a privacidade podem ser postos em causa. Por isso, é compreensível que se sinta algum receio, tal como se sentiu com a introdução de servidores, computadores portáteis e todos os métodos de transporte de informação e dados (e.g. disquetes, CDs, DVDs e *pen drives*). Ainda assim, o maior desafio foi introduzido pela internet, que acaba por ser exemplificativo da evolução e adaptação dos utilizadores. Durante anos as pessoas, por serem informadas ou por simples receio, não se aventuravam a introduzir qualquer tipo de informação numa página de internet. No entanto, hoje em dia e cada vez, as pessoas têm uma crescente e cada vez mais detalhada pegada na internet, sendo bem característico as áreas de comércio eletrónico e as redes sociais. Hoje em dia, a norma começa a ser uma onde o utilizador não tem grande receio de partilhar e facilitar informação pessoal e bancária, o que por si só pode ser um fator de risco.

Voltando à *cloud*, os receios começam a torna-se aparentes e compreensíveis. A *cloud* vem combinar tudo o que foi mencionado. Ainda assim, também é defendida a ideia que, em igualdade de circunstâncias, apesar da *cloud* ser algo mais público, mais exposto, é, ainda assim, a solução mais segura. Numa perspetiva empresarial e como podemos ler num artigo de Joe McKendrick (2014) para a Forbes, podemos ver que, segundo um estudo pela Alert Logic, os principais receios de segurança e privacidade (ataques externos), começam a ser quantitativamente semelhantes entre soluções *cloud* e as tradicionais soluções internas (*in-premises*). Isto significa que, excetuando as grandes empresas, com vastos recursos para a criação e a manutenção de soluções próprias, a *cloud*, mesmo uma pública, terá medidas de segurança superiores. Numa perspetiva de um utilizador individual, para uso pessoal, levanta-se, também, uma ideia que, apesar de a *cloud* e as grandes empresas, estarem mais expostas ao mundo, logo, potencialmente mais suscetíveis a ataques, a verdade é que as medidas de segurança que estas são capazes de criar e aplicar, protegem a nossa informação e dados melhor, do que um utilizador pessoal, tendo recursos, conhecimento e tecnologia que o utilizador não tem.

Como podemos ler no livro de Barnatt (2010), a realidade é que *cloud computing*, como referido, é uma necessidade e vai continuar a ser adotada progressivamente. Uns serão mais receosos que outros, podendo perder alguns benefícios da tecnologia colhidos e apreciados pelos pioneiros, seja numa vertente pessoal, ou, ainda mais significativamente, numa vertente empresarial. Mesmo assim, “isto não significa que devemos ignorar legitimas preocupações de

segurança . . . No entanto, com as devidas precauções, a maioria das situações, incluindo *cloud computing*, podem ser enfrentadas com um nível aceitável de risco." (Barnatt, 2010, p. 109).

O que se vai abordar de seguida, baseia-se nos trabalhos de Mather, Kumaraswamy e Latif (2009), Barnatt (2010), Halpert (2011), Jansen e Grance (2011), Macia e Thomas (2011b), T-Systems (2012), T-Systems (2010), Shimba (2010), Javaid (2014), Kok (2010), Muijnck-Hughes (2011), Saleem (2011) e Badger et al. (2012). Outras fontes utilizadas, tal como anteriormente, serão utilizadas e identificadas em citações.

Finalmente, antes de se passar ao real estudo de segurança e privacidade, salvaguarda-se dois pontos. Em primeiro lugar, existem três perspetivas, a do consumidor, a do fornecedor e a do regulador, apesar de se focar mais a do consumidor. Tal, como anteriormente, as observações serão feitas em conjunto, fazendo notas e referências a uma específica perspetiva quando necessário. Em segundo lugar é necessário dissipar o equívoco em que privacidade é meramente um subconjunto da categoria de segurança. "Pode-se ter segurança e não privacidade, mas, não se pode ter privacidade sem segurança" (Mather, 2011, p. 145). Segurança e privacidade estão inter-relacionadas e é verdade que é a segurança que propicia e possibilita a privacidade, mas, privacidade é algo demasiado importante ideologicamente e levanta questões únicas. Assim sendo, devem ser tidas como dois conceitos íntimos, mas únicos.

4.3 - Privacidade

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei." (Artº 12º, Declaração Universal dos Direitos Humanos, 1948)

Esta ideia deveria englobar a nossa informação e dados e é nesse sentido que se estão a levar a cabo esforços de legislação, mas, tal não é o caso, embora existam movimentos nesse sentido.

Vários trabalhos (Antikainen, 2014; Lessig, 2006; Vogl, 2000) apontam esta ideia de desfasamento entre evolução tecnológica e a evolução legislativa, embora existam esforços no sentido de uma melhor legislação e regulamentação, como por exemplo, as diretivas de proteção de dados da União Europeia (UE) e que refletem um compromisso para que a privacidade de dados seja um direito humano, como a liberdade de expressão. A realidade é que legislação para privacidade está muito atrasada, relativamente à evolução tecnológica. Alias, a ideia que parece dominar, é que a legislação, num todo, relativa à área tecnológica, parece estar constantemente atrasada. Este constante atraso é compreensível através de um puro exercício mental. Estando todos outros possíveis fatores de parte, não se pode legislar sobre algo que não existe e a

tecnologia prima em caminhar para o desconhecido. Segundo a Lei de Moore[23], a tecnologia computacional cresce exponencialmente, o que produz inovações inesperadas em períodos de apenas cinco a dez anos e isto traduz-se num moroso acompanhamento da sociedade e política e, consequentemente, da legislação.

Como foi referido, tem havido avanços, mas, como refere Monique Goyens[24](citada em *theguardian*, Julho de 2015), no caso concreto da Europa, as leis "estão a atrasar-se relativamente ao ritmo das tecnologias e práticas negociais", acrescentando ainda algo importante, na perspetiva do consumidor, que é o facto de "os nossos dados pessoais serem colecionados e posteriormente utilizados e transferidos, de formas, às quais, a maioria dos consumidores são totalmente ignorantes. Uma atualização adequada deve voltar a colocar o controlo de dados pessoais nas mãos dos consumidores europeus."

Complementando esta ideia e para se ter uma melhor noção deste desfasamento, a partir de uma análise por Van Eecke (2009) publicada pela *Information Systems Audit and Control Association* (ISACA), podemos ver na figura abaixo o nível de atividade no que toca à evolução tecnológica e à legislativa.

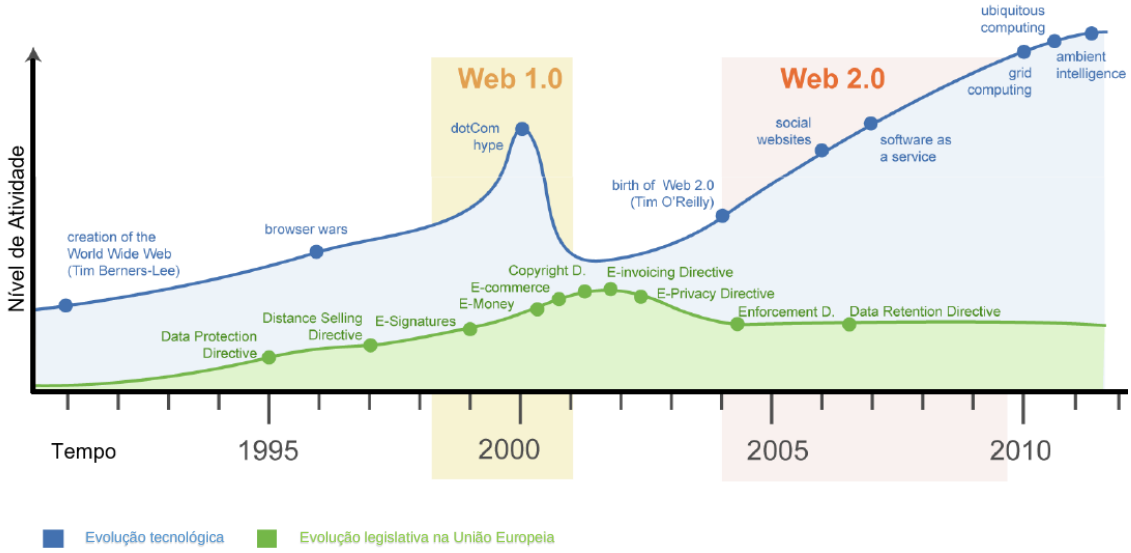

Figura 5 – Nível de atividade (evolução) tecnológica e legal pela passagem de tempo.

Fonte 1: adaptado de Van Eecke (2009, p. 2).

[23] Lei de Moore: "O número de transístores, incorporados num chip, deverão, aproximadamente, duplicar a cada 24 meses." (Moore, 1965) – Predição confirmada e adotada pela indústria de semicondutores para planeamento a longo prazo.
[24] Diretora geral da European Consumer Organisation

Ainda relativamente à legislação e à regulamentação, de mencionar que, de acordo com alguns artigos (Ryan 2014, p. 505; Trope & Hughes, 2011; Von Baum, 2012), os dois principais modelos existentes, para lidar com as questões de segurança e privacidade, são o dos Estados Unidos, onde a regulamentação é fragmentada e exercida questão a questão e o modelo Europeu, que opta por uma direta regulamentação da tecnologia de computação em nuvem.

Relativamente ao caso Europeu, algo muito importante, é o facto de a legislação procurar alcançar maior facilidade de portabilidade entre os fornecedores de serviço, regras uniformes além-fronteiras, bem como, uma obrigação para que os dados pessoais, tratados por empresas estrangeiras, estejam sujeitas à mesma regulamentação (Ryan 2014; Comissão Europeia, 2012). Isto representa um dos maiores e mais atuais problemas que atacam a privacidade, mas, não será necessariamente o único.

4.3.1 - Definição de privacidade

Começando pelo início, o que é privacidade? Como já vem sendo referido, "o conceito de privacidade varia largamente entre (e por vezes, dentro) países, culturas e jurisdições. É moldada pelas expectativas do público e interpretações legais" (Mather et al. 2009, p. 146), o que impossibilita uma definição rígida e única.

Dito isto, existe uma definição que se tem tornado na geralmente aceite, conceptualizada pela *American Institute of Certified Public Accountants* (AICPA) e *Canadian Institute of Chartered AccountatsI* (CICA) para os standards GAPP, que diz que, privacidade remete-se para "os direitos e obrigações dos indivíduos e organizações, no que respeita à recolha, uso, retenção e divulgação de dados pessoais[25]" (AICPA, 2005, p. 2), ao longo de um ciclo de vida onde de espera a responsabilização e transparência por parte da organização que fornece o serviço, para com o seu consumidor.

Complementarmente, a Organização para a Cooperação e Desenvolvimento Económico (OCDE), define privacidade como um "estatuto concedido a dados, acordado entre a pessoa ou organização que que fornece os dados e a organização que os recebe, que descreve o grau proteção que será provida" (OCDE[26], 2005).

4.3.2 - Ciclo de vida de dados

Interessa, neste momento, concretizar e demonstrar o ciclo de vida de dados, lingando-o a conceitos já abordados. É neste ciclo, que se espera que a organização faça uma gestão correta e transparente dos dados pessoais.

Segue-se, então, conforme a publicação de Mather et al. (2009), o gráfico representativo deste ciclo, bem como, as componentes de cada uma das representadas fases. É importante perceber,

[25] Dados Pessoais: "Qualquer informação relativa a um individuo identificado ou identificável" (OCDE, 2013)
[26] https://stats.oecd.org/glossary/detail.asp?ID=6959

em cada estágio, quais as relevantes questões que se impõem e que devem ser ponderadas pelo consumidor. Mais uma vez, é no caso de um consumidor organizacional que todas as questões levantadas se tornam realmente importantes. Dados pessoais são um assunto cada vez mais importante e, o consumidor pessoal, apenas tem o poder e a preocupação de decidir se usa, ou não, determinado serviço. Já o empresarial tem que dar toda a atenção ao impacto que o ambiente *cloud* tem na proteção de dados.

De seguida apresenta-se a representação do ciclo de vida de dados.

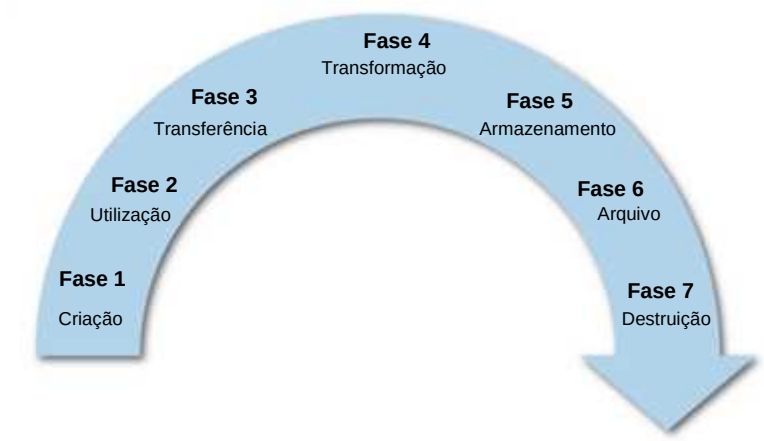

Figura 6 - Representação do Ciclo de Vida de Dados, por KPMG

Fonte: Mather et al. (2009, p. 147)

Após a apresentação da representação do ciclo de vida de dados, passamos, para, a descrição de cada fase e indicação questões/problemas pertinentes em cada uma destas. A abordagem que se segue é suportada pelos trabalhos de Mather et al. (2009) e Bhushan, Khetan e Gupta (2013) e, ainda, Yu e Wen (2010).

Começando pela fase um, criação de informação. É nesta fase que se cria dados, do nada. Esta criação pode acontecer do lado do consumidor ou do lado do fornecedor. Independentemente de onde os dados são criado, assim que estes estejam na *cloud*, deve-se questionar qual das partes envolvidas detém os direitos de propriedade sobre estes, quais os parâmetros que o fornecedor utiliza para proceder à classificação daquilo que é, ou não, informação pessoal e, ainda, a questão de se existirá, logo neste momento, uma definida infraestrutura de governança, que, assegure a gestão e proteção dos dados do consumidor.

Passando para a fase dois, utilização de dados, fazer, antes de mais, uma salvaguarda. O ciclo de vida representado na figura acima, é diferente, daquele que é abordado por Yu e Wen (2010) e Bhushan et al. (2013), no sentido em que, estes apontam para pequenas diferenças na ordenação das fases do ciclo de vida dos dados. Esta é uma diferença, conceptual, é mínima e,

não tem impacto neste trabalho. Assim, seguiremos conforme a apresentada representação, pela KPMG ilustrada em Mather et al. (2009, p. 147). Assim, esta fase refere-se ao acesso, extração e diversos tipos de utilização dos nossos dados, logo, levantam-se imediatamente questões no que concerne à segurança e privacidade dos mesmos. Quem é que acede e utiliza os nossos dados, apenas a empresa com quem subscrevemos o serviço, ou, os dados são terceirizados? Ao mesmo tempo, é necessário clarificar se utilização é adequada aos propósitos pelos quais os dados foram recolhidos, se há encriptação e, novamente, se há uma infraestrutura capaz de gerir e garantir privacidade e segurança, bem como, observância para com requisitos e procedimentos legais, a todo o momento e caso seja necessário.

Na terceira fase, temos a transferência de dados, que se prende, como o nome indica, com o transito dos dados, sendo que a questão é se o transito é exclusivamente interno (i.e não sai do fornecedor de serviços), ou, se há um movimento para fora do fornecedor, a referida terceirização de dados. Primeiro caso, não há grandes problemas, mas, no segundo, transito externo, requer vários cuidados, é necessária proteção e encriptação adequada dos dados. Ao mesmo tempo, o transito de dados entre organizações, pode significar diferentes regulamentações e legislações, as quais devem ser obedecidas. Por fim, mais uma vez, deve existir uma infraestrutura capaz de gerir e controlar o acesso a esses mesmos dados.

Passando para a quarta fase, a transformação de dados. Como referido, a partir do momento que os dados entram na *cloud*, são categorizados e, consequentemente, transformados e processados, processo denominado de derivação. Neste momento deve-se questionar se esta transformação implica uma alteração das proteções e restrições de utilização dos dados, isto, porque, se há uma transformação de dados, a caracterização inicial mantem-se, ou, é alterada. Se for alterada, o uso que pode ser dado aos dados, pode ser diferente. Como exemplo, após a derivação, existe a agregação de dados. Quando os nossos dados são agregados com os de outros, será que deixam de ser identificáveis como os meus dados pessoais? Sendo esse o caso, então deixam de ser considerados dados pessoais e, novamente, temos uma situação onde os níveis e tipos de utilização, permitida, sobre os dados é alterada, significando uma perda de integridade dos mesmos.

Armazenamento de dados, a quinta fase do ciclo. O armazenamento significa a colação dos dados, numa espécie de estado de descanso, algures nas plataformas da *cloud*. Neste momento, as questões que se devem por é se existe um, adequado, controlo de acessos, como é que os dados são armazenados, como é assegurada e mantida a integridade, confidencialidade e disponibilidade de dados que, deverão estar em repouso. Por fim, existe legislação que obriga a que certo tipo de dados pessoais, sejam armazenados apenas quando encriptados, logo, é necessário garantias de que o fornecedor não só é capaz de o fazer, como se facto o faz. Terminado esta ideia, convém focar uma inerente dicotomia. Por um lado, os dados devem estar encriptados, da forma mais coesa possível, por outro, devem estar disponíveis a qualquer momento. Sendo que encriptação afeta performance, origina-se mais um problema.

Seguindo para a sexta fase, o arquivo de dados. Esta fase refere-se a um mais profundo estado de armazenamento, sendo uma espécie de hibernação de dados. Ou seja, é processo de armazenamento de dados que, supostamente, não serão acedidos durante algum tempo. Normalmente, o arquivo de dados significa a transferência destes para dispositivos média (e.g. *pen drive,* CD, DVD, ou outros), isto, ou, então, os dados são "simplesmente" lançados e armazenados noutra plataforma da *cloud*, própria para este profundo armazenamento. Em qualquer dos casos, há transito ou transferência de dados, logo, todas as questões anteriores de infraestruturas capazes, transparência, observância legal e outros, volta a ter que ser questionado. Outras questões são mesmo, qual a solução escolhida (i.e. outra plataforma *cloud*, dispositivos media físicos), onde serão armazenados (i.e. *in-premises* ou *off-premises*) e se esses meios garantem a integridade e longevidade dos dados, bem como, o seu futuro acesso.

Por fim, a sétima fase, destruição de dados. O objetivo de destruição de dados é, supostamente, um de nunca mais existir utilização de referidos dados. É suposto haver uma total e irreversível destruição de dados, mas, é necessário saber que garantias existem, que, tal destruição aconteceu e é irreversível, não deixando qualquer possibilidade de recobro e "má" utilização desses mesmos dados.

Estas sãos as principais preocupações da *cloud*, os acessos, garantias de observância legal, a forma como o armazenamento de dados é feita e mantida, as consequências da retenção/arquivamento de dados e, ainda, as garantias de que os dados serão mesmo destruídos e irrecuperáveis. Em todos as mencionadas fases existem enumeras questões de auditoria, monitorização e possíveis violações de privacidade.

Todas estas questões tornam mais percetíveis, mais palpáveis as preocupações que se deve ter. De seguida, passamos então para uma abordagem, semelhante, relativamente à segurança.

4.4 - Segurança

A "computação em nuvem é um pesadelo de segurança e não pode ser tratado de forma tradicional", diz CEO da Cisco John Chambers, citado por McMillan (2009). A complexidade de computação em nuvem faz com que a segurança seja algo de suprema importância, tanto para fornecedor de serviço, como para consumidor, sendo que, o nível de confiança entre os dois depende como e quanto o fornecedor consegue apelar aos sentimentos do consumidor (Shimba, 2010). Claro que tem de existir uma relação positiva entre as expectativas criadas e a eficácia real de medidas e resultados de segurança.

Neste momento vamos explorar estes elementos, os diferentes problemas de segurança de computação em nuvem, aludindo a como estes representam uma possível barreira à utilização da tecnologia, conceito de confiança e, ainda, possíveis formas de mitigação das referidas vulnerabilidades.

4.4.1 - Definição de segurança

A segurança, normalmente, "refere-se ao nível de proteção contra dano, perda, perigo ou atividade" (Changchit, 2014, p. 314) e "ter consciência de segurança é algo importante para todos os indivíduos que lidam com dados sensíveis no seu dia-a-dia" (Changchit, 2008). Segurança "é, ao mesmo tempo, um sentimento e uma realidade . . . não são a mesma coisa" (Schneier[27], 2008) sendo que, uma definição de segurança varia conforme o contexto.

Por exemplo, no caso de E-commerce [28], Yesisey, Ozok & Salvendy (2005) definem segurança como o nível de segurança que os utilizadores sentem enquanto efetuam compras *online*.

Numa visão tecnológica mais abrangente, Roca, Garcia e De La Veja (2009) definem segurança percebida como uma ameaça que gera circunstâncias, condições ou eventos com potencial para provocar constrangimentos a dados ou recursos de redes informáticas, através da destruição, divulgação ou modificação de dados, ou, ainda, através de atos de fraude, desperdício, abuso e ataques *DDoS*. Todos estes temas abordados previamente neste trabalho.

Flavian e Guinalíu (2006), complementam a ideia de segurança com algo relevante a este trabalho, defendendo que a segurança percebida pelo utilizador se trata de uma mera probabilidade subjetiva, com a qual, os utilizadores acreditam que, de acordo com as suas confiantes expectativas, a sua informação pessoal (dados) não será visualizada, armazenada ou manipulada, por intervenientes impróprios, durante o trânsito e armazenamento desses mesmos dados.

Algo que se percebe perfeitamente, tendo em conta o que foi abordado, neste trabalho, relativamente ao ciclo de vida de dados. Mesmo em repouso, leia-se armazenamento, os dados podem ser alvo de tais práticas, ações como o mero acesso a estes apenas aumentam a probabilidade e/ou pontos de falha para que referidos atos aconteçam. (e.g. piratas informáticos).

4.4.2 - Importância

Aproveitando a síntese de Hashemi (2013), pondo tudo o resto de parte, a verdade é que a segurança de dados é um fator chave de qualquer TI e a computação em nuvem não foge à regra (Sachdeva, 2011). Ao longo de toda a revisão de literatura ficam patentes lacunas de conhecimento por parte do utilizador (e.g. como e onde os seus dados são armazenados e tratados) e, por isso, independentemente do quão influente é e como influencia o utilizador, o fornecimento de segurança parece proeminente (Gharehchopogh & Hashemi, 2012).

Neste seguimento, podemos também compreender que a importância da segurança é diretamente proporcional à quantidade, ou nível, de riscos de segurança e estes variam, como

[27] https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html
[28] *E-Commerce*: Atividades relativas à venda e compra de bens e serviços através da internet (Merriam-Webster.com, 2015)

foi sendo abordado ao longo do trabalho, com as próprias características e modelos de implementação da tecnologia. No entanto, os controlos e os protocolos de segurança aplicados à *cloud* são os mesmos, ou semelhantes, àqueles utilizados, geralmente, nas TI, mas, ao contrário das TI, o controlo de segurança é realizado não pelo utilizado, empresarial ou pessoal, mas, sim, pelo fornecedor de serviços (Pearson, 2012), o que mais uma vez nos leva a questões da necessidade de regulamentação e homogeneização de práticas e SLA's (Hashemi, 2013).

4.5 - Principais problemas de segurança

Durante a definição da tecnologia foram dados alguns exemplos, na abordagem ao ciclo de dados, na parte de privacidade, bem como, foram levantadas perguntas, mas, agora, vai-se identificar, clara e sucintamente, os principais problemas e ameaças de segurança na *cloud*.

Aproveitando a identificação das principais ameaças e problemas, por parte de *Cloud Security Alliance* (2013) e Jansen e Grance (2011), complementando com os trabalhos de Kwofie (2013), Muijnck-Hughes (2011), Shimba (2010) e Kok (2010), seguimos, então, para a abordagem destes problemas.

4.5.1 - Violação de dados

Seja na *cloud*, seja no computador ou qualquer dispositivo pessoal, se está ligado à internet há o risco de alguém conseguir entrar, aceder e controlar os seus dados.

4.5.2 - Perda de dados

Seja por ataque de terceiros, por erro humano ou de sistema, falha de sistema ou dano físico provocado ao *hardware*, a perda de dados é sempre uma possibilidade, sendo considerada a segunda maior ameaça aos nossos dados.

4.5.3 - Invasão de conta e serviços

Tida como a terceira maior ameaça, temos a invasão/roubo (*hijacking*) de conta e serviços. Ou seja, tanto os dados em repouso como em uso/transferência podem ser acedidos e roubados, seja por métodos de *phishing*, fraude ou simples más praticas no que toca a *passwords*. Uma pessoa pode conseguir acesso a uma conta ou serviço e, a partir dai, aumentar o seu domínio, diminuindo o nosso, numa situação algo semelhante e que também pode resultar em roubo de identidade. Simplesmente, antigamente, tentava-se através da obtenção de informação física, como cartas e, agora, faz-se através de dados eletrónicos.

4.5.4 - APIs inseguros

A quarta ameaça, com tendência a deixar de o ser, são as interfaces dos programas que o consumidor utiliza para interagir com a *cloud*. Sendo, na essência, um programa, está sujeito a tornar-se vulnerável a nível de codificação. Mesmo que não seja o caso, existem APIs mais seguros do que outros. Por exemplo, fazer o *login* num fórum qualquer, sendo necessário apenas utilizador e *password*, será, à partida, menos seguro do que fazer login num banco, onde temos de introduzir números de contrato, *passwords*, código de um documento físico e, ainda, possivelmente, um código enviado para o telemóvel no ato de login.

4.5.5 - DoS

Algo que tem estado muito presente na atualidade e que por isso tem subido na escala de ameaça são os ataques de negação de serviço, os *DoS* ou *DDoS*. É algo que compromete a disponibilidade dos nossos dados ou serviços, a nossa capacidade de aceder ou utilizá-los, através de uma sobrecarga do sistema. Embora, por norma, sejam direcionados ao fornecedor de serviços, podem, também, ser direcionados ao consumidor. Muito cedo neste trabalho foi dado o exemplo de uma vulnerabilidade do programa Skype, que permitia a terceiros obterem o endereço IP do consumidor, dirigindo a este um ataque *DDoS*.

4.5.6 - Pessoa maliciosa (do lado do fornecedor)

Embora seja algo que esteja em queda, a ameaça de um funcionário, ex-funcionário ou um parceiro, do fornecedor de serviços, que tem ou teve credenciais de acesso aos nossos dados, continua a ser uma situação real. Não é impossível que alguém com referidas credenciais, seja por que motivo for, decida exceder os seus limites e deveres, alterando, divulgando ou destruindo os dados do consumidor.

4.5.7 - Abuso dos serviços *cloud*

Foi dado o exemplo de “invasão de conta e serviços”, sendo exemplificado o consumidor como alvo, mas, é possível que o alvo de semelhante ato seja o fornecedor de serviços e não o consumidor final. Embora seja extremamente mais difícil alguém conseguir acesso e controlo ilícito sobre os recursos de um fornecedor de serviços, podem utilizar a capacidade dos recursos do fornecedor, para atacar todos os utilizadores. Por exemplo, alguém que consiga tal acesso, pode infetar todos os consumidores de um dado fornecedor/serviço com um vírus.

4.5.8 - Diligências insuficientes

Este problema liga bem com este trabalho, pois, remete-nos para uma situação em que um consumidor adota totalmente a *cloud,* sem qualquer conhecimento ou compreensão desta. Simplificadamente conforme estamos a avaliar, a *cloud* tem riscos, independentemente do nosso

nível de conhecimento. Logo, o adotar a *cloud* sem qualquer diligencia, sem qualquer cuidado para minimizar riscos, é, por si só, um acréscimo de risco.

4.5.9 - Problemas de partilha de tecnologia

A partilha de recursos no ambiente de computação em nuvem significa partilha de riscos. Qualquer coisa que afete recursos que sejam utilizados, por um dado consumidor, vai provocar danos nos dados daquele. É algo que se retira e compreende dos outros problemas de segurança, se os recursos *cloud* de um fornecedor forem comprometidos, *malware,* acessos por piratas ou qualquer outro problema, todos os recursos ligados àqueles que foram comprometidos, estão comprometidos. Ou seja, é uma questão de multiplicação de risco no que toca ao acesso e a qualquer tipo de manipulação ou perda de dados, visto que um determinado consumidor não tem que ser o alvo por forma a ser afetado. Componentes interligados têm o mesmo destino.

4.6 - Confiança

Aproveitando a sintetização de Hashemi (2013), define-se agora o conceito de confiança. Tal como outras definições, mais notoriamente a definição de computação em nuvem, a confiança pode ser definida de várias formas, de acordo com quem a define, área ou finalidade, mas, para a tecnologia em questão, segundo termos e fontes mais académicas, a mais aceite diz que "confiança é um estado psicológico, que compreende a intenção de aceitar vulnerabilidade, com base em expectativas positivas sobre as intenções ou comportamentos de um outro" (Rousseau, Sitkin, Burt & Carmer, 1998, p. 395). A confiança é um conceito que se pode associar a seguidores (Pearson, 2012; Jaeger & Fleischmann, 2007) e, neste caso, esta definição tem que ser vista como algo dinâmico e mutável, tanto na sua dimensão como capacidade, sendo uma extensão do conceito de segurança que inclui critérios psicológicos e práticos, dividindo, assim, confiança em tipos ou níveis (Pearson, 2012; Rousseau, Sitkin & Camerer, 1998): a) *hard trust* - orientada para a segurança; b) *soft trust* - não orientada para a segurança. Ou seja, existe uma confiança mais rígida (*hard trust*) que inclui fatores mais palpáveis e racionais como validade, codificação e segurança dos processos, enquanto a *soft trust* se encaixa numa dimensão mais imaterial, como é a psicologia do ser humano (neste caso o utilizado), lealdade para com uma marca e facilidade de utilização (Wang & Lin, 2008).

Um claro exemplo de *soft trust* é o fator fama que hoje em dia algo que se observa cada vez mais, dada a crescente componente *online* e, também, por aqui conseguimos compreender a importância de fatores como a segurança e privacidade, isto porque, o gostar de uma marca significa confiar nessa marca e se ela falha em aspetos que afetem essa confiança (como a privacidade), essa marca vai perder para outras, tanto em notoriedade como em fidelização (Singh & Morley, 2009).

Passando para uma explicação mais concreta e mais relativa à computação em nuvem e que nos permite compreender melhor os possíveis comportamentos do utilizador, em primeiro lugar, as pessoas ainda tendem a confiar mais no aspeto físico e palpável, ao invés da abstração da *cloud* (Pearson, 2012; Osterwalder,2001; Best, Krueger & Ladewig, 2008). Há mesmo quem defenda que o nível de segurança não afeta a confiança (Pearson, 2012; Nissenbaum, 1999), mas, em pessoas que já tenham intenção de uso de um dado serviço, podem ver a sua confiança, num fornecedor de serviço aumentar, caso lhe sejam dadas mais garantias de segurança (Giff, 2000), o que, novamente, explica alguma parte do comportamento dos utilizadores.

Então, se a *cloud* ainda tem um menor nível de confiança, e esta é algo volátil e relativa, é necessário compreender como aumentar a confiança dos utilizadores para com a tecnologia e fornecedores de serviço. Neste sentido, Hashemi (2013), Gharehchopogh e Hashemi (2012) e Zissis e Lekkas (2012) dão um exemplo claro, quando comparam a situação com o ato de levantar dinheiro numa caixa multibanco. Nós, consumidores, confiamos numa caixa multibanco, porque sempre que levantamos dinheiro ela dá-nos o dinheiro certo, existe essa certeza. A tecnologia de computação em nuvem, os seus fornecedores e outros intervenientes precisam de apontar a esse nível de certeza, criando e construindo, gradualmente, confiança, tal e qual à caixa multibanco.

4.6.1 – Risco percebido

Conforme se pode ler no trabalho de Lourenço e Fortes (2013), risco percebido, deriva de confiança, sendo, objetivamente, a falta de confiança. Risco percebido é uma grande barreira à adoção de tecnologias, especialmente, relativamente a tecnologias *online*. Esta perceção, que se pode definir como uma combinação de incertezas, uma expectativa de perdas associadas a um especifico comportamento, sendo, por isso, um inibidor de tal comportamento.

Complementarmente, Mitchell (1999), afirma que esta perceção pode inibir, de facto, a adesão de tecnologias, especialmente, no caso de inovações, dado que, os consumidores têm menos experiência.

4.7 - Controlo percebido

Controlo percebido, uma importante variável neste estudo, é definida por Ajzen (1991), como um conjunto de perceções individuais, de diferenciação, do quão fácil ou difícil é manifestar um comportamento especifico, sendo que, um estudo de Mathieson (1991), descobre e comprova que controlo percebido era determinante na adoção de uma dada tecnologia.

4.8.1 - Definição

Como podemos ver nos trabalhos de Davis (1989), Bagozzi, Davis e Warshaw (1989) e Bagozzi, Davis e Warshaw (1992), o Modelo de Aceitação de Tecnologia (TAM), foi introduzido por Fred Davis em 1986 e tinha como base a Teoria de Ação Racional (TRA). Como o nome indica, este modelo lida com a previsão da aceitação de tecnologia, tendo como objetivo identificar o porquê de os utilizadores aceitarem ou rejeitarem uma tecnologia, identificando-se, por consequência, as alterações necessárias para que uma dada tecnologia fosse aceite pelos utilizadores.

4.8.2 – Modelo TAM

De acordo com Bagozzi (2007) e Davis et al. (1989) este modelo foi um sucesso e segundo autores como Lee, Kozar e Larsen (2003), o TAM é mesmo considerado o mais influente e utilizado modelo desta área.

Na figura que se segue, é apresentado o modelo TAM. Um modelo que, funcionalmente, aponta à medição do impacto de fatores externos sobre as perceções internas, sobre as atitudes e sobre as intenções comportamentais do utilizador, tentando projetar o real uso de uma tecnologia por parte deste (Davis et al. 1989).

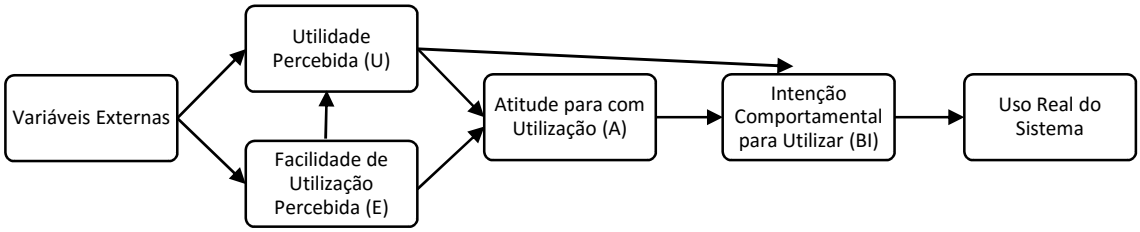

Figura 7 - Teoria de Aceitação de Tecnologia (TAM)

Fonte: Davis et al. (1989)

Ou seja, o modelo tem quatro principais variáveis: i) utilidade percebida; ii) facilidade de utilização percebida; iii) atitude para com utilização; iv) intenção comportamental para utilizar;

Dentro destas quatro, os dois principais constructos para o comportamento de aceitação são (Davis et al. 1989, p. 895): i) utilidade percebida (U) referente à "a probabilidade subjetiva que a utilização de um sistema de aplicação específico, por parte de um potencial utilizador, irá aumentar o seu desempenho dentro de um contexto organizacional."; ii) facilidade de utilização percebida (E) que representa o "grau em que, o potencial utilizador, espera que o sistema em causa seja livre de esforço."

A utilidade percebida tem uma influência significativa na intenção de uso (Agarwal & Prasad, 1999; Vankatesh & Davis, 2000; Vankatesh, 2000; Davis, Bagozzi & Warshaw, 1989).

A facilidade de utilização percebida é um fator crucial na compreensão de sensibilidades individuais para com tecnologias de informação (Agarwal & Karahanna, 2000; Hong, Thing, Wong & Tam, 2001; Chau & Hu, 2001) e, tal como a utilidade percebida, a sua clara influência sobre a intenção comportamental para utilizar (BI) está mais que comprovada (Agarwal & Prasad, 1999; Vankatesh & Davis, 2000; Vankatesh, 2000).

Segundo Davis et al. (1989), explicando o modelo, o uso real do sistema é determinado pela intenção comportamental para o utilizar, o que por sua vez é motivada pela utilidade percebida e pela atitude para com a utilização de tal sistema. Por sua vez, U e A são diretamente influenciadas pela facilidade de utilização percebida, sendo que U é também influenciado por variáveis externas que também influenciam E. Ou seja, as variáveis externas e/ou os fenómenos diretos de utilidade percebida e a facilidade de utilização percebida, afetam diretamente a atitude e a intenção de utilização de um sistema, o que irá ditar a uso ou não deste.

4.8.3 - Evolução e limites do TAM

Apesar de ter sido validade ao longo dos tempos, a verdade é que, conforme sumariado por Lee, Kenneth e Larsen (2003, p. 756), os mesmos estudos que validavam este modelo, encontravam, por vezes, resultados curiosos ou mesmo contraditórios.

Inicialmente Adams et al. (1992) validavam completamente este modelo, mas, posteriormente, Segars e Grover (1993) afirmaram que, embora, o uso de técnicas estatísticas clássicas o validem, uma analise fatorial confirmatória encontrava resultados contrários, sugerindo um modelo que adicionava o fator efetividade a par de utilidade percebida e facilidade de utilização percebida. Esta teoria foi suportada por Barki e Hartwick (1994) e foi refutada por Chin e Todd (1995).

Com isto, a TAM foi sendo adaptada e trabalhada, dando origem a várias versões até à mais recente teoria de Venkatesh, Morris, Davis e Davis, F. (2003), a Teoria Unificada de Aceitação e Utilização de Tecnologia (*Unified Theory of Acceptance and use of Technology* – UTAUT), conforme expresso na figura seguinte.

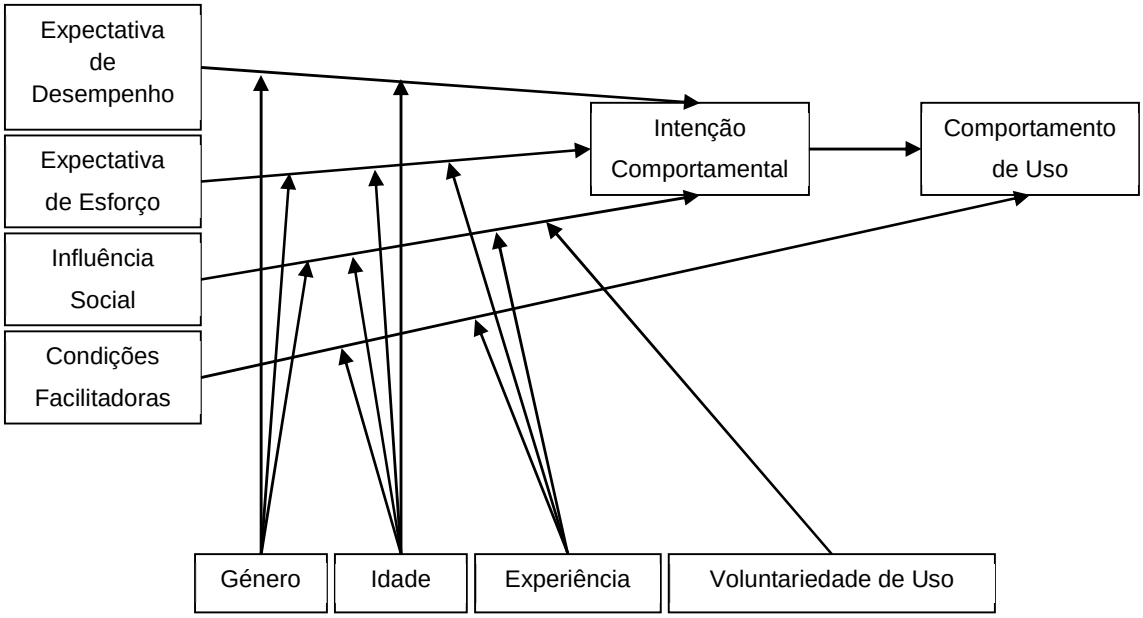

Figura 8 – Teoria Unificada de Aceitação e Utilização de Tecnologia

Fonte: Venkatesh et al. (2003, p. 447)

Sucintamente, segundo Venkatesh et al. (2003), trata-se de um modelo de compilação das diferentes variações da TAM, ao longo dos tempos, e que apresenta, agora, sete constructos que, como podemos ver na figura acima, influenciam a intenção comportamental que, por sua vez, influencia o comportamento de uso, tal como o constructo de condições facilitadoras.

Ainda a salientar que Vankatesh et al. (2003) identificam que o seu modelo explica “apenas” 70% da variância da intenção de utilização. Esta analise leva-nos ao que se aborda de seguida.

Toda a evolução da TAM, deve-se ao facto de ter alguns limites, tal com UTAUT as tem. Um modelo não pode servir para tudo e relativamente aos constructos destes modelos, “não existem medidas absolutas para aqueles constructos para todos os diferentes contextos tecnológicos e organizacionais . . . Modelos de medida devem ser rigorosamente avaliados e alterados conforme necessário.” (Segars & Grover, 1993, p. 525).

Seja pelo modelo em si, ou pela forma como o modelo é empregue nos estudos, existem limites e relativamente aos estudos, conforme sumariado por Lee et al. (2003).

Ou seja, a TAM é um modelo globalmente estabelecido, mas, tem os seus limites, como referido e como se costuma dizer “um tamanho não serve a todos”. Dai, a existência de algumas evoluções e, por isso, os autores sentem a necessidade de realizar algumas adaptações a este modelo, por forma a desenvolverem as suas investigações.

Assim, embora não se vá proceder a uma adaptação direta destes modelos, os mesmos permitem uma melhor compreensão, interpretação e abstração de conceitos, por forma a conseguirmos desenhar e sugerir, com maior confiança e suporte, um modelo teórico especifico a esta tecnologia e área de aplicação.

4.9 – Sintetização de conceitos e variáveis

Antes de concluirmos este capitulo, visto que, este marca o fim da revisão de literatura e o inicio da parte empírica, será útil fazer breve sintetização, com alguns autores e respetivas definições e conceitos, de forma extremamente sucinta.

Assim, apresenta-se na tabela que se segue, as principais definições e/ou conceitos, sendo que, tirando a definição de computação em nuvem, as outras representam as principais variáveis do estudo.

Autor	Conceito	Definição de conceito e variáveis
Mell & Grance (2011, p. 2)	Computação em nuvem.	"Modelo que possibilita o acesso por rede, de forma ubíqua, conveniente e sob pedido, a um conjunto partilhado de recursos computacionais configuráveis (e.g. redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente providos e libertados, com mínimo esforço de gestão e interação com o fornecedor de serviço. Este modelo *cloud* é composto por cinco características essenciais, três modelos de serviços e quatro modelos de implementação."
Artº 12º, Declaração Universal dos Direitos Humanos (1948)	Expectativa de privacidade.	"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."
AICPA (2005, p. 2)	Privacidade	"Direitos e obrigações dos indivíduos e organizações, no que respeita à recolha, uso, retenção e divulgação de dados pessoais."

OCDE[29] (2005)	Privacidade	"estatuto concedido a dados, acordado entre a pessoa ou organização que que fornece os dados e a organização que os recebe, que descreve o grau proteção que será provida."
Schneier[30] (2008)	Segurança	"é, ao mesmo tempo, um sentimento e uma realidade . . . não são a mesma coisa"
Rousseau, Sitkin, Burt e Carmer (1998, p. 395)	Confiança	"confiança é um estado psicológico, que compreende a intenção de aceitar vulnerabilidade, com base em expectativas positivas sobre as intenções ou comportamentos de um outro"
Lourenço e Fortes (2013); Mitchell (1999)	Risco percebido	Representa a ausência de confiança, sendo uma combinação de incertezas conjugadas com uma expectativa de perda associado a um especifico comportamento, que neste caso em concreto, pode inibir a adesão de tecnologias, em especial, inovações.
Ajzen (1991); Mathieson (1991)	Controlo percebido	Conjunto de perceções individuais, que procura averiguar o grau de dificuldade para a manifestação de um comportamento especifico, sendo uma perceção capaz de determinar a utilização, ou não, de uma tecnologia.
Davis et al. (1989, p. 895)	Utilidade percebida	"probabilidade subjetiva que a utilização de um sistema de aplicação específico, por parte de um potencial utilizador, irá aumentar o seu desempenho dentro de um contexto organizacional."
Davis et al. (1989, p. 895)	Facilidade de utilização percebida	"grau em que, o potencial utilizador, espera que o sistema em causa seja livre de esforço."

Tabela 1 – Sintetização das principais definições e variáveis para o estudo.

Fonte: adaptação própria dos autores referidos na tabela.

Com esta importante sintetização, termina-se este capitulo, seguindo-se agora uma sucinta conclusão antes de passarmos para as metodologias do estudo.

[29] https://stats.oecd.org/glossary/detail.asp?ID=6959
[30] https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

4.10 - Conclusão

Neste capitulo fez-se duas abordagens distintas. Por um lado, abordou-se, concretamente, as fragilidades e possíveis pontos de falha da tecnologia, no que toca à segurança e privacidade, enquanto, por outro lado, se abordou conceito sobre perceções do utilizador, que, segundo os estudos abordados, podem justificar a sua utilização, ou não, da tecnologia, bem como, ajudar a perceber a sua preocupação com este tipo de questões.

Neste momento é, provavelmente, mais importante, focar esses aspetos psicológicos.

Schneier (2008), aponta que a realidade de segurança se baseia na probabilidade de diferentes riscos e os quão eficazes são as medidas de mitigação de riscos são. Ou seja, a perceção de segurança é algo muito psicológica, o que significa que a tecnologia de computação em nuvem tem que criar sentimentos positivos no consumidor, sentimentos esses como a confiança.

Mantendo esta linha de pensamento, de fatores de foro psicológico, temos os abordados conceitos de confiança, risco percebido, controlo percebido, bem como, facilidade e utilidade percebidas.

Com isto em mente, os conceitos e definições de segurança e privacidade, parecem apontar, também eles, a um sentimento de pertença, como é o caso da necessidade de privacidade, que é algo que está presente em algo tão importante como a Declaração Universal dos Direitos Humanos. A nível de segurança, novamente, é uma questão de expectativas por parte do utilizador.

O próprio modelo TAM e as suas evoluções, apontam a isto mesmo. A adoção de tecnologias tem um cariz muito pessoal, sempre ligado aos conceitos abordados e supramencionados.

Este foco é importante, porque, ajuda-nos a fazer a transição para a parte do estudo empírico deste trabalho.

Capitulo V - Metodologia de investigação

5.1 - Introdução

Após a revisão de literatura procede-se, agora, neste capítulo à contextualização empírica da investigação, definindo-se o tipo e as metodologias de investigação, bem como, as bases e as hipóteses formuladas neste trabalho.

Em primeiro lugar, será apontada a questão de investigação que origina este estudo e que serviu de base às hipóteses formuladas.

De seguida, apresenta-se o formato de pesquisa efetuada, a identificação e a análise operacional das variáveis do estudo, da população alvo e amostra, bem como, o procedimento de recolha de dados.

Por fim, será explanado o processo de análise de dados e o tratamento das variáveis e testes estatísticos realizados.

5.2 - Metodologia

A metodologia de estudo traduz o conjunto de métodos de investigação escolhidos e utilizados, por forma a alcançar os objetivos definidos dentro de uma área de estudo (Bisquerra, 1989).

Segundo Kaplan (1988), a metodologia preocupa-se com a identificação de técnicas e princípios, os quais, ele designa de métodos. Estes devem ser suficientemente gerais, por forma a serem comuns às diferentes ciências e incluem procedimentos, como a realização de observações e medidas, descrição de protocolos, formulação de conceitos e hipóteses e a construção de modelos e teorias. A metodologia procura, ainda, descrever, analisar, assinalar limites e recursos, clarificando os seus pressupostos e consequências, tendo como finalidade absoluta a compreensão “não dos resultados do método científico, mas o próprio processo em si” (Kaplan, 1988, p. 23). Ou seja, antes da apresentação dos resultados, devemos, através da metodologia, compreender o método pelos quais aqueles foram obtidos.

5.3 - Tipo de pesquisa e estudo

Adequando-nos a o objeto de estudo em causa e visto que o objetivo é quantificar e descrever um fenómeno e estabelecer relações possíveis entre variáveis, utilizou-se uma investigação quantitativa, que, segundo Wilfred e Kemmis (1988), assenta num modelo hipotético-dedutivo que assume que um determinado problema tem uma solução objetiva.

Aliaga e Gunderson (2002) descrevem a investigação quantitativa como a explicação de um fenómeno, através da coleção de dados quantitativos (numéricos), para posterior análise

matemática e estatística. É um tipo de investigação que utiliza dados quantitativos, mas, também, dados não quantitativos, como crenças ou atitudes, "que são transformados para um formato quantitativo através da utilização de instrumentos de medida, como escalas de Likert" (Boutellier, Gasmann, Reader & Zeschky, 2013, p. 3).

Segundo Bisquerra (1989), Creswell (1994) e Wiersma (1995), citados por Coutinho (2011, p. 25), a pesquisa quantitativa caracteriza-se por:

- *enfâse nos factos, comparações, relações, causas, produtos e resultados do estudo";*
- *investigação é baseada na teoria, consistindo muitas das vezes em testar, verificar, comprovar teorias e hipóteses;*
- *plano de investigação estruturado e estático;*
- *estudos sobre grandes amostras de sujeitos, através de técnicas de amostragem probabilística;*
- *aplicação de testes válidos, estandardizados e medidas de observação objetiva do comportamento;*
- *investigador externo ao estudo preocupado com questões de objetividade";*
- *utilização de técnicas estatísticas na análise de dados;*
- *objetivo do estudo é desenvolver generalizações que contribuam para aumentar o conhecimento e permitam prever, explicar e controlar fenómenos*

Ainda segundo Coutinho (2011), os processos da metodologia quantitativa são, de forma ordenada, as seguintes: a) teoria a testar; b) problema e hipóteses derivados da teoria; c) conceitos e variáveis operacionalizados a partir da teoria; d) recolha de dados que confirmem a teoria

Relativamente ao nosso tipo de estudo este é de cariz exploratório, em termos de aplicação empírica em Portugal, podendo, eventualmente, gerar conhecimento sobre o tema de estudo. Este método tem o intuito de possibilitar a alteração de abordagem, por parte do investigador, conforme vão surgindo novos dados ou ideias (Saunders, Lewis & Thrinhill, 2009), algo que, segundo Adams e Schvaneveldt (1991) não significa ausência de direção, mas, sim, um natural afunilamento de ideias com o decorrer do estudo.

5.4 - Formulação de hipóteses de estudo e modelo proposto

Segundo Malhotra e Birks (2006a), as questões de investigação consistem em declarações refinadas que representam as componentes do problema em estudo, podendo ser conceptualizadas a partir de conhecimentos prévios e/ou adquiridos, ao longo do estudo atual, pelo qual, se procura a obtenção de respostas.

Neste trabalho a revisão de literatura assenta na tecnologia de computação em nuvem, colocando-se o foco sobre as suas vantagens e as desvantagens, dando-se uma às questões de segurança e privacidade. Assim, a questão geral de investigação é: “Será que, nas tecnologias de computação em nuvem, existe alguma relação entre as perceções de segurança, privacidade, conhecimento, confiança e frequência de utilização da tecnologia, que permita antever ou justificar o nível de preocupação, do consumidor, para com a proteção dos seus dados?”

Apresentada a questão de investigação, este trabalho apresenta, também, a formulação de hipóteses operacionais.

Uma hipótese é uma “suposição provisória ou declaração preliminar, sobre a relação entre duas ou mais coisas que precisam de ser examinadas” (Welman, Kruger & Mitchel, 2005, p. 12) constitui uma “afirmação não comprovada ou sobre um fator ou fenómeno que é de interesse para o investigador” (Malhotra & Birks, 2006b, p. 47) tendo como objetivo, segundo Kumar (2005), trazer clareza e especificidade, possibilitando, ainda, a criação de uma teoria e modelo.

Assim, tendo em conta a revisão de literatura realizada e enunciada a questão de investigação, formulou-se um modelo conceptual (figura 8) onde se combinam o problema e o objetivo, numa predição de resultados esperados (Reis, 2010).

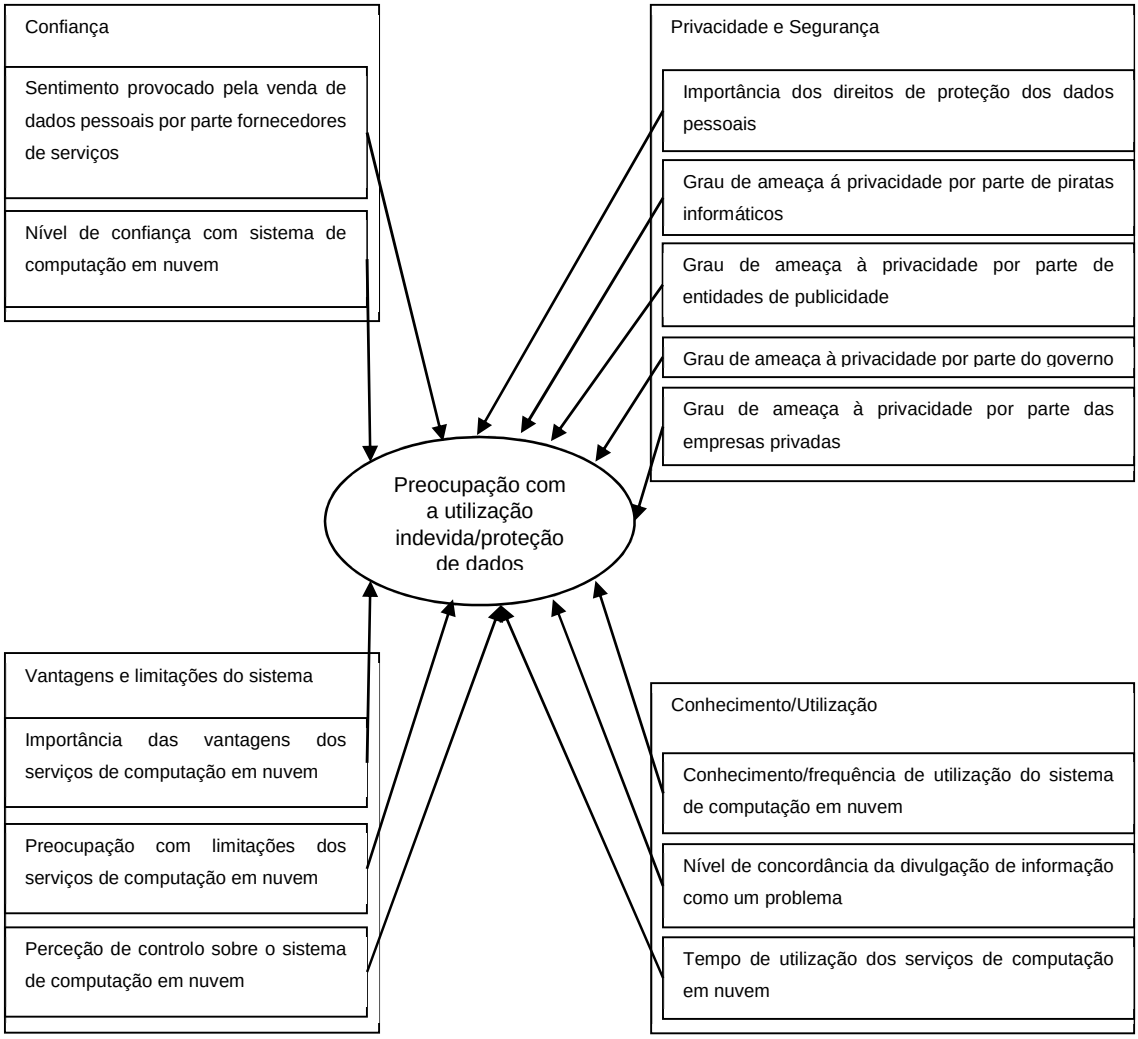

Figura 9 - Modelo de estudo proposto.

Fonte: elaboração própria.

Como referido, este estudo não é uma réplica, no todo ou em parte, de um pré-existente estudo ou modelo. Assim, a formulação de hipóteses deste trabalho será, com base na revisão de literatura realizada, levada a cabo através de associações, por nós estabelecidas, entre literatura, conceitos e modelos abordados neste trabalho.

A primeira hipótese foi construída com base na TAM[31], nomeadamente, na influência de variáveis externas na ideia ou perceção para com a tecnologia.

No trabalho de Lee, Kozar e Larsen (2003), podemos observar possíveis variáveis externas para a TAM, as quais foram sendo introduzidas por diversos autores como Rogers (1983), Agarwal e Karahanna (2000) e Martocchio (1992), sendo elas, respetivamente, as variáveis externas "grau de complexidade percebida de utilização de uma inovação" (Lee et al. 2003, p. 761), "traços

[31] TAM – Modelo de aceitação de tecnologia, abordado na revisão de literatura e que aponta, resumidamente, que variáveis externas influenciam a utilidade percebida e facilidade de utilização percebida de uma tecnologia. Consequentemente influenciam a atitude para com a utilização e intenção comportamental de utilização, ditando assim o uso, ou não, real da tecnologia.

psicológicos que refletem a predisposição/vontade de o utilizador utilizar uma tecnologia nova" (Lee et al. 2003, p. 761) e "nível de capacidade/espontaneidade cognitiva na utilização de tecnologias" (Lee et al. 2003, p. 761).

Hubona e Geitz (1997) estudam, a introdução específica das variáveis da "frequência de utilização" e "quantidade de utilização", bem como, "experiência com o sistema" e "experiência com computadores" como variáveis externas, isto, novamente relativamente ao TAM. Neste estudo, podemos, concretamente, ver as variáveis de frequência de utilização e conhecimento (discutivelmente como homologo de experiencia para com a tecnologia e computadores) a funcionarem como constructos da TAM.

Com este contexto, vemos que as nossas variáveis de conhecimento e frequência de utilização, já foram utilizadas noutros estudos com sucesso, embora, introduzidas como variáveis separadas. No nosso estudo, os itens de reposta juntam as duas variáveis.

Visto que a TAM se traduz, de forma básica, na influência de variáveis externas sobre perceções do utilizador (e que se influenciam entre si), influenciando a atitude e a intenção deste, resultando na utilização (ou não) do sistema, ficamos com a ideia de que quase tudo poderá ser considerado uma variável com influencia, como de resto podemos observar no referido trabalho de Lee et al. (2003), onde podemos observar inúmeras novas variáveis que foram sendo introduzidas e testadas ao longo dos anos. Assim, aquilo que nos propomos é o testar esta ideia, até que ponto e quais variáveis externas mais, podem ser consideradas e que exerçam influência sobre as perceções nucleares do utilizador.

Assim, com base nos estudos de Lee et al. (2003) e, mais concretamente, no estudo de Hubona e Geitz (1997), argumentamos, que, como "frequência de utilização" e "conhecimento", parecem ser variáveis válidas, por forma a tentar perceber se a utilização pode ser um fator de influência sobre as variáveis nucleares da TAM, a perceção do utilizador sobre a tecnologia e, não apenas, o resultado final, formula-se a primeira hipótese;

H1: Existe uma relação significativa e negativa entre o conhecimento/frequência de utilização do sistema de computação em nuvem e a preocupação com utilização/proteção de dados.

De acordo com a TAM, uma das variáveis principais, se não a principal, é a de "utilidade percebida", a qual, é influenciada pela segunda mais importante variável, a "facilidade de utilização percebida" e por "variáveis externas".

Segundo o sumário realizado por Lee et al. (2003, p. 761), "vantagem relativa" para com outra solução é uma variável válida para o modelo TAM, logo, argumentamos que as vantagens da *cloud* e grau de importância percebida das mesmas influenciem, diretamente, as duas referidas principais variáveis da TAM, visto que, estas vantagens, provavelmente, compreendem uma melhor performance comparativa e maior facilidade de adesão e utilização. No entanto, poem-se a questão de saber se esta influência se traduz numa maior ou menor preocupação para com

a proteção de dados. Complementarmente, ainda relativamente ao modelo TAM, Davis et al. (1989, p. 895) definem e apontam utilidade percebida e facilidade de utilização percebida, como variáveis capazes de influenciar a perceção e utilização de uma tecnologia. Assim, se as vantagens da tecnologia forem, de facto, percecionadas como vantagens, uteis e facilitadores, deve poderá existir uma relação significativa com o grau de preocupação para com a proteção dos seus dados.

Assim, a segunda hipótese apresenta-se de seguida.

H2: Existe uma relação significativa e positiva entre a importância das vantagens dos serviços de computação em nuvem com preocupação e a utilização/proteção de dados.

Em contraposto com o referido na hipótese 2, será expectável que, quanto mais importância for dada a uma das quaisquer limitações da tecnologia apontadas e inquiridas, a um aspeto menos positivo da *cloud*, maior será a preocupação com a proteção de dados. Assim, apresenta-se a terceira hipótese.

H3: A preocupação com as limitações dos serviços de computação em nuvem encontra-se significativa e positivamente relacionada com a preocupação com utilização/proteção de dados.

Segundo a literatura abordada a "confiança é um estado psicológico, que compreende a intenção de aceitar vulnerabilidade, com base em expectativas positivas sobre as intenções ou comportamentos de um outro" (Rousseau et al. 1998, p. 395). A confiança é como uma relação que se estende no tempo e depende da experiencia continua da pessoa para com o "objeto". Estes autores defendem que confiança é uma extensão do conceito de segurança, o que, também, tem uma componente psicológica, sendo que, segundo Shimba (2010), o nível de confiança, relativamente à segurança de um serviço, depende de como e quanto o fornecedor consegue apelar aos sentimentos do consumidor. Ainda sobre esta definição, Lourenço e Fortes (2013) e Mitchell (1999), definem risco percebido, como algo contrario à confiança e, mais importantemente, como algo capaz de ditar a adesão/utilização, ou não, de tecnologias.

Dito isto, pretende-se confirmar que um aumento de confiança se traduz num decréscimo na preocupação com a proteção de dados.

H4: Existe uma relação significativa e negativa entre o nível de confiança com sistema de computação em nuvem e com os fornecedores de serviços e a preocupação com utilização/proteção de dados.

Para a 5ª hipótese utilizamos um raciocínio semelhante à da hipótese anterior, procurando, agora, aprofundar um pouco o conhecimento. Ao invés de nos focarmos na confiança que o utilizador tem na tecnologia ou fornecedor de serviço, tentamos observar a influência da ausência de confiança, ou melhor dizendo, a ameaça percebida relativamente a diversas entidades. Para isso, mencionamos, também, a definição de privacidade que, segundo Mather et al. (2009), é

algo que varia largamente entre e dentro de países, culturas e jurisdições. Isto é facilmente compreendido ao lermos que privacidade são “os direitos e obrigações dos indivíduos e organizações, no que respeita à recolha, uso, retenção e divulgação de dados pessoais” (AICPA, 2005, p. 2). Isto deve significar, que, diferentes entidades podem provocar diferentes perceções e níveis de ameaça.

Complementarmente e tal como na hipótese anterior, Lourenço e Fortes (2013) e Mitchell (1999), que risco percebido é algo capaz de ditar a adesão/utilização, ou não, de tecnologias, sendo estas, variáveis de cariz psicológico e que apontam à mensuração de risco, perceba-se, preocupação.

Assim, propõem-se a seguinte hipótese, com 5 diferentes sub-hipóteses, atentando a diferentes entidades/intervenientes do mercado.

Em primeiro lugar, segue-se a hipótese geral.

H5: Um maio grau de ameaça á privacidade por parte de certas entidades está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

De seguida, conforme referido, apresentam-se as várias sub-hipóteses referentes às diferentes entidades.

H5a: Um maior grau de ameaça á privacidade por parte do governo está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5b: Um maior grau de ameaça á privacidade por parte das empresas privadas está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5c: Um maior grau de ameaça á privacidade por parte de entidades de publicidade está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5d: Um maior grau de ameaça á privacidade por parte de piratas informáticos está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

De acordo com os já mencionados conceitos e definições de privacidade, segurança e confiança, em concreto o seu aspeto psicológico, pretende-se, agora, abordar tópicos desse mesmo foro, psicológico. Sem nunca esquecer que este tipo de questões, podem ser considerados como variáveis externas no modelo TAM. Deste modo, criamos as cinco últimas hipóteses.

Relativamente às práticas levadas a cabo com os nossos dados, tenta-se, através de um exemplo concreto, ver a influência de uma prática comum sobre a preocupação com a utilização indevida de dados, através da hipótese 6, descrita de seguida.

H6: O sentimento que provoca a venda de dados pessoais por fornecedores de serviços está relacionado de forma significativa e positiva com a preocupação com a utilização indevida/proteção de dados.

Mais uma vez, mantendo em mente a natureza psicológica dos conceitos de confiança, privacidade e segurança, bem como o TAM, procura-se averiguar a influência provocada pelo sentimento de necessidade de direitos de proteção de dados, independente do país onde os dados são processados. Assim, construímos a hipótese 7.

H7: Existe uma relação significativa e positiva entre a importância dos direitos de proteção dos dados pessoais e a preocupação com a utilização indevida/proteção de dados.

Mantendo a mesma ideologia, é importante saber como é que o "controlo percebido" do utilizador, relativamente aos seus dados/sistema *cloud*, vai influenciar o seu nível de preocupação com a proteção dos mesmos. Alias, Ajzen (1991) e Mathieson (1991) defendem, que, controlo perceibo, é um conjunto de perceções individuais, capazes de influenciar a utilização, ou não, de uma tecnologia.

Com isto e, sendo uma questão logica, tendo em conta os conceitos, construiu-se a hipótese 8.

H8: Um maior controlo sobre o sistema de computação em nuvem implica uma menor preocupação com a utilização indevida/proteção de dados pessoais.

Tendo em conta uma variável detalhada na analise da hipótese 1, separando os conceitos e simplificando a "frequência de utilização" para "tempo de utilização", tendo em conta há quanto tempo se utiliza serviços *cloud*, se for o caso. Deste modo, apresenta-se a hipótese 9.

H9: O tempo de utilização dos serviços de computação em nuvem está relacionado de modo significativo e negativa com a preocupação com a utilização indevida/proteção dos dados pessoais.

Por fim, mantendo esta abordagem no foro psicológico, procura-se perceber a opinião do utilizador, relativamente ao estado atual da tecnologia, no que toca à necessidade, ou não, de ser necessária a divulgação de dados pessoais. Está em cause se esta quase que "obrigação", é percebida como tal pelo consumidor, se pode ser um problema ou se o utilizador vê isso com naturalidade. Assim, apresenta-se, de seguida, a última hipótese.

H10: O nível de concordância da divulgação de informação como um problema esta significativa e positivamente correlacionado com a preocupação com a utilização indevida/proteção dos dados pessoais.

Deste modo, depois de enunciarmos as hipóteses, apresentamos, na figura que se segue, o modelo onde se identifica os tipos de associações

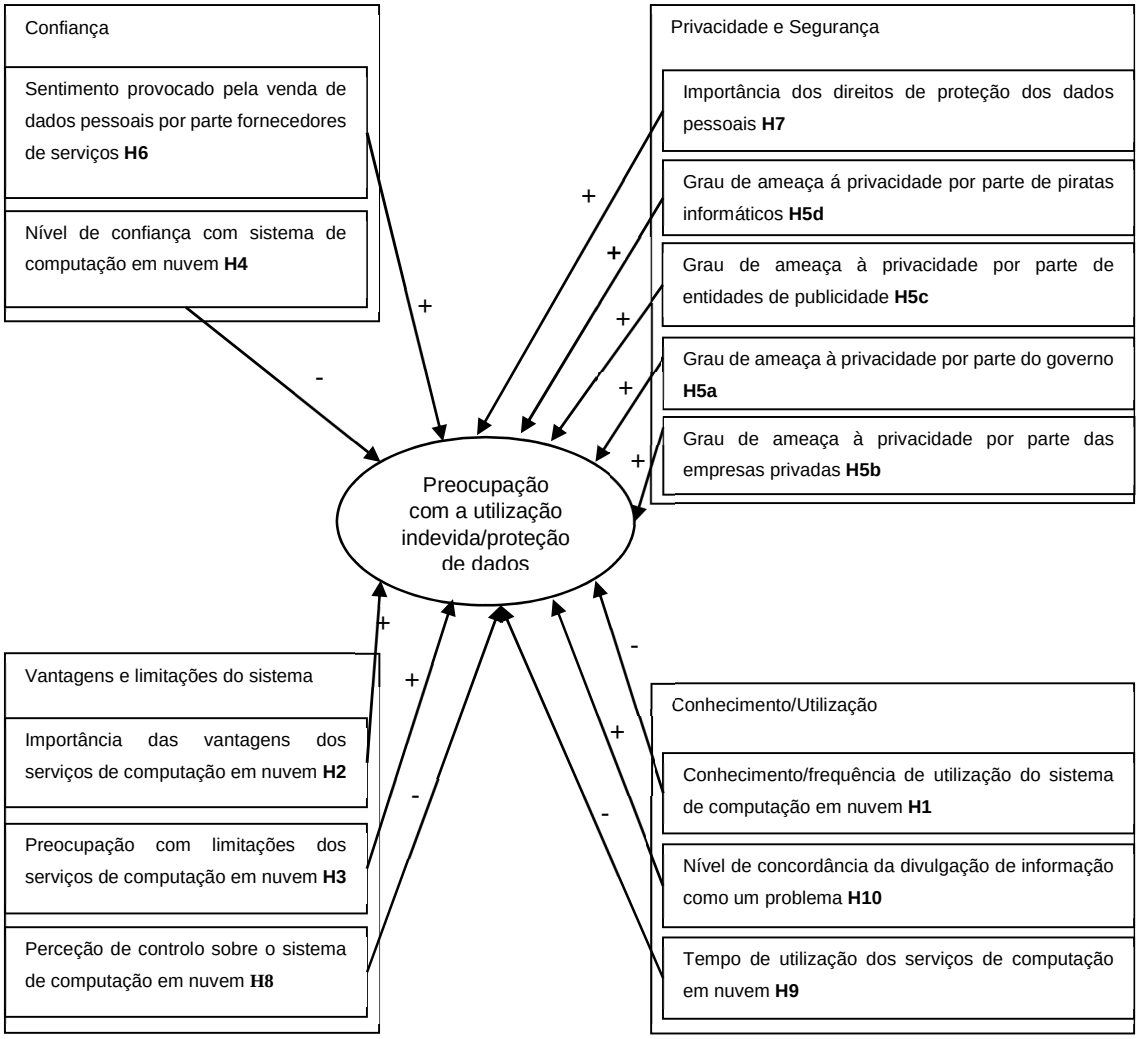

Figura 10 - Modelo final de investigação.

Fonte: elaboração própria.

5.5 - Procedimento de recolha de dados

Segundo Reis (2010), tipicamente, a metodologia de investigação quantitativa utiliza como instrumento de recolha de dados o inquérito por questionário, o qual, permite analisar as relações entre fatores. Aquele autor refere, ainda, que as vantagens desta metodologia passam por ser de baixo custo. Hair, Babin Money e Philip (2005) e Malhotra, Rocha, Laudisio, Altheman e Borges (2005b) vão de encontro a esta ideia, apontando que é um método bastante utilizado

neste tipo de estudos e que permite uma eficaz investigação de possíveis relações existentes entre variáveis e constructos em análise, mediante a proposição de hipóteses de pesquisa.

Segundo Lakatos e Marconi (2006), um questionário é um instrumento de recolha de dados estruturado, de grande e rápido alcance de respostas, o qual, pode ser respondido de forma anónima e sem intervenção do entrevistador, algo que, permite ao inquirido maior liberdade e segurança e um menor risco de distorção na resposta.

Tendo em conta estas vantagens e o tipo de estudo, optou-se por este tipo de instrumento de medida na recolha de dados.

Construído e pré testado o questionário, a versão final deste foi introduzido na plataforma *Limesurvey*[32], que, sendo uma plataforma e *website* cedido pelo ISCAP, confere uma maior veracidade, confiança e validade científica a este estudo, bem como, possibilita a realização do mesmo com menores custos na recolha de dados.

Igualmente importante é o facto de o *limesurvey* permitir uma fácil exportação de dados para o tratamento e a análise estatística. Aliado a esta situação e tendo, também, em conta que a internet é o mais rápido meio e canal de comunicação, o que é importante para a obtenção de uma amostra, optamos por este tipo de procedimento.

5.5.1 - Pré teste

Como referido, antes da distribuição do questionário, este foi sujeito a um pré-teste.

Segundo Lakatos e Marconi (2006), o pré-teste é tido como uma forma de avaliar a fidedignidade e validade do instrumento utilizado, neste caso, o inquérito. Quer isto dizer, encontrar erros ortográficos, ambiguidade de perguntas ou respostas, construção frásica excessivamente complexa ou mesmo errónea, bem como, possíveis dissonâncias criadas entre perguntas e escalas, dimensão das perguntas e do questionário num todo, ou, qualquer outro fator que possa deturpar ou complicar o estudo devido a erros ou má construção do inquérito.

O inquérito foi enviado a um grupo de pessoas, constituído por seis docentes, quatro alunos e cinco conhecidos. As análises recebidas foram extremamente positivas, não tendo sido apontados nenhuns problemas significativos, excetuando uns simples erros de pontuação.

5.5.2 - Distribuição do questionário

Para a distribuição do endereço, onde o questionário se encontrava alojado, teve-se em conta as mesmas indicações supramencionadas.

[32] Ferramenta *online,* disponibilizada pelo ISCAP, a qual permite a criação e a publicação de questionários, bem como, a obtenção e a exportação de respostas.

Assim, a distribuição do questionário foi feita através de:

- *e-mai*l – A difusão por *e-mail* foi realizada em três vias:
    a) pedido formal realizado junto do Instituto Superior de Contabilidade e Administração do Porto (ISCAP) para a distribuição do questionário pelos seus alunos e funcionários;
    b) pedido formal realizado junto do Instituto Politécnico do Porto (IPP) para a distribuição do questionário pelos alunos e funcionários do universo IPP (exceto ISCAP visto que já tinha sido feito);
    c) envio por *mailing lists*[33] obtidas e que continham endereço de ex-alunos.
- redes Sociais – O *link* do questionário foi partilhado em redes sociais, havendo um cuidado específico, com vista a evitar enviesamentos do "foro psicológico" devido a relações pessoais ou conhecimento entre o inquirido e o autor, nomeadamente, a partilha não foi feita em contas pessoais. Foi pedido a algumas pessoas para que fizessem tal partilha, mas, apenas direcionado a terceiros, excluindo família e amigos mais próximos;
- *word-of-mouth*[34] - Embora seja algo característico das redes sociais e que com toda a certeza aconteceu, esta forma de difusão apareceu de uma forma não esperada. Embora não fosse pedido no texto enviado por e-*mail*, várias pessoas usaram o contacto fornecido para transmitir o interesse que tiveram no trabalho e para dizer que o tinham passado a outras pessoas.

5.6 - Amostra

A amostra é definida por Malhotra e Birks (2006) como um subgrupo da população selecionada, para participar num estudo, onde as características da amostra se traduzem em estatísticas passiveis de, através de estimativas e teste de hipóteses, fazer deduções sobre determinados parâmetros para a população.

Tendo em conta o método de distribuição do questionário, estamos perante uma amostra não aleatória, mais especificamente, uma amostra por conveniência, definida por Coutinho (2011) como uma técnica que seleciona as unidades amostrais por conveniência. Logo, por não se determinar a probabilidade de selecionar elementos específicos para a amostra, foi aplicado técnicas de amostragem não-probabilística (Malhotra & Birks, 2006).

Assim, segundo Malhotra e Birks (2006), embora se possam fazer boas estimativas das características da população acessível, não podemos fazer uma avaliação objetiva da precisão

[33] *Mailing list*: "Lista de nomes e endereços…" (*Cambridge Dictionaries Online*, 2015a)
[34] *Word-of-mouth*: Informação "dada ou feita através de conversas, entre pessoas, sobre algo." (*Cambridge Dictionaries Online*, 2015b)

de resultados, em especial, da sua extrapolação, visto que não é possível determinar a probabilidade de selecionar um elemento específico para a inclusão na amostra.

Deste modo, este estudo tem como população alvo cidadãos Portugueses, sem qualquer tipo de restrição ou limite de participação no estudo, ou seja, estamos a falar de 10 562 178 de cidadãos segundo os Censos (Instituto Nacional de Estatística, 2011). Contudo, dadas as limitações "logísticas", monetárias e metodológicas do estudo, a população acedida por este, não foi realizado de modo probabilístico.

5.7 - Instrumento de recolha de dados

Este estudo visa a obtenção de dados primários, ou seja, dados obtidos e criados pelo investigador para um fim específico, embora, isto seja um processo mais demorado, especialmente, na recolha de dados (Malhotra & Birks, 2005).

O instrumento utilizado para a recolha de dados, neste estudo, foi um questionário estruturado, o qual, obedeceu às fases seguintes de elaboração de questionários descritas por Reis (2010):

a) especificação de dados a recolher;
b) definição de conteúdo e contexto das questões;
c) definição da forma de resposta para cada questão;
d) questionário de pré-teste;
e) distribuição do questionário;

Os dados foram recolhidos durante o mês de outubro de 2014, tendo-se obtido um total de 345 de respostas, das quais, 90 foram "postas de parte" devido a preenchimento incompleto do questionário, sendo o número final de respostas válidas totais de 255.

5.8 - Conceção do questionário

Não tendo sido encontrado um questionário, publicado e suscetível de ser usado, que estivesse de acordo com os objetivos deste trabalho ou que fosse suscetível de medir os fenómenos que este trabalho se propunha identificar e "medir", este questionário foi criado pelo investigador, pelo que, não se trata de uma replicação, parcial ou total, de um outro estudo.

O questionário estava estruturado em quatro partes:

grupo I – Era pedida uma reflexão e opinião sobre a tecnologia e utilização da mesma, tentando a isto medir o conhecimento, utilização e perceção da tecnologia;

grupo II – Era pedida a opinião sobre questões de segurança e privacidade, inerentes à tecnologia, para tentar medir a perceção dos inquiridos sobre essas questões, bem como, o nível de consciência e controlo percebido;

grupo III – Foi pedido um autodiagnóstico sobre o conhecimento percebido e opinião sobre a tecnologia;

grupo IV – Foi pedida uma pequena caracterização, sociodemográfica, do inquirido, desde sexo, idade e estudos académicos até à situação profissional.

Na tabela que se segue, é explanado o questionário de forma a evidenciar as possíveis determinantes, que possam influenciar a preocupação com a proteção de dados, bem como, questões e escalas utilizadas. Apesar de, como referido, aquele não ser, de forma alguma, uma replicação de um outro trabalho, são, também, apontados autores de estudos, maioritariamente de natureza/alvo empresarial, sobre os quais nos debruçamos e tentamos adaptar questões, estilos de construção frásica, tanto das questões em si, como dos itens de resposta, bem como, as escalas de Likert, por forma a tentar "produzir" um questionário válido.

Determinantes	Itens	Autores
Conhecimento, utilização e perceção da tecnologia		
Grau de confiança e conhecimento sobre utilização de serviços	1. Correio eletrónico (*Gmail*, *Outlook*, *Yahoo*, entre outros).* 2. Navegador de internet (*Internet Explorer*, *Firefox*, *Chrome*, entre outros).* 3. Conversação online (vídeo, voz ou texto, como *Skype* ou *Hangouts*, entre outros).* 4. Fóruns ou grupos de discussão.* 5. *Wikis* (sítios de colaboração, como *Wikipedia*).* 6. Blogues.* 7. Armazenamento online (*Onedrive*, *Google Drive*, *Dropbox*, entre outros).* 8. Produtividade (*Office 365*, *Google Docs*, *Limesurvey*, entre outros).* 9. Redes Sociais (*Facebook*, *Youtube*, *Tumblr*, *Twitter*, *Google+*, *Linkedin*, *Instagram*, *Pinterest*, *Orkut*, *Snapchat*, *WhatsApp*, entre outros).*	Cruz (2013)

	10. Outras aplicações (meteorologia, noticias, entre outras).*	
Nível de importância atribuída às vantagens da tecnologia *cloud*	1. Menores custos (menor compra de discos rígidos, cd, dvd, pen, entre outros, componentes físicos e programas).** 2. Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita).** 3. Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos).** 4. Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço).** 5. Segurança de dados.** 6. Mobilidade (acesso em qualquer local).** 7. Disponibilidade (acesso a qualquer momento).**	Cruz (2013), Kwofie (2013) e Kajiyama (2012)
Nível de preocupação atribuída a limitações do sistema	1. Custos não esperados (por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas").*** 2. Integridade de dados (referente à manutenção de precisão e consistência de dados).*** 3. Possibilidade de perda de dados.*** 4. Segurança de dados.*** 5. Privacidade de dados.*** 6. Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente).***	Cruz (2013), Kajiyama (2012), Duranti (2013)

	7. Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade).*** 8. Disponibilidade (se o serviço e/ou dados estão sempre online e disponíveis).*** 9. Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem).*** 10. Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação).*** 11. Questões legais e regulamentares.***	
Nível de confiança	1. Tecnologia de computação em nuvem.**** 2. Fornecedores de serviços.****	Kajiyama (2012)
Segurança e Privacidade.		
Nível de concordância	1. Questões de segurança são um problema que impedem a adoção de serviços baseados em computação em nuvem.***** 2. Em geral, sinto-me mais confiante com a utilização de soluções proprietárias que correm e existem no meu dispositivo (computador pessoal, telemóvel e tablets).***** 3. Sinto que a tecnologia de computação na nuvem está pronta para salvaguardar os meus dados e informação mais importantes.***** 4. Sinto que a computação em nuvem será mais segura no futuro.*****	Kwofie (2013), Kajiyama (2012)

Nível de preocupação	1. A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.****** 2. Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.****** 3. Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser utilizados e implicados em ações menos éticas ou mesmo ilegais, por parte de terceiros.****** 4. Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.****** 5. Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.******	Kajiyama (2012)
Segurança	1. Quem pensa ser responsável pela segurança dos seus dados?	Spideroak (2013)
Probabilidade de utilização de serviços *cloud* tendo em conta acontecimentos que afetam a perceção de privacidade	1. Várias agências de inteligência, como NSA, acedem à base de dados de empresas de telecomunicações, fornecedores de internet e fornecedores de serviços de computação em nuvem, com o objetivo de aceder e monitorizar os dados e informação dos utilizadores.*******	Spideroak (2013)

	2. A empresa Facebook, manipulou o histórico de Noticias de 689 003 utilizadores, removendo ou todas as mensagens negativas, ou todas as mensagens positivas, num estudo que comprovou que, as emoções são contagiáveis, induzindo um estado de felicidade ou depressão.*******	
Perceção de ameaça à privacidade	1. Governo.******** 2. Empresas privadas.******** 3. Entidades de publicidade.******** 4. Piratas Informáticos.********	Spideroak (2013)
Sentimento para com utilização de dados pessoais	1. Que sentimento lhe provoca a venda dos seus dados pessoais pelos fornecedores de serviços (à semelhança do Facebook)?*********	Spideroak (2013)
Perceção sobre responsabilidade de manutenção de privacidade	1. Quem pensa ser responsável pela proteção da sua privacidade online?	Spideroak (2013)
Perceção de proteção de dados	1. Pensa que deveria ser necessária a sua concreta e especifica aprovação, antes de serem recolhidos e processados, quaisquer, tipo de dados pessoais? 2. Em que circunstancias, se alguma, desejaria que os seus dados pessoais, armazenados e recolhidos por um serviço, fossem completamente apagados?	Eurobarometer (2011) Eurobarometer (2011)
Importância de mesmos direitos e proteção de dados pessoais	1. Quão importante é para si, ter os mesmos direitos e proteção dos seus dados pessoais, independentemente do país onde esses dados são processados?**********	Eurobarometer (2011)

Consciência e controlo percebido	1. Qual o nível de controlo que sente ter, sobre a informação e dados que divulgou e utiliza nos serviços baseados nesta tecnologia.********** 2. Quando tem intenções de utilizar um serviço, baseado nesta tecnologia, sente-se informado sobre as condições de compilação dos seus dados e futura utilização dos mesmos?	Eurobarometer (2011) Eurobarometer (2011)
Auto diagnóstico do seu conhecimento e opinião sobre a tecnologia.		
Perceção de conhecimento sobre o sistema	1. Como classificaria o seu conhecimento sobre computação em nuvem?**********	Kowfie (2013)
Complemento de tipologia de utilização da tecnologia	1. Há quanto tempo utiliza serviços de computação em nuvem?	Duranti (2013)
Perceção sobre situação atual relativamente à divulgação de informação pessoal	1. Divulgar informação pessoal é uma situação crescente da vida moderna.***** 2. Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal.***** 3. Para mim, divulgar informação pessoal é um problema.***** 4. Para mim, divulgar informação pessoal em troca de serviços *online* grátis é um problema.***** 5. Sinto-me obrigado a divulgar dados privados na internet.*****	Eurobarometer (2011)
Informação pessoal.		

Perfil sociodemográfico	20.	Sexo	Cruz (2013)
	21.	Idade	
	22.	Estudos Académicos	
	23.	Situação Profissional	

Tabela 2 - Determinantes, questões e escalas do questionário.

Fonte: elaboração própria.

Nas questões não assinaladas, com asterisco, as repostas eram de escolha múltipla.

*Escala de frequência de 5 pontos de Likert com os valores de 1 (Sei o que é e utilizo com muita frequência), 2 (Sei o que é e utilizo com frequência), 3 (Sei o que é e já utilizei pelo menos uma vez), 4 (Sei o que é mas nunca utilizei) e 5 (Não sei o que é).

**Escala de importância de 5 pontos de Likert com os valores de 1 (Muito importante), 2 (Bastante importante), 3 (Importante), 4 (Pouco importante), 5 (Nada importante).

***Escala de preocupação de 5 pontos de Likert com os valores de 1 (Muito preocupante), 2 (Bastante preocupante), 3 (Preocupante), 4 (Pouco preocupante), 5 (Nada preocupante).

****Escala de confiança de 5 pontos de Likert com os valores de 1 (Muito confiante), 2 (Bastante confiante), 3 (Confiante), 4 (Pouco confiante), 5 (Nada confiante).

*****Escala de concordância de 5 pontos de Likert com os valores de 1 (Concordo totalmente), 2 (Concordo), 3 (Não concordo nem discordo), 4 (Discordo), 5 (Discordo totalmente).

******Escala de preocupação de 5 pontos de Likert com os valores de 1 (Absoluta preocupação), 2 (Muita preocupação), 3 (Nem preocupado nem despreocupado), 4 (Pouca preocupação), 5 (Nenhuma preocupação).

*******Escala de probabilidade de 5 pontos de Likert com os valores de 1 (Utilizo de certeza), 2 (Muito provável), 3 (Nem preocupado nem despreocupado), 4 (Pouca preocupação), 5 (Nenhuma preocupação).

********Escala de ameaça de 5 pontos de Likert com os valores de 1 (Ameaça total), 2 (Muita ameaça), 3 (Indiferente), 4 (Alguma ameaça), 5 (Ausência de ameaça).

*********Escala de perturbação de 5 pontos de Likert com os valores de 1 (Fico escandalizado), 2 (Fico muito perturbado), 3 (Fico perturbado), 4 (Fico algo perturbado), 5 (Não me importo).

**********Escala de importância de 5 pontos de Likert com os valores de 1 (Muito importante), 2 (Importante), 3 (Indiferente), 4 (Pouco importante), 5 (Nada importante).

***********Escala de controlo percebido de 5 pontos de Likert com os valores de 1 (Controlo total), 2 (Controlo elevado), 3 (Não sei), 4 (Controlo baixo), 5 (Nenhum controlo).

************Escala de conhecimento percebido de 5 pontos de Likert com os valores de 1 (Totalmente informado(a)), 2 (Muito informado(a)), 3 (Informado(a)), 4 (Pouco informado(a)), 5 (Nada informado(a)).

5.9 - Tratamento de dados

A ferramenta utilizada para a análise e tratamento de dados foi o programa *Statistical Package for the Social Science* (SPSS), visto ser uma ferramenta completa e capaz de realizar todos os testes estatísticos necessários para este estudo e que serão abordados na análise de resultados.

Foi também utilizada a ferramenta Excel (versões 2013 e 2016), mas, meramente como suporte para a criação de tabelas e gráficos mais percetíveis.

De seguida serão indicadas todas as técnicas utilizadas ao longo do tratamento de dados.

5.9.1 - Análise da validade fatorial

Relativamente à análise de validade fatorial, utilizou-se, principalmente, o a medida de adequabilidade *Kaiser-Meyer-Olkin* (KMO).

O teste de *Kaiser-Meyer-Olkin* é uma estatística que indica a proporção da variância dos dados, que, pode ser considerada comum a todas as variáveis (i.e. pode ser atribuída a um fator comum) (Pestana & Gageiro, 2005; Maroco & Garcia-Marques, 2006).

Apresenta-se, de seguida, uma tabela com os valores de referência.

Kaiser-Meyer-Olkin	
Maior que 0,9	Muito boa
Entre 0,8 e 0,9	Boa
Entre 0,7 e 0,8	Razoável
Entre 0,6 e 0,7	Fraca
Abaixo de 0.6	Medíocre

Tabela 3 – Valores de referência do KMO

Fonte: adaptação própria de Pestana e Gageiro (2005)

5.9.2 - Análise de fiabilidade: consistência Interna

Para analisarmos a fiabilidade e consistência do instrumento, recorremos ao índice de consistência interna de *alpha* de *Cronbach*.

Alpha de *Cronbach* pode ser definida como a correlação que se espera obter, entre a escala usada e escalas hipotéticas, podendo variar entre 0 e 1 (Pestana & Gageiro, 2005). Foi uma solução encontrada por *Cronbach* "para a o problema da estimação da fiabilidade *split-half*" (Hill & Hill, 2012, p. 147). O teste de *alpha* de *Cronbach* permite estimar o coeficiente de fiabilidade interna (*alpha*) dos itens referentes a uma componente de variável. Este teste analisa o efeito de um fator na variável endógena, testando se as medidas desta variável, em cada categoria do fator, são, ou não, iguais entre si (Pestana & Gageiro, 2005).

De seguida é apresentada uma tabela com os valores de referência.

Alpha de Cronbach	
Maior que 0,9	Excelente
Entre 0,8 e 0,9	Bom
Entre 0,7 e 0,8	Razoável
Entre 0,6 e 0,7	Fraco
Abaixo de 0.6	Inaceitável

Tabela 4 – Valores de referência do *alpha* de *Cronbach.*

Fonte: Hill e Hill (2012, p. 149).

De mencionar, ainda, que, embora valores de 0,6 sejam considerados fracos e o ideal seja 0,7, dado se tratar de um estudo exploratório, este tipo de valores de 0,6 perfeitamente suficientes (Nunnally, 1978; Maroco & Garcia-Marques, 2006).

5.9.3 - Análise descritiva dos resultados

Para a realização da análise descritiva, recorreu-se à análise de frequências (n) e percentagens (%), medidas de tendência central (média, mediana e intervalo de confiança para média), medidas de dispersão (valores mínimos e máximos e desvio padrão), variância, amplitude, simetria, valores curtose, e teste de Kolmogorov-Smirnov.

5.9.4 - Estatística inferencial – Relação entre variáveis – Teste de hipóteses

Para a realização de estatística inferência, relação entre variáveis e teste de hipóteses, recorreu-se ao coeficiente de correlação de *Spearman* e, ainda, aos métodos *Stepwise* e *Enter*.

A escolha da medida, não paramétrica, de *Spearman*, deve-se ao facto de amostra suficientemente grande, ao ponto de ser necessária outro tipo de abordagem, bem como, a forma de distribuição do questionário (i.e. livre e sem restrições). Sendo dos coeficientes mais conhecidos, esta correlação exige, segundo Siegel (1975), que as duas variáveis se apresentem em escala de mensuração ordinal. Ainda segundo Siegel (1975), este coeficiente varia de 0 a 1 e o resultado é tanto mais significativo quanto mais próximo de 1.

5.10 - Conclusão

Para terminar o capítulo de metodologias de investigação, apresenta-se, na tabela abaixo, as hipóteses de estudo formuladas, assinaladas com o resultado obtido a nível da sua verificação, ou não.

Hipóteses
H1-: Existe uma relação significativa e negativa entre o conhecimento/frequência de utilização do sistema de computação em nuvem e a preocupação com utilização/proteção de dados.
H2+: Existe uma relação significativa e positiva entre a importância das vantagens dos serviços de computação em nuvem com preocupação e a utilização/proteção de dados.
H3+: A preocupação com as limitações dos serviços de computação em nuvem encontra-se significativa e positivamente relacionada com a preocupação com utilização/proteção de dados.
H4-: Existe uma relação significativa e negativa entre o nível de confiança com sistema de computação em nuvem e com os fornecedores de serviços e a preocupação com utilização/proteção de dados.
H5: Um maio grau de ameaça á privacidade por parte de certas entidades está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais. H5a+: Um maior grau de ameaça á privacidade por parte do governo está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais. H5b+: Um maior grau de ameaça á privacidade por parte das empresas privadas está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais. H5c+: Um maior grau de ameaça á privacidade por parte de entidades publicidade está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais. H5d+: Um maior grau de ameaça á privacidade por parte de piratas informáticos está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.
H6+: O sentimento que provoca a venda de dados pessoais por fornecedores de serviços está relacionado de forma significativa e positiva com a preocupação com a utilização indevida/proteção de dados.
H7+: Existe uma relação significativa e positiva entre a importância dos direitos de proteção dos dados pessoais e a preocupação com a utilização indevida/proteção de dados.
H8-: Um maior controlo sobre o sistema de computação em nuvem implica uma menor

preocupação com a utilização indevida/proteção de dados pessoais.
H9-: O tempo de utilização dos serviços de computação em nuvem está relacionado de modo significativo e negativo com a preocupação com a utilização indevida/proteção dos dados pessoais.
H10+: O nível de concordância da divulgação de informação como um problema esta significativa e positivamente correlacionado com a preocupação com a utilização indevida/proteção dos dados pessoais.

Tabela 5 - Quadro resumo das hipóteses de estudo.

Fonte: elaboração própria.

Capitulo VI – Apresentação e análise de resultados

6.1 - Introdução

Após a apresentação da metodologia utilizada, passamos, agora, para a apresentação dos dados primários obtidos. Os resultados apresentados, neste capítulo, têm como objetivo final, verificar se as hipóteses propostas são ou não corroboradas, bem como, a apresentação de um modelo fatorial explicativo da preocupação com a proteção de dados.

Assim, os resultados serão apresentados da seguinte forma: a) caracterização da amostra; b) análise da validade fatorial; c) análise de da consistência interna; d) análise descritiva; e) estatística inferencial para o teste de hipóteses; f) modelo fatorial explicativo da preocupação com a proteção de dados; g) conclusão e discussão de resultados;

6.2 - Caracterização da amostra

A amostra válida do presente estudo é constituída por 255 indivíduos, na sua maioria do sexo feminino (n=144, 56.5%) e com idades compreendidas entre os 18 e os 23 anos (n=86, 33.7%). Grande parte dos participantes são licenciados (n=100, 39.2%), sendo que a maioria são estudantes (n=100, 39.2%), conforme se pode observar na tabela que se segue.

Sexo	n	%
Feminino	144	56,5
Masculino	111	43,5
Idade	n	%
Menos de 18 anos	6	2,4
Entre 18 e 23 anos	86	33,7
Entre 24 e 30 anos	44	17,3
Entre 31 e 40 anos	57	22,4
Entre 41 e 50 anos	34	13,3
Entre 51 e 60 anos	17	6,7
Mais de 60 anos	11	4,3
Habilitações Académicas	n	%

Secundário	75	29,4
Bacharelato	7	2,7
Licenciatura	100	39,2
Pós-Graduação	12	4,7
Mestrado	47	18,4
Doutoramento	11	4,3
Pós-Doutoramento	1	0,4
Não responde	2	0.8
Situação Profissional	n	%
Sem ocupação	1	0,4
Estudante	100	39,2
Trabalhador-Estudante	31	12,2
Trabalhador por contra de outrem	90	35,3
Trabalhador por conta própria	12	4,7
Desempregado	12	4,7
Não responde	9	3,5

Tabela 6 - Caracterização sociodemográfica da amostra.

Fonte: elaboração própria com base nos outputs estatísticos.

6.3 - Análise da validade fatorial das escalas formuladas

De modo a se obter uma escala explicativa do conjunto dos itens relativos às diversas questões do questionário foi realizada uma análise fatorial exploratória, em que se procurou extrair um único fator, de modo a obter uma estrutura unidimensional

Relativamente ao conjunto de itens da pergunta 1, verificou-se que, de acordo com os valores de KMO e do Teste de Bartlett (KMO[35]=0.78, Bartlett=710.24, p=0.00), é possível recorrer-se ao

[35] Segundo Pestana e Gageiro (2005), a partir de 0,6 é um resultado válido e, neste caso, em concreto, é um resultado razoável, praticamente no nível “bom” (0,8).

método de análise fatorial para extração de fatores. Assim, da análise realizada, obtivemos uma estrutura fatorial definida por um fator que explica 36.88% da variância, conforme tabela seguinte.

Podemos, também, observar, na tabela 7, que as comunalidades existentes com o fator único geral se apresentam razoáveis variando entre 0.24 e 0.46. Quanto aos níveis de saturação dos itens com o fator que representam notamos que os mesmos se apresentam todos superiores a 0.4[36], condição necessária para a sua extração.

Itens	*Grau de confiança e conhecimento sobre utilização dos serviços de computação em nuvem*	
	s	h^2
Conversação *online* (vídeo, voz ou texto, como Skype ou Hangouts, entre outros)	0,67	0.46
Correio eletrónico (Gmail, Outlook, Yahoo, entre outros)	0,66	0.45
Redes Sociais (Facebook, Youtube, Tumblr, Twitter, Google+, Linkedin, Instagram, Pinterest, Orkut, Snapchat, WhatsApp, entre outros)	0,64	0.42
Navegador de internet (Internet Explorer, Firefox, Chrome, entre outros)	0,62	0.39
Produtividade (Office 365, Google Docs, Limesurvey, entre outros)	0,60	0.36
Fóruns ou grupos de discussão	0,59	0.36
Armazenamento online (Onedrive, Google Drive, Dropbox, entre outros)	0,59	0.36
Outras aplicações (meteorologia, noticias, entre outras)	0,57	0.33
Blogues	0,55	0.31
Wikis (sítios de colaboração, como Wikipedia)	0,49	0.24
% de variância	36.68%	

[36] De acordo com Hair, Black, Babin, Anderson e Tatham (2006), o valor de 0,40 é considerado o mínimo aceitável.

Tabela 7 - Análise fatorial da escala de frequência e conhecimento sobre os serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

A análise fatorial efetuada sobre as questões relacionadas com a importância das vantagens dos serviços de computação em nuvem, resultou numa estrutura unidimensional que explica 50.83% da variância. Foram também realizados os testes de KMO e Bartlett para averiguar a plausibilidade da realização de uma análise fatorial com estes itens, sendo que a mesma se verifica considerando os resultados satisfatórios e significativos obtidos (KMO=0.77, Bartlett=928.35, p=0.00). Relativamente às comunalidades dos itens com o fator geral as mesmas apresentam-se, em geral, satisfatórias variando entre 0.29 e 0.63. Todos os itens apresentam um nível de saturação superior ou igual a 0.4 com o fator que representam. Conforme se pode observar na tabela que se segue.

Itens	Importância das vantagens dos serviços de computação em nuvem	
	s	h^2
Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos)	0,79	0.63
Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita)	0,78	0.61
Menores custos (menor compra de discos rígidos, cd, dvd, pen, entre outros, componentes físicos e programas)	0,75	0.56
Mobilidade (acesso em qualquer local)	0,74	0.56
Disponibilidade (acesso a qualquer momento)	0,74	0.55
Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço)	0,60	0.36
Segurança de dados	0,54	0.29
% de variância	50.83%	

Tabela 8 - Análise fatorial das questões relativas à importância das vantagens dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Foi, também, realizada uma análise fatorial ao conjunto de questões relacionadas com a preocupação com as limitações do sistema de computação em nuvem, de modo a obter uma estrutura uni-fatorial. Os resultados dos testes KMO e de Bartlett para análise da adequação fatorial encontram-se satisfatórios e significativos (KMO= 0.87, Bartlett=1482.54, '), sendo como tal plausível a realização deste tipo de análise.

Foi obtida uma percentagem de variância de 48.83%. As comunalidades verificadas variam entre 0.40 e 0.57, sendo que todos os itens apresentam uma carga fatorial com o fator que representam superior a 0.4 (Tabela 9).

Itens	Preocupação com limitações do sistema de computação em nuvem	
	s	h^2
Integridade de dados (referente à manutenção de precisão e consistência de dados)	0,75	0.57
Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente)	0,74	0.56
Questões legais e regulamentares	0,73	0.54
Segurança de dados	0,71	0.51
Privacidade de dados	0,71	0.51
Possibilidade de perda de dados	0,70	0.50
Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação)	0,68	0.47
Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem)	0,67	0.45
Disponibilidade (se o serviço e/ou dados estão sempre online e disponíveis)	0,66	0.45

Custos não esperados (Por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter “fechado portas”)	0,64	0.41
Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade)	0,63	0.40
% de variância	48.83%	

Tabela 9 - Análise fatorial dos itens relacionados com a preocupação com as limitações do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Da análise fatorial do conjunto de itens relacionados com a preocupação com a utilização/proteção dos dados obteve-se uma estrutura definida por apenas um fator responsável por 59.46% da variância explicada. Também se verificou que os valores relativos aos testes KMO e teste Bartlett para análise da adequação fatorial se revelam satisfatórios e adequados (KMO= 0.77, Bartlett=488.48, p=0.00). No que refere a comunalidades estas variam entre 0.40 e 0.57. Por fim, verificámos, também, que na estrutura unidimensional todos os itens apresentam uma carga fatorial superior a 0.4.

Itens	Preocupação com utilização/proteção de dados	
	s	h^2
Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser utilizados	0,84	0.70
Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.	0,81	0.66
Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.	0,79	0.64

Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.	0,73	0.54
A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.	0,66	0.44
% de variância	59.46%	

Tabela 10 - Análise fatorial e consistência interna dos itens relacionados com a preocupação com a utilização indevida/proteção dos dados.

Fonte: elaboração própria com base nos outputs estatísticos.

De acordo a análise fatorial realizada, em que se procurou obter uma estrutura uni-fatorial representativa dos vários itens relacionados com a importância da opinião sobre a divulgação dos dados pessoais na internet, verificou-se que a estrutura inicial obtida, constituída por todos os itens explica 33.76% da variância total. Os resultados obtidos nos testes de adequação fatorial não se revelam muito adequados, considerando o valor inadequado de KMO (KMO=0,55), apesar do teste de Bartlett se apresentar significativo (Bartlett=182,00, p=0.00). Porém, prosseguimos com a análise no sentido de verificar quais os itens que explicam um fator comum, sendo que concluímos de acordo com a tabela 11, que os itens "Divulgar informação pessoal é uma situação crescente da vida moderna" e "Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal" apresentam uma carga fatorial inferior a 0.4, o que implica a sua retirada e a realização de uma nova análise fatorial, conforme podemos ver na tabela 6.

Itens	Opinião sobre divulgação de dados na net	
	s	h^2
Para mim, divulgar informação pessoal, em troca de serviços online grátis, é um problema	0,81	0,66
Para mim, divulgar informação pessoal, é um problema	0,79	0,63
Sinto-me obrigado a divulgar dados privados na internet	0,47	0,22
Divulgar informação pessoal é uma situação crescente da vida moderna	**<0,4**	**0,09**

Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal	**<0,4**	**0,09**
% de variância	33.76%	

Tabela 11 - Análise fatorial e consistência interna dos itens relacionados com a opinião sobre a divulgação dos dados na internet (Análise inicial).

Fonte: elaboração própria com base nos outputs estatísticos.

A análise fatorial efetuada apenas com os três restantes itens permitiu obter uma estrutura fatorial que explica 55.24% da variância (Tabela 12). No entanto, é importante salientar que a adequação fatorial analisada pelos testes KMO e de esfericidade de Bartlett (KMO=0.52, Bartlett=125.84, p=0.00), aponta, apesar da significância do teste de Bartlett, para uma inadequabilidade para a realização da análise fatorial considerando o resultado de KMO. Também se verificou que um dos itens não apresenta de novo uma carga fatorial igual ou superior a 0.4, apresentando o mesmo item uma comunalidade muito baixa, tendo-se como tal procedido à sua exclusão e efetuado uma nova análise fatorial com os restantes 2 itens.

Itens	Opinião sobre divulgação de dados na net	
	s	h^2
Para mim, divulgar informação pessoal, em troca de serviços online grátis, é um problema	0,89	0,79
Para mim, divulgar informação pessoal, é um problema	0,88	0,78
Sinto-me obrigado a divulgar dados privados na internet	**<0,4**	**0,09**
% de variância	55,24%	

Tabela 12 - Análise fatorial e consistência interna dos itens relacionados com a opinião sobre a divulgação dos dados na internet (2ª análise).

Fonte: elaboração própria com base nos outputs estatísticos.

A última análise fatorial realizada apenas com os dois últimos itens permitiu obter um fator explicativo com uma percentagem de variância de 80,95%. Analisando a consistência interna dos itens, verificamos que a mesma se apresenta altamente satisfatória, tendo em consideração

o valor elevado do *alpha* de *Cronbach* obtido (0,77[37]). Este fator, considerando os seus itens, seria então denominado de opinião sobre a divulgação da informação como um problema (Tabela 13).

Itens	Opinião sobre divulgação de dados na net	
	s	h^2
Para mim, divulgar informação pessoal em troca de serviços online grátis é um problema	0,90	0,81
Para mim, divulgar informação pessoal é um problema	0,90	0,81
% de variância	80,95%	

Tabela 13 - Análise fatorial e consistência interna dos itens relacionados com a opinião sobre a divulgação dos dados na internet (Análise final).

Fonte: elaboração própria com base nos outputs estatísticos.

Em suma, em relação a esta última análise apesar da sua inadequabilidade fatorial optamos por criar um fator denominado divulgação como um problema em geral, considerando a forte variância obtida pelo conjunto dos itens "Para mim, divulgar informação pessoal em troca de serviços *online* grátis é um problema" e "Para mim, divulgar informação pessoal é um problema".

Após a análise da validade fatorial das escalas a utilizar nas análises posteriores do nosso estudo, passamos, também, à análise da sua fiabilidade, tendo em conta a análise da consistência interna dos itens, recorrendo ao valor de *alpha* de *Cronbach*.

6.4 - Análise da fiabilidade: consistência interna

Passamos, agora, para uma análise de consistência interna das escalas utilizadas.

No que refere a escala alusiva ao "Grau de Confiança e Conhecimento" sobre utilização dos serviços de computação em nuvem, de acordo com a tabela 14, verificamos que se obteve um valor de *alpha* de *Cronbach* adequado (0.79), sendo deste modo fiável a escala e a consistência

[37] Segundo Hill e Hill (2012), o valor de *alpha* de *Cronbach* é aceitável a partir de 0,6 e, de acordo com Nunnally (1978) e Maroco e Garcia-Marques (2006), sendo este um estudo exploratório, valores de 0,6 são suficientes.

interna dos seus itens. As correlações existentes entre os itens e o fator total também se apresentam moderadas variando entre 0.43 e 0.54

Itens	Correlação item-total	*Alpha* de *Cronbach* se item removido	*Alpha* de *Cronbach*
Correio eletrónico (Gmail, Outlook, Yahoo, entre outros)	0,49	0,77	
Navegador de internet (Internet Explorer, Firefox, Chrome, entre outros)	0,44	0,77	
Conversação online (vídeo, voz ou texto, como Skype ou Hangouts, entre outros)	0,54	0,75	
Fóruns ou grupos de discussão	0,50	0,76	
Wikis (sítios de colaboração, como Wikipedia)	0,37	0,78	
Blogues	0,46	0,76	0.79
Armazenamento online (Onedrive, Google Drive, Dropbox, entre outros)	0,50	0,76	
Produtividade (Office 365, Google Docs, Limesurvey, entre outros)	0,50	0,76	
Redes Sociais (Facebook, Youtube, Tumblr, Twitter, Google+, Linkedin, Instagram, Pinterest, Orkut, Snapchat, WhatsApp, entre outros)	0,48	0,76	
Outras aplicações (meteorologia, noticias, entre outras)	0,43	0,77	

Tabela 14 - Análise da consistência interna dos itens da escala Grau de Confiança e Conhecimento sobre utilização dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Para a escala Importância das vantagens dos serviços de computação em nuvem, o valor de *alpha* obtido (0.83), apresenta-se adequado, sendo assim fiável o fator apresentado, assim como, a consistência interna entre os seus itens. Também é possível observar correlações moderadas, que variam entre 0.42 e 0.69 entre os itens e o fator total apresentado (Tabela 9).

Itens	Correlação item-total	*Alpha* de *Cronbach* se item removido	*Alpha* de *Cronbach*
Menores custos (menor compra de discos rígidos, cd, dvd, pen, entre outros, componentes físicos e programas)	0,64	0,79	
Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita)	0,68	0,78	
Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos)	0,69	0,78	0.83
Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço)	0,48	0,83	
Mobilidade (acesso em qualquer local)	0,59	0,80	
Disponibilidade (acesso a qualquer momento)	0,58	0,81	
Segurança de dados	0,42	0,83	

Tabela 15 - Análise da consistência interna dos itens da escala Importância das vantagens dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

No que concerne à escala “Preocupação com limitações do sistema de computação em nuvem” o valor de *alpha* obtido apresenta-se adequado (0.89), o que implica uma boa fiabilidade e consistência interna dos seus itens. As correlações item-total observadas são moderadas variando entre 0.55 e 0.69 (Tabela 10).

Itens	Correlação item-total	*Alpha* de *Cronbach* se item removido	*Alpha* de *Cronbach*

Custos não esperados (Por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas")	0,55	0,89	
Segurança de dados	0,62	0,88	
Privacidade de dados	0,61	0,88	
Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente	0,67	0,88	
Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade)	0,57	0,89	
Disponibilidade (se o serviço e/ou dados estão sempre online e disponíveis)	0,60	0,88	0.89
Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem)	0,60	0,88	
Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação)	0,64	0,88	
Questões legais e regulamentares	0,66	0,88	
Integridade de dados (referente à manutenção de precisão e consistência de dados)	0,69	0,88	
Possibilidade de perda de dados	0,63	0,88	

Tabela 16 - Análise da consistência interna dos itens da escala Preocupação com limitações do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Relativamente á escala "Preocupação com utilização/proteção de dados", conforme o valor de *alpha* obtido (0.82) (Tabela 17), podemos dizer que a mesma apresenta uma adequada fiabilidade e uma boa consistência interna entre os seus itens. Também se nota que as correlações item-total se apresentam moderadas e altas, variando entre 0.51 e 0.70.

Itens	Correlação item-total	*Alpha* de *Cronbach* se item removido	*Alpha* de *Cronbach*
A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.	0,51	0,82	0.82
Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.	0,65	0,78	
Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser ut	0,70	0,76	
Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.	0,67	0,77	
Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.	0,58	0,80	

Tabela 17 - Análise da consistência interna dos itens da escala Preocupação com utilização/proteção de dados.

Fonte: elaboração própria com base nos outputs estatísticos.

Por fim, em relação a escala “Divulgação da informação” como um problema o valor de *alpha* obtido apresenta-se adequado (0.77), sendo boa a fiabilidade da escala assim como a consistência interna dos seus itens. As correlações item-total verificadas são moderadas, podendo ser observadas na tabela que se segue.

Itens	Correlação item-total	*Alpha* de *Cronbach* se item removido	*Alpha* de *Cronbach*
Para mim, divulgar informação pessoal, é um problema]	0,62	.	0.77
Para mim, divulgar informação pessoal, em troca de serviços online grátis, é um problema]	0,62	.	

Tabela 18 - Análise da consistência interna dos itens da escala Divulgação de informação como problema.

Fonte: elaboração própria com base nos outputs estatísticos.

Após a análise da fiabilidade e validade fatorial das escalas definidas, passamos às análises dos seus resultados gerais.

6.5 - Análise descritiva de resultados

Depois da criação de algumas escalas explicativas de itens do questionário e respetiva análise da validade e fiabilidade fatorial, passamos a descrever os resultados obtidos em cada um dos itens do questionário, assim como, de alguns dos fatores (escalas) construídos a partir dos mesmos. Assim, no que se refere, aos itens associados ao grau de conhecimento e confiança dos participantes com os vários serviços de computação em nuvem, notamos, conforme os dados da tabela 19, que a maioria dos participantes referem conhecer e utilizar com muita frequência o correio eletrónico (n=206, 80.8%), navegador de internet (n=230, 90.2%), conversação *online* (n=109, 42.7%), armazenamento online (n=95,37.3%), redes sociais (n=165, 64.7%) e outras aplicações (n=126, 49.4%).

Um número superior afirma que conhece e utiliza frequentemente *wikis* (n=106, 41.6%) e programas de produtividade e armazenamento (n=71, 27.8%).

Por fim também se nota que um número superior de indivíduos conhece e já utilizou pelo menos uma vez fóruns ou grupos de discussão (n=101, 39.6%) e blogues (n=105, 41.2%).

Grau de conhecimento/frequência sobre a utilização dos serviços de computação em nuvem	Não sei o que é		Sei o que é mas nunca utilizei		Sei o que é e já utilizei pelo menos uma vez		Sei o que é e utilizo com frequência		Sei o que é e utilizo com muita frequência	
	n	%	n	%	n	%	n	%	n	%
Correio eletrónico (*Gmail*, *Outlook*, *Yahoo*, entre outros)	0	0,0	3	1,2	3	1,2	43	16,9	**206**	**80.8**
Navegador de internet (Internet Explorer, Firefox, Chrome, entre outros)	0	0,0	2	0,8	1	0,4	22	8.6	**230**	**90.2**
Conversação online (vídeo, voz ou texto, como Skype ou Hangouts, entre outros)	0	0,0	11	4,3	55	21.6	80	31.4	**109**	**42.7**
Fóruns ou grupos de discussão	2	0,8	68	26,7	**101**	**39,6**	53	20.8	31	12,2
Wikis (sítios de colaboração, como *Wikipedia*)	4	1.6	36	14,1	51	20.0	**106**	**41.6**	58	22,7
Blogues	1	0,3	53	20,8	**105**	**41,2**	65	25,5	32	12,5
Armazenamento online (*OneDrive*, *Google Drive*, *Dropbox*, entre outros)	1	0,4	44	17.3	48	18.8	67	26,3	**95**	**37,3**
Produtividade (*Office 365*, *Google Docs*, *Limesurvey*, entre outros)	22	8,6	43	16,9	63	24,7	**71**	**27.8**	56	22.0
Redes Sociais (*Facebook*, *Youtube*, *Tumblr*, *Twitter*, *Google+*, *Linkedin*, *Instagram*, *Pinterest*, *Orkut*, *Snapchat*, *WhatsApp*, entre outros)	1	0,8	8	3,1	18	7,1	63	24.7	**165**	**64,7**
Outras aplicações (meteorologia, noticias, entre outras)	2	0,8	8	3,1	33	12,9	86	33.7	**126**	**49,4**

Tabela 19 - Análise de frequências relativas às questões sobre o grau de conhecimento e frequência dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Em termos de valores médios obtidos podemos verificar de acordo com a figura 10, que os participantes referem frequentar mais e conhecer melhor os navegadores de internet (M=4.88),

assim como, os serviços de correio eletrónico (M=4.77), e, também, as redes sociais (M=4.50). Por outro lado, existe uma menor tendência para conhecer e frequentar fóruns ou grupos de discussão na internet (M=3.17).

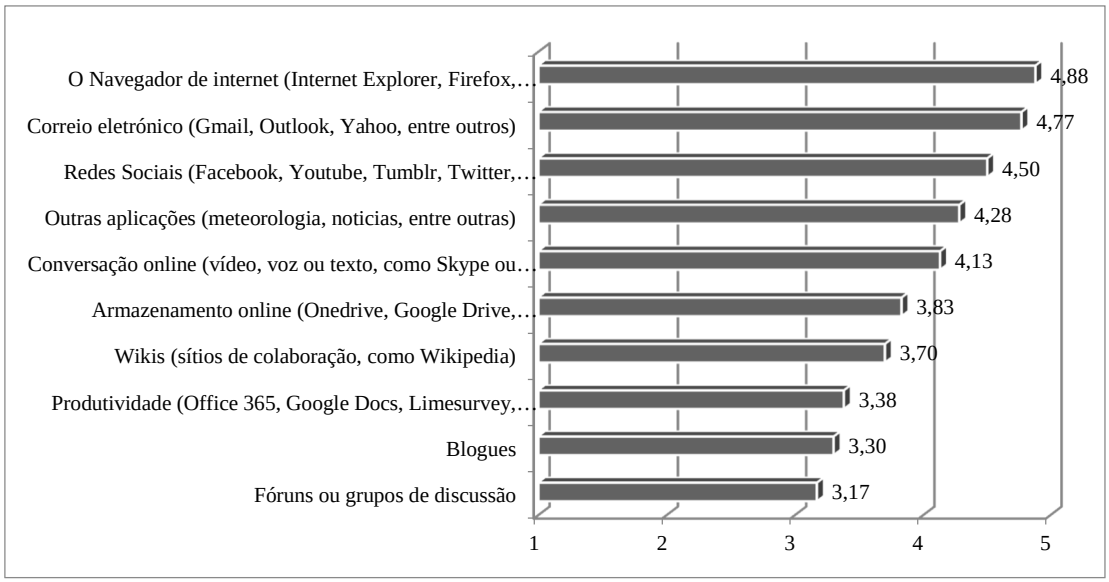

Figura 11 - Resultados médios relativos às questões sobre o conhecimento/frequência de utilização dos vários serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto à análise do fator geral obtido do conjunto de itens (Escala de conhecimento/frequência de utilização dos serviços de computação em nuvem) podemos constatar da tabela 20, que o valor médio obtido (M=3.99), assim como, o valor mediano (Md=4.10) se apresentam elevados tendo em conta uma escala que varia entre 1 e 5 pontos. Estes valores podem ser significativos de um elevado grau de conhecimento/frequência de utilização dos participantes dos serviços de computação em nuvem. Conforme os valores dos coeficientes de simetria (Simetria/Erro padrão=3.80), podemos também confirmar esta tendência para resultados mais elevados. Este coeficiente (distribuição assimétrica) e, também, o valor não significativo do teste de *Kolgomorov-Sminorv* (K-S=0.09, p<0.05) revelam que a distribuição dos resultados não se apresenta normal (Tabela 20 e Figura 11).

Grau de conhecimento/utilização dos serviços proporcionados pela computação em nuvem		Valor	Erro padrão
Média		3,99	0,04
95% intervalo de confiança para média	Limite mínimo	3,92	

	Limite máximo	4,05	
Mediana		4,10	
Variância		0,28	
Desvio Padrão		0,53	
Mínimo		2,00	
Máximo		5,00	
Amplitude		3,00	
Simetria		-0,57	0,15
Curtose		0,49	0,30
K-S (Sig)		0.09	0.00

Tabela 20 - Medidas de tendência central, dispersão e distribuição dos resultados relativos ao Grau de conhecimento/frequência de utilização dos serviços proporcionados pela computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

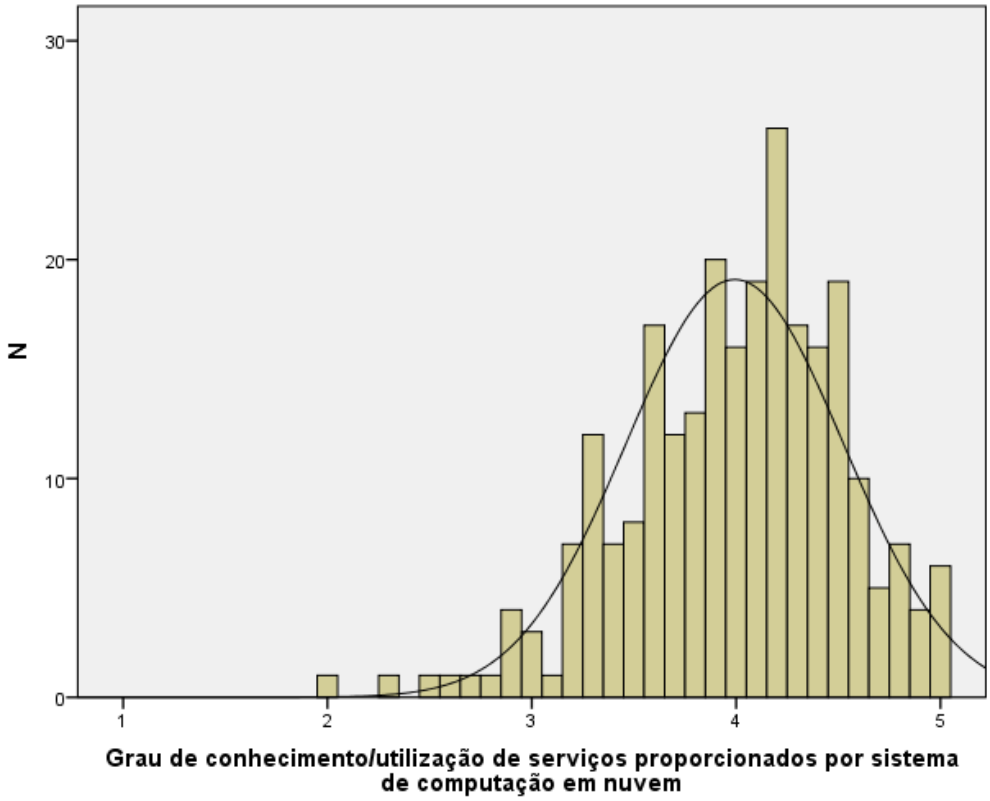

Figura 12 - Histograma relativo a distribuição dos resultados da variável grau de conhecimento/frequência dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Em relação às questões relativas à importância das vantagens dos serviços de computação em nuvem, verifica-se na tabela 21, que os participantes consideram muito importante os menores custos (n=103, 40.4%), o aumento das capacidades disponíveis (n=102, 40.0%), a segurança dos dados (n=178, 69.8%), a mobilidade (n=187, 73.3%) e a disponibilidade (n=184, 72.2%).

Um número superior considera bastante importante a estabilidade do sistema (n=95, 37.3%) e um número mais elevado de indivíduos consideram apenas importante o menor grau de conhecimento necessário para a utilização deste sistema (n=84, 32.9%).

Importância das vantagens dos serviços de computação em nuvem	Nada importante		Pouco importante		Importante		Bastante importante		Muito Importante	
	n	%	n	%	n	%	n	%	n	%

Menores custos (menor compra de discos rígidos, cd, dvd, pen, entre outros, componentes físicos e programas)	0	0.0	13	5,1	46	18.0	93	36,5	**103**	**40,4**
Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita)	1	0,4	12	4,7	57	22.4	**95**	**37,3**	90	35,3
Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos)	1	0,4	11	4,3	40	15,7	101	39,6	**102**	**40,0**
Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço)	9	3,5	39	15,3	**84**	**32,9**	81	31.8	42	16,5
Segurança de dados	2	0,8	3	1,2	29	11,4	43	16,9	**178**	**69,8**
Mobilidade (acesso em qualquer local	0	0.0	3	1,2	18	7,1	47	18,4	**187**	**73,3**
Disponibilidade (acesso a qualquer momento)	0	0.0	1	0,4	20	7.8	50	19,6	**184**	**72.2**

Tabela 21 - Frequências relativas à importância das vantagens dos vários serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

De acordo com a figura 12, verifica-se que existe uma maior tendência para os participantes considerarem mais importante a maior mobilidade (M=4.64), a segurança dos dados (M=4.54) e a disponibilidade (M=4.53). Por outro lado, há menor tendência para considerar relevantes aspetos como a escalabilidade (M=4.12) e o menor grau de conhecimento necessário para utilização dos serviços (M=3.42).

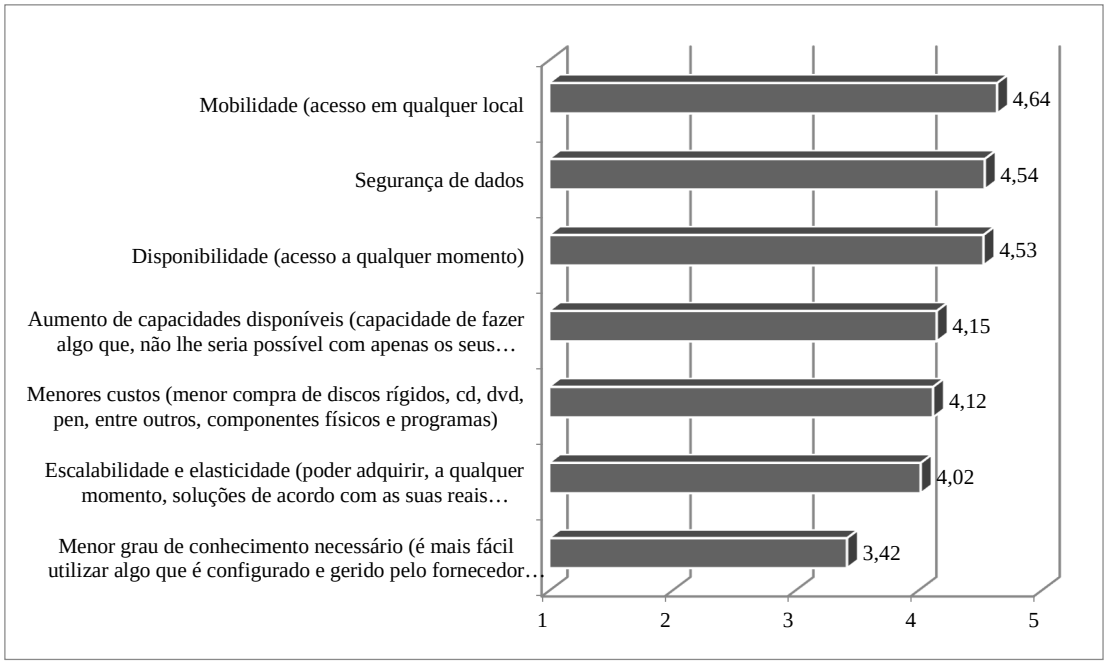

Figura 13 - Resultados médios relativos às questões relacionadas com a importância das vantagens dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto aos resultados do fator geral, alusivo ao grau de importância das vantagens do sistema de computação em nuvem, é possível verificar, de acordo com o valor médio (M=4.21) e mediano (Md=4.28) obtidos, que os participantes conferem grande importância às vantagens do sistema de computação em nuvem. Também o coeficiente de simetria obtido (6.53) indica uma maior tendência dos dados para valores superiores. Ainda de acordo com a assimetria verificada e também pelo valor significativo do teste de *kolgomorov sminorv* (K-S=0.11, p<0.05) que a distribuição dos resultados não se apresenta normal (Tabela 22)

Grau de importância das vantagens do sistema de computação em nuvem		Valor	Erro padrão
Média		4,21	0,03
95% intervalo de confiança para média	Limite mínimo	4,14	
	Limite máximo	4,29	
Mediana		4,28	
Variância		0,34	
Desvio Padrão		0,58	

Mínimo	2,14	
Máximo	5,00	
Amplitude	2,86	
Simetria	-0,98	0,15
Curtose	0,96	0,30
K-S (Sig)	0.11	0.00

Tabela 22 - Medidas de tendência central, dispersão e distribuição relativas ao grau de importância das vantagens do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

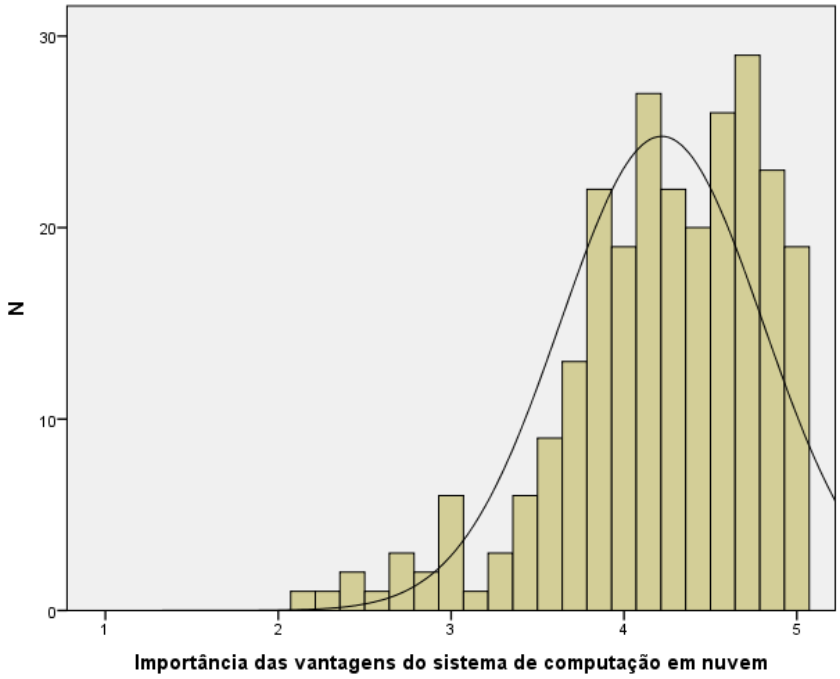

Figura 14 - Histograma da distribuição dos resultados relativos ao grau de importância das vantagens do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Em relação às questões relativas com a preocupação com as limitações da utilização do sistema de computação em nuvem podemos observar que a maioria dos participantes considera muito preocupante os custos não esperados (n=137, 53.7%), a integridade dos dados (n=95, 37.3%), a possibilidade de perda de dados (n=174, 68.2%), a segurança dos dados (n=195, 76.5%), a

privacidade dos dados (n=206, 80.4%), perda de controlo sobre dados e aplicações (n=145, 56.9%).

Notamos, também, que um número superior de participantes considera apenas bastantes importante a dependência da rede (n=91,35.7%), disponibilidade (n=93, 36.5%), complexidade de adoção e utilização (n=86, 33,7%), a possibilidade de ficar dependente de um serviço (n=89, 34.9%) e as questões legais e regulamentares (n=79, 31.0%) (Tabela 23).

Preocupação com limitações da utilização do sistema de computação em nuvem	Nada preocupante		Pouco preocupante		Preocupante		Bastante preocupante		Muito preocupante	
	n	%	n	%	n	%	n	%	n	%
Custos não esperados (por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas")	3	1.2	10	3,9	47	18.4	58	22,7	**137**	**53,7**
Integridade de dados (referente à manutenção de precisão e consistência de dados)	6	2,4	20	7,8	45	17,6	89	34,9	**95**	**37,3**
Possibilidade de perda de dados	5	2,0	9	3,5	22	8,6	45	17,6	**174**	**68,2**
Segurança de dados	0	0.0	8	3.1	19	7.5	33	12,9	**195**	**76,5**
Privacidade de dados	0	0.0	7	2.7	18	7,1	24	9.4	**206**	**80.4**
Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente)	2	0,8	10	3,9	33	12.9	65	25,5	**145**	**56.9**
Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade)	5	2,0	21	8,2	54	21,2	**91**	**35,7**	84	32,9

Disponibilidade (se o serviço e/ou dados estão sempre *online* e disponíveis)	6	2,4	17	6,7	47	18,4	**93**	**36,5**	92	36,1
Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem)	16	6.3	37	14,5	66	25,9	**86**	**33,7**	50	19,6
Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação)	3	1,2	29	11,4	61	23,9	**89**	**34,9**	72	28,6
Questões legais e regulamentares	9	3,5	32	12,5	62	24,3	**79**	**31,0**	73	28,6

Tabela 23 - Frequências relativas às questões sobre a preocupação com as limitações da utilização do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Conforme os resultados médios expostos na figura 14, podemos verificar que existe uma maior tendencia para os participantes se preocuparem com as limitaçoes que o sistema de computaçao em nuvem confere em relação à privacidade dos dados (M=4.68), assim como a sua segurança (M=4.63). Não se verifica já tanta tendencia para existir preocupação com as questoes legais e regulamentares (M=3.69), assim como com a complexidade da adoção e utilizaçao do sistema (M=3.46).

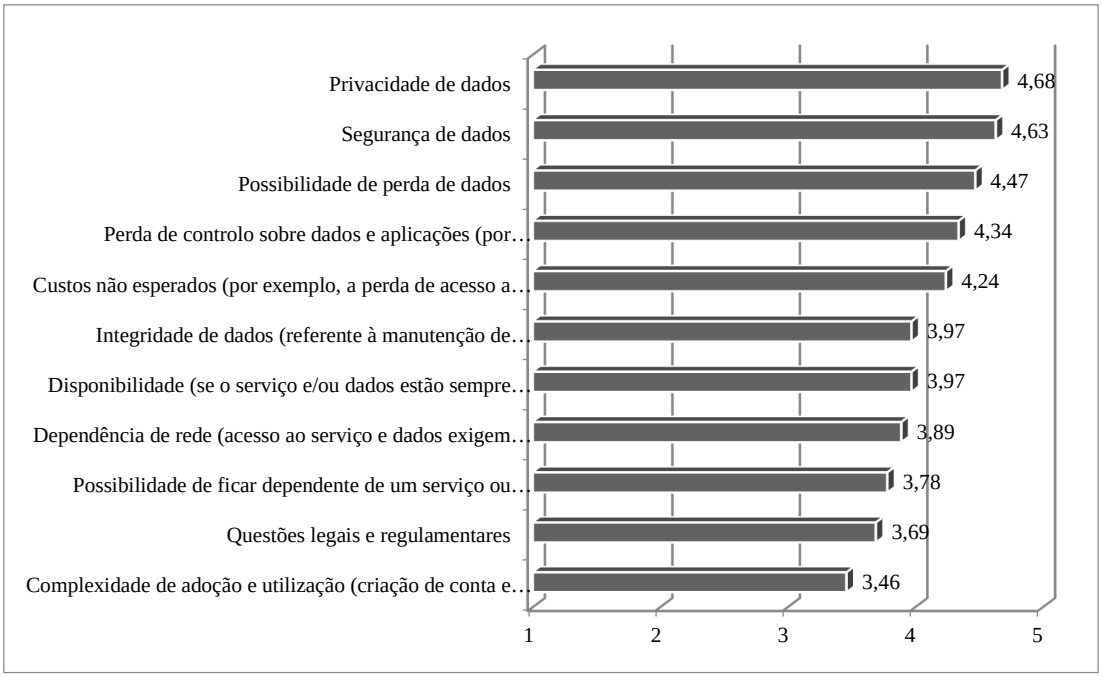

Figura 15 - Resultados médios relativos à preocupação com as limitações dos serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Os resultados obtidos para o fator geral preocupação com as limitações da tecnologia de computação em nuvem apresentam-se na tabela 24, sendo de verificar um valor médio de M=4.08 e uma mediana de Md=4.20 o que parece indicar valores elevados de preocupação com as limitações do sistema de computação em nuvem. O valor do coeficiente de simetria obtido (6.53) releva, também, que existe um número elevado de casos com valores mais elevados nesta variável, sendo que a distribuição dos resultados se apresenta assimétrica e com maior tendência para valores elevados. Para além desta distribuição assimétrica que torna a distribuição dos resultados não normal, também o valor não significativo do teste de *kolgomorov sminorv* (K-S=0.13, p<0.05), confirma a ausência de uma distribuição normal (Tabela 24 e Figura 15, ambas de seguida).

Preocupação com limitações da tecnologia de computação em nuvem		Valor	Erro padrão
Média		4,08	0,04
95% Intervalo de confiança para média	Limite mínimo	4,00	
	Limite máximo	4,17	
Mediana		4,20	

Variância	0,47	
Desvio Padrão	0,68	
Mínimo	1,80	
Máximo	5,00	
Amplitude	3,20	
Simetria	-0,98	0,15
Curtose	0,75	0,30
K-S (Sig)	0.13	0.00

Tabela 24 - Medidas de tendência central, dispersão e distribuição relativas ao grau de importância das vantagens do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

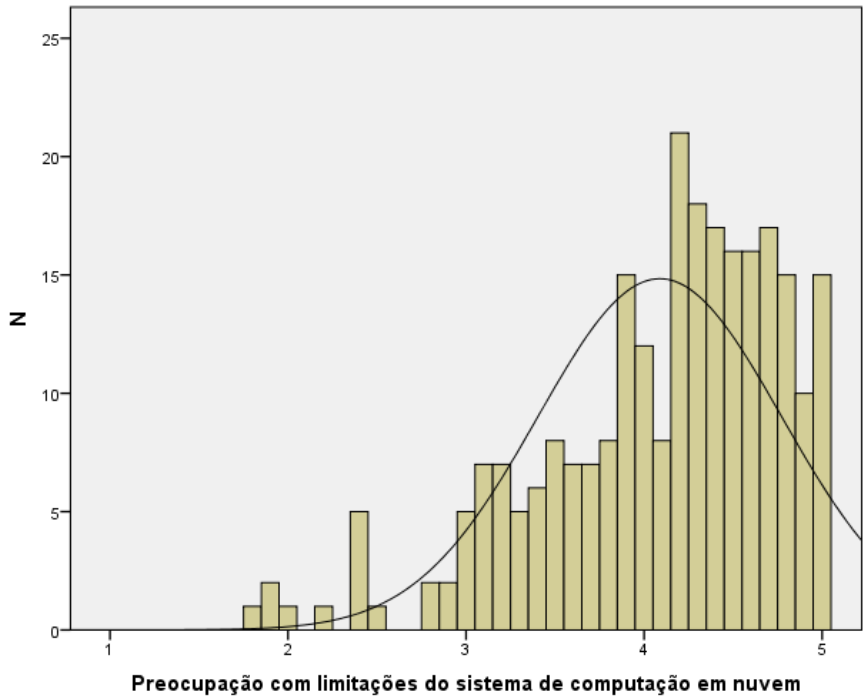

Figura 16 - Histograma de distribuição de resultados relativos à preocupação com limitações do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Relativamente à confiança que os participantes têm na tecnologia de computação em nuvem podemos verificar da figura 16, abaixo, que a maioria afirma encontrar-se ou confiante (40.0%) ou bastante confiante (33.7%) com esta tecnologia. Verificamos, também, que a maioria dos indivíduos relata estar confiante (n=42.7%) ou bastante confiante (32.2%) com os fornecedores de serviços.

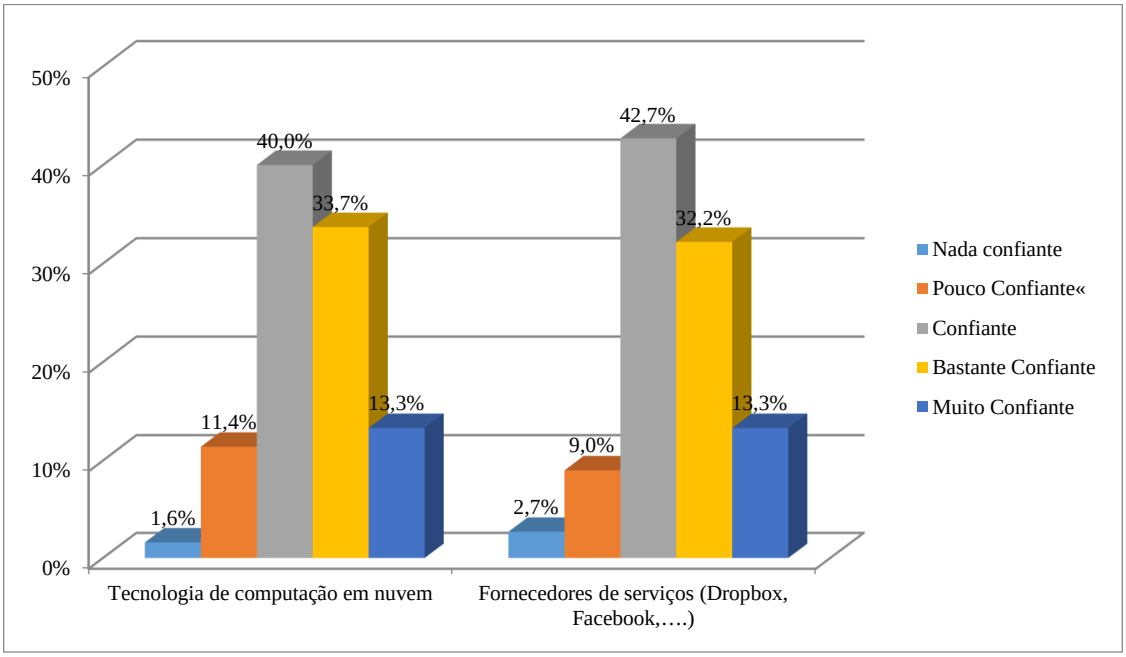

Figura 17 - Grau de confiança com o sistema de tecnologia de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto ao grau de concordância com questões de segurança do sistema de computação em nuvem, conforme os resultados da tabela que se segue, podemos observar que a maioria afirma concordar que as questões de segurança são um problema que impende a adoção de serviços baseados em computação em nuvem (n=119, 46.7%), e que, em geral, se sentem mais confiantes com a utilização de soluções proprietárias que correm e existem nos seus dispositivos (n=126, 49.4%), que sentem que a tecnologia de computação na nuvem está pronta para salvaguardar os seus dados e informação mais importante (n=101, 39.6%) e que sentem que o sistema será mais seguro no futuro (n=114, 44.7%).

Grau de Concordância com questões de segurança do sistema de computação em nuvem	Discordo Totalmente	Discordo	Não concordo nem discordo	Concordo	Concordo Totalmente

	n	%	n	%	n	%	n	%	n	%
Questões de segurança são um problema que impedem a adoção de serviços baseados em computação em nuvem.	4	1,6	19	7,5	40	15.7	**119**	**46,7**	73	28,6
Em geral, sinto-me mais confiante com a utilização de soluções proprietárias que correm e existem no meu dispositivo (computador pessoal, telemóvel e tablets)	4	1,6	18	7.1	44	17,3	**126**	**49.4**	63	24.7
Sinto que a tecnologia de computação na nuvem está pronta para salvaguardar os meus dados e informação mais importantes	13	5,1	34	13,3	83	32.5	**101**	**39,6**	24	9,4
Sinto que a computação em nuvem será mais segura no futuro	4	1,6	12	4.7	48	18.8	**114**	**44.7**	77	30,2

Tabela 25 - Frequências relativas a questões sobre o grau de concordância com a segurança do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Também de acordo com a figura 17 podemos verificar que existe uma maior tendência para os participantes concordarem mais com o facto de a computação em nuvem vir a ser mais segura no futuro (M=3.97), de que as questões de segurança são um problema que impede a adoção de serviços de computação em nuvem (M=3.93) e sentem-se mais confiantes com a utilização de soluções proprietárias que correm e existem nos seus dispositivos (M=3.89).

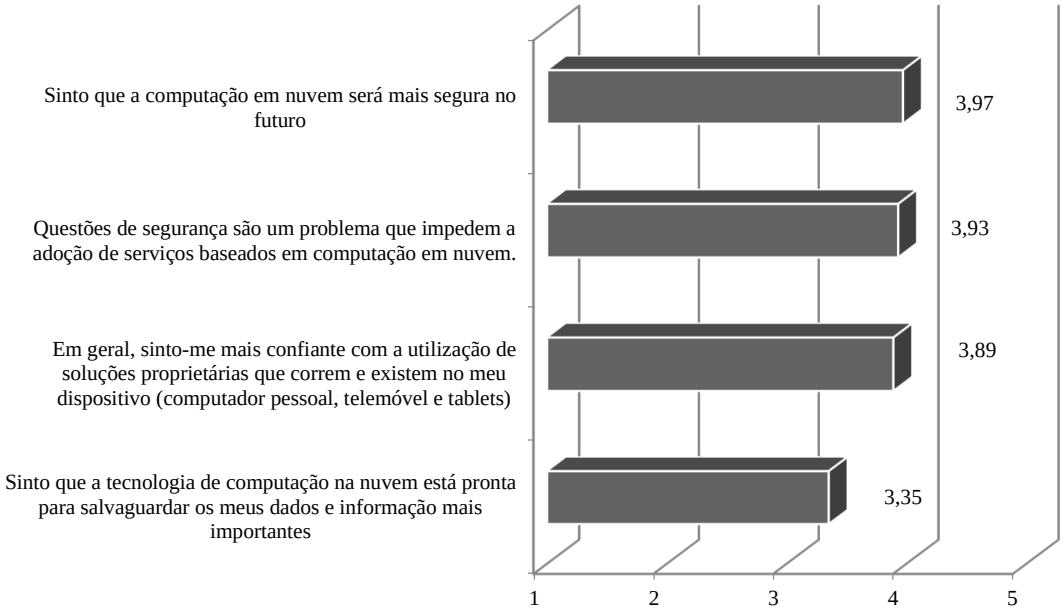

Figura 18 - Resultados médios relativos às questões sobre o grau de segurança do sistema de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

No que concerne à preocupação com a proteção e utilização indevida de dados pessoais, os participantes relatam na sua maioria que sentem muita preocupação com a localização física dos dados não ser conhecida (n=99, 38.8%) e com problemas de programação ou fracos parâmetros de segurança, entre outros, que podem colocar em risco a confidencialidade integridade e disponibilidade dos dados (n=112, 43.9%). Também se consideram totalmente preocupados com o facto dos recursos em nuvem utilizados para armazenar dados serem partilhados entre utilizadores (n=107, 42.0%), dos utilizadores não autorizados, como piratas, poderem aceder aos dispositivos pessoais através de falhas de configuração do sistema (n=163, 63.9%) e, também, de algo imprevisto, como um desastre natural num centro de dados fornecedor de serviços conduzir a perda total e definitiva dos dados (n=119, 46.7%). Conforme se pode observar na seguinte tabela.

Preocupação com a proteção/utilização indevida dos dados	Nenhuma preocupação		Pouca preocupação		Nem preocupado nem despreocupado		Muita preocupação		Absoluta preocupação	
	n	%	n	%	n	%	n	%	n	%

A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.	9	3,5	22	8,6	78	30,6	**99**	**38,8**	47	18,4
Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.	1	0,4	11	4,3	30	11,8	**112**	**43,9**	101	39,6
Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser utilizados e implicados em ações menos éticas ou mesmo ilegais, por parte de terceiros.	3	1,2	16	6,3	31	12,2	98	38.4	**107**	**42,0**
Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.	0	0.0	11	4,3	18	7,1	63	24,7	**163**	**63,9**
Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.	7	2,7	17	6,7	35	13,7	77	30,2	**119**	**46,7**

Tabela 26 - Frequências relativas às questões sobre a preocupação com a utilização indevida/proteção dados dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

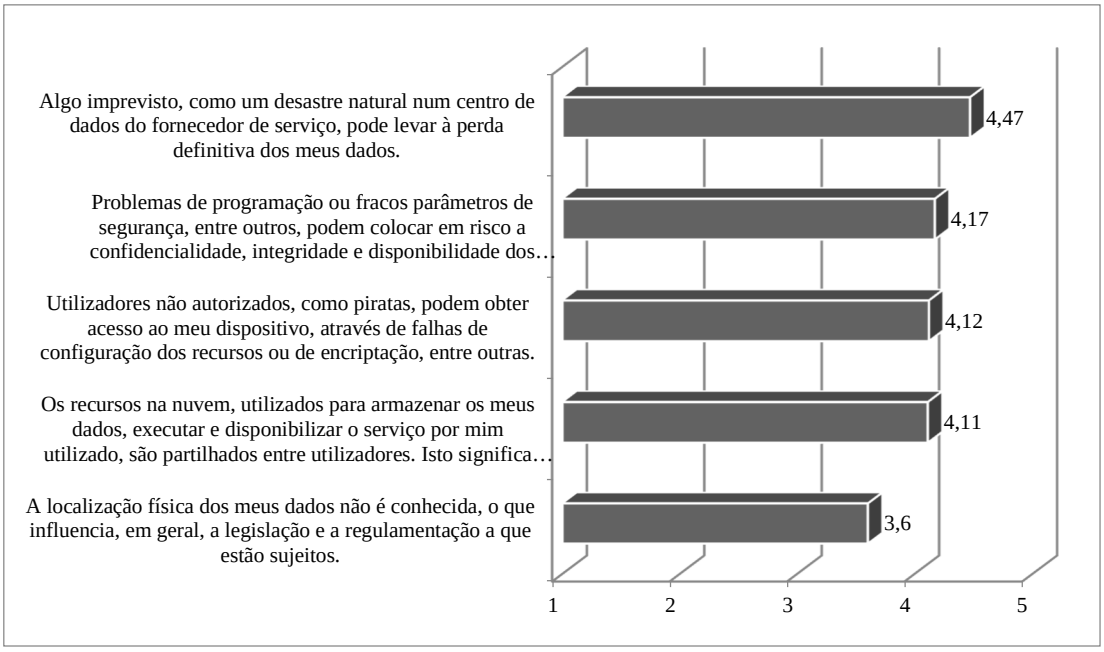

Figura 19 - Resultados médios relativos às questões sobre a preocupação com a proteção e utilização indevida de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto aos resultados do fator geral preocupação com a utilização indevida/proteção dos dados, conforme a tabela 27, verifica-se que os resultados médios (M=4.10) e medianos (Md=4.20) obtidos se apresentam elevados, o que significa que se verifica uma grande preocupação por parte dos participantes com a utilização indevida e com a proteção dos seus dados pessoais. Também o coeficiente de simetria obtido (6.53) comprova essa mesma maior distribuição dos resultados para valores mais elevados. Esta assimetria revela, também, que a distribuição dos resultados não é normal, questão esta também comprovada pelo valor não significativo obtido no teste de *Kolgomorov Sminorv* (Ks=0.14, p<0.05) (Figura 19)

Preocupação com a utilização indevida/proteção dos dados		Valor	Erro padrão
Média		4,10	0,04
95% Intervalo de confiança para média	Limite mínimo	4,01	
	Limite máximo	4,19	
Mediana		4,20	
Variância		0,50	

Desvio Padrão	0,71	
Mínimo	1,60	
Máximo	5,00	
Amplitude	3,40	
Simetria	-0,98	0,15
Curtose	0,70	0,30
K-S (Sig)	0.14	0.00

Tabela 27 - Medidas de tendência central, dispersão e distribuição relativas à variável preocupação com a utilização indevida/proteção de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

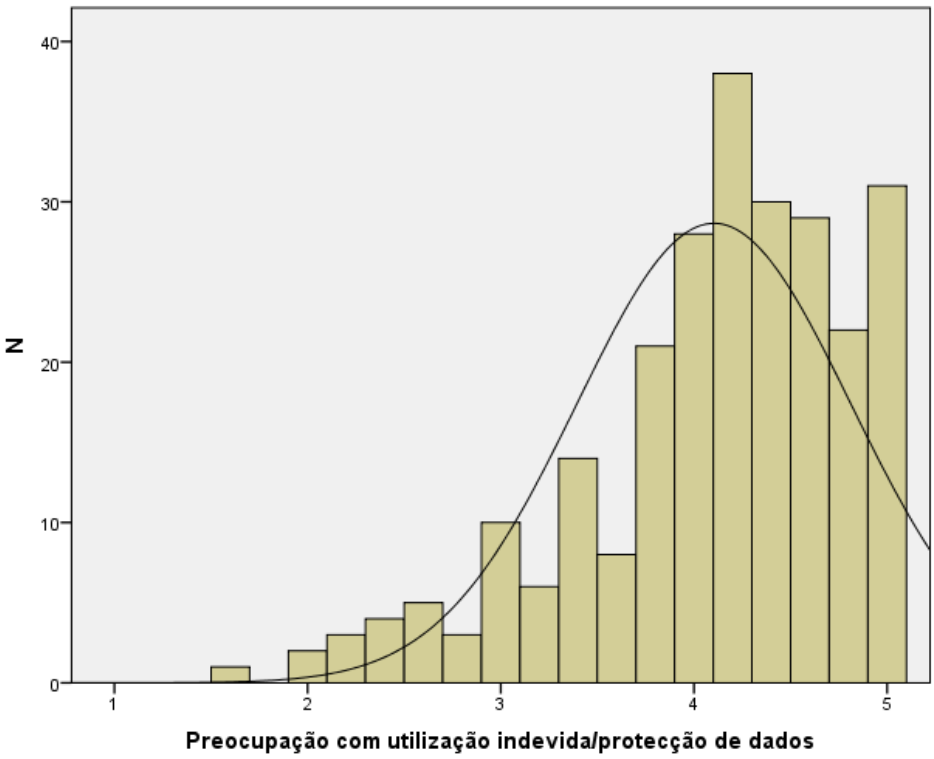

Figura 20 - Histograma de distribuição de resultados relativos ao fator preocupação com utilização/proteção indevida de dados.

Fonte: elaboração própria com base nos outputs estatísticos.

No que respeita à opinião sobre quais as principais entidades responsável pela segurança dos dados, a maioria dos participantes afirmam ser eles próprios (n=76, 29.8%) ou os fornecedores

de serviços (n=128, 50.2%). Uma minoria aponta as empresas privadas (n=5, 2.0%) e o governo (n=2, 0.8%) (Figura 20).

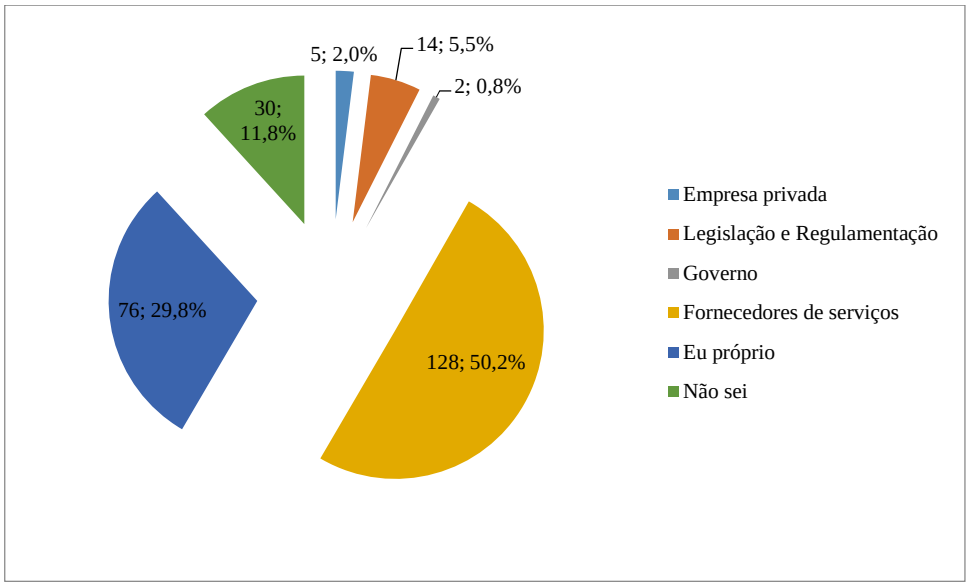

Figura 21 - Entidades responsáveis pela segurança dos dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto ao modo como os participantes classificam as entidades de acordo com o grau de ameaça que representam a proteção dos seus dados pessoais, podemos observar na tabela 28, que um número superior considera os piratas informáticos como uma ameaça total aos seus dados (n=173, 67.8%). Também um número superior considera uma ameaça muito grande aos seus dados o governo (n=85, 33.3%), as empresas privadas (n=98, 38.4%) e as entidades de publicidade (n=114, 44.7%).

Classificação de entidades por grau de ameaça	Ausência de ameaça		Alguma ameaça		Indiferente		Muita ameaça		Ameaça total	
	n	%	n	%	n	%	n	%	n	%
Governo	10	3,9	36	14,1	63	24.7	**85**	**33.3**	61	23,9
Empresas privadas	7	2,7	45	17,6	56	22,0	**98**	**38,4**	49	19,2
Entidades de publicidade	6	2,4	32	12,5	39	15,3	**114**	**44,7**	64	25,1
Piratas Informáticos	3	1,2	6	2,4	12	4,7	61	23,9	**173**	**67,8**

Tabela 28 - Frequências relativas à classificação das entidades por grau de ameaça aos dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Também de acordo com a figura 21, podemos confirmar que os piratas informáticos são considerados a maior ameaça aos dados pessoais (M=4.55), enquanto as empresas privadas são consideradas como menos ameaçadoras (M=3.54).

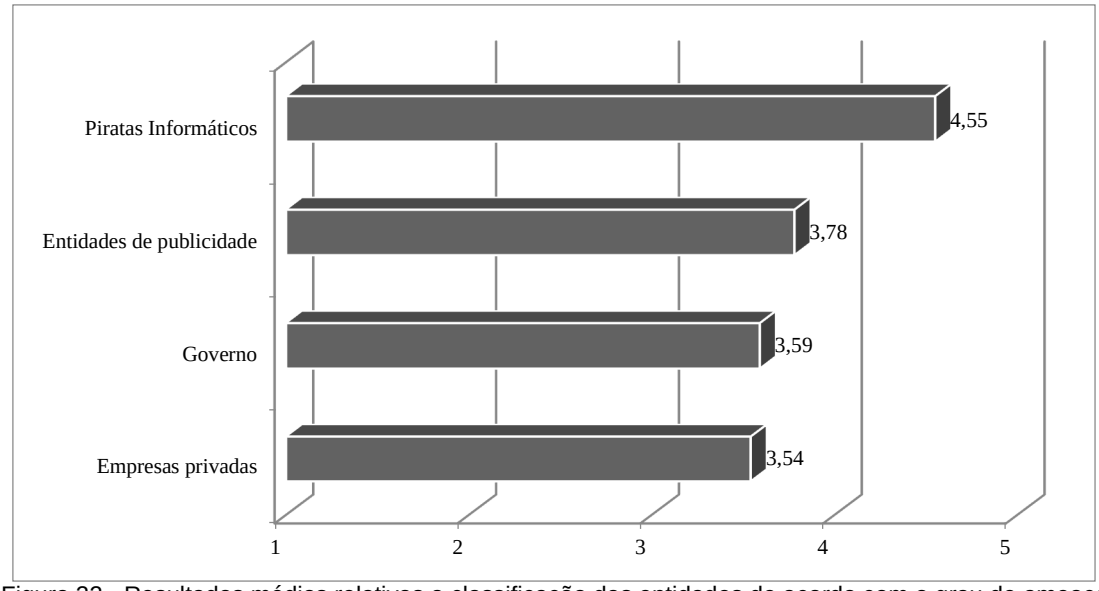

Figura 22 - Resultados médios relativos a classificação das entidades de acordo com o grau de ameaça aos dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

No que refere ao sentimento que provoca a venda dos dados informáticos uma proporção superior de participantes afirma que fica completamente escandalizado (30.2%) seguindo-se os que referem que ficam muito perturbados (27.1%). Uma minoria refere não se importa com a venda dos seus dados informáticos (3.5%) (Figura 22).

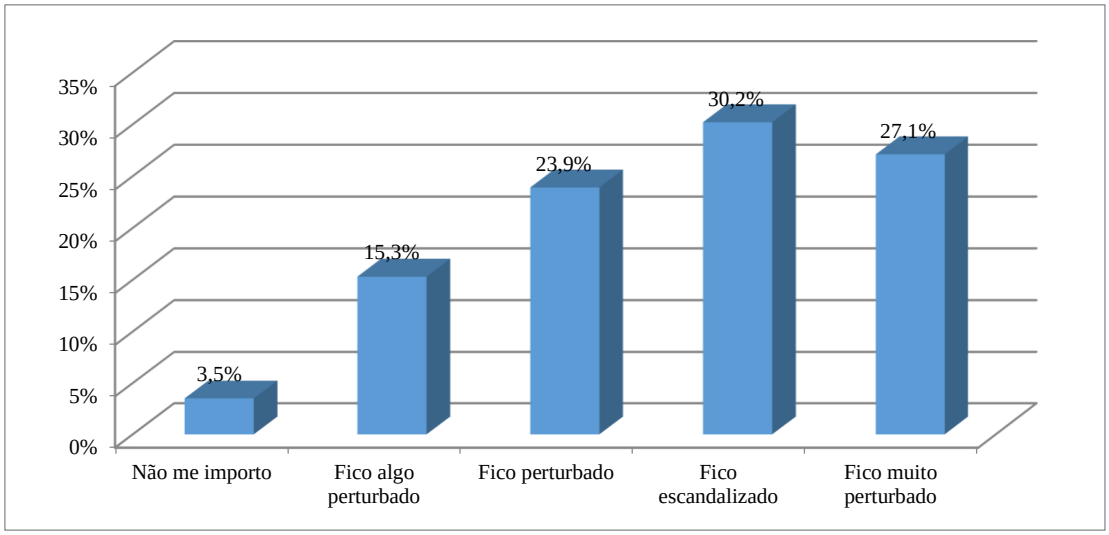

Figura 23 - Sentimento que provoca a venda de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Relativamente ao principal responsável pela proteção de privacidade *online* os participantes afirmam ser os fornecedores de serviços (n=97, 38.0%) seguindo-se eles próprios (n=82, 32.2%). Uma proporção inferior afirma ser o governo (n=35, 13.7%) e um número igualmente inferior (n=34, 13.3) desconhece e apenas 7 (2.7%) não respondem à questão (Figura 23).

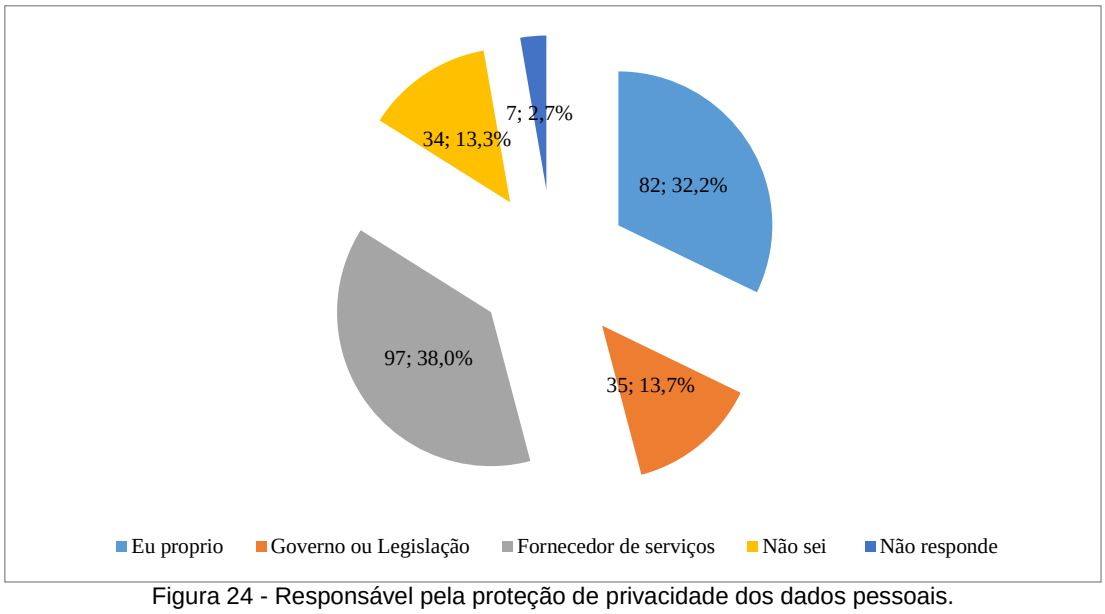

Figura 24 - Responsável pela proteção de privacidade dos dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

De acordo com a figura 24, podemos observar qual é a opiniao que os participantes têm dos momentos em que devem autorizar a divulgação dos seus dados pessoais, sendo que a maioria

afirma que devem ser em todos os casos (n=185,72,5%). Um numero inferior refere que deve ser no contexto de informação pessoal solicitada na internet (n=47, 18.4%) e no caso de informação mais sensivel (n=17, 6.7%).

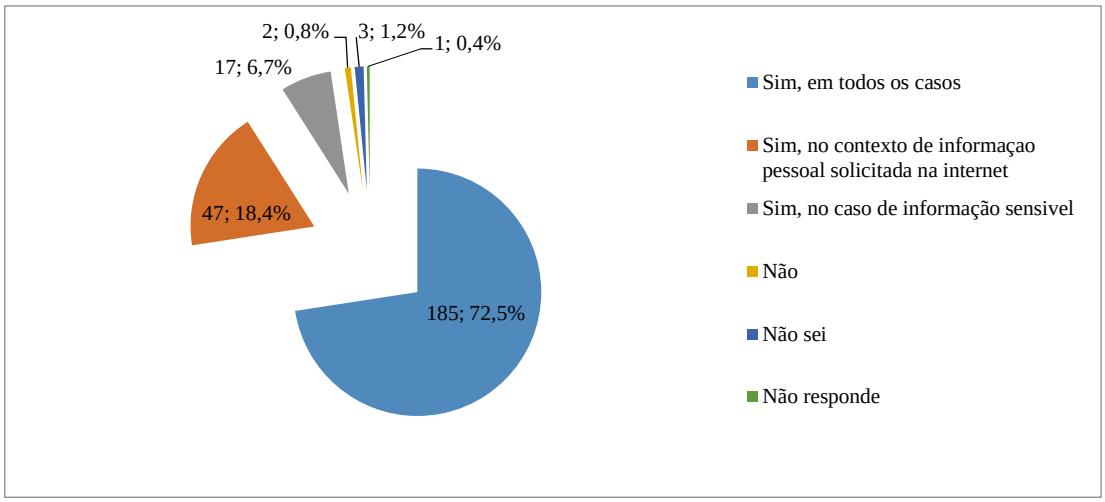

Figura 25 - Momentos de autorização de divulgação de dados pessoais na internet.

Fonte: elaboração própria com base nos outputs estatísticos.

No que diz respeito às circunstâncias em que os dados pessoais devem ser apagados um número superior afirma que deve ser sempre que decidam apagar (n=233, 91.4%). Em proporção inferior estão os que afirmam que deve ser quando mudam de fornecedor de internet (n=5, 2.0%) ou que deixem de usar determinado serviço *cloud* (n=13, 5.1%).

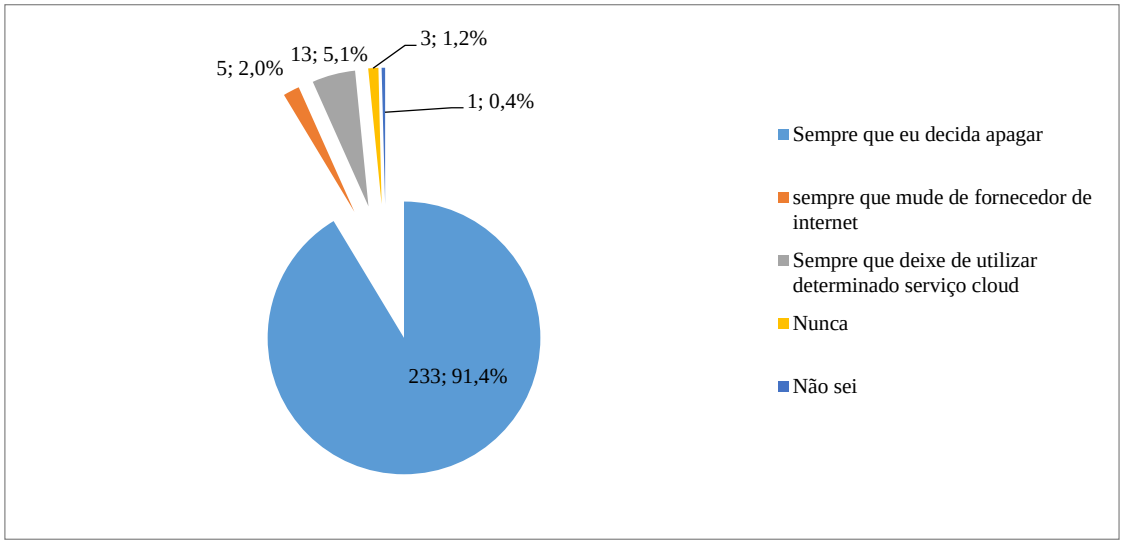

Figura 26 - Momento de apagar dados pessoais na *cloud.*

Fonte: elaboração própria com base nos outputs estatísticos.

Em relação á importância dos direitos de proteção e segurança dos dados pessoais a maior parte dos participantes afirma considerar muito importante este facto. Um número mais inferior considera apenas importante (10.6%) ou mesmo pouco importante (1.0%) ou mesmo indiferente (1.2%) (Figura 26).

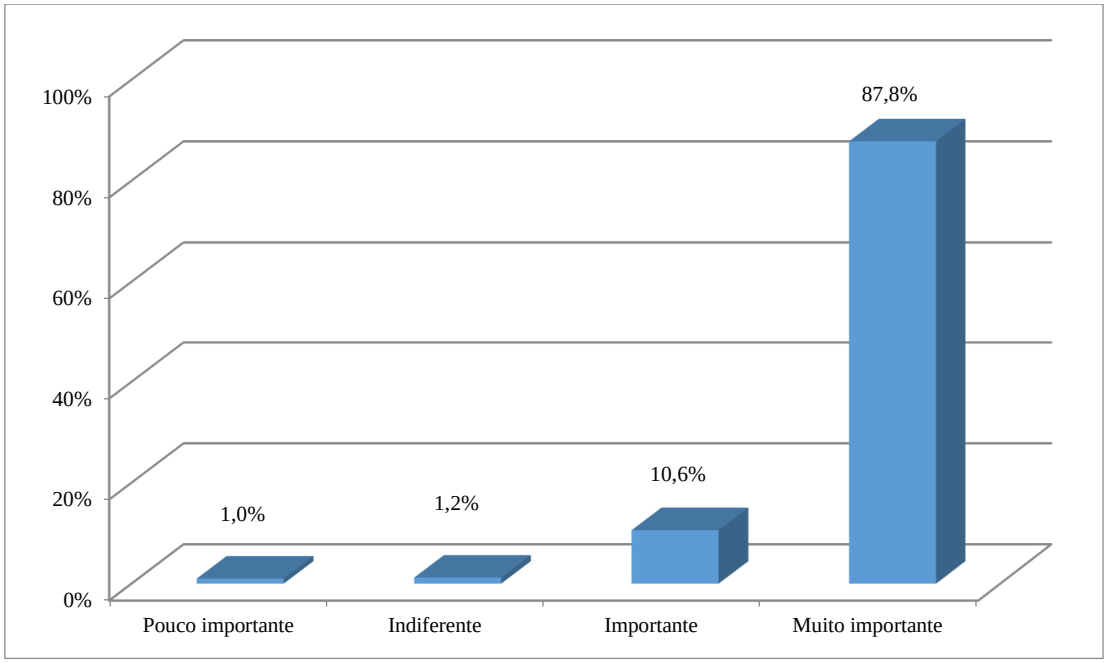

Figura 27 - Importância dos direitos de proteção de dados.

Fonte: elaboração própria com base nos outputs estatísticos.

Quanto ao controlo percebido dos dados pessoais é possível afirmar em conformidade com os resultados da figura 27, que a maioria dos participantes referem ter um baixo nível de controlo sobre a informação e dados divulgados pelos serviços de computação em nuvem (38.4%). Porém, um número ainda razoável refere, também, ter um alto controlo (26.3%), notando-se, assim, uma tendência para o equilíbrio no que respeita ao controlo percebido dos participantes.

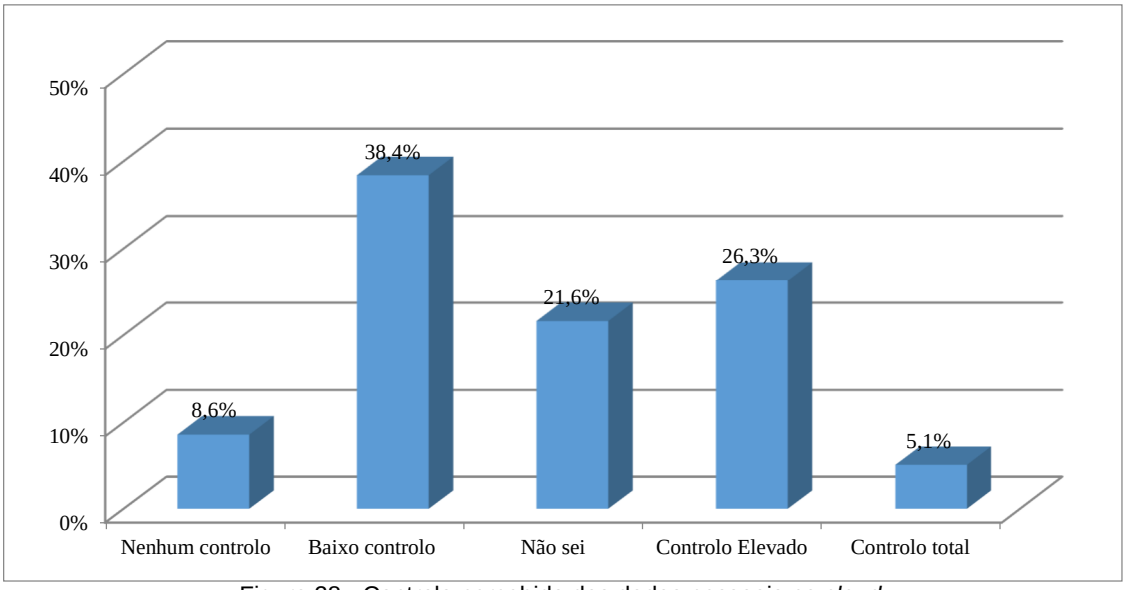

Figura 28 - Controlo percebido dos dados pessoais na *cloud.*

Fonte: elaboração própria com base nos outputs estatísticos.

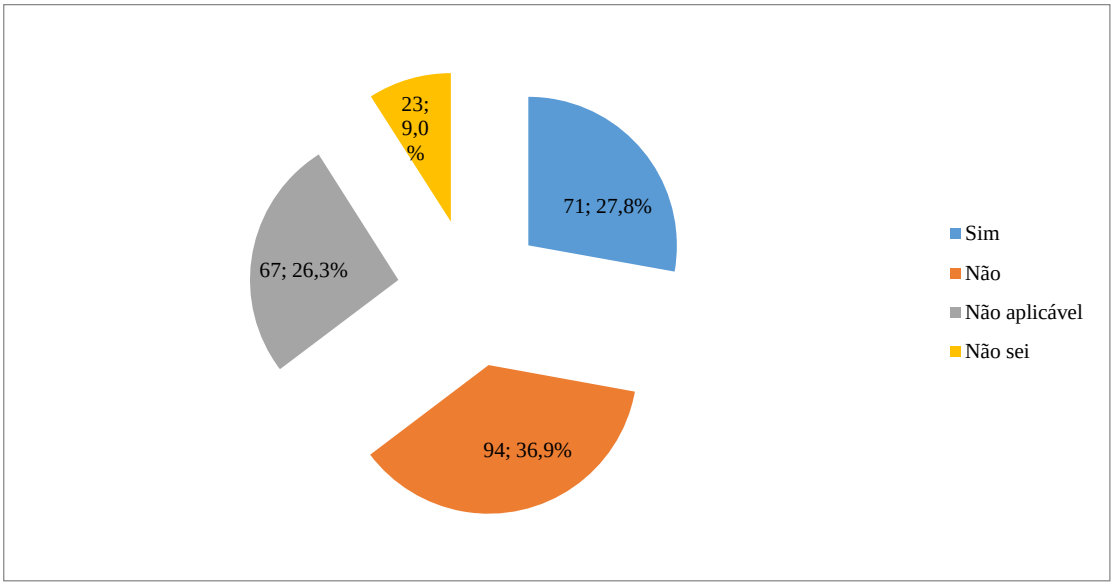

Figura 29 - Quando tem intenções de utilizar um serviço, baseado nesta tecnologia, sente-se informado sobre as condições de compilação dos seus dados e futura utilização dos mesmos?

Fonte: elaboração própria com base nos outputs estatísticos.

No que se refere ao conhecimento sobre a computação em nuvem, a maioria dos participantes afirmam estar informados (47.8%). Um número inferior refere estar muito informado (19.20%) e uma clara minoria refere estar ou nada informado (3.5%) ou muito informado (2.70%).

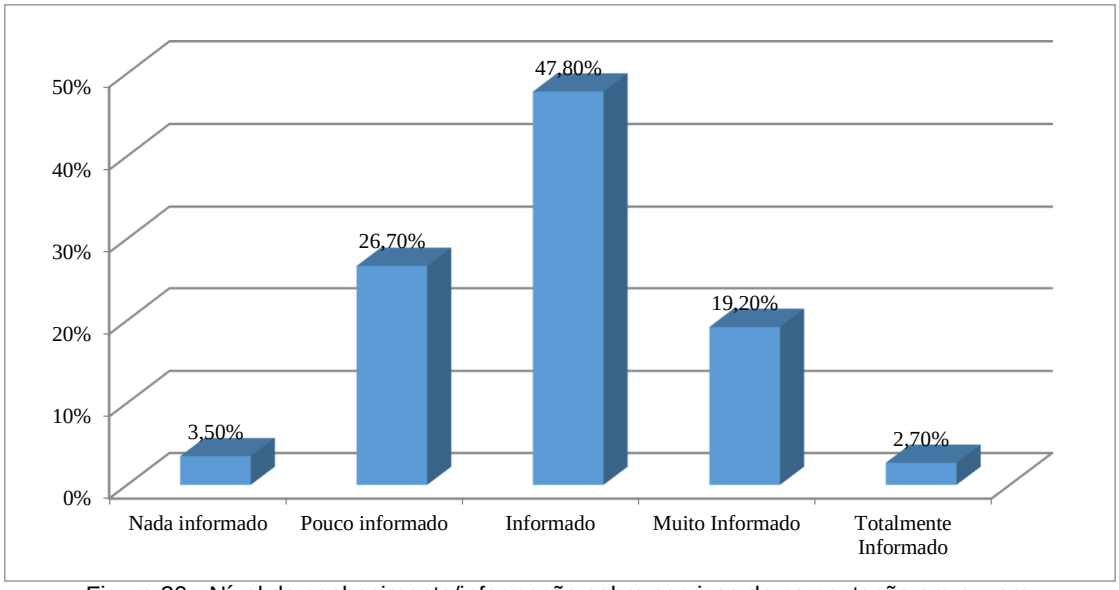

Figura 30 - Nível de conhecimento/informação sobre serviços de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

Relativamente ao tempo de utilização dos serviços de computação em nuvem, a maioria dos participantes refere utilizar este tipo de serviço há menos de 5 anos (20.0%). Um número também superior afirma que só utiliza o serviço há menos de um ano (18.8%), enquanto 12.5% dos indivíduos afirma nunca ter utilizado o serviço e um número bastante elevado (25.9%) não sabem a quanto tempo utilizam o serviço.

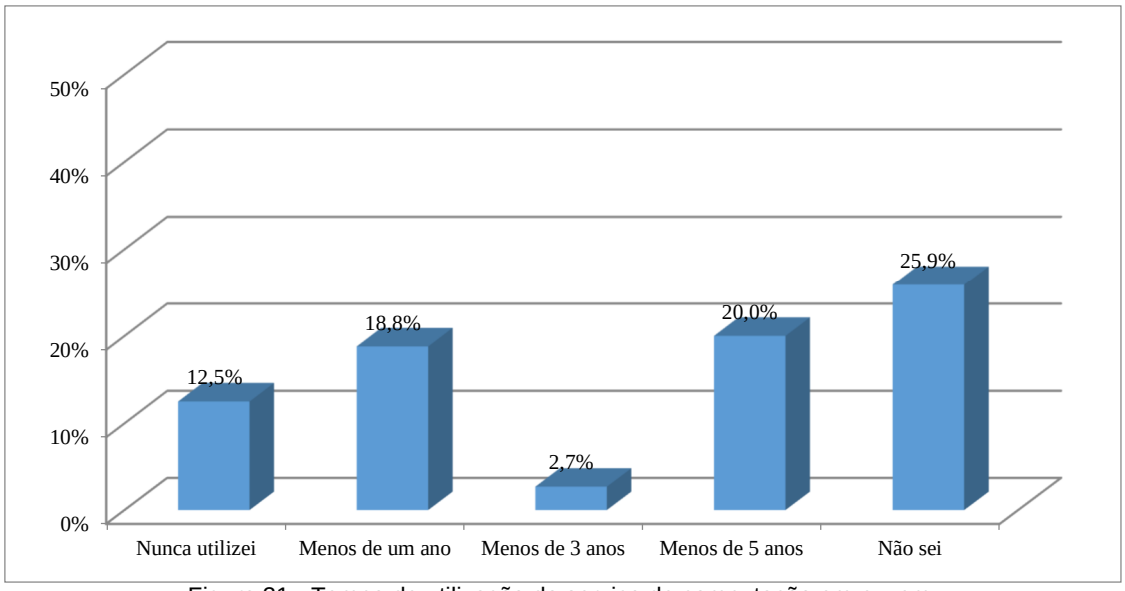

Figura 31 - Tempo de utilização do serviço de computação em nuvem.

Fonte: elaboração própria com base nos outputs estatísticos.

No que concerne a questões relacionadas com a divulgação dos dados pessoais a maioria dos indivíduos refere que concorda que divulgar informação pessoal é uma situação crescente da vida moderna (n=115, 45.1%), que para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal (n=69, 27.1%), que divulgar informação pessoal é um problema (n=104, 40.8%) e que sentem obrigados a divulgar dados privados na internet (n=82, 32.2%). Também se verifica que um número superior concorda totalmente que divulgar informação pessoal em troca de serviços *online* grátis é um problema (n=120, 47.1%).

Quanto ao fator geral de concordância, da divulgação da informação como um problema, podemos observar dos resultados, das tabelas que se seguem, que os valores médios (M=3.62) e medianos (Md=3.60) obtidos apresentam-se elevados, indicando, como tal, uma forte concordância com a divulgação de informação como um problema. Relativamente ao resultados do teste de *kolgomorov sminorv* o valor significativo obtido revela que estamos perante uma distribuição não normal dos resultados (K-S=0.08, p<0.05) (Figura 31)

Questões relacionadas com a divulgação de dados pessoais	Discordo Totalmente		Discordo		Não concordo nem discordo		Concordo		Concordo Totalmente	
	n	%	n	%	n	%	n	%	n	%
Divulgar informação pessoal é uma situação crescente da vida moderna	5	2.0	26	10.2	40	15,7	**115**	**45,1**	69	27,1
Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal	28	11,0	73	28,6	65	25,5	**69**	**27,1**	20	7,8
Para mim, divulgar informação pessoal é um problema	3	1,2	6	2,4	49	19,2	**104**	**40,8**	93	36,5
Para mim, divulgar informação pessoal em troca de serviços online grátis é um problema	1	0,4	9	3,5	33	12,9	92	36,1	**120**	**47,1**
Sinto-me obrigado a divulgar dados privados na internet	45	17,6	58	22,7	38	14,9	**82**	**32,2**	32	12,5

Tabela 29 - Frequência de resultados relativos a concordância com questões relacionados com a divulgação de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Divulgação de informação como problema		Valor	Erro Padrão
Média		3,62	0,04
95% intervalo de confiança para média	Limite mínimo	3,54	
	Limite máximo	3,69	
Mediana		3,60	
Variância		0,36	
Desvio Padrão		0,60	
Mínimo		1,60	
Máximo		5,00	
Amplitude		3,40	
Simetria		-0,01	0,15
Curtose		0,07	0,30
K-S (Sig)		0.08	0.00

Tabela 30 - Medidas de tendência central, dispersão e distribuição dos resultados do fator geral da concordância da divulgação da informação como um problema.

Fonte: elaboração própria com base nos outputs estatísticos.

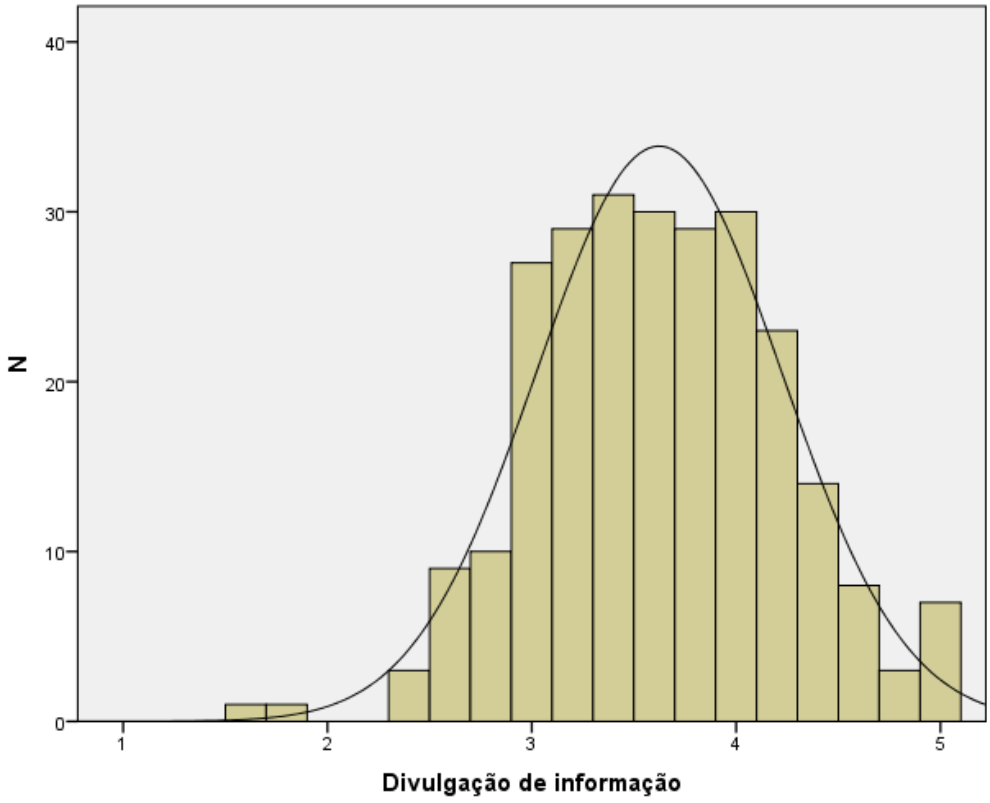

Figura 32 - Histograma da distribuição dos resultados relativos ao fator nível de concordância com a divulgação de dados como um problema.

Fonte: elaboração própria com base nos outputs estatísticos.

6.6 - Estatística inferencial – Relação entre variáveis – Teste de hipóteses

Após descrever os resultados gerais obtidos no questionário passamos a apresentar os resultados que permitem verificar os objetivos e as hipóteses levantadas para o presente estudo e trabalho.

Hipótese 1

H1: Existe uma relação significativa e negativa entre o conhecimento/frequência de utilização do sistema de computação em nuvem e a preocupação com utilização/proteção de dados.

De acordo com os resultados do teste de correlação de *Spearman*, podemos verificar na que se segue, que apenas existe uma correlação negativa significativa entre o nível de conhecimento/frequência de *Wikis* (r_s=-0.16, $p<0.05$) e de programas de produtividade, como o Office (r_s=-0.19, $p<0.05$) e o fator geral de preocupação com a proteção e utilização indevida dos dados pessoais. Também se verifica uma correlação negativa e significativa entre o nível de conhecimento/frequência de utilização das ferramentas do sistema de computação em nuvem e a preocupação geral com a utilizada indevida e proteção de dados pessoais (r_s=-0.14, $p<0.05$),

o que revela que a um maior conhecimento e utilização das varias ferramentas associadas a um sistema de computação em nuvem, corresponde uma menor preocupação com a utilização indevida e proteção dos dados pessoais.

Mas, especificamente, podemos da mesma tabela 31, constatar que o conhecimento/utilização frequente de ferramentas de produtividade se encontram associados uma menor preocupação com o desconhecimento da localização dos dados pessoais (rs=-0.13, p<0.05), problemas de programação ou fracos parâmetros de segurança (rs=-0.14, p<0.05), partilha de recursos de computação em nuvem entre utilizadores (rs=-0.18, p<0.05), e ocorrência de algum acidente que possa levar a perda total dos dados pessoais (rs=-0.15, p<0.05).

	Q1.1	Q1.2	Q1.3	Q1.4	Q1.5	Q1.6	Q1.7	Q1.8	Q1.9	Q1.10	Q1 Geral
Q 6.1.	-0,04 (n.s)	-0,05 (n.s)	-0,11 (n.s)	**-0,16***	-0,12 (n.s)	-0,10 (n.s)	**-0,13***	-0,03 (n.s)	0,03 (n.s)	-0,00 (n.s)	**-0,14***
Q 6.2	0,00 (n.s)	0,04 (n.s)	-0,03 (n.s)	-0,04 (n.s)	0,06 (n.s)	-0,05 (n.s)	**-0,14***	-0,10 (n.s)	0,07 (n.s)	0,07 (n.s)	-0,07 (n.s)
Q 6.3	-0,00 (n.s)	-0,00 (n.s)	-0,10 (n.s)	-0,10 (n.s)	0,00 (n.s)	-0,03 (n.s)	**-0,18***	-0,09 (n.s)	0,02 (n.s)	0,03 (n.s)	-0,11 (n.s)
Q 6.4	0,04 (n.s)	0,10 (n.s)	0,03 (n.s)	-0,11 (n.s)	0,05 (n.s)	0,03 (n.s)	-0,12 (n.s)	-0,11 (n.s)	0,08 (n.s)	0,04 (n.s)	-0,05 (n.s)
Q 6.5	-0,02 (n.s)	0,02 (n.s)	-0,06 (n.s)	-0,07 (n.s)	-0,02 (n.s)	-0,02 (n.s)	**-0,15***	-0,06 (n.s)	-0,01 (n.s)	-0,02 (n.s)	-0,11 (n.s)
Q 6 Geral	-0,03 (n.s)	0,00 (n.s)	-0,07 (n.s)	**-0,13***	-0,04 (n.s)	-0,05 (n.s)	**-0,19****	-0,10 (n.s)	0,05 (n.s)	0,03 (n.s)	**-0,14***

***p<0.05, **p<0.01, n.s. – não significativo**

Tabela 31 - Correlação de *Spearman* entre questões do conhecimento/utilização de ferramentas de computação em nuvem e nível de preocupação com utilização indevida/proteção de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Q1.1: O Navegador de internet (Internet Explorer, Firefox, Chrome, entre outros)

Q1.2: Conversação online (vídeo, voz ou texto, como Skype ou Hangouts, entre outros)

Q1.3: Fóruns ou grupos de discussão

Q1.4. Wikis (sítios de colaboração, como Wikipedia)

Q1.5: Blogues

Q1.6: Armazenamento online (Onedrive, Google Drive, Dropbox, entre outros)

Q1.7: Produtividade (Office 365, Google Docs, Limesurvey, entre outros)

Q1.8: Redes Sociais (Facebook, Youtube, Tumblr, Twitter, Google+, Linkedin, Instagram, Q1.9: Pinterest, Orkut, Snapchat, WhatsApp, entre outros)

Q1.10: Outras aplicações (meteorologia, noticias, entre outras)

Q1 Geral: Grau de confiança/conhecimento na utilização de serviços proporcionados pelo sistema de computação em nuvem

Q6.1: A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.

Q6.2: Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.

Q6.3: Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser utilizados e implicados em ações menos éticas ou mesmo ilegais, por parte de terceiros.

Q6.4: Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.

Q6.5: Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.

Q6 Geral: Grau de preocupação com utilização/proteção de dados

Numa análise mais geral e complementar, ajustamos um modelo de regressão explicativo das questões relacionadas com o nível de conhecimento/utilização de ferramentas do sistema de computação em nuvem, pelo método *stepwise* e, constatamos que, apenas o conhecimento/frequência de utilização de programas de produtividade parece explicar de modo significativo a preocupação com a proteção/utilização indevida do sistema de computação em nuvem ($F=12.95$, $p<0.05$), explicando a mesma apenas em 5% ($r^2=0.05$). De modo mais específico podemos afirmar que a um aumento no conhecimento/frequência de programas de produtividade é previsível uma diminuição de 0.14 pontos ($b=-0.14$, $p=0.00$) no valor médio da preocupação geral com a utilização indevida/proteção de dados pessoais (tabela 32).

Modelo	Coeficiente não estandardizado		Coeficiente estandardizado	R^2	t	p	F	P
	B	Erro padrão	Beta					
(Constant)	4,64	0,16	-		29,99	0,00		
				0.05			12.95	0.00
Q1.7	-0,14	0,04	-0,22		-3,59	0,00		

Tabela 32 - Modelo de Regressão linear explicativo da influência do conhecimento/frequência de utilização de ferramentas de serviços de computação em nuvem no grau de preocupação com a utilização indevida/proteção de dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 2

H2: Existe uma relação significativa e positiva entre a importância das vantagens dos serviços de computação em nuvem com preocupação e a utilização/proteção de dados.

Esta hipótese foi testada através da correlação de *spearman*. A correlação positiva e significativa entre o grau geral de importância das vantagens do sistema de computação em nuvem e a preocupação geral com a proteção/utilização indevida dos dados pessoais, permite confirmar esta mesma hipótese. Também se observa, mais especificamente, que existe uma relação positiva entre a importância da escalabilidade e elasticidade deste sistema e a preocupação geral com a proteção de dados e utilização indevida dos mesmos (rs=0.15, p<0.,05), entre essa mesma preocupação e a importância da necessidade de um menor grau de conhecimento necessário (rs=0.19, p<0.01). A importância dada ao aumento das capacidades disponíveis, também se encontra associada à preocupação com a partilha dos recursos do sistema entre utilizadores (rs=0.15, p<0.05), preocupação com o possível acesso de piratas ou outros utilizadores não autorizados aos dados pessoais existentes no sistema (rs=0.13, p<0.05) e preocupação com a possível perda total de dados devido a algum acidente no sistema (rs=0.16, p<0,05).

Também, ainda, na mesma tabela se salientam as correlações positivas significativas entre a importância da disponibilidade imediata da informação e a preocupação com o desconhecimento da localização física dos dados (rs=0.18, p<0.01), preocupação com problemas de programação e fracos parâmetros de segurança (rs=0.23, p<0,01), preocupação com a partilha de recursos em nuvem com outros utilizadores (rs=0.17, p<0.05) e preocupação com o acesso não autorizado a dados por outros utilizados ou mesmo piratas informáticos (rs=0.16, p<0.05).

O grau de importância em geral das vantagens da utilização de sistema de computação em nuvem também esta correlacionado de modo positivo e significativo com a preocupação com o desconhecimento da localização física dos dados (rs=0.19, p<0.01), com problemas de programação ou fracos parâmetros de segurança (rs=0.19, p<0.01) e a partilha dos recursos entre utilizadores (0.16, p<0.01).

Conforme podemos observar na tabela que se segue.

	Q 2.1	Q 2.2	Q 2.3	Q 2.4	Q 2.5	Q 2.6	Q 2.7	Q 2 Geral
Q 6.1	0,07 (n.s)	**0,15***	0,12 (n.s)	**0,19****	-0,03 (n.s)	-0,04 (n.s)	**0,18****	**0,19****
Q 6.2	0,05 (n.s)	0,10 (n.s)	0,11 (n.s)	0,15*	0,09 (n.s)	0,09 (n.s)	**0,23****	**0,19****
Q 6.3	0,12 (n.s)	0,09 (n.s)	**0,15****	0,09 (n.s)	0,05 (n.s)	0,01 (n.s)	**0,17***	**0,16****

Q 6.4	0,03 (n.s)	0,04 (n.s)	**0,13***	0,07 (n.s)	0,06 (n.s)	0,04 (n.s)	**0,16***	0,10 (n.s)
Q 6.5	0,08 (n.s)	-0,02 (n.s)	**0,16****	0,07 (n.s)	0,03 (n.s)	0,02 (n.s)	0,09 (n.s)	0,10 (n.s)
Q6 Geral	0,11 (n.s)	**0,13***	**0,20****	**0,19****	0,06 (n.s)	0,05 (n.s)	**0,21****	**0,23****

***p<0.05, **p<0.01, n.s. – não significativo**

Tabela 33 - Correlação de *Spearman* entre a importância das vantagens do sistema de computação em nuvem e a preocupação com a utilização indevida e proteção dos dados pessoais.

Fonte: elaboração própria com base nos outputs estatísticos.

Q 2.1 - Menores custos (menor compra de discos rígidos, *cd*, *dvd*, *pen*, entre outros, componentes físicos e programas)
Q 2.2 - Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita)
Q 2.3 - Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos)
Q 2.4 - Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço)
Q 2.5 - Segurança de dados
Q 2.6 - Mobilidade (acesso em qualquer local)
Q 2.7 - Disponibilidade (acesso a qualquer momento)
Q2 Geral – Importância das vantagens do sistema de computação em nuvem

Após a análise de correlação apresentada acima procuramos, também, ajustar um modelo explicativo no sentido de verificar quais as vantagens do sistema de computação em rede e se predizem de modo significativo a preocupação geral com a proteção/utilização indevida dos dados pessoais. Conforme a tabela 34, foi possível verificar que apenas a importância da segurança dos dados prediz, de modo significativo, a preocupação com a utilização indevida/proteção de dados pessoais (F=6.88, p=0.01), explicando a mesma em apenas 3% (r^2=0.03). Especificamente, notamos que a um aumento da importância da segurança dos dados é previsível um aumento de 0.14 pontos (b=0.14, p=0.00) na média da preocupação com a utilização indevida/proteção dos dados pessoais.

Modelo	Coeficiente não estandardizado		Coeficiente estandardizado	R^2	t	p	F	P
	Beta	Erro padrão	B					
(Constant)	3,45	0,25	-		13,64	0,00		
Segurança de dados	0,14	0,06	0,16	0.03	2,62	0,00	6.88	0.01

Tabela 34 - Regressão linear explicativa da importância das vantagens do sistema de computação em rede na preocupação com a utilização indevida/proteção de dados pessoais (Método *Stepwise*).

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 3

H3: A preocupação com as limitações dos serviços de computação em nuvem encontra-se significativa e positivamente relacionada com a preocupação com utilização/proteção de dados.

Relativamente a esta hipótese, podemos verificar que todas a questões relacionadas com a preocupação com as limitações do serviço se encontram positiva e significativamente correlacionadas com as questões relativas a preocupação com a utilização indevida de dados e respetiva proteção. No geral, notamos uma correlação positiva e significativa entre a preocupação com as limitações do sistema e a preocupação geral com a proteção de dados e utilização indevida dos mesmos ($rs=0.55$, $p<0.01$), o que significa que a uma maior preocupação com as limitações do sistema de computação em nuvem, está associada uma maior preocupação com a utilização indevida dos dados e com a proteção dos mesmos.

Este resultado permite, assim, confirmar a hipótese levantada.

	Q 3.1	Q 3.2	Q 3.3	Q 3.4	Q 3.5	Q 3.6	Q 3.7	Q 3.8	Q 3.9	Q 3.10	Q 3.11	Q 3 Geral
Q 6.1.	0,29**	0,27**	0,31**	0,34**	0,27**	0,27**	0,34**	0,36**	0,47**	0,30**	0,26**	0,48**
Q 6.2	0,30**	0,34**	0,35**	0,35**	0,23**	0,21**	0,24**	0,34**	0,38**	0,34**	0,33**	0,44**
Q 6.3	0,32**	0,32**	0,36**	0,40**	0,17*	0,15*	0,21**	0,31**	0,33**	0,30**	0,38**	0,39**
Q 6.4	0,29**	0,29**	0,38**	0,24**	0,15**	0,16**	0,16**	0,20**	0,27**	0,26**	0,40**	0,30**

Q 6.5	0,35**	0,29**	0,31**	0,29**	0,22**	0,24**	0,26**	0,22**	0,34**	0,35**	0,37**	0,38**
Q 6 Geral	0,41**	0,37**	0,42**	0,43**	0,31**	0,29**	0,35**	0,41**	0,49**	0,40**	0,44**	0,55**

***p<0.05, **p<0.01**

Tabela 35 - Correlação de *Spearman* entre as questões relativas á preocupação com as limitações do sistema de computação em nuvem e a preocupação com a utilização indevida de dados e respetiva proteção.

Fonte: elaboração própria com base nos outputs estatísticos.

Q3.1 - Custos não esperados (por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas")
Q3.2 - Integridade de dados (referente à manutenção de precisão e consistência de dados)
Q3.3 - Possibilidade de perda de dados
Q3.4 - Segurança de dados
Q3.5 - Privacidade de dados
Q3.6 - Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente)
Q3.7 - Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade)
Q3.8 - Disponibilidade (se o serviço e/ou dados estão sempre *online* e disponíveis)
Q3.9 - Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem)
Q3.10 - Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação)
Q3.11 - Questões legais e regulamentares

No sentido de ajustar um modelo explicativo da preocupação com a utilização indevida de dados e proteção, em função das questões relacionadas com a preocupação com as limitações do sistema, podemos verificar de acordo com a tabela 36, em que se apresentam os resultados da análise de regressão linear múltipla realizada, que o modelo mais válido e significativo (F=35.11, p=0.00) é apenas definido pela preocupação com custos não esperados (por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas") (t=3.86, p=0.00), pela preocupação com a segurança de dados (t=2.62, p=0.00), pela preocupação com a complexidade de adoção e utilização (t=3.86, p=0.00) e também pela preocupação com questões legais e regulamentares (t=3.46, p=0.00). Estes fatores explicam conjuntamente 30% (r^2=0.30) da variação na preocupação com a utilização indevida dos dados, sendo a complexidade de adoção e utilização que mais contribui para esta variância (r2ch=0.19, 19%).

Mais, especificamente, podemos afirmar que é possível um aumento na preocupação com a utilização indevida e proteção dos dados de 0.15 pontos (b=0.15) devido ao aumento da preocupação com a complexidade de adoção e utilização do sistema, de 0.16 pontos (b=0.16) devido ao aumento da preocupação com questões legais, de 0.,16 pontos devido a preocupação

com a segurança dos dados (b=0.16) e de 0.13 pontos (b=0.13) por aumento da preocupação com os custos não esperados.

Modelo		Coeficiente não estandardizado		Coeficiente estandardizado	R^2	R^2ch	t	p	F	P
		Beta	Erro padrão	Beta						
1	(Constant)	2.99	0,14	-	0.19	0.19	22,16	0,00	75.03	0.00
	Q 3.9	0,30	0,04	0,48			8,66	0,00		
2	(Constant)	2,25	0,19	-	0.25	0.07	11,88	0,00	55.83	0.00
	Q 3.9	0,22	0,04	0,34			5,94	0,00		
	Q 3.11	0,24	0,04	0,31			5,34	0,00		
3	(Constant)	1.60	0,25	-	0.28	0.03	6,40	0,00	44.00	0.00
	Q 3.9	0,18	0,04	0,28			4,65	0,00		
	Q 3.11	0,18	0,05	0,24			4,05	0,00		
	Q 3.4	0,22	0,06	0,23			3,80	0,00		
4	(Constant)	1.53	0,25	-	0.30	0.01	6,11	0,00	35.11	0.00
	Q 3.9	0,15	0,04	0,24			3,86	0,00		
	Q 3.11	0,16	0,05	0,21			3,46	0,00		
	Q 3.4	0,16	0,06	0,17			2,62	0,00		
	Q 3.1	0,13	0,05	0,16			2,42	0,02		

Tabela 36 - Modelo de regressão linear múltipla explicativo da influência das várias questões associadas a preocupação com as limitações do sistema e a preocupação geral com a utilização indevida de dados pessoais e respetiva proteção (Utilizamos o Método *Stepwise*).

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 4

H4: Existe uma relação significativa e negativa entre o nível de confiança com sistema de computação em nuvem e com os fornecedores de serviços e a preocupação com utilização/proteção de dados.

Para testar esta hipótese, recorremos ao teste de correlação de *Spearman*, tendo-se verificado uma correlação negativa e significativa entre o nível de confiança no sistema de computação em nuvem (rs=-0.21, p<0.01) e com os fornecedores de serviços (rs=-0.19, p<0.05) e a preocupação com a utilização indevida e proteção dos dados. Estes resultados permitem confirmar a hipótese número 4. Assim, quanto maior for a confiança no sistema de computação em nuvem e nos fornecedores de serviços, menor é a preocupação com a utilização indevida e proteção dos dados pessoais.

Conforme se observa na seguinte tabela.

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Q 4.1	-0,15*	-0,15*	-0,23**	-0,13*	-0,19**	-0,21**
Q 4.2	-0,16*	-0,21**	-0,14*	-0,10	-0,12	-0,19**

***p<0.05; **p<0.01**

Tabela 37 - Correlação de *Spearman* entre as questões associadas ao nível de confiança com o sistema de computação em nuvem e fornecedores de serviços.

Fonte: elaboração própria com base nos outputs estatísticos.

Q 4.1 – Tecnologia de computação em nuvem

Q 4.2 - Fornecedores de serviços (Dropbox, Facebook, Google, Microsoft, entre outros)

Hipótese 5

No que respeita á relação entre o grau de ameaça de entidades a privacidade e preocupação com utilização/proteção dos dados, levantou-se a hipótese geral:

H5: Um maio grau de ameaça á privacidade por parte de certas entidades está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

Esta hipótese foi testada em função de um conjunto de sub-hipóteses:

H5a: Um maior grau de ameaça á privacidade por parte do governo está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5b: Um maior grau de ameaça á privacidade por parte das empresas privadas está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5c: Um maior grau de ameaça á privacidade por parte de entidades de publicidade está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

H5d: Um maior grau de ameaça á privacidade por parte de piratas informáticos está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.

As presentes hipóteses foram testadas através do teste de correlação de *Spearman* sendo que, de acordo com tabela 38 apenas se verifica correlação significativa entre a preocupação com a utilização indevida/proteção de dados pessoais e o grau de ameaça á privacidade da parte do governo (rs=0.13, p<0.05) e o grau de ameaça dos piratas informáticos (rs=0.27, p<0.01), o que permite apenas confirmar as sub-hipóteses 5a e 5d.

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Q 9.1	0,15**	0,08	-0,00	0,06	0,11	0,13*
Q 9.2	0,24**	0,09	0,03	0,01	0,05	0,12
Q 9.3	0,13**	0,06	0,07	-0,03	0,00	0,05
Q 9.4	0,24**	0,24**	0,16*	0,31**	0,15**	0,27**

***p<0.05; **p<0.01**

Tabela 38 - Correlação de *Spearman* entre as questões associadas à preocupação com a utilização/proteção de dados pessoais e o grau de ameaça de entidades á privacidade.

Fonte: elaboração própria com base nos outputs estatísticos.

Q 9.1. Grau de ameaça do Governo

Q 9.2 Grau de ameaça das empresas privadas

Q 9.3. Grau de ameaça de entidades de publicidade

Q 9.4. Grau de ameaça de piratas informáticos

Também se ajustou um modelo significativo explicativo da influência do grau de ameaça à privacidade por parte das entidades, tendo-se obtido um modelo constituído por apenas uma variável que é o grau de ameaça por parte dos piratas informáticos (F=12.71, p=0.00). Este resultado permite afirmar que uma análise da influência conjunta do grau de ameaça de várias entidades, apenas a ameaça dos piratas informáticos contribui para uma maior preocupação por parte dos participantes com a utilização indevida e proteção dos seus dados, explicando apenas 5% (r2=0.05) dessa relação. Assim pode-se também afirmar que a um aumento do grau de ameaça dos piratas informáticos à privacidade corresponde um aumento de 0.20 pontos (b=0.20) na média do nível de preocupação com a utilização/proteção dos dados pessoais (tabela 39).

	Modelo	Coeficiente não estandardizado		Coeficiente estandardizado	R^2	t	p	F	p
		Beta	Erro padrão	Beta					
1	(Constant)	3,21	0,25	-	0.05	12,64	0,00	12.71	0.00
	Piratas informáticos	0,20	0,06	0.22		3,56	0,00		

Tabela 39 - Modelo de regressão linear múltipla explicativo da influência do grau de ameaça de entidades na privacidade e preocupação com utilização indevida/proteção de dados pessoais (Utilizando o Método *Stepwise*).

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 6

H6: O sentimento que provoca a venda de dados pessoais por fornecedores de serviços está relacionado de forma significativa e positiva com a preocupação com a utilização indevida/proteção de dados.

Para esta hipótese recorreu-se ao teste de correlação de *Spearman*, sendo o resultado obtido na correlação entre a preocupação geral com a utilização indevida/proteção de dados e o sentimento provocado pela venda de dados pessoais por fornecedores estatisticamente significativa (rs=0.18, p<0.01) (Tabela 40).

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Sentimento que provoca venda de dados pessoais	0,15**	0,12 (n.s)	0,15*	0,12*	0,16*	0,18**

n.s – não significativo, *p<0.05, **p<0.01

Tabela 40 - Correlação de *Spearman* entre sentimentos que provoca a venda dos dados pessoais por fornecedores de serviços e preocupação com utilização/proteção de dados.

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 7

H7: Existe relação uma significativa e positiva entre a importância dos direitos de proteção dos dados pessoais e a preocupação com a utilização indevida/proteção de dados.

O resultado significativo do teste de correlação de *Spearman* (rs=0.28, p<0.01) permite comprovar esta hipótese, sendo que a um maior grau de importância dos direitos de proteção de dados pessoais corresponde uma maior preocupação com a utilização indevida/proteção dos dados pessoais (tabela 41).

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Importância dos direitos de proteção de dados pessoais	0,21**	0,16**	0,28**	0,26**	0,18**	0,28**

****p<0.01**

Tabela 41 - Correlação de *Spearman* entre importância dos direitos de proteção de dados e a preocupação com a utilização indevida/proteção.

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 8

H8: Um maior controlo sobre o sistema de computação em nuvem implica uma menor preocupação com a utilização indevida/proteção de dados pessoais.

O resultado não significativo obtido no teste de correlação de *Spearman* (rs=-0.07, p>0.05) não permitiu confirmar a hipótese número 8.

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Controlo sobre o sistema de computação em nuvem	-0,04 (n.s)	-0,16**	-0,14**	-0,06 (n.s)	0,01 (n.s)	-0.07 (n.s)

n.s – não significativo, **p<0.01

Tabela 42 - Correlação de *Spearman* entre o controlo sobre o Sistema de Computação em Nuvem e a preocupação com utilização indevida/proteção dos dados.

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 9

H9: O tempo de utilização dos serviços de computação em nuvem está relacionado de modo significativo e negativo com a preocupação com a utilização indevida/proteção dos dados pessoais.

Também não foi possível confirmar a hipótese número 9, dado o resultado não significativo obtido no teste de correlação de *Spearman* (rs=-0.09, p>0.05).

	Q 6.1	Q 6.2	Q 6.3	Q 6.4	Q 6.5	Q 6 Geral
Q 18	-0.05 (n.s)	-0.03 (n.s)	-0.07 (n.s)	-0.08 (n.s)	-0.09 (n.s)	-0.09 (n.s)

n.s – não significativo

Tabela 43 - Correlação de *Spearman* entre o tempo de utilização de serviços de computação em nuvem e preocupação com utilização indevida/proteção dos dados.

Fonte: elaboração própria com base nos outputs estatísticos.

Hipótese 10

H10: O nível de concordância da divulgação de informação como um problema esta significativa e positivamente correlacionado com a preocupação com a utilização indevida/proteção dos dados pessoais.

Por ultimo no que refere á hipótese número 10, o resultado significativo do teste de correlação de *Spearman* (rs=0.15, p<0.05) permitiu a sua confirmação, sendo que neste caso a um maior nível de concordância na divulgação da informação, como um problema, está relacionado um maior nível de preocupação com a utilização indevida de dados pessoais (tabela 44).

	Q 19.1	Q 19.2	Q 19.3	Q 19.4	Q 19.5	Q 19 Geral
Q 6.1	-0,00	0,09	0,22**	0,18**	0,18**	0,22**
Q 6.2	0,06	0,01	0,24**	0,18**	0,05	0,16*
Q 6.3	-0,03	-0,07	0,12*	0,16*	0,08	0,07
Q 6.4	-0,05	-0,12	0,08	0,10	-0,01	-0,02
Q 6.5	-0,02	-0,03	0,06	0,11	0,00	0,03
Q 6 Geral	0,00	-0,01	0,20**	0,20**	0,10	0,15*

n.s – não significativo, *p<0.05, **p<0.01

Tabela 44 - Correlação de *Spearman* entre nível de concordância da divulgação de dados pessoais e nível de preocupação com a utilização indevida/proteção.

Fonte: elaboração própria com base nos outputs estatísticos.

Q 19.1 - Divulgar informação pessoal é uma situação crescente da vida moderna

Q 19.2 - Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal

Q 19.3 - Para mim, divulgar informação pessoal é um problema

Q 19.4 - Para mim, divulgar informação pessoal em troca de serviços *online* grátis é um problema

Q 19.5 - Sinto-me obrigado a divulgar dados privados na internet

Q 19 Geral – Divulgação de informação como um problema

6.7 - Modelo fatorial explicativo da preocupação dos dados pessoais

Por fim, para além do teste das hipóteses levantadas para o presente estudo, também se estabeleceu como objetivo ajustar um modelo explicativo da preocupação com a utilização indevida/proteção dos dados pessoais. Para o efeito, foram utilizadas diversas variáveis analisadas como o grau de conhecimento/frequência de utilização da computação em nuvem, Importância das vantagens do sistema de computação em nuvem, Preocupação com as limitações do sistema, Nível de confiança com a tecnologia de computação em nuvem, Nível de confiança com os fornecedores de serviços (*Dropbox*, *Facebook*, Google, Microsoft, entre outros), Grau de ameaça à privacidade por parte do governo, Grau de ameaça à privacidade por parte de empresas privadas, Grau de ameaça à privacidade por parte das entidades de publicidade, Grau de ameaça à privacidade por de piratas informáticos, Sentimento lhe provoca a venda de dados pessoais pelos fornecedores de serviços, Grau de importância de ter os mesmos direitos e proteção dos dados pessoais, independentemente do país onde esses dados são processados, Nível de controlo sobre a informação e dados que divulgou e utiliza nos serviços baseados nesta tecnologia, classificação do conhecimento sobre computação em

nuvem, divulgação de informação como problema e tempo que utiliza serviços de computação em nuvem. Foram, também, utilizadas como variáveis de controlo o sexo e a idade.

Para o efeito recorreu-se a uma análise de regressão linear múltipla em que foram introduzidas todas as variáveis acima referidas. O resultado obtido permitiu a obtenção de um modelo significativo (F=10.74, p=0.00) que explica 44% (r^2=0.44) da variação da preocupação com a utilização indevida/proteção dos dados. Porém apenas a preocupação com as limitações do sistema (t=8.65, p=0,00), o nível de confiança com os fornecedores de serviços (t=-3.31, p=0.00) e o grau de importância de ter os mesmos direitos de proteção de dados pessoais (t=3.02, p=0.00).

Tais resultados podem ser observados na tabela que se segue.

Modelo	Coeficientes não estandardizados		Coeficientes estandardizados	t	p	R^2	F	p
	Beta	Erro Padrão	Beta					
(Constant)	0,66	0,64	-	1,03	0,30			
Sexo	0,01	0,08	0,01	0,19	0,84			
Idade	0,03	0,02	0,07	1,37	0,17			
Grau de conhecimento/utilização do sistema de computação em nuvem	-0,03	0,07	-0,02	-0,39	0,69			
Importância das vantagens do sistema de computação em nuvem	0,10	0,06	0,08	1,44	0,15	0.44	10.74	0.00
Preocupação com as limitações do sistema	**0,51**	**0,05**	**0,49**	**8,65**	**0,00**			
Nível de confiança com a tecnologia de computação em nuvem	-0,05	0,05	-0,07	-1,02	0,30			
Nível de confiança com os fornecedores de serviços (Dropbox, Facebook, Google, Microsoft, entre outros)	**-0,17**	**0,05**	**-0,21**	**-3,31**	**0,00**			

Grau de ameaça à privacidade por parte do governo	0,01	0,03	0,01	0,26	0,79
Grau de ameaça à privacidade por parte de empresas privadas.	0,00	0,04	0,00	0,02	0,97
Grau de ameaça à privacidade por parte das entidades de publicidade	-0,05	0,04	-0,08	-1,41	0,15
Grau de ameaça à privacidade por de piratas informáticos	0,09	0,05	0,10	1,92	0,06
Sentimento lhe provoca a venda de dados pessoais pelos fornecedores de serviços	0,00	0,03	0,00	0,04	0,96
Grau de importância de ter os mesmos direitos e proteção dos dados pessoais, independentemente do país onde esses dados são processados	**0,28**	**0,09**	**0,16**	**3,02**	**0,00**
Nível de controlo sobre a informação e dados que divulgou e utiliza nos serviços baseados nesta tecnologia.	-0,00	0,03	-0,01	-0,19	0,84
Classificação do conhecimento sobre computação em nuvem	-0,02	0,05	-0,03	-0,52	0,60
Tempo que utiliza serviços de computação em nuvem	0,03	0,04	0,04	0,79	0,43
Divulgação de informação como problema	0,00	0,06	0,00	0,02	0,97

Tabela 45 - Modelo de Regressão linear múltipla explicativo da preocupação com a utilização indevida/proteção de dados pessoais (Utilizando Método *Enter*).

Fonte: elaboração própria com base nos outputs estatísticos.

Assim, no sentido de proceder ao ajustamento de um modelo significativo que permita explicar a preocupação com a utilização indevida dos dados pessoais e respetiva proteção apenas em função de fatores estatisticamente significativos, recorreu-se a análise de regressão linear com o método *stepwise* de entrada e saída de variáveis, tendo-se obtido um modelo estatisticamente significativo (F=58.34, p=0,00) cujo o conjunto de variáveis explicam 41% (r^2=0.41) da

preocupação que os participantes apresentam com a utilização indevida/proteção dos seus dados pessoais (tabela 46).

Podemos também dizer que a preocupação com as limitações do sistema de computação em nuvem é o fator que mais contribui para a preocupação com a utilização indevida dos dados (32%, $r^2ch=0.32$), seguindo-se o nível de confiança (6%, $r^2ch=0.06$) e por fim a importância de ter os mesmos direitos de proteção de dados pessoais independentemente do país (4%, $r^2ch=0.04$) (tabela 46 e figura 32).

	Modelo	Coeficientes não estandardizados		Coeficientes estandardizados	t	p	R^2	R^2ch	F	p
		Beta	Erro Padrão							
1	(Constant)	1,71	0,22	-	7,68	0,00	0.32	0.32	118.73	0.00
	Preocupação com limitações do sistema	0,59	0,05	0,57	10,90	0,00				
2	(Constant)	2,27	0,25	-	9,28	0,00	0.37	0.06	75.43	0.00
	Preocupação com limitações do sistema	0,60	0,05	0,58	11,60	0,00				
	Nível de confiança com fornecedores de serviços (Dropbox, Facebook, Google, Microsoft, entre outros)	-0,18	0,04	-0,24	-4,71	0,00				
3	**(Constant)**	**0,86**	**0,43**	**-**	**2,01**	**0,05**	**0.41**	**0.04**	**58.34**	**0.00**
	Preocupação com limitações do sistema	**0,55**	**0,05**	**0,53**	**10,46**	**0,00**				
	Nível de confiança com fornecedores de serviços (Dropbox, Facebook, Google, Microsoft, entre outros)	**-0,19**	**0,04**	**-0,25**	**-5,10**	**0,00**				

Importância de ter os mesmos direitos e proteção dos dados pessoais, independentemente do país onde esses dados são processados	**0,34**	**0,09**	**0,20**	**3,94**	**0,00**

Tabela 46 - Modelo de Regressão linear múltipla explicativo da preocupação com a utilização indevida/proteção de dados pessoais (Utilizando o Método *Stepwise*).

Fonte: elaboração própria com base nos outputs estatísticos.

Em baixo apresentamos o modelo final em termos de esquema para melhor compreensão dos resultados

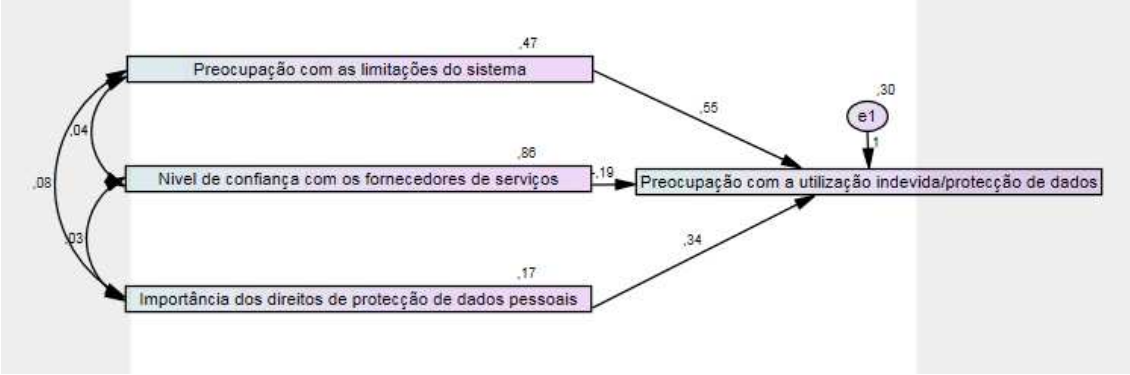

Figura 33 - Modelo Explicativo dos fatores que influenciam a preocupação com a utilização indevida/proteção de dados.

Fonte: elaboração própria com base nos outputs estatísticos.

6.8 - Conclusão e discussão de resultados

Apresentado o trabalho empírico realizado e os resultados obtidos, passa-se, agora, para uma discussão destes, cruzando a sua discussão, sempre que possível, com a revisão de literatura e trabalhos semelhantes. Convém lembrar que este trabalho não é um estudo replicado, total nem parcial, de um outro estudo e, ao mesmo tempo, não foram encontrados estudos semelhantes ao realizado. Como tal, o cruzamento com literatura e estudos será feita com base nos conceitos abordados ou estudos relativamente homólogos, isto é, inquéritos da mesma natureza, levados a cabo a nível empresarial, portanto, com uma unidade de análise diferente.

Antes de prosseguir, relembra-se que desta amostra não probabilística, foram obtidas 255 respostas válidas, sobre as quais, foram realizadas as análises estatísticas e, consequente, discussão de resultados.

Começando pelo perfil sociodemográfico, a caracterização da amostra, embora a distribuição de dados obtidos possa vir a ajudar a compreender ou enquadrar alguns resultados obtidos, por si só, não há nada de especial a apontar. Quanto ao sexo, a sua distribuição encontra-se equilibrada com 56,5% inquiridos do sexo feminino e 43,5% do sexo masculino, algo que vai de encontro ao esperado, dado que a maioria dos inquiridos são estudantes (estudante 39.2%, trabalhador estudante 12,2%, total de 51,4% estudantes). A Direção Geral do Ensino Superior (DGES, 2015) registou 58,5% e 59,3% de colocados do sexo feminino, para a primeira fase de colocação de ensino superior público de 2013 e 2014, respetivamente; já a PORDATA (2015), utilizando como fontes a Direção Geral de Estatísticas da Educação e Ciência (DGEEC), aponta para um total de colocados do sexo feminino de 53,2% e 53,5% para os anos de 2013 e 2014, respetivamente. Da mesma forma, sendo a maioria dos inquiridos estudantes, a distribuição de idades também faz sentido, tendo a maioria 18 a 23 anos (33,7%), tal como o nível de habilitações académicas, distribuídas, maioritariamente, por secundário (29,4%) e licenciatura (39,2%).

Conforme referido na apresentação de resultados, de modo a obter-se uma escala explicativa do conjunto de itens relativos a diversas questões do questionário, realizou-se uma análise fatorial exploratória em que se procurou extrair um único fator, de modo a obter uma estrutura unidimensional, sendo que, para tal, recorreu-se a testes de *Kaiser-Meyer-Olkin* (KMO) e teste de *Barllet.*

A análise realizada às questões 1, 2 e 3, relativas ao "Grau de confiança e conhecimento sobre utilização dos serviços de computação em nuvem" (KMO=0.78, Bartlett=710.24, p=0.00), "Importância das vantagens dos serviços de computação em nuvem" (KMO=0.77, Bartlett=928.35, p=0.00) e "Preocupação com as limitações do sistema de computação em nuvem" (KMO= 0.87, Bartlett=1482.54, p=0.00), respetivamente, e com carga fatorial superior a 0,4, demonstram resultados adequados e significativos, especialmente na questão 3, possibilitando uma análise fatorial com os itens em causa.

Relativamente à questão 6, "preocupação com utilização indevida/proteção de dados" (KMO= 0.77, Bartlett=488.48, p=0.00), mais uma vez, obteve-se valores adequados, com todos os itens a apresentar uma carga fatorial superior a 0,4, tendo-se obtido uma estrutura definida por apenas um fator responsável por 59,46% da variância explicada.

O mesmo não pode ser dito da questão 19 do questionário. O baixo valor de KMO (0,55) e cargas fatoriais, de alguns itens, inferiores a 0,4, invalidam a estrutura inicial. No entanto, no sentido de verificar quais os itens que explicam um fator comum, procedemos à eliminação de referidos itens, obtendo-se, novamente, valores desadequados (KMO=0.52, Bartlett=125.84, p=0.00) e um

item com carga fatorial inferior a 0,4. Numa última tentativa foi retirado o item “Sinto-me obrigado a divulgar dados privados na internet” e procedeu-se a nova análise fatorial, com a variável reduzida, agora, a 2 itens. Feita esta alteração, obtiveram-se resultados extremamente satisfatórios, com um fator explicativo de 87,95% da variância e cargas fatoriais de 0,81 para os dois itens restantes. Realizada, ainda, uma análise de consistência interna, obteve-se ainda um satisfatório valor de *alpha* de *Cronbach* (0,77). Tudo isto levou-nos a dar uma nova denominação ao fator em causa, de acordo com os seus itens, para “Opinião sobre a divulgação da informação como um problema”.

De seguida, fizemos para as questões 1, 2, 3, 6 e a “nova” 19, uma análise de fiabilidade e consistência interna, através da realização do teste de *alpha* de *Cronbach,* sendo que todas as questões mencionadas, obtiveram valores adequados de *alpha* de *Cronbach* e correlação entre itens e fator total. Isto permitiu-nos avançar para a análise descritiva dos seus resultados gerais.

Passando, então, para a análise descritiva dos resultados mais relevantes e começando pela questão 1, que se refere aos itens associados ao grau de conhecimento e confiança dos participantes com os vários serviços de computação em nuvem, notamos um elevado grau de conhecimento e utilização dos serviços, onde se obtiveram resultados semelhantes aos de Cruz (2013). Comparado com referido trabalho, obtém-se valores semelhantes, mas, com algumas alterações que poderão ser sintomáticas da evolução de conhecimento e utilização destas ferramentas. Os itens redes sociais, *chat online*, *wikis*, blogues, fóruns e serviços de armazenamento são o maior espelho disso mesmo. Comparando os resultados médios obtidos (com os de referido autor), temos redes sociais com uma utilização média ligeiramente superior, com M=4,50 (contra M=4,14), *chat online* com uma ligeira subida M=4,13 (M=4,03), *wikis* igualmente superior M=3,70 (M=2,61), blogues e fóruns com uma utilização inferior M=3,30 (M=3,49) e M=3,17 (M=3,48), respetivamente e serviços de armazenamento com uma subida de utilização M=3,83 (M=3,30/3,56). Estes resultados compreendem-se, pois são serviços que, embora, já estivessem extremamente disseminados, continuam a ver a sua adoção e utilização a aumentar, com uma exceção e um dado a notar. A exceção são os blogues e fóruns, que, de facto, a perceção é mesmo que caíram um pouco em desuso, visto que a comunicação, agora, é feita de forma muito mais direta, via redes sociais e *chat online* (mensagens instantâneas – IM), podendo ser apontado como o efeito mais notório da transição da *web 1.0* para a *web 2.0*, o que inclui a crescente influência da *cloud*. Um dado a notar é a utilização dos serviços de armazenamento de dados, os quais, não só acabam por ser dos serviços mais recentes, como aquele que potencialmente é mais “afetado” por receios de proteção de dados. Aliás, relativamente a serviços mais recentes, também neste sentido os resultados fazem sentido, sendo os mais antigos os mais conhecidos e utilizados, enquanto os mais recentes e diferentes, como armazenamento e produtividade, são os menos utilizados. De resto, analisando os valores descritivos obtidos, com M=3,99 e Md=4,10, o que transparece é uma grande utilização deste tipo de serviços.

Em relação à questão 2, a importância das vantagens proporcionadas pelos serviços de computação em nuvem, apesar de serem estudos com público-alvo empresas e questionários diferentes, os resultados obtidos são, até certo, comparáveis com os trabalhos de Kajiyama (2012), Cruz (2013) e Kwofie (2013). Os resultados de todos os trabalhos mencionados apontam "menores custos" como a principal vantagem, algo confirmado pelos nossos resultados, em que 40,4% dos inquiridos considera "Muito Importante", com M=4,12. Embora existam mais um ou outro resultado semelhante, o mais interessante é olhar para as diferenças. O que é mais notório é que, embora, esses estudos tenham questões, escalas e alguns resultados semelhantes, os resultados são extremamente polarizados, enquanto que neste trabalho, o fator geral tem M=4,21 e Md= 4,28, já nos outros trabalhos, por exemplo, o de Kwofie (2013), temos resultados de 54% para importância de menores custos, 10% assinala melhor segurança e existem mesmo valores de 0% como é o caso do item colaboração. Isto pode dever-se à forma/tipo de resposta (e.g. escolha múltipla, com o máximo de três escolhas, no caso de Kwofie), ou, meramente ao facto de as empresas terem necessidades mais focadas. Neste trabalho, acima de menores custos, "Segurança", "Disponibilidade" e "Mobilidade", são apontados como vantagens muito importantes por 69,8%, 72,2% e 73,3%, respetivamente. À exceção de "Menor grau de conhecimento necessário", onde a maior dos inquiridos aponta apenas como "importante" (32,9%) e a "Escalabilidade" e "Elasticidade" com 37,3% em bastante importante, todos os outros itens vêm a maioria dos inquiridos dar a importância máxima. Esta diferença pode ser explicada, segundo nossa opinião, por dois motivos. Com o decurso do tempo houve uma maturação da tecnologia e do conhecimento sobre esta, o que aumentou logo as vantagens que foram apontadas pela revisão de literatura e inseridas no questionário são melhor percecionadas agora, do que há uns anos atrás, ou, então, esta diferença deve-se ao facto dos estudos mencionados serem sobre empresas, enquanto, este foi feito junto de consumidores finais. É muito provável que as empresas inquiridas, pelo menos grande parte, tenham já soluções próprias, internas, logo, a passagem para uma solução *cloud,* externa, obviamente, terá ponderações mais focadas, tendo em conta as soluções que já têm, comparar com um serviço *cloud*. Esta ideia parece ser suportada se, por exemplo, compararmos os resultados de Kwofie (2013), com Duranti (2013). Algumas semelhanças, mas, alguns resultados completamente diferentes para mesmos itens. Um segundo possível motivo, é que, é muito menos provável que o consumidor final tenha algum tipo de solução própria e, mesmo, que a tenha, será, em comparação com as de uma empresa, consideravelmente inferior, logo, a ponderação quando feita a comparação para uma solução *cloud*, não será tão focada, sendo provável que todos os aspetos sejam vistos como vantagens e, dada a diferença referida, o grau de importância atribuído será extremamente elevado, em quase todas os itens.

Passando para a questão 3, a preocupação com limitações da tecnologia, retirou-se ideias semelhantes às supramencionadas, através de comparação com os mesmos trabalhos de Kajiyama (2012), Cruz (2013), Kwofie (2013) e Duranti (2013), observando-se, novamente, uma polarização dos resultados.

Neste trabalho, ao contrário dos supramencionados, não existe essa polarização, sendo que, para o fator geral temos M=4,08 e Md=4,20. A nossa opinião e justificação é semelhante à apresentada na questão anterior. Concretamente, é de mencionar que os inquiridos atribuem o nível máximo de preocupação à "possibilidade de perda de dados" (68,2%), "segurança de dados" (76,5%) e "privacidade de dados" (80,4%). São número que não deixam margem para duvidas quanto às preocupações dos consumidores, mas, constata-se um facto interessante. Na questão anterior 69,8% dos inquiridos apontou a "segurança de dados" como uma vantagem muito importante e agora, em conjunto com os outros dois resultados mencionados, 76,5% referem que questões de "segurança de dados" são muito preocupantes. Isto pode ser explicado por uma ideia muito simples e que começa a ser mais ou menos generalizada. Em primeiro lugar, a verdade é que os colossos como a Microsoft, a Google ou Amazon investem milhares de milhões nas suas infraestruturas *cloud* e segurança das mesmas e graças a economias de escala e pura concorrência, seja uma empresa ou, especialmente, um consumidor individual, para além de ficar muito mais barato aderir a uma solução *cloud* dessas empresas, o nível de segurança que elas proporcionam é impensável para uma outra qualquer solução própria que um consumidor possa ter. Logo, o consumidor deverá ver esses dois lados. Por um lado, sim, é uma enorme vantagem de segurança, mas, ao mesmo tempo, a segurança e a privacidade não deixam de ser algo extremamente preocupante.

Passando para questões de mais rápida análise e começando pela "confiança" para com a tecnologia e fornecedores de serviço, os inquiridos revelam um nível de confiança semelhante entre os dois. Relativamente à tecnologia dizem estar confiantes (40%), bastante confiantes (35,7%) e muito confiantes (13,3%), enquanto relativamente aos fornecedores estão confiantes (42,7%), bastante confiantes (32,2%) e muito confiantes (13,3%). Tendo em conta as definições abordadas de privacidade, segurança e confiança, a justificação pela elevada semelhança pode partir do facto de estas duas noções serem, na mente das pessoas, um único constructo e não dois. Por exemplo, um consumidor que utiliza e gosta do serviço de Facebook, gosta da imagem que tem da empresa, logo, instintivamente, liga os conceitos e não consegue separar a imagem que tem da empresa e os seus serviços, da tecnologia em si.

Em relação à questão 5, 46,7% dos inquiridos concorda que questões de segurança são um problema que impedem a adoção deste tipo de serviços e 49,4% concorda com a afirmação de que se sentem mais confiantes com a utilização de soluções próprias, algo que parece ir contra a opinião postulada em que o consumidor, embora, não perca o receio, sente que a *cloud* oferece melhor proteção de segurança e privacidade de dados, contudo, nesta mesma questão, 39,6% diz concordar com a afirmação de que sente que a "tecnologia de computação em nuvem está pronta para salvaguardar os meus dados e informação mais importantes" e 44,7% concorda com "sinto que a computação em nuvem será mais segura no futuro". Ao mesmo tempo, 30,2% concorda totalmente que a "tecnologia será mais segura no futuro" e 32,5% não concorda nem discorda sobre se a tecnologia está pronta para salvaguardar a sua informação mais importante. Isto parece indicar alguma confusão e indecisão relativamente a estas ideias. Assim, havendo

de facto preocupação com a segurança e a privacidade, o que foi postulado, sobre o consumidor ver segurança como uma das maiores vantagens e, ao mesmo tempo, preocupação da *cloud*¸ pode ser válido. No entanto, é uma questão que carece de maior e mais profunda investigação.

Passando para a questão 6, a maioria dos inquiridos demonstra muita preocupação relativamente ao desconhecimento da localização física dos seus dados (38,8%) e problemas de programação ou fracos parâmetros de segurança, entre outros, que podem colocar em risco a confidencialidade, integridade e disponibilidade dos dados (43,9%). Já, relativamente ao facto dos recursos em nuvem utilizados para armazenar dados serem partilhados entre utilizadores, o que pode significar uma utilização ou implicação dos seus dados em ações ilícitas, por parte de terceiros, 42,0% dos inquiridos demonstram "absoluta preocupação". Quanto à possibilidade de utilizadores não autorizados, como piratas, poderem aceder aos dispositivos pessoais através de falhas de configuração do sistema (63,9%) e, também, de algo imprevisto, como um desastre natural num centro de dados fornecedor de serviços conduzir à perda total e definitiva dos dados, a maioria (46,7%) assinala, novamente, "absoluta preocupação". Á parte de ficar, novamente, patente a crónica preocupação com utilização indevida e proteção dos seus dados, o que podemos retirar daqui é que a elevada preocupação, relativamente, à localização física dos dados pode ser algo sintomático na resposta à hipótese 7. Também pode ser sintomático o receio de atividade maliciosa por parte de terceiros, visto que os restantes itens se prendem com o aproveitamento de fragilidades do sistema e não falhas do sistema por si só, algo que se pode refletir nos resultados da hipótese 5. Sendo que, no entanto, a média de preocupação mais elevada encontra-se no item de imprevistos, como um desastre natural destruir um centro de dados (M=4,47).

Quando questionados sobre quem pensam ser responsável pela segurança e a privacidade dos seus dados, questões 7 e 11, respetivamente, os resultados obtidos são curiosos, semelhantes e, mais uma vez, podemos falar do facto de segurança ser visto como um benefício muito importante e ao mesmo tempo ser atribuído o maior nível de preocupação. Respetivamente, de responsáveis pela segurança para a responsáveis pela privacidade, as respostas em "fornecedor de serviços" passam de 50,2% para 38% e a opção "eu próprio" de 29,8% para 32,2%. Serem semelhantes, é esperado. Como abordado na literatura, embora sejam duas coisas diferentes, privacidade advém de segurança. Se há quebra de privacidade é porque falhou segurança. No entanto, o interessante é que as duas principais respostas são "Fornecedores de serviço" e "Eu próprio". Isto pode ajudar a explicar a questão de segurança ser tida como uma "muito importante" vantagem e "muito preocupante" limitação, visto que, há duas claras visões sobre quem detém o ónus da segurança e privacidade.

Na questão 9 sobre a classificação de entidades por grau de ameaça, a maioria dos inquiridos classifica com "muita ameaça" o governo (33,3%), as empresas privadas (38,4%) e entidades de publicidade (44,7%). Já 67,8% considera piratas informáticos como uma "ameaça total". São resultados esperados, tendo em conta os dias que correm, com constantes notícias sobre

práticas das empresas para com os nossos dados e, especialmente, a forma como os governos se parecem movimentar para ter acesso indevido aos nossos dados. Aliás, a ameaça por parte de governo, com M=3,59, liga bem com os resultados obtidos na questão 7, onde apenas 0,8% diz ser o governo o responsável por assegurar a segurança dos nossos dados.

As respostas à questão 10 são, também, interessantes, visto que 30,2% dizem ficar escandalizado com as práticas de vendas dos dados, mas, a perceção de ameaça por parte de empresas privadas (questão 9) é de "muita ameaça" (38,4%); na questão 7, os inquiridos apontam ao "fornecedor de serviços" como o responsável pela "segurança de dados" (50,2%) e na questão 4, os inquiridos mostram-se confiantes (42,7%), bastante confiantes (32,2%) e muito confiantes (13,3%) para com os fornecedores de serviços (e.g. Facebook – dado como exemplo na questão 10). Assim, temos, novamente, esta sensação de confusão, de falta de discernimento do consumidor em conseguir separar a tecnologia, dos factos e da imagem que têm sobre a empresa, da qual utilizam serviços.

Relativamente às questões 12 e 13 obtemos resultados semelhantes ao estudo do Eurobarometer (2011), sem qualquer espanto. A opinião dos inquiridos, aponta para que deveriam deter total controlo sobre os seus dados, apesar de não ser necessariamente o caso. Relativamente à necessidade da sua expressa autorização para divulgação de dados, 72,5% dos inquiridos diz que deveria ser necessária em todos os casos. Quanto à capacidade/circunstâncias em que os dados deveriam ser apagados, 91,4% aponta para a opção "Sempre que eu decida apagar".

Passando para a questão 14, relativa à importância dos "direitos de proteção de dados pessoais, independentemente do país onde estes são processados", os resultados são claros, com 87,8% dos inquiridos a responder que é algo "muito importante", algo que nos pode, desde já, prever um resultado para a hipótese 7.

Relacionada com as questões 12 e 13 temos a questão 15, onde se pergunta, diretamente, o "controlo percebido", por parte do consumidor para com os seus dados na *cloud*. Os resultados estão bastante dispersos, dando mais uma vez a sensação de falta de consciência/perceção ou conhecimento. Por um lado, 8,6% diz não ter nenhum controlo, enquanto, 5,1% diz ter controlo total. Já, baixo controlo é a resposta dada pela maioria (38,4%), enquanto controlo elevado é apontado por 26,3%. Por fim, 21,6% simplesmente responde que não sabe. De novo, pode ser a tal confusão, já várias vezes mencionada, ou, também, pode ter a ver com os serviços utilizados pelos inquiridos, visto que uns podem de facto fornecer mais controlo do que outros, enquanto que, ainda outros, em especial as redes sociais, são um completo e propositado imbróglio de desinformação.

No sentido do que acabou de ser supramencionado, temos a questão 16, a qual, aborda se o utilizador se sente informado quando tem intenções de utilizar um serviço suportado pela *cloud*. Com resultados algo semelhantes, se bem que mais dispersos, ao estudo da Eurobarometer

(2011). Sendo que neste estudo a opção “não sei” e “não aplicável” recolhem mais respostas. No entanto, a maioria vota, igualmente, no “não” (36,9%).

Em contraponto, a questão 17, questiona o nível de conhecimento sobre serviços de computação em nuvem e não deixa de ser algo a assinalar o facto de a maioria se considerar “informado” (47,80%), demonstrando, aparente e novamente, um desfasamento de perceções e de conhecimento sobre a tecnologia, factos, serviços e fornecedores de serviços.

Passando para a questão 18, sobre o tempo de utilização de serviços de computação em nuvem, a maioria respondeu “não sei” (25,9%) o que pode revelar uma falta de conhecimento sobre a matéria, seguindo-se a opção “menos de 5 anos” com 20%.

Por fim, a questão 19, relacionada com a divulgação dos dados pessoais. Com valores de M=3,62 e Md=3,60, a ideia geral é que de facto há um elevado nível de concordância no que toca há necessidade de divulgar informação, bem como, o facto de isso ser, pessoalmente, um problema.

Passando agora para os resultados da estatística inferencial, apresentam-se os resultados das hipóteses, embora, como já referido, não tenham sido encontrados trabalhos para estabelecer uma comparação direta e homologa de resultados.

A discussão, sobre os resultados da análise de hipóteses, será realizada, não por ordem numérica das hipóteses, mas, sim, por ordem de ideias, agrupados pelas variáveis de “confiança”, “privacidade e segurança”, “vantagens e limitações de sistema” e “conhecimento/utilização”, conforme o modelo apresentado na figura 8 (p. 63) no capitulo de metodologias.

Começando pelo conhecimento e frequência de utilização de serviços de computação em nuvem, temos a hipótese 1. Inicialmente, de acordo com teste de correlação de *Spearman*, verificou-se uma correlação negativa significativa para o conhecimento e frequência de utilização de *Wikis e* programas de produtividade para com o fator geral de utilização indevida de dados pessoais. Alias, verifica-se igual relação entre conhecimento e a frequência de utilização de ferramentas *cloud* com a utilização indevida de dados, o que significa que, quanto maior o conhecimento e utilização, menor será o nível de preocupação com a proteção de dados, mais concretamente, menor será o nível de preocupação com o desconhecimento da localização dos dados pessoais ($rs=-0.13$, $p<0.05$), problemas de programação ou fracos parâmetros de segurança ($rs=-0.14$, $p<0.05$), partilha de recursos de computação em nuvem entre utilizadores ($rs=-0.18$, $p<0.05$), e ocorrência de algum acidente que possa levar a perda total dos dados pessoais ($rs=-0.15$, $p<0.05$). Ainda assim, através de uma análise complementar, observamos que apenas o item de programas de produtividade parece explicar de modo significativo a preocupação com a utilização indevida e proteção de dados.

Procura-se, com a hipótese 9, extrapolar esta noção de “frequência de utilização” para o tempo efetivo de utilização de serviços *cloud*. No entanto, não se conseguiu corroborar esta hipótese. Não se conseguiu provar que, uma maior utilização da tecnologia, em anos, esteja relacionada com a preocupação de proteção de dados.

Complementarmente, a esta área de conhecimento e utilização da tecnologia, a hipótese 10 foi comprovada. Como mencionado, anteriormente, os consumidores concordam que a divulgação de dados é algo, cada vez mais, normal e necessária e, ao mesmo, tempo concordam, também, maioritariamente, que é algo que os preocupa. O que se conseguiu comprar é que quanto maior for este nível de concordância, maior será a preocupação com a proteção de dados.

Passando para questões diretamente relacionadas com a privacidade e a segurança, iniciamos com a abordagem à hipótese 7, através da análise da importância dos direitos de proteção de dados pessoais. Como se tinha observado, a maioria dos inquiridos (38,8%) tinha declarado “muita preocupação”, relativamente ao desconhecimento da localização física dos seus dados e, de facto, conseguiu-se comprovar que uma maior preocupação com esta igualdade de direitos significa um aumento de preocupação com a utilização indevida e proteção dos nossos dados.

Complementarmente, a hipótese 5, relativa ao grau de ameaça percecionado pelo utilizador, relativamente a várias entidades, nomeadamente, governos, empresas privadas, entidades de publicidade e piratas informáticos, a maioria dos inquiridos classifica com “muita ameaça” o “governo” (33,3%), as “empresas privadas” (38,4%) e “entidades de publicidade” (44,7%). Já 67,8% considera “piratas informáticos” como “ameaça total”. Mais uma vez, através de correlação de *Spearman* conseguimos confirmar a relação duas destas variáveis com a preocupação com proteção de dados. Quanto maior grau de ameaça for atribuído aos piratas informáticos e governos, maior será a preocupação com a utilização indevida dos nossos dados.

Relativamente ao constructo de confiança, começamos com a hipótese 4, relativa ao nível de confiança para com o sistema de computação em nuvem. Na questão 4 os resultados foram claros, com uma enorme confiança depositada tanto na tecnologia como nos fornecedores de serviço e na realidade ainda conseguimos comprovar que existe uma relação, negativa e significativa entre este nível de confiança e o nível de preocupação com proteção de dados. Ou seja, quanto maior a confiança, menor a preocupação.

Relativamente aos fornecedores de serviço, fomos buscar algumas práticas destes, relativas aos dados do consumidor e medir o sentimento provocado neste e tentar perceber se existe alguma relação com a preocupação com a proteção de dados. Como vimos pelos resultados descritivos da questão 10, 30,2% dos inquiridos revelam-se escandalizados e conseguimos correlacionar significativamente e positivamente este nível de perturbação, com o a preocupação com proteção de dados, logo, quanto mais perturbado o utilizador estiver perante as práticas dos fornecedores de serviço, maior o nível de preocupação, sendo esta a hipótese 6.

Relativamente às determinantes de vantagens e limitações de sistema, seguem-se as hipóteses 2, 3 e 8.

Em primeiro lugar, para a hipótese 2, tentou-se avaliar a correlação e a importância dada às vantagens da tecnologia (questão 2), com a preocupação de proteção de dados. Tal correlação foi observada de forma positiva e significativa, corroborando a hipótese 2, concretamente e significativamente o item de segurança de dados. Parece contrassenso, mas, faz sentido, quanto maior importância damos à segurança de dados, significa que existe uma maior preocupação com essa segurança.

Ao mesmo tempo, as preocupações com as limitações do sistema (questão 3) estão positiva e significativamente correlacionadas com a preocupação com proteção de dados, logo, uma maior preocupação com estes limites, conforme foi observado, significa uma maior preocupação com a base de dados, corroborando assim a hipótese 3.

Por fim, a hipótese 8. Relativamente à questão 15, sobre o controlo percebido sobre o sistema de computação em nuvem, não foi possível corroborar a hipótese de que um maior controlo percebido afetaria a preocupação com a proteção de dados.

Abordadas todas as hipóteses e antes de se concluir, apresenta-se na tabela abaixo a síntese de hipóteses e os seus resultados.

	Hipóteses	Testes estatísticos	Resultado
H1	Existe uma relação significativa e negativa entre o conhecimento/frequência de utilização do sistema de computação em nuvem e a preocupação com utilização/proteção de dados.	Teste correlação de *Spearman*	Corroborada parcialmente
H2	Existe uma relação significativa e positiva entre a importância das vantagens dos serviços de computação em nuvem com preocupação e a utilização/proteção de dados.	Teste correlação de *Spearman*	Corroborada
H3	A preocupação com as limitações dos serviços de computação em nuvem encontra-se significativa e positivamente relacionada com a preocupação com utilização/proteção de dados.	Teste correlação de *Spearman*	Corroborada

H4	Existe uma relação significativa e negativa entre o nível de confiança com sistema de computação em nuvem e com os fornecedores de serviços e a preocupação com utilização/proteção de dados.	Teste correlação de *Spearman*	Corroborada
H5	Um maio grau de ameaça á privacidade por parte de certas entidades está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Corroborada parcialmente
H5a	Um maior grau de ameaça á privacidade por parte do governo está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Corroborada
H5b	Um maior grau de ameaça á privacidade por parte das empresas privadas está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Não corroborada
H5c	Um maior grau de ameaça á privacidade por parte de entidades de publicidade está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Não corroborada
H5d	Um maior grau de ameaça á privacidade por parte de piratas informáticos está relacionado de modo significativo com uma maior preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Corroborada
H6	O sentimento que provoca a venda de dados pessoais por fornecedores de serviços está relacionado de forma significativa e positiva com a preocupação com a utilização indevida/proteção de dados.	Teste correlação de *Spearman*	Corroborada
H7	Existe relação uma significativa e positiva entre a importância dos direitos de proteção dos dados pessoais e a preocupação com a utilização indevida/proteção de dados.	Teste correlação de *Spearman*	Corroborada

H8	Um maior controlo sobre o sistema de computação em nuvem implica uma menor preocupação com a utilização indevida/proteção de dados pessoais.	Teste correlação de *Spearman*	Não corroborada
H9	O tempo de utilização dos serviços de computação em nuvem está relacionado de modo significativo e negativo com a preocupação com a utilização indevida/proteção dos dados pessoais.	Teste correlação de *Spearman*	Não corroborada
H10	O nível de concordância da divulgação de informação como um problema esta significativa e positivamente correlacionado com a preocupação com a utilização indevida/proteção dos dados pessoais.	Teste correlação de *Spearman*	Corroborada

Tabela 47 – Resultado final das hipóteses propostas.

Fonte: elaboração própria.

6.8.1 - Modelo estrutural final

Para alem do teste de hipóteses, tinha-se estabelecido o objetivo de apresentar um modelo explicativo da preocupação com a utilização indevida dos nossos dados, ou, proteção de dados.

Após os devidos testes e adaptações até mencionadas, apresenta-se abaixo o modelo estrutural fatorial e corroborado final:

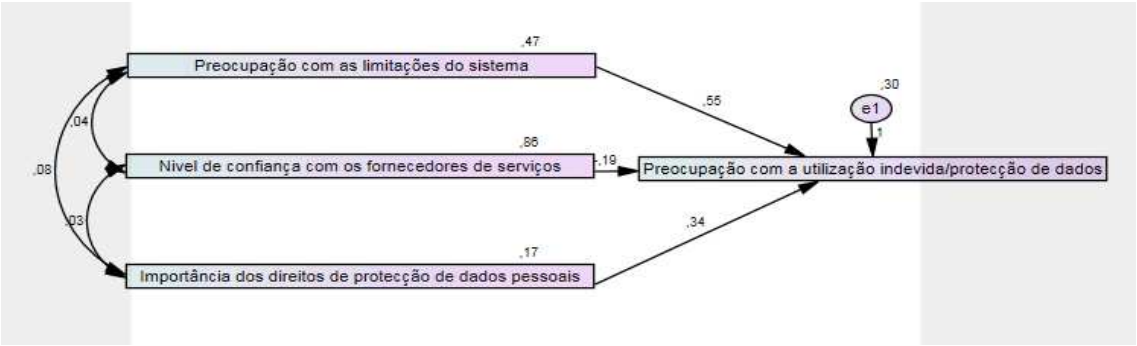

Figura 34 – Modelo estrutural fatorial.

Fonte: elaboração própria.

Capitulo VII - Conclusão

7.1 - Introdução

Chegando a este ponto do trabalho, neste capítulo, importa perguntar o que se retira deste trabalho? Quais as conclusões concretas, as considerações finais deste estudo, bem como, quais a limitações encontradas e as sugestões que se pode dar para trabalhos futuros.

É isto que será apresentado de seguida.

7.2 - Considerações finais

Neste trabalho, tentou-se fornecer um *State-of-the-Art* acerca da tecnologia de computação em nuvem, sobre o seu funcionamento geral e não técnico, tendo em conta as suas principais características, modelos de implementação e serviço, afunilando o trabalho com um foco na área de privacidade e segurança de dados. Através da revisão de literatura, esse objetivo terá sido conseguido.

Relativamente ao estudo empírico, este trabalho conseguiu extrair alguns resultados válidos e extremamente interessantes, podendo contribuir com um pequeno valor cientifico para a comunidade académica e demais. Os resultados obtidos, permitem uma mais fácil compreensão e estudo deste recente paradigma que é a *cloud*.

Não só de um ponto de vista académico, mas, também, de um ponto de vista pessoal e/ou empresarial, este trabalho fornece informação capaz de auxiliar a tomada de decisão relativamente ao processo de adoção e utilização das tecnologias *cloud*, algo que parece inevitável.

Este trabalho conseguiu medir e comprovar as principais vantagens e desvantagens da tecnologia, que advêm das suas inerentes características.

Conseguiu-se medir que, aparentemente, as pessoas confiam na tecnologia e, igualmente importante, nos fornecedores de serviço, apesar de os receios de segurança e privacidade estarem presentes.

Os resultados demonstram que as pessoas sentem que hoje em dia é necessário divulgar informação pessoal, embora, isso seja uma preocupação, o que atesta a importância, vantagem e crescimento da *cloud*, algo que foi comprovado pela enorme utilização de serviços, conforme medido.

Conseguiu-se medir que os inquiridos dão muita importância à igualdade de direitos de proteção e, que, não só não esperam essa proteção, por parte do governo, como vêem este como uma das principais ameaças à segurança e privacidade dos seus dados, embora, tenham a perceção

que eles próprios e/ou o fornecedor de serviços são os responsáveis pela proteção dos seus dados.

Apesar de já utilizarem os serviços, os resultados apontam para uma esperança de maior, ou, mesmo total, controlo dos seus dados, como o objetivo máximo e melhoria da proteção dos seus dados.

Falando de proteção de dados, conseguimos comprovar empiricamente, através de análise inferencial, que o receio por esta proteção é influenciado pelas preocupações com os limites do sistema *cloud*, pelo nível de confiança para com os fornecedores de serviço e pela importância dos direitos de proteção de dados pessoais.

Dito isto, quais as implicações deste estudo? Tentamos responder a esta questão de seguida.

7.3 - Síntese de conclusões e implicações gerais teóricas do estudo

No decorrer desta dissertação abordamos de forma básica, mas, compreensivamente, a tecnologia de computação em nuvem

Identificada, definida e caracterizado o ambiente *cloud*, a literatura revista permite-nos estabelecer uma ligação entre as características chave da tecnologia, bem como, o meio pela qual a utilizamos (i.e. internet) e os principais benefícios e desafios à sua adoção.

Relativamente aos benefícios, estes prendem-se intimamente com a utilidade, facilidade de utilização e benefícios económicos, quando comparado com outras soluções, ou mesmo, a criação de novas possibilidades e capacidades.

Quanto aos desafios, estes estarão relacionados, especialmente, com a falta de conhecimento, entenda-se, pouca compreensão do funcionamento da tecnologia e, inclusive, a dependência de rede, que é algo que torna a tecnologia em algo ubíquo, mas que, ao mesmo tempo, implica a existência de acesso à internet. O outro grande aspeto dos desafios da *cloud* são os fatores fora do controlo, nosso e do fornecedor de serviços, como por exemplo, desastres naturais num centro de dados, que de resto, é algo que pode gerar mais uma problemática, além de custos inesperados. Finalmente, temos, ainda, a dificuldade de interoperabilidade entre fornecedores e serviços.

Por fim, o que influência, maioritariamente, a utilização, ou não, desta tecnologia, parecem mesmo ser questões de privacidade e segurança. Segundo a literatura abordada, existem fragilidades de segurança e privacidade na tecnologia, mas, o interessante é que, aparentemente, não é o conhecimento dessas fragilidades que influência a adoção e utilização da *cloud*, mas sim, um conjunto de fatores do foro psicológico da parte do utilizador. O que parece

exercer referida influência são as perceções do consumidor, como a utilidade e facilidade de utilização da tecnologia, bem como, a confiança deste, não tanto para com a tecnologia, mas, para com a empresa que fornece os serviços. São as perceções, valores, ideologias e experiência do utilizador que parecem influenciar a sua adoção da tecnologia. Ou seja, por um lado, parece existir influencia dos valores da própria pessoa, por outro, relativamente à tecnologia, o juízo é feito relativamente à sua utilidade e facilidade de utilização e, relativamente ao fornecedor de serviços é feito o juízo de confiança.

7.4 - Síntese de conclusões e implicações práticas do estudo

Relativamente aos resultados do trabalho empírico, realizamos uma caracterização da amostra, uma análise fatorial das escalas formuladas, bem como, uma análise da consistência interna e, ainda, uma analise descritiva dos resultados, teste de hipóteses e, por fim, a proposta de criação de um modelo fatorial explicativo compatível com os resultados.

Relativamente à validade fatorial das escalas formuladas, apenas na questão 19 do questionário encontrarmos alguns problemas, com um valor inadequado de KMO=0,55, sendo que, no entanto, prosseguimos com a análise por forma a verificar quais os itens explicativos do fator comum. Após duas análises, apesar de significativos valores no teste de Bartlett, de acordo com os resultados de KMO e cargas fatoriais, eliminaram-se 3 dos 5 itens, mantendo-se "apenas" o item "Para mim, divulgar informação pessoal em troca de serviços online grátis é um problema" e "Para mim, divulgar informação pessoal é um problema", que, sozinhos, apresentam uma consistência interna altamente satisfatória, com um valor de *alpha* de *Cronbach* de 0,77. Com isto, decidiu-se criar um fator denominado de "divulgação como um problema em geral".

Esta dissertação pretendia, também, analisar hipóteses operativas, agrupadas em áreas "mãe" de confiança, vantagens e limitações do sistema, privacidade e segurança e, ainda, conhecimento/utilização". Assim, no que toca ao teste das hipóteses elaboradas, apresentamos uma síntese dos resultados obtidos na tabela que se segue.

Hipóteses	Relação proposta	Correlação de *Spearman*
H1	-	-
H2	+	+
H3	+	+

H4	-	-
H5		
H5a	+	+
H5b	+	+
H5c	+	+
H5d	+	+
H6	+	+
H7	+	+
H8	-	-
H9	-	-
H10	+	+

Tabela 48 – Síntese de resultados dos testes de hipóteses.

Fonte: elaboração própria.

Em relação aos resultados obtidos, há que mencionar que a hipóteses 5a, 5b, 8 e 9, não obtiveram valores significativos, logo, não foram corroboradas. Quanto às restantes, o coeficiente de correlação obtido foi significativo e não foram contrariados nenhuns sentidos de associação propostos.

7.5 - Recomendações para a gestão

A *cloud* está a ser implementada de forma imparável e quem não tirar partido dos seus benefícios ficará para trás.

As empresas, ou a gestão, enfrentam um processo de decisão para a adoção e a utilização desta tecnologia. O que não deixa de ser um dilema visto que existem aspetos positivos e negativos. Em suma, estas são as implicações para a gestão. Esta tem que saber como funciona a tecnologia e, acima de tudo, saber identificar as vantagens e as desvantagens, bem como, saber como tentar mitigar as desvantagens.

Dito isto, previsivelmente, a maior vantagem continuará a ser a redução de custos, sejam os custos iniciais, como os custos operacionais e de manutenção. Já o maior desafio será sempre a segurança, se bem que, durante a revisão de literatura ficou patente a ideia de que, a não ser

que a sua empresa seja uma Microsoft, Google ou Amazon, pelos mesmos custos, compra melhor segurança utilizando o serviço destas empresas.

Ainda assim, uma empresa deve ter sempre em mente as principais vantagens e desvantagens e nunca se focar em apenas um ponto. Deve conseguir perceber que a *cloud* lhe permite ter, para além de menores custos, um melhor funcionamento, maior eficiência, redução de complexidades e desperdícios. Em suma, a *cloud* pode simplificar uma empresa a nível processual, aumentar a sua produtividade e competitividade, é o aumentar da flexibilidade da empresa.

Outro ponto de vista é se a empresa em questão for uma fornecedora ou integradora de serviços *cloud*. Nessa altura, todos os resultados obtidos, neste trabalho, principalmente a nível de hipóteses e o modelo são fulcrais para uma melhor compreensão do consumidor final e, consequentemente, uma melhor aproximação, adesão e fidelização do mesmo.

Em qualquer dos casos, há algo que a gestão de empresas tem que perceber e interiorizar, de uma vez por todas. É necessário uma constante evolução e adaptação aos tempos, neste caso, às tecnologias.

Parte dessa adaptação passa por uma constante procura de mitigação de riscos e no caso de uma empresa que adota a *cloud*, isso passa, basicamente, pela constante comunicação e negociação com o fornecedor de serviços, por forma a tentar obter garantias de redundância, continuidade de serviços e recobro de desastre.

7.4 - Limitações

Como é expectável neste tipo de estudos, existem sempre algumas limitações, seja de origem teórica, inerente à revisão da literatura, ou empírica, na formulação e desenvolvimento de uma válida investigação. Estas limitações podem limitar os resultados obtidos e a generalização de conclusões.

Começando pela literatura e estudos teóricos, denotou-se uma imensa escassez de trabalhos homólogos a este. Sim, a tecnologia abordada encontra-se imensamente estudada e publicada, mas, com o foco no lado técnico da tecnologia e o seu funcionamento, ou no lado de adoção empresarial, sendo que este último, também, tem limitações na profundidade e complexidade de trabalhos empíricos realizados. Passando para trabalhos de natureza como o nosso, com o foco mais no consumidor final, suportando o estudo com criação de hipóteses e modelos, foi algo que se revelou difícil de operacionalizar, pois, simplesmente não há, ou melhor, deve-se dizer, não foram encontrados tais tipos de estudos durante a revisão de literatura.

Este simples facto afetou a realização deste trabalho a vários níveis. O não conseguir encontrar trabalhos homólogos levou a um enorme gasto de tempo na procura de literatura e desenvolvimento de um possível modelo teórico. O facto de encontrarmos literatura escassa e dispersa, sem ligação aos conceitos desejados, “obrigou” à elaboração de ligações ténues e não 100% seguras, entre variáveis estudadas, o que por sua vez aumentou a complexidade do trabalho empírico. Deste modo, por prevenção, construiu-se um instrumento de recolha de dados mais complexo do que, provavelmente, seria necessário. Por sua vez a criação deste instrumento consumiu mais tempo que desejado e a sua operacionalização e alguma dificuldade na sua rápida compreensão sobre as questões “muitas vezes técnicas” terá sido dissuasiva e determinante para as muitas desistências de preenchimento do questionário e que foram registadas.

Ainda relativamente ao questionário, outra limitação terá sido a necessidade de utilizar uma amostra por conveniência, face ao tempo disponível de recolha e custos associados à elaboração deste trabalho

Como consequência de tudo isto, a própria criação de hipóteses foi afetada visto, que, teve que ser realizada por interpretação própria de conceitos dispersos e a análise de resultados, também, foi mais demorada, pelo simples facto de não haver resultados homólogos para fazer comparações e a discussão daqueles.

No entanto, a verdade é que, com estas limitações de literatura, estudos e tempo, conseguiram-se obter alguns e válidos resultados, o que significa que este trabalho pode ser um bom ponto de partida para algo mais maduro e profundo.

7.5 - Sugestões para investigações futuras

Para trabalhos futuros, focando-nos em fatores controláveis, assinalamos desde logo o tipo de amostra. Obter amostras maiores e até probabilísticas, inerentes a certos setores, poderá levar à obtenção de resultados mais robustos.

Ainda melhor poderá ser um diferente tipo de estudo, embora, seja necessário mais tempo e recursos, mas, um estudo espaçado no tempo, com base, também, ao recurso a abordagens qualitativas antecedentes das quantitativas para melhorar e aperfeiçoar as escalas de medida utilizadas.

Outras sugestões podem ser retiradas dos limites ou incapacidades de corroboração deste mesmo estudo. Por exemplo, Segurança é apontada como uma vantagem muito importante da tecnologia e ao mesmo tempo uma limitação muito preocupante. Embora isto possa fazer sentido, racionalmente, era extremamente interessante dissecar o porque, o que afeta cada perspetiva e como.

Outra sugestão prende-se com a TAM. Este trabalho tentou-se suportar neste modelo, mas, ficou-se por uma fase de perceções do consumidor, não conseguiu ligar e estabelecer um modelo de início ao fim, lendo-se fim como a adesão e utilização da tecnologia. Pegar nas vantagens e limites da tecnologia e chegar a um modelo que explique porque que apesar de tanto receio, esta é adotada e o que é preciso para haver uma total quebra de confiança e, consequente, abandono da mesma.

Ainda, relativamente, a constructos abordados neste trabalho, seria interessante perceber e estudar a perceção e distinção que o consumidor faz, ou não, entre a tecnologia em si e o fornecedor de serviços.

Por fim, e possivelmente a sugestão mais simples, é pegar neste trabalho e melhora-lo, em termos das escalas utilizadas. Voltar a avaliar e melhorar e/ou adotar melhores escalas e metodologias e, tambem, o simplificar do instrumento de recolha de dados. A verdade é que ficou alguma base metodológica feita, a qual, pode servir para uma replicação ou simples primeiro passo para um melhor estudo.

Referências

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication. *MIS QUarterly, 16(2)*, pp. 227-247. Obtido em 12 de Fevereiro de 2015, de http://misq.org/cat-articles/perceived-usefulness-ease-of-use-and-usage-of-information-technology-a-replication.html

Adams, G., & Schvaneveldt, J. (1991). *Understanding Research Methods.* New York: Longman.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*, pp. 665-694.

Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of information technologies? *Decision Sciences, 30*, pp. 361-391.

AICPA. (2005). *Generally Accepted Privacy Principles.* White Paper, American Institute of Certified Public Accountants. Obtido em 13 de Fevereiro de 2014, de http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour Human Decision Processes*, pp. 179-211.

Aliaga, M., & Gunderson, B. (2002). *Interactive statistics.* New Jersey: Prentice Hall.

Ammori, M. (4 de Novembro de 2013). *So the Internet is About to Lose its Net Neutrality*. Obtido em 1 de Janeiro de 2014, de Wired: http://www.wired.com/2013/11/so-the-internets-about-to-lose-its-net-neutrality/

Antikainen, A. (2014). *Risk-Based Approach as a Solution to Secondary Use of Personal Data.* Dissertação de Mestrado, Universidade de Helsinki. Obtido em 18 de Maio de 2015, de https://helda.helsinki.fi/bitstream/handle/10138/136409/Summary%20and%20Thesis%20RiskBased%20Approach%20as%20a%20Solution%20to%20Secondary%20Use%20of%20Personal%20Data.pdf?sequence=1

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, . . . Zaharia, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing.* Universidade da California Berkeley. doi:Technical Report Nº: UCB/EECS-2009-28

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, . . . Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM, 53(4)*, pp. 50-58. doi::10.1145/1721654.1721672

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *Cloud Computing Synopsis and Recommendations - Recommendations of the National Institute of Standards and Technology.* U.S. Department of Commerce, Computer Security Division. doi:Special Publication 800-146

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems, 8*, pp. 244-254.

Bagozzi, R., Davis, F., & Warshaw, P. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35 (8)*, pp. 982-1003.

Bagozzi, R., Davis, F., & Warshaw, P. (Julho de 1992). Development and Test of a Theory of Technological Learning and Usage. *Human Relations, 45 (7)*, pp. 660-686. doi:10.1177/001872679204500702

Barki, H., & Hartwick, J. (1994). Measuring User Participation, User Involvement, and User. *MIS Quarterly, 18(1)*, pp. 58-82. Obtido em 20 de Abri de 2015, de http://dl.acm.org/citation.cfm?id=198646

Barnatt, C. (2010). *A Brief Guide to Cloud Computing.* Londres: Robinson. doi:ISBN: 978-1-84901-406-9

Best, S. J., Krueger, B. S., & Ladewig, J. (2008). The Effect of Risk Perceptions on Online Political Participatory Decisions. *Journal of Information Technology & Politics, 4(1)*, pp. 5-17. doi:10.1300/J516v04n01_02

Bhisikar, A. (Maio de 2011). G-Cloud: New Paradigm Shift for Online Public Services. *International Journal of Computer Applications*, pp. 24-29. doi:10.5120/2603-3629

Bisquerra, R. (1989). *Métodos de Investigacion Educativa: Guia Prática.* Barcelona: Ediciones CEAC.

Boss, G., Malladi, P., Quan, D., Legregni, L., & Harold, H. (2007). *Cloud Computing.* White Paper, IBM. Obtido em 13 de Maio de 2015, de http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf

Bushan, V., Khetan, A., & Gupta, S. C. (2013). Data-a-Service and their Security Concerns in Cloud. *International Journal of Engineering Research & Technology, 2(2)*. Obtido em 13 de Maio de 2015, de http://www.ijert.org/download/2282/data-a-service-and-their-security-concerns-in-cloud

Cambridge Dictionaries Online. (2015a). Mailing list. Obtido em 15 de Maio de 2015, de http://dictionary.cambridge.org/dictionary/english/mailing-list

Cambridge Dictionaries Online. (2015b). Word-of-mouth. Obtido em 18 de Maio de 2015, de http://dictionary.cambridge.org/dictionary/english/word-of-mouth

Castillo Vera, P. d., Trautmann, C., Adersdotter, A., Ernst, C., & Kari, R. R. (2014). *European Single Market for Electronic Communications COM(2013)0627 – C7-0267/2013 – 2013/0309(COD).* Emenda - Proposta para regulamentação, Parlamento Europeu. Obtido em 1 de Abril de 2014

Cellary, W., & Strykowski, S. (2009). E-Government Based on Cloud Computing and Service-Oriented Architecture. *ICEGOV '09 Proceedings of the 3rd international conference on Theory and practice of electronic governance*, (pp. 5-10). Nova Iorque. doi:10.1145/1693042.1693045

Chandrasekaran, A., & Kapoor, M. (2011). *State of Cloud Computing in the Public Sector – A Strategic Analysis of the Business Case and Overview of Initiatives Across Asia Pacific.* White Paper. Obtido em 1 de Abril de 2014, de http://www.frost.com/prod/servlet/cio/232651119

Changchit, C. (2008). Data Protection and Privacy Issue. *Journal of Information Privacy and Security, 4 (3)*, pp. 1-2. doi:10.1080/2333696X.2008.10855842

Changchit, C. (2014). Student's Perceptions of Cloud Computing. *Issues in Information Systems, 15(1)*, pp. 312-322. Obtido em 12 de Agosto de 2015, de http://iacis.org/iis/2014/60_iis_2014_312-322.pdf

Chao, H.-C. (2011). Internet of Things and Cloud Computing for Future Internet. *Ubiquitous Intelligence and Computing, XVI*, 1. doi:10.1007/978-3-642-23641-9_1

Chau, P., & Hu, P. (2001). Information technology acceptance by individual professionals: a model comparison approach. *Decision Sciences, 32*, pp. 699-719.

Chee, F. Y. (2014). *Reuters*. Obtido em 1 de Janeiro de 2015, de EU Parliament votes to end roaming, protect "net neutrality".: http://uk.reuters.com/article/2014/04/03/us-eu-telecomunications-parliament-idUKBREA320S520140403

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science & Education - ICCSE*, *1*, pp. 647-651. doi:10.1109/ICCSEE.2012.193

Chin, W. W., & Todd, P. A. (Junho de 1995). On the Use, Usefulness, and Ease of Use of Structural Equation Modeling in MIS Research: A Note of Caution. *MIS Quarterly, 19(2)*, pp. 237-246. doi:10.2307/249690

CIO Focus. (2008). *Forecast: Cloud Computing Looms Big on the Horizon.* White Paper.

Cloud Security Alliance. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* White Paper, Cloud Security Alliance. Obtido em 18 de Maio de 2014, de https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cloud Security Alliance. (2013). *The Notorious Nine - Cloud Computing Top Threats in 2013.* Cloud Security Alliance. Obtido em 5 de Março de 2015, de https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Cloud Security Alliance; Information Systems Audit and Control Association. (2012). *Cloud Computing Market Maturity.* Estudo. Obtido em 01 de Fevereiro de 2014, de https://cloudsecurityalliance.org/research/collaborate/#_isaca

Columbus, L. (26 de Julho de 2015). *Analytics, Cloud Computing Dominate Internet Of Things App Developers' Plans.* Obtido em 18 de Maio de 2015, de Forbes: http://www.forbes.com/sites/louiscolumbus/2015/07/26/analytics-cloud-computing-dominate-internet-of-things-app-developers-plans/

Comissão Europeia. (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.* Obtido em 12 de Março de 2015, de http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

Comissão Europeia. (2012a). *Comission Staff Working Document - Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.* Unleashing the Potential of Cloud Computing in Europe, Bruxelas. Obtido em 01 de Abril de 2014, de http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/swd_com_cloud.pdf

Coutinho, C. (2011). *Metodologia de investigação em ciências sociais e humanas: teoria e prática.* Coimbra: Edições Almedina.

Creswell, J. W. (1994). *Research Design: Qualitative & Quantitative Approaches.* Sage Publications.

Cruz, J. (2013). *Ambientes de Aprendizagem com Cloud Computing: Uma Visão Sobre o Conceito e a Realidade Portuguesa no Ensino Secundário.* Dissertação de Mestrado. Obtido em 15 de Maio de 2014, de http://repositorio.ul.pt/bitstream/10451/10277/1/ulfpie046303_tm_tese.pdf

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13 (3)*. doi:10.2307/249008

Demarest, G., & Wang, R. (2010). *Oracle Cloud Computing.* Oracle. Obtido em 15 de Fevereiro de 2014, de http://www.oracle.com/us/technologies/cloud/oracle-cloud-computing-wp-076373.pdf

Dialogic. (2014). *Introduction to Cloud Computing.* White Paper, Montreal. Obtido em 03 de Janeiro de 2014, de http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf

Direção Geral do Ensino Superior. (2015). *Acesso ao Ensino Superior 2013-2014 - 1ª Fase do Concurso Nacional de Acesso .* Estatistica de Colocados no Concurso Nacional de Acesso (Público), DGES. Obtido em 15 de Maio de 2015, de http://www.dges.mctes.pt/guias/pdfs/statcol/2014/Resumo14.pdf

Duranti, L. (20113). *Records in the Cloud: User Survey Report.* User Survey, University of British Columbia. Obtido em 1 de Janeiro de 2014, de http://recordsinthecloud.org/assets/documents/RiC_Oct232013_User_Survey_Report.pdf

Elbadawi, I. (2011). Cloud Computing for E-government in UAE: Opportunities, Challenges and Service Models. *ICEGOV '11 Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, (pp. 387-388). Nova Iorque. doi:10.1145/2072069.2072155

Eurobarometer. (2011). *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union.* SPECIAL EUROBAROMETER - Survey, Comissão Europeia. Obtido em 2 de Janeiro de 2014, de http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Fisher, D. (2013). What is a Botnet? *Kaspersky Lab, Daily*. Obtido em 1 de Janeiro de 2015, de https://blog.kaspersky.com/botnet/1742/

Flavian, C., & Guinalíu, M. (2006). Consumer Trust, Perceived Security and Privacy: Three Basic Elements of Loyalty to a Web Site. *Industrial Management & Data Systems, 106 (5)*, pp. 601-620. doi:10.1108/02635570610666403

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop, 2008. GCE '08* , pp. 1-10. doi:10.1109/GCE.2008.4738445

Gartner. (26 de Junho de 2008). Gartner Says Cloud Computing Will Be As Influential As E-business. Obtido em 01 de Março de 2014, de Gartner: http://www.gartner.com/newsroom/id/707508

Gartner. (2013). *Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016.* Gartner. Obtido em 15 de Maio de 2015, de http://www.gartner.com/newsroom/id/2613015

Gartner. (2015). *IT Glossary*. Obtido em 05 de Janeiro de 2014, de Gartner: https://www.gartner.com/it-glossary/big-data/

Gartner. (2015a). *IT Glossary*. Obtido em 15 de Janeiro de 2014, de Gartner: http://www.gartner.com/it-glossary/multitenancy

Gartner. (12 de Janeiro de 2015c). *Gartner Says Worldwide IT Spending on Pace to Grow 2.4 Percent in 2015.* Gartner. Obtido em 15 de Maio de 2015, de http://www.gartner.com/newsroom/id/2959717

Gharehchopogh, F. S. (Julho de 2012). Security Challenges in Cloud omputing with. *International Journal of Scientific & Technology Research, 1(6)*, pp. 49-54. Obtido em 13 de Janeiro de 2015, de http://www.ijstr.org/final-print/july2012/Security-Challenges-In-Cloud-Computing-With-More-Emphasis-on-Trust-And-Privacy.pdf

Giff. (2000). *The Influence of Metaphor, Smart Cards and Interface Dialogue on Trust in eCommerce.* Mestrado, Universidade de Londres.

Google. (2015a). *Trends*. Obtido em 01 de Janeiro de 2014, de Google: http://www.google.com/trends/explore#q=cloud%20computing

Google. (2015b). *Trends*. Obtido em 02 de Março de 2014, de Google: http://www.google.com/trends/explore#q=%2Fm%2F02y_9m3

Gorelik, E. (2013). *Cloud Computing Models (Tese de Mestrado).* Obtido em 20 de Dezembro de 2013, de http://dspace.mit.edu/handle/1721.1/79811

Granick, J. (8 de Agosto de 2013). *NSA Lies About the Fact that Americans Are Routinely Spied on by Our Government Time for a Special Prosecutor*. Obtido em 15 de Dezembro de 2013, de Forbes: http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/

Hair Jr, J., Babin, B., Money, A., & Philip, S. (2005). *Fundamentos de métodos de pesquisa de administração.* Porto Alegre: Bookman.

Hair, J., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis.* (6ª ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Halpert, B. (2011). *Auditing Cloud Computing: A Security and Privacy Guide.* Atalanta: Wiley. doi:ISBN: 978-0-470-87474-5

Hashemi, S. (Outubro de 2013). Cloud Computing Technology: Security and Trust Challenges. *International Journal of Security, Privacy and Trust Management, 2(5)*. Obtido em 1 de Janeiro de 2015, de http://airccse.org/journal/ijsptm/papers/2513ijsptm01.pdf

Herbst, N. R., Kounev, S., & Reussner, R. (2013). Elasticity in Cloud Computing: What It Is, and What It Is Not. *Proceedings of the 10th International Conference on Autonomic Computing. 38.* usenix. Obtido em 15 de Janeiro de 2014, de http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/11719-icac13_herbst.pdf

Hong, W., Thing, J., Wong, W., & Tam, K. (2001). Determinants of user acceptance of digital libraries: an empirical examination of individual differences and system characteristics. *Journal of Management Information Systems, 18*, pp. 97-125.

Hubona, G. S., & Geitz, S. (1997). External Variables, Beliefs, Attitudes and Information Technology Usage Behavior. *Proceedings of The Thirtieth Annual Hawwaii International Conference*, (pp. 21-28). Obtido em 15 de Fevereiro de 2015, de http://www.computer.org/csdl/proceedings/hicss/1997/7734/03/7734030021.pdf

Instituto Nacional de Estatística. (2001). Censos. Portugal. Obtido em 3 de Abril de 2015, de http://censos.ine.pt/xportal/xmain?xpgid=censos2011_apresentacao&xpid=CENSOS

Jackson, K. L. (17 de Setembro de 2011). *The Economic Benefit of Cloud Computing*. Obtido em 13 de Fevereiro de 2014, de Forbes: http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/

Jaeger, P. T., & Fleischmann, K. R. (2007). Public libraries, values, trust, and e-government. *Information Technology and Libraries, 26(4)*. doi:10.6017/ital.v26i4.3268

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* Publicação Especial 800-144, National Institute of Standards and Technology, Gaithersburg. Obtido em 02 de Dezembro de 2013, de http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

Javaid, M. A. (08 de Janeiro de 2014). Cloud Computing Security and Privacy. doi:http://dx.doi.org/10.2139/ssrn.2388377

Kajiyama, T. (2012). *Cloud Computing Security: How Risks and Threats are Affecting Cloud Adoption Decisions.* Dissertação de Mestrado, San Diego Stat University. doi:10.1.1.465.9097

Kang, C. (2010). Obtido em 1 de Janeiro de 2014, de The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html

Kaplan, A. (1988). *The Conduct of Inquiry: Methodology for Behavioral Science.* London: Transaction Publishers.

Kok, G. (2010). *Cloud Computing & Confidentiality.* Dissertação de Mestrado, Twente. Obtido em 05 de Dezembro de 2013, de http://essay.utwente.nl/61039/1/MSc_G_Kok_DIES_CTIT.pdf

KPMG; Forbes Insights. (2012). *Breaking Through the Cloud Adoption Barriers.* Estudo. Obtido em 02 de Dezembro de 2013, de https://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/Advisory-ICE-Breaking-through-the-Cloud-Adoption-Barriers-Glob.pdf

Krikos, A. C. (2010). *Disruptive Technology Business Models in Cloud Computing.* Dissertação de Mestrado, Massachusetts Institute of Technology. Obtido em 15 de Janeiro de 2014, de http://dspace.mit.edu/bitstream/handle/1721.1/59255/667662907-MIT.pdf?sequence=2

Kroes, N. (10 de Março de 2014). Securing our digital economy. *CEBIT, Cyber Security Conference.* Comissão Europeia. Obtido em 13 de Maio de 2015, de http://europa.eu/rapid/press-release_SPEECH-14-197_en.htm

Kumar, R. (2005). *Research Methodology: A Step by Step Guide for Beginners.* Londres: Sage Publications.

Kundra, V. (2011). *Federal Cloud Computing Strategy.* The White House, Washington. Obtido em 10 de Fevereiro de 2014, de https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf

Kwofie, B. (2013). *Cloud computing opportunities, risks and challenges with regard to Information Security in the context of developing countries.* Tese de Mestrado, Luleá University of Technology, Department of Computer Science, Electrical and Space Engineering. Obtido em 15 de Outubro de 2014, de https://pure.ltu.se/portal/files/43913340/LTU-EX-2013-43878766.pdf

Lakatos, E. M., & Marconi, M. (2006). *Fundamentos de metodologia ciêntifica.* São Paulo: Editora Atlas.

Larsen, K., Lee, Y., & Kozar, K. (2003). The Technology Acceptance Model: Past, Present, and Future. *Communications of the Association for Information Systems, 12*, pp. 752-780.

Lessig, L. (2006). *Code.* New York: Basic Books. Obtido em 10 de Maio de 2015, de http://codev2.cc/download+remix/Lessig-Codev2.pdf

Liang, J. (2012). Government Cloud: Enhancing Efficiency of E-Government and Providing Better Public Services. *2012 International Joint Conference on Service Sciences (IJCSS)*, pp. 261-265. doi:10.1109/IJCSS.2012.20

Licklider, J. (1963). *Topics for Discussion at the Forthcoming Meeting, Memorandum For: Members and Affiliates of the Intergalactic Computer Network.* Memorando, Washington, D.C. Obtido em 2 de Janeiro de 2014, de http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network

Loganayagi, B., & Sujatha, S. (2011). Enhanced Cloud Security by Combining Virtualization and. *The International Conference on Communication Technology and System Design*, (pp. 654-661). doi:10.1016/j.proeng.2012.01.911

Lourenço, F., & Fortes, N. (2013). Participação em Campanhas de Mobile Marketing com Tecnologia Bluetooth: Contributos para a Construção de um Modelo Conceptual. *Jornadas Hispano-Lusas de Gestión Científica.*

Macias, F., & Thomas, G. (2011a). *Cloud Computing Advantages in the Public Sector.* White Paper, CISCO. Obtido em 10 de Janeiro de 2014, de http://www.cisco.com/web/strategy/docs/gov/pscloudadvntgs.pdf

Macias, F., & Thomas, G. (2011b). *Cloud Computing Concerns in the Public Sector.* White Paper, CISCO. Obtido em 10 de Janeiro de 2014, de http://www.cisco.com/web/strategy/docs/gov/pscloudconcerns.pdf

Malhotra, N. K., & Birks, D. F. (2005). *Marketing Research: An Applied Approach - European* (2ª ed.). Financial Times Management.

Malhotra, N. K., & Birks, D. F. (2006a). *Marketing Research: An Applied Approach* (1ª ed.). Pearson Prentice Hall, Inc.

Malhotra, N. K., & Birks, D. F. (2006b). *Marketing Research: An Applied Approach* (3ª ed.). Pearson Prentice Hall.

Malhotra, N., Rocha, I., Laudisio, M. C., Altheman, É., & Borges, F. M. (2005b). *Introdução à pesquisa de marketing.* São Paulo: Prentice Hall.

Maroco, J., & Garcia-Marques, T. (2006). Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas? *Laboratório de Psicologia, 4(1)*, pp. 65-90. Obtido em 3 de Maio de 2015, de http://publicacoes.ispa.pt/index.php/lp/article/viewFile/763/706

Martínez, D. J. (2013). *Privacy and Confidentiality issues in Cloud Computing Architectures.* Dissertação de Mestrado, Universidade Politecnica da Catalunha. Obtido em 19 de Maio de 2015, de http://upcommons.upc.edu/bitstream/handle/2099.1/20816/thesis-david.jimenez-martinez-1.pdf?sequence=1

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy* (1ª ed.). O'Reilly Media. doi:ISBN: 978-0-596-80276-9

Mathieson, K. (1991). Predicting user intention: Comparing the technology acceptance model with the theory of planned behavior. pp. 173-191.

Mattoon, S., Hensle, B., & Baty, J. (2011). *Cloud Computing Maturity Model Guiding Success with Cloud Capabilities.* White Paper, CISCO. Obtido em 15 de Janeiro de 2014, de http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-maturity-model-r3-0-1434934.pdf

McKendrick, J. (7 de Julho de 2013). *5 Benefits of Cloud Computing You Aren't Likely to See in a Sales Brochure*. Obtido em 15 de Janeiro de 2014, de Forbes: http://www.forbes.com/sites/joemckendrick/2013/07/21/5-benefits-of-cloud-computing-you-arent-likely-to-see-in-a-sales-brochure/

McKendrick, J. (22 de 04 de 2014). *joemckendrick - Cloud is Just as Secure (or Insecure) as Traditional On-Premises Systems*. Obtido de Forbes: http://www.forbes.com/sites/joemckendrick/2014/04/22/cloud-is-just-as-secure-or-insecure-as-traditional-on-premises-systems/?ss=cio-network&utm_content=5002857&utm_medium=social&utm_source=twitter

McMillan, R. (2009). *Cloud Computing a security Nightmare*. Obtido de PCworld: http://www.pcworld.com/article/163681/article.html

Mell, P., & Grance, T. (Setembro de 2011). *The NIST Definition of Cloud Computing.* doi:Special Publication 800-145

Merriam-Webster. (1 de Setembro de 2015). E-Commerce. Obtido em 1 de Setembro de 2015, de http://www.merriam-webster.com/dictionary/e-commerce

Microsoft. (s.d.). *Academic Research*. Obtido em 02 de Março de 2014, de Microsoft: http://academic.research.microsoft.com/Keyword/6051/cloud-computing?query=cloud%20computing

Mirzaei, N. (s.d.). *Cloud Computing.* Universidade de Indiana. Pervasive Technology Institute Report, Community Grid Lab. Obtido em 13 de Fevereiro de 2015, de http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.158.2549

Mitchell, V.-W. (1999). Consumer Perceived Risk: Conceptualizations and Models. *European Journal of Marketing, 33*, 163-195. doi:10.1108/03090569910249229

Moore, G. (1965). *Museu Gordon Moore Law.* Obtido em 05 de Janeiro de 2014, de Intel: http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html

Muijnck-Hughes, J. d. (2011). *Data Protection in the Cloud.* Dissertação de Mestrado, Institute for Computing and Information Sciences, Gelderland. Obtido em 03 de Dezembro de 2013, de http://www.ru.nl/publish/pages/578936/201103-s0819824-masterthesis-print.pdf

Nações Unidas. (1948). *Declaração Universal dos Direitos Humanos.* Obtido em 05 de Janeiro de 2014, de Nações Unidas: http://www.un.org/en/documents/udhr/

Nissenbaum, H. (1999). Can Trust be Secured Online? A Theoretical Perspective. *Etica e Politica, 2*. Obtido em 8 de Setembro de 2015, de http://etabeta.univ.trieste.it/dspace/bitstream/10077/5544/1/Nissenbaum_E%26P_I_1999_2.pdf

Nunnally, J. (1978). *Psychometric theory.* New York: McGraw Hill.

Organização para a Cooperação e Desenvolvimento Económico. (10 de Novembro de 2005). Privacidade. Obtido em 13 de Maio de 2015, de https://stats.oecd.org/glossary/detail.asp?ID=6959

Organização para a Cooperaçao e Desenvolvimento Económico. (2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Obtido em 03 de Março de 2014, de OCDE: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Osterwalder, D. (2001). Trust Through Evaluation and Certification. So-cial Science Computer Review. *Social Science Computer Review, 19(1)*, pp. 32-46. doi:10.1177/089443930101900104

Oxford Dictionaries. (2015). *Internet of Things*. (O. U. Press, Editor) Obtido em 11 de Março de 2014, de OxfordDictionaries: http://www.oxforddictionaries.com/definition/english/Internet-of-things

Pearson, S. (2012). *Privacym Security and Trust in Cloud Computing.* HP Laboratories. Obtido em 1 de Fevereiro de 2015, de http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf

Pestana, M. H., & Gageiro, J. N. (2005). *Análise de dados para as ciências sociais: a complementaridade para o SPSS* (4ª ed.). Lisboa: Editora Sílabo.

PORDATA. (2015). *Alunos matriculados no ensino superior: total e por sexo.* Estatistica de Colocados no Concurso Nacional de Acesso. Obtido em 15 de Maio de 2015, de http://www.pordata.pt/Portugal/Ambiente+de+Consulta/Tabela/5690905

Proteste. (s.d.). *Investe*. Obtido em 25 de Janeiro de 2014, de Proteste: https://www.deco.proteste.pt/investe/economias-de-escala-s1680801.htm

Ramalho Correia, A. M., & Mesquita, A. (2013). *Mestrados & Doutoramentos.* Portugal: Vida Económica.

Reis, F. (2010). *Como Elaborar uma Dissertação de Mestrado Segundo Bolonha* (1ª ed.). Lisboa: Pactor.

Roca, J., Garcia, J., & De La Vega, J. (s.d.). The Importance of Perceived Trust, Security, and Privacy in Online Trading Systems. *Information Management and Computer Security, 17 (2)*, pp. 96-113. Obtido de http://www.emeraldinsight.com/doi/pdfplus/10.1108/09685220910963983

Rogers, E. M. (1983). *Diffusion of Innovations.* New Yorque: The Free Press.

Rousseau, D., Sitkin, S., & Camerer, C. (1998). Not so Different after All: a Cross-discipline View of Trust. *Academy of Management Re-view, 23(3)*, pp. 493-404. Obtido em 15 de Fevereiro de 2015, de http://portal.psychology.uoguelph.ca/faculty/gill/7140/WEEK_3_Jan.25/Rousseau,%20Sitkin,%20Burt,%20%26%20Camerer_AMR1998.pdf

Ryan, J. (02 de 06 de 2014). The Uncertain Future: Privacy and Security in Cloud Computing. *Santa Clara Law Review, 54(2)*, pp. 497-525. Obtido em 02 de Fevereiro de 2015, de http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2778&context=lawreview

Sachdeva, K. (2011). *Cloud Computing: Security Risk Analysis and Recommendations.* Tese de Mestrado, Universidade do Texas. Obtido em 5 de Janeiro de 2015, de

http://repositories.lib.utexas.edu/bitstream/handle/2152/ETD-UT-2011-12-4592/SACHDEVA-THESIS.pdf?sequence=1

Saglam, O., & Milanova, V. (s.d.). How do qualitative and quantitative research differ? *Doctoral Seminar: Research Methodology.* Zurich. Obtido em 15 de Junho de 2015, de http://www.tim.ethz.ch/education/courses/courses_fs_2013/DocSem_Fall13/10_summary

Saleem, R. (2011). *Cloud Computing's Effect on Enterprises.* Dissertação de Mestrado, Lund University. Obtido em 25 de Setembro de 2013, de https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1764306&fileOId=1764311

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students.* England: Pearson Education Limited. Obtido em 13 de Fevereiro de 2015, de http://is.vsfs.cz/el/6410/leto2014/BA_BSeBM/um/Research_Methods_for_Business_Students__5th_Edition.pdf

Schneier, B. (18 de Janeiro de 2008). The Psychology of Security (Part 1). Obtido em 19 de Fevereiro de 2015, de https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

Segars, A. H., & Grover, V. (1993). Re-examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis. *MIS Quarterly, 17(4)*, pp. 517-525. Obtido em 20 de Abril de 2015, de http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCgQFjAAahUKEwjXzKGo6d_HAhUD7xQKHeMLDXQ&url=http%3A%2F%2Fmisq.org%2Fmisq%2Fdownloads%2Fdownload%2Feditorial%2F318%2F&usg=AFQjCNHw-iMbHzg7Y0d5sIn0TJYE4WvFuA&sig2=9XBO26DuU0EE

Shimba, F. (2010). *Cloud Computing: Strategies for Cloud Computing Adoption.* Dissertação de Mestrado, Instituto de Tecnologia de Dublin. Obtido em 02 de Dezembro de 2013, de http://arrow.dit.ie/cgi/viewcontent.cgi?article=1028&context=scschcomdis

Siegel, S. (1975). *Estatística não-paramétrica: para as ciências do comportamento.* São Paulo: McGraw-Hill do Brasil.

Singh, S., & Morley, C. (2009). Young Australians' privacy, security and trust in internet banking. *Australian Computer-Human Interaction Special Interest Group*, *21*, pp. 121-128. doi:10.1145/1738826.1738846

Spideroak. (2013). *State of Privacy Survey.* Survey, Spideroak. Obtido em 6 de Janeiro de 2014, de https://spideroak.com/static/v09.2013/pdf/SpiderOak-SOP-2013.pdf

Sungardas. (2014). *Adapting Security in the Cloud - How to create a secure cloud Architecture.* White Paper. Obtido em 25 de Abril de 2014, de http://www.sungardas.com/Documents/cloud-based-computing-adapting-cloud-security-CLD-WPS-072.pdf

Takai, T. M. (2012). *Cloud Computing Strategy.* White Paper, USA Department of Defense. Obtido em 14 de Janeiro de 2014, de http://www.disa.mil/Services/~/media/Files/DISA/Services/Cloud-Broker/dod-cloud-strategy.pdf?new

Techsoup. (2012). *The Cloud: 2012 Global Cloud Computing Survey Results.* Estudo. Obtido em 02 de Janeiro de 2014, de http://www.techsoupglobal.org/2012-global-cloud-computing-survey

The Verge. (17 de Julho de 2013). *NSA Spying Prism Surveillance Cheat Sheet*. Obtido em Dezembro20 de 2013, de The Verge: http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

theguardian. (15 de Junho de 2015). *EU states agree framework for pan-European data privacy rules*. (S. Gibbs, Editor) Obtido em 11 de Julho de 2015, de theguardian: http://www.theguardian.com/technology/2015/jun/15/eu-privacy-laws-data-regulations

Trope, R., & Hughes, S. J. (2011). Red Skies in the Morning - Professional Ethics at the Dawn of Cloud Computing. *William Mitchell Law Review*. Obtido em 01 de Maio de 2015, de http://open.wmitchell.edu/cgi/viewcontent.cgi?article=1438&context=wmlr

T-systems. (2010). *Security in the Cloud.* White Paper. Obtido em 05 de Setembro de 2013, de http://www.t-systems.nl/white-papers/download/143682_1/blobBinary/WhitePaper_Security-in-the-cloud-ps.pdf?ts_layoutId=392544

T-Systems. (2012). *Cloud Security.* T-Systems. Frankfurt: T-Systems International GmbH. Obtido em 02 de Janeiro de 2014, de http://www.t-systems.com/news-media/white-papers/761550_2/blobBinary/White-Paper_Cloud-Security.pdf

Turk, V. (3 de Abril de 2014). *Motherboard*. Obtido em 3 de Janeiro de 2015, de The EU Voted to Save Net Neutrality: http://motherboard.vice.com/read/the-eu-voted-to-save-net-neutrality

Van Eecke, P. (2009). *Cloud Computing Legal Issues.* DLA Piper Global Law Firm. Brussels: DLA Piper. Obtido em 13 de Abril de 2015, de http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=842

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (Janeiro de 2009). A Break in the Clouds: Towards a Cloud Definition. *ACM SIGCOMM Computer Communication Review, 39(1)*, pp. 50-55. doi:10.1145/1496091.1496100

Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the Technology Acceptance Model. *Information Systems Research, 11*, pp. 342-365.

Venkatesh, V. M. (Setembro de 2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Qarterly, 27(3)*, pp. 425-478. Obtido em 13 de Maio de 2015, de https://csdl-techreports.googlecode.com/svn/trunk/techreports/2005/05-06/doc/Venkatesh2003.pdf

Venkatesh, V., & Davis, F. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science, 46(2)*, pp. 186-204.

Vogl, R. (2000). *The EU - U.S. Privacy Controversy: A Question of Law or Governance?* Dissertação de Mestrado, Universidade de Stanford. Obtido em 19 de Maio de 2015, de http://law.stanford.edu/wp-content/uploads/2015/03/VoglRoland-tft2000.pdf

von Baum, F. (2012). *New Draft European Data Protection Regime.* M Law Group, Munique. Obtido em 15 de Maio de 2015, de http://mlawgroup.de/news/publications/pdf/2012_02_01-EU_data_protection.pdf

Wang, Y., & Lin, K.-J. (2008). Reputation-Oriented Trustworthy Computing in E-Commerce Environments. *Internet Computing, IEEEE, 12(4)*, pp. 55-59. Obtido em 5 de Outubro de 2014, de http://web.science.mq.edu.au/~yanwang/IEEE_IC_08.pdf

Webster, J., & Martocchio, J. J. (1992). Microcomputer Playfulness: Development of a Measure with Workplace Implications. *MIS Quarterly, 16(2)*. Obtido em 5 de Fevereiro de 2015, de http://www.jstor.org/stable/249576?seq=1#page_scan_tab_contents

Welman, C., Kruger, F., & Mitchell, B. (2005). *Research Methodology* (3ª ed.). Cidade do Cabo (África do Sul): Oxford University Press. doi:ISBN: 0195789016

Wiersma, W. (1995). *Research Methods in Education: An Introduction* (6ª ed.). Boston: Allyn and Bacon.

Wilfred, C., & Kemmis, S. (1988). Teoria Critica de la ensenanza. *Revista Española de Pedagogía*, pp. 200-204. Obtido de http://www.jstor.org/stable/23763322?seq=1#page_scan_tab_contents

Woods, A. (9 de Janeiro de 2014). *US Companies Look to Canadian Servers in Wake of NSA Spy Scandal*. Obtido em 5 de Fevereiro de 2014, de The Star:

http://www.thestar.com/news/canada/2014/01/09/us_companies_look_to_canadian_servers_in_wake_of_nsa_spy_scandal.html

Yesisey, M., Ozok, A., & & Salvendy, G. (2005). Perceived security determinants in E-commerce among Turkish university students. *Behavior & Information Technology, 24*, pp. 259-274.

Yu, X., & Wen, Q. (2010). A View about Cloud Data Security from Data Life Cycle. *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, (pp. 1-4). Wuhan. doi:10.1109/CISE.2010.5676895

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an Open Cloud Computing Architecture. *Government Information Quaterly, 28*, pp. 239-251. doi:10.1016/j.giq.2010.05.010

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28(3)*, pp. 583-592. doi:10.1016/j.future.2010.12.006

Anexos

Anexo I – Questionário

Este questionário é parte integrante de um trabalho de investigação do Mestrado em Assessoria e Administração, do Instituto Superior de Contabilidade e Administração do Porto, tendo como finalidade, a avaliação do conhecimento e perceções dos utilizadores, sobre a utilização dos recursos computacionais designados de computação em nuvem (*cloud computing*).

Computação em nuvem refere-se à utilização de recursos computacionais, que existem, não no computador pessoal (ou outros dispositivos, como telemóveis e *tablets*) do utilizador, mas, sim, nos computadores e servidores do fornecedor de serviços, aos quais acedemos através da internet. Claros exemplos são as redes sociais, como *Facebook* ou *Twitter* e serviços de armazenamento de dados, como *GoogleDrive*, *Onedrive* ou *Dropbox*. Ao utilizarmos estes serviços, as fotos, textos, documentos e todos os dados e informação que introduzimos, são processados e armazenados pelos recursos do fornecedor, aos quais acedemos e utilizamos através da internet. A facilidade de aceder, a qualquer momento e lugar, ao que um colega escreveu na sua página de *Facebook* ou aceder a um ficheiro *word* que guardamos *online*, é possível, porque tanto o *post*, como o documento, existem nos servidores do fornecedor de serviço e, é a estes que estamos a aceder quando abrimos a página de *Facebook* ou o documento.

Mesmo que não possua qualquer conhecimento sobre computação em nuvem, pode basear-se na sua utilização e conhecimento de algo, como *Facebook*, *Dropbox* ou *Office 360*, enquanto responde a este questionário.

Este questionário é anónimo, confidencial e as respostas serão utilizadas, exclusivamente, para fins científicos. As questões apresentadas não têm associadas respostas corretas ou incorretas, pretendendo-se apenas recolher opiniões sinceras.

O questionário está dividido em quatro partes:

parte I - Conhecimento, utilização e perceção da tecnologia.

parte II - Segurança e Privacidade.

parte III - Auto diagnóstico do seu conhecimento e opinião sobre a tecnologia.

parte IV - Informação pessoal.

Agradeço, desde já, a sua participação neste estudo, a qual, é indispensável para a concretização deste estudo.

José Filipe Macedo

Existem 23 perguntas neste inquérito

Parte I

Parte I – Nesta parte, é pedida a sua reflexão e opinião, sobre a tecnologia e utilização da mesma. Através da exemplificação de serviços e o fornecimento de situações concretas, espera-se avaliar a sua utilização e perceção desta tecnologia.

1 [1]1. Assinale o grau de confiança e conhecimento, que considera deter, sobre a utilização dos seguintes serviços proporcionados pela tecnologia de computação em nuvem: *

Por favor, seleccione uma resposta apropriada para cada item:

	Sei o que é e utilizo com muita frequência	Sei o que é e utilizo com frequência	Sei o que é e já utilizei pelo menos uma vez	Sei o que é mas nunca utilizei	Não sei o que é
Correio eletrónico (*Gmail, Outlook, Yahoo*, entre outros)	○	○	○	○	○
Navegador de internet (Internet Explorer, Firefox, Chrome, entre outros)	○	○	○	○	○
Conversação online (vídeo, voz ou texto, como Skype ou Hangouts, entre outros)	○	○	○	○	○
Fóruns ou grupos de discussão	○	○	○	○	○
Wikis (sítios de colaboração, como Wikipedia)	○	○	○	○	○
Blogues	○	○	○	○	○
Armazenamento online (Onedrive, Google Drive, Dropbox, entre outros)	○	○	○	○	○
Produtividade (Office 365, Google Docs, Limesurvey, entre outros)	○	○	○	○	○
Redes Sociais (Facebook, Youtube, Tumblr, Twitter, Google+, Linkedin, Instagram, Pinterest, Orkut, Snapchat, WhatsApp, entre outros)	○	○	○	○	○
Outras aplicações (meteorologia, notícias, entre outras)	○	○	○	○	○

2 [2]2. Em seguida, são mencionadas vantagens dos serviços possibilitados pela computação em nuvem. Segundo a sua experiência, indique o nível de importância que atribui a cada um. *

Por favor, seleccione uma resposta apropriada para cada item:

	Muito importante	Bastante importante	Importante	Pouco importante	Nada importante
Menores custos (menor compra de discos rígidos, cd, dvd, pen, entre outros, componentes físicos e programas)	○	○	○	○	○
Escalabilidade e elasticidade (poder adquirir, a qualquer momento, soluções de acordo com as suas reais necessidades. Adquirir e utilizar apenas aquilo que necessita)	○	○	○	○	○
Aumento de capacidades disponíveis (capacidade de fazer algo que, não lhe seria possível com apenas os seus próprios recursos)	○	○	○	○	○
Menor grau de conhecimento necessário (é mais fácil utilizar algo que é configurado e gerido pelo fornecedor do serviço)	○	○	○	○	○
Mobilidade (acesso em qualquer local)	○	○	○	○	○
Disponibilidade (acesso a qualquer momento)	○	○	○	○	○
Segurança de dados	○	○	○	○	○

3 [3]3. Que tipo de limitações considera preocupantes, relativamente à utilização desta tecnologia? *

Por favor, seleccione uma resposta apropriada para cada item:

	Muito preocupante	Bastante preocupante	Preocupante	Pouco preocupante	Nada preocupante
Custos não esperados (Por exemplo, a perda de acesso a dados e informação, por o fornecedor de serviços ter "fechado portas")	○	○	○	○	○
Segurança de dados	○	○	○	○	○
Privacidade de dados	○	○	○	○	○
Perda de controlo sobre dados e aplicações (por exemplo, problemas de direitos de autor sobre os seus dados e informação ou, ser incapaz de os eliminar completa e definitivamente)	○	○	○	○	○
Dependência de rede (acesso ao serviço e dados exigem uma ligação à internet de suficiente qualidade)	○	○	○	○	○
Disponibilidade (se o serviço e/ou dados estão sempre online e disponíveis)	○	○	○	○	○
Complexidade de adoção e utilização (criação de conta e subscrição de serviços, transferência de dados, politicas de utilização dos meus dados, entre outros fatores de aprendizagem)	○	○	○	○	○
Possibilidade de ficar dependente de um serviço ou fornecedor específico (capacidade de mudar, livremente, entre serviços e fornecedores, conseguindo transferir os seus dados e informação)	○	○	○	○	○
Questões legais e regulamentares	○	○	○	○	○
Integridade de dados (referente à manutenção de precisão e consistência de dados)	○	○	○	○	○
Possibilidade de perda de dados	○	○	○	○	○

4 [4]4. Em geral, qual o seu nível de confiança com: *

Por favor, seleccione uma resposta apropriada para cada item:

	Muito confiante	Bastante confiante	Confiante	Pouco confiante	Nada confiante
Tecnologia de computação em nuvem	○	○	○	○	○
Fornecedores de serviços (Dropbox, Facebook, Google, Microsoft, entre outros)	○	○	○	○	○

Parte II

Parte II - Nesta parte, é-lhe pedido que exprima a sua opinião sobre questões de segurança e privacidade, inerentes à tecnologia de computação em nuvem e que transitam para os serviços que nela se baseiam.

5 [5]5. Para cada uma das ideias seguintes, refira o seu nível de concordância: *

Por favor, seleccione uma resposta apropriada para cada item:

	Concordo totalmente	Concordo	Não concordo nem discordo	Discordo	Discordo totalmente
Questões de segurança são um problema que impedem a adoção de serviços baseados em computação em nuvem	○	○	○	○	○
Em geral, sinto-me mais confiante com a utilização de soluções proprietárias que correm e existem no meu dispositivo (computador pessoal, telemóvel e tablets)	○	○	○	○	○
Sinto que a tecnologia de computação na nuvem está pronta para salvaguardar os meus dados e informação mais importantes	○	○	○	○	○
Sinto que a computação em nuvem será mais segura no futuro	○	○	○	○	○

6 [6]6. Para cada uma das ideias seguintes, refira o seu nível de preocupação: *

Por favor, seleccione uma resposta apropriada para cada item:

	Absoluta preocupação	Muita preocupação	Nem preocupado nem despreocupado	Pouca preocupação	Nenhuma preocupação
A localização física dos meus dados não é conhecida, o que influencia, em geral, a legislação e a regulamentação a que estão sujeitos.	○	○	○	○	○
Problemas de programação ou fracos parâmetros de segurança, entre outros, podem colocar em risco a confidencialidade, integridade e disponibilidade dos meus dados e serviços.	○	○	○	○	○
Os recursos na nuvem, utilizados para armazenar os meus dados, executar e disponibilizar o serviço por mim utilizado, são partilhados entre utilizadores. Isto significa que os recursos na nuvem por mim utilizados e os meus próprios dados podem ser utilizados e implicados em ações menos éticas ou mesmo ilegais, por parte de terceiros.	○	○	○	○	○
Utilizadores não autorizados, como piratas, podem obter acesso ao meu dispositivo, através de falhas de configuração dos recursos ou de encriptação, entre outras.	○	○	○	○	○
Algo imprevisto, como um desastre natural num centro de dados do fornecedor de serviço, pode levar à perda definitiva dos meus dados.	○	○	○	○	○

7 [7]7. Quem pensa ser responsável pela segurança dos seus dados? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Eu próprio
- ○ O fornecedor de serviço
- ○ O governo
- ○ A legislação e regulamentação
- ○ As empresas privadas
- ○ Não sei
- ○ Outro

8 [8]8. Tendo em conta os seguintes acontecimentos, indique a probabilidade de utilizar serviços baseados na computação em nuvem. *

Por favor, seleccione uma resposta apropriada para cada item:

	Utilizo de certeza	Muito Provável	Sem impacto	Pouco provável	Nunca utilizarei
Várias agências de inteligência, como a NSA, acedem à base de dados de empresas de telecomunicações, fornecedores de internet e fornecedores de serviços de computação em nuvem, com o objetivo de aceder e monitorizar os dados e informação dos utilizadores.	○	○	○	○	○
A empresa Facebook manipulou o histórico de notícias de 689 003 utilizadores, removendo ou todas as mensagens negativas, ou todas as mensagens positivas, num estudo que comprovou que, as emoções são contagiáveis, induzindo um estado de maior felicidade ou depressão.	○	○	○	○	○

9 [9]9. Classifique cada uma das seguintes entidades, de acordo com o grau de ameaça à sua privacidade. *

Por favor, seleccione uma resposta apropriada para cada item:

	Ameaça total	Muita ameaça	Indiferente	Alguma ameaça	Ausência de ameaça
Governo	○	○	○	○	○
Empresas privadas	○	○	○	○	○
Entidades de publicidade	○	○	○	○	○
Piratas informáticos	○	○	○	○	○

10 [10]10. Que sentimento lhe provoca a venda dos seus dados pessoais pelos fornecedores de serviços (à semelhança do *Facebook*? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Fico escandalizado
- ○ Fico muito perturbado
- ○ Fico perturbado
- ○ Fico algo perturbado
- ○ Não me importo

11 [11]11. Quem pensa ser responsável pela proteção da sua privacidade *online*? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Eu próprio
- ○ O governo ou legislação
- ○ O fornecedor de serviços
- ○ Não sei
- ○ Outro

12 [12]12. Pensa que deveria ser necessária a sua concreta e especifica aprovação, antes de serem recolhidos e processados, quaisquer, tipo de dados pessoais? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sim, em todos os casos
- ○ Sim, no contexto de informação pessoal solicitada na internet
- ○ Sim, no caso de informação sensível? (como saúde, religião, preferências politicas ou sexuais)
- ○ Não
- ○ Não sei
- ○ Outro

13 [13]13. Em que circunstancias, se alguma, desejaria que os seus dados pessoais, armazenados e recolhidos por um serviço, fossem completamente apagados? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sempre que eu decida apagar
- ○ Sempre que mude de fornecedor de internet
- ○ Sempre que deixe de utilizar determinado serviço cloud
- ○ Nunca
- ○ Não sei

14 [14]14. Quão importante é para si ter os mesmos direitos e proteção dos seus dados pessoais, independentemente do país onde esses dados são processados? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Muito importante
- ○ Importante
- ○ Indiferente
- ○ Pouco importante
- ○ Nada importante

15 [15]15. Qual o nível de controlo que sente ter, sobre a informação e dados que divulgou e utiliza nos serviços baseados nesta tecnologia. *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Controlo total
- ○ Controlo elevado
- ○ Não sei
- ○ Controlo baixo
- ○ Nenhum controlo

16 [16]16. Quando tem intenções de utilizar um serviço, baseado nesta tecnologia, sente-se informado sobre as condições de compilação dos seus dados e futura utilização dos mesmos? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sim
- ○ Não
- ○ Não aplicável (ato espontâneo da minha parte, não li informação apresentada)
- ○ Não sei

Parte III

Parte III - Nesta parte, ser-lhe-á pedido um breve auto diagnóstico do seu conhecimento e opinião sobre a tecnologia.

17 [17]17. Como classificaria o seu conhecimento sobre computação em núvem? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Totalmente informado(a)
- ○ Muito informado(a)
- ○ Informado(a)
- ○ Pouco informado(a)
- ○ Nada informado(a)

18 [18]18. Há quanto tempo utiliza serviços de computação em nuvem? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Nunca utilizei
- ○ Menos de um ano
- ○ Menos de 3 anos
- ○ Menos de 5 anos
- ○ Mais de 5 anos

19 [19]19. Para cada uma das ideias seguintes, refira o seu nível de concordância. *

Por favor, seleccione uma resposta apropriada para cada item:

	Concordo totalmente	Concordo	Não concordo nem discordo	Discordo	Discordo totalmente
Divulgar informação pessoal é uma situação crescente da vida moderna	○	○	○	○	○
Para se poder utilizar produtos e serviços disponibilizados na nuvem é necessário divulgar informação pessoal	○	○	○	○	○
Para mim, divulgar informação pessoal, é um problema	○	○	○	○	○
Para mim, divulgar informação pessoal, em troca de serviços *online* grátis, é um problema	○	○	○	○	○
Sinto-me obrigado a divulgar dados privados na internet	○	○	○	○	○

Parte IV

Parte IV - Nesta última parte, é-lhe pedida alguma informação pessoal.

20 [20]20. Sexo *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Feminino
- ○ Masculino

21 [21]21. Idade *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Menos de 18 anos
- ○ Entre 18 e 23 anos
- ○ Entre 24 e 30 anos
- ○ Entre 31 e 40 anos
- ○ Entre 41 e 50 anos
- ○ Entre 51 e 60 anos
- ○ Mais de 60 anos

22 [22]22. Estudos Académicos *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Secundário (ou equivalente)
- ○ Bacharelato (ou equivalente)
- ○ Licenciatura (ou equivalente)
- ○ Pós-graduação ou formação especializada
- ○ Mestrado
- ○ Doutoramento
- ○ Pós-doutoramento
- ○ Outro

23 [23]23. Situação Profissional *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sem ocupação profissional
- ○ Estudante
- ○ Trabalhador-estudante
- ○ Trabalhador por conta de outrem
- ○ Trabalhador por conta própria
- ○ Desempregado
- ○ Outro

)brigado pela sua contribuição.

Apêndices