Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

As perceções e expectativas dos estudantes universitários sobre a *Internet of Things* (IoT)

Catarina Alexandra Ribeiro de Vasconcelos

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Gestão de Sistemas de Informação

Orientador:
Doutor Abílio Gaspar de Oliveira, Professor Auxiliar,
ISCTE-IUL

outubro, 2018

"O significado das coisas não está nas próprias coisas,
mas na nossa atitude em relação a elas."
Antoine de Saint-Exupéry

Agradecimentos

Este trabalho de investigação foi um grande desafio para mim e, desta forma, agradeço a todos aqueles que fizeram parte do mesmo.

Um agradecimento muito especial aos meus pais, a quem foram retiradas muitas horas da minha presença, que me apoiaram incondicionalmente e me incentivaram para continuar.

Os meus agradecimentos, ao orientador desta dissertação, o Professor Doutor Abílio Oliveira por todo o seu apoio, incentivo, disponibilidade e conhecimento transmitido, indispensáveis à concretização deste trabalho.

A todos os professores de Mestrado que contribuíram para a minha formação, conhecimento e crescimento para aplicar neste trabalho.

Andreia, Jorge e Nelson pelos momentos de partilha e união, amizade e paciência demonstrada para me suportar nos momentos mais difíceis. A caminhada foi intensa e cheia de aprendizagens. Por isso, hoje é dia de agradecer a cada um de vocês, por tudo o que tivemos juntos. Sem vocês eu não teria tido a mesma força de vontade, energia e motivação. Obrigada pelo vosso apoio, amigos!

A todos aqueles que contribuíram com as suas respostas no meu questionário e dispenderam algum do seu tempo com o mesmo.

Ao João, pela amizade em todos os momentos.

A todos que enumerei o meu sincero “Obrigada”.

Resumo

A *Internet of Things* (IoT) criará um mundo onde os objetos físicos serão integrados em redes de informação para fornecer serviços avançados e inteligentes aos seres humanos. A gestão de confiança desempenha um papel importante na IoT para a junção de dados confiáveis, serviços qualificados com reconhecimento de contexto e maior privacidade e segurança das informações do utilizador. Isso ajuda as pessoas a superar a incerteza e o risco e envolve a aceitação e o consumo do utilizador em serviços e aplicações de IoT (Yan *et al*., 2014).

A presente investigação tem como objetivos determinar e verificar as perceções e expectativas dos estudantes universitários sobre a IoT. No mesmo âmbito, pretende-se clarificar a confiança nesta tecnologia, riscos e ameaças, em que áreas é mais aplicada e com mais utilidade. Foram realizados dois estudos, divididos em duas fases, a primeira, de índole exploratória – onde foi utilizado o método de entrevistas para recolhermos dados, essenciais para o levantamento dos principais indicadores que envolvem a temática – a segunda, inferencial – onde foi desenvolvido um questionário, com base nos indicadores da primeira fase e na revisão de literatura, de acordo com os objetivos propostos.

Os resultados obtidos permitiram compreender que perceções e expectativas os estudantes universitários têm sobre a IoT, assim como se consideravam esta tecnologia confiável, se tinha riscos ou ameaças associadas, bem como áreas mais aplicada e com mais utilidade. Este trabalho contribuiu para que todos os estudantes entendam o que é esta tecnologia e o que ela pode trazer às suas vidas e à sociedade.

Palavras-Chave: *Internet of Things*; Perceções; Expectativas; Estudantes universitários; Vulnerabilidades; Tecnologia.

Abstract

The IoT will create a world where physical objects are integrated into information networks in order to provide advanced and intelligent services to humans. Trust management performs an important role in IoT for the fusion of reliable data, skilled services with context awareness, and greater privacy and security of user information. This helps people overcome their perceived uncertainty and risk and involves user acceptance and consumption in IoT services and applications (Yan *et al*., 2014).

The main goal of this research is to determine and verify the perceptions and expectations that college students have about the Internet of Things. In the same context, it is intended to clarify the trust in this technology, risks or threats, in which areas it is more applied and with more utility. This research integrates two studies, divided in two phases, the first one is exploratory - where the interview method was used to collect data, essential for the survey of the main indicators that involve the theme - the second, inferential - with a questionnaire, based on the indicators of the first phase and the literature review, according to the proposed objectives.

The results obtained allowed us to understand which perceptions and expectations collegue students have about IoT, as well as they considered this technology reliable, if it had associated risks or threats, as well as areas is more applied and more useful. This work has helped all students understand what this technology is and what it can bring to their lives and society.

Keywords: Internet of Things; Perceptions; Expectations; College students; Vulnerabilities; Technology.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas e Siglas

API – *Application Programming Interface*

DNS – *Domain Name System*

ERP – *Enterprise Resource Planning*

GPRS – *General Packet Radio Service*

GPS – *Global Positioning System*

IoT – *Internet of Things*

LTE – *Long Term Evolution*

M2M – *Machine to Machine*

NFC – *Near Field Communication*

OSI – *Open Systems Interconnection*

RFID – *Radio Frequency Identification*

SIoT – *Social Internet of Things*

SMS – *Short Message Service*

TCP/IP – *Transmission Control Protocol/Internet Protocol*

TIC – Tecnologias de Informação e Comunicação

UDP – *User Datagram Protocol*

WAP – *Wireless Application Protocol*

Capítulo 1 – Introdução

1.1. Enquadramento do tema

Este trabalho centra-se nas perceções e expectativas de estudantes universitários, na área de Ciências e Tecnologias de Informação, sobre a *Internet of Things* (IoT). Focamo-nos na problemática da adoção desta tecnologia avançada, vulnerabilidades e riscos que podem estar associados com o seu uso. Mediante esses fatores pretende-se averiguar o nível de confiança na utilização da IoT pelos estudantes universitários com ou sem experiência profissional.

A Internet é utilizada cada vez mais como um meio de comunicação por excelência. Com a crescente facilidade e acesso à comunicação virtual, nomeadamente através das redes sociais, constata-se que os relacionamentos entre as pessoas têm assumido novas formas de expressão e outros níveis de importância na sociedade. Para além da comunicação entre as pessoas, verifica-se também, cada vez mais, a possibilidade de qualquer objeto comunicar e ligar-se a outros objetos, com uma maneira única de identificação, em qualquer parte, com dispositivos ligados à Internet, sendo este o conceito essencial de *Internet of Things* (IoT).

A IoT vai criar um mundo onde os objetos físicos são perfeitamente integrados nas redes de informação, a fim de fornecer serviços avançados e inteligentes para os seres humanos. A gestão da confiança desempenha um papel importante na IoT para a fusão de dados confiáveis, serviços qualificados com consciência de contexto e maior privacidade e segurança da informação do utilizador. Isso ajuda as pessoas a superar as suas perceções de incerteza e risco e envolve a aceitação e o consumo dos utilizadores nos serviços e aplicações da IoT (Yan *et al.*, 2014).

1.2. Motivação e relevância do tema

A motivação para a escolha deste tema veio da curiosidade e do querer saber mais sobre a *Internet of Things* (IoT), assim como ter a perceção do que esta tecnologia avançada poderá vir a implicar na vida das pessoas e, em particular, dos estudantes universitários.

O tema desta investigação baseia-se em analisar as perceções e as expectativas que os estudantes universitários têm sobre a IoT e, do seu ponto de vista, qual o impacto que esta poderá ter nas suas vidas, e na sociedade.

A utilização cada vez maior da Internet, para os mais diversificados fins, levou a um crescimento muito grande dos dispositivos a ela conectados. Numa fase inicial, o crescimento das entidades conectadas fazia-se pelo aumento da utilização, mais humanos conectados resulta em mais computadores, logo em mais servidores (Coelho, 2017).

A revolução tecnológica dos dispositivos móveis, através dos *smartphones* e *tablets*, resultou num crescimento adicional do número de dispositivos, porque possibilitou também o crescimento entre o público que já usava a Internet nos computadores, ligando novos dispositivos (Coelho, 2017).

Atualmente, com a IoT é possível a ligação de todo o tipo de objetos na rede, originando um aumento exponencial de objetos conectados.

Até há pouco tempo, este era um conceito pouco divulgado através das organizações e de instituições internacionais, mas tal não invalidou que cada vez mais dispositivos se fossem ligando à rede. Segundo alguns relatórios de fabricantes em 2009 houve um aumento de dispositivos ligados à Internet do que pessoas (em 2010 havia um total de 12500 milhões de objetos conectados à Internet, quase o dobro da população mundial). A tendência global é que cada vez mais dispositivos estejam ligados em rede. Esses dispositivos cumprem funções distintas, tais como, monitorização, sensorização, aviso, interação ou distribuição do processamento.

Esta situação leva a que analistas, consultoras e fabricantes estejam de acordo: em 2020 o número de dispositivos conectados ultrapassará os 26000 milhões, com um crescimento exponencial (em 2009 o número de dispositivos conectados à rede era aproximadamente de 900 milhões). E isso representa uma fatia muito importante das receitas de Tecnologias de Informação e Comunicações já num futuro muito próximo (Coelho, 2017).

Os dispositivos conectados através da rede sem fios excedeu os 16 biliões em 2014, um incremento de 20% face ao ano de 2013. Com esta tendência, o número de dispositivos será mais do que o dobro do atual, com 40,9 biliões previstos para 2020. O crescimento entre os dias de hoje e o final desta década, virá de dispositivos, como os nós de sensores e acessórios (Press, 2014).

Segundo a organização Intel, a IoT é uma rede robusta de dispositivos, todos integrados com *software* e sensores que lhes permitem trocar e analisar dados. A IoT tem transformado a forma como vivemos ao longo de quase duas décadas, preparando o caminho para soluções recetivas, produtos inovadores, fabricação eficiente e, finalmente, novas maneiras (até há pouco incríveis) de fazer negócios.

A IoT representa uma solução com potencial para a melhoria da vida das pessoas. Além das trocas de dados entre máquinas, facilitando o acesso às informações, existe ainda a possibilidade da economia de energia, segurança, saúde, educação e outros aspetos do quotidiano. Um dos inúmeros exemplos disso mesmo é o *smartwatch*, que monitoriza a saúde e ainda está ligado a uma *cloud*.

Em indústrias e em empresas que se relacionam diretamente com o cliente final, sistemas intercomunicantes têm o poder de aumentar a produtividade, criar novas estratégias de produção e conhecer melhor o mercado. Esse conceito é chamado de *Smart Industries* ou Indústria 4.0 (Araujo, 2017).

1.3. Questões e objetivos de investigação

Partimos da questão inicial: Quais são as perceções e as expectativas que os estudantes universitários têm sobre a IoT?

Como função de investigação, pretende-se compreender como é que os estudantes universitários percecionam a IoT, que expectativas têm sobre a mesma, que confiança esta lhes desperta e que aplicações lhe associam.

Os objetivos desta pesquisa, a realizar com estudantes universitários, são os seguintes:

- Determinar as perceções dos estudantes universitários sobre a IoT
- Verificar as expectativas dos estudantes universitários face à IoT
- Analisar a confiança que os estudantes universitários têm na IoT
- Determinar os riscos e ameaças associados à IoT
- Verificar as principais áreas de aplicação da IoT
- Determinar as áreas em que a IoT é útil

1.4. Abordagem metodológica

O principal estudo a realizar será baseado num questionário, que desenvolveremos com base na revisão de literatura, levantamento concetual e nos resultados obtidos em entrevistas realizadas por nós, a especialistas na área da IoT, numa fase exploratória da investigação – a estudantes universitários com ou sem experiência profissional.

Esse questionário será composto por grupos de perguntas relativos a:

- Caracterização da amostra - questões que permitem definir algumas variáveis como a idade, o género, o tipo de curso, o ano, a instituição frequentada.
- Ideias ou pensamentos e sentimentos face à IoT e aos usos que pode ter.
- Conhecimentos sobre aplicações da IoT, necessidades, oportunidades e expectativas associadas à IoT – questões que incidem sobre as necessidades de uso desta tecnologia, os seus conhecimentos, ideias e expectativas sobre a mesma.
- Riscos e Ameaças que podem estar associados à IoT.
- Grau de confiança que se perspetiva com o uso da IoT.
- Importância da IoT na sociedade atual.

Os dados obtidos a partir do questionário serão analisados estatisticamente, com recurso ao *software* SPSS, e em conformidade com os objetivos traçados.

1.5. Estrutura e organização da dissertação

O presente trabalho está organizado em cinco capítulos que pretendem refletir as suas diferentes fases, até à sua conclusão.

O primeiro capítulo introduz o tema da investigação e objetivos da mesma, bem como uma breve descrição da estrutura do trabalho.

O segundo capítulo reflete o enquadramento teórico, designado por revisão da literatura.

O terceiro capítulo é dedicado à metodologia e análise de resultados utilizada no processo de recolha e tratamento de dados bem como os métodos de análise utilizados.

O quarto capítulo apresenta a discussão dos resultados obtidos, de acordo com a metodologia que se entendeu apropriada.

No quinto e último capítulo apresentam-se as conclusões deste estudo bem como as recomendações, limitações encontradas e sugestões para trabalhos futuros.

Capítulo 2 – Revisão de Literatura

2.1. A *Internet of Things* (IoT)

O termo "*Internet of Things*" foi mencionado há quase duas décadas, em 1999, pelos fundadores do Auto-ID Center da MIT, com menção especial a Kevin Ashton que o propôs, em primeiro lugar. O termo "Auto-ID" refere-se a qualquer classe de tecnologias de identificação usadas na indústria para automatizar, reduzir erros e aumentar a eficiência. Estas tecnologias incluem códigos de barras, cartões inteligentes, sensores, reconhecimento de voz e dados biométricos. Desde 2003 que a tecnologia Auto-ID principal foi a *Radio Frequency Identification* (RFID).

Kevin Ashton referiu que a IoT era definida como objetos conectados interoperáveis de identificação única com tecnologia de identificação por radiofrequência (RFID).

O objetivo do Auto-ID Labs é desenvolver uma rede, de modo a ligar computadores a objetos, incluindo tudo o que é necessário para criar uma Internet de Coisas, como *hardware* acessível (RFID e leitores), *software*, protocolos de rede e linguagens para descrever objetos de maneira a que os computadores possam comunicar e interligar com eles.

Há muitos anos que a tecnologia RFID tem sido utilizada em vários setores de atividade, tais como, logística, retalho, na área farmacêutica. Contudo, apenas desde 2010 que tem existido avanços a nível dos sensores inteligentes, comunicações sem fios e nas tecnologias de rede de sensores, pelo facto de cada vez mais existir a necessidade de "coisas" conectadas em rede com a IoT (Li *et al*., 2015).

2.2. Comunicações na IoT

Tradicionalmente, as comunicações de dados faziam-se pelas redes disponibilizadas pelos operadores de comunicação, fixos ou móveis, tais como, GPRS, 3G, 4G, *wi-fi* e rede de cobre ou fibra. Contudo, para uma adequada implementação de soluções IoT é necessário efetuar uma análise ao tipo de comunicação a adotar em termos de custo e disponibilidade de rede. Todavia, o desenvolvimento acelerado da IoT está a suscitar o advento de redes específicas, adequadas para este tipo de comunicações (Coelho, 2017).

Cada vez mais se verifica a necessidade das pessoas estarem sempre conectadas aos

diversos conjuntos de serviços disponíveis *online*, através dos mais diversos meios. Em muitos casos essa ligação é transparente, por exemplo através de *smartphones* quando se ligam a redes *wi-fi*, rede móvel 3G/4G/LTE do próprio operador, ou de um outro operador em *roaming*.

Se o nível de conectividade estivesse sempre disponível de forma direta para o uso de qualquer dispositivo remoto de IoT, os sensores e os próprios dispositivos não conseguiam incorporar tudo devido a certas restrições, tais como:

- Bateria – manter dispositivos ligados a uma rede de comunicações requer bateria ou uma ligação permanente à corrente. Se as comunicações forem frequentes, a capacidade necessária pode tornar a operação inviável.
- Custo – se o custo de manter o dispositivo ligado à rede for elevado, torna-se inviável financeiramente ligar muitos dispositivos para um determinado fim. Em qualquer negócio o benefício tem que suplantar o custo.
- Cobertura – em muitas situações, os sensores de IoT podem ser utilizados em que a cobertura da rede não é perfeita ou mesmo inexistente e, dessa forma também se pode tornar inacessível.

Para que as aplicações IoT possam comunicar é necessário haver conectividade através do protocolo de comunicações usado na Internet, o *Transmission Control Protocol/Internet Protocol*(TCP/IP), permitindo duas formas de comunicação:

- Baseada em TCP, um protocolo definido ao nível da camada de transporte do modelo *Open Systems Interconnection* (OSI), que se caracteriza pela eficiência no estabelecimento de comunicações *online*.
- Baseada em *User Datagram Protocol* (UDP), que é o protocolo mais simples definido ao nível da camada de transporte, que se caracteriza por não garantir a entrega dos pacotes de dados (não confiáveis). Desta forma, as aplicações é que têm que garantir a integridade da comunicação, mas em contrapartida beneficiam de menos latência na rede.

O TCP é um protocolo orientado à conexão, que lida com aspetos relacionados com controlo de fluxo, garantindo a correção de erros e a recuperação de pacotes que se percam na rede, em *full-duplex* (comunicação nos dois sentidos). O UDP não é orientado à conexão, dando às aplicações que o utilizam acesso ao envio de mensagens para os servidores (Coelho, 2017).

Deve-se sempre equacionar, consoante a solução pretendida, se é necessária uma conectividade absoluta (Coelho, 2017), sem presumir que as soluções de conectividade que estão disponíveis para aplicações IoT, são as que se utilizam normalmente na vida quotidiana nas comunicações na Internet. A nível da conectividade IoT já se avançou bastante no sentido de dar resposta às limitações que este tipo de comunicação implica.

2.3. Perceções sobre a IoT

Definir o que é a *Internet of Things* parece ser uma tarefa complexa, dado que podem existir diferentes perceções para a mesma. A Tabela 1 mostra possíveis perceções, segundo vários autores.

Tabela 1 – Perceções sobre a IoT definidas por diferentes autores

Autores	Conceito
ITU (2005)	*Internet of Things* engloba a ligação de objetos e dispositivos do quotidiano em todos os tipos de redes, por exemplo: intranets, redes *peer-to-peer*[1] e a Internet global.
Mattern e Floerkemeier (2010)	*Internet of Things* representa uma visão na qual a Internet se estende no mundo real através de objetos do quotidiano.
Tan e Wang (2010)	*Internet of Things* será a próxima geração da Internet, em que todos os objetos estarão conectados. Representa uma nova era da computação ubíqua.
Atzori et al. (2010)	*Internet of Things* é um novo paradigma que consiste na presença dos objetos e "coisas" inteligentes ao nosso redor – tais como etiquetas RFID, sensores, atuadores, telemóveis, que estarão prontos para interagir e cooperar uns com os outros com o fim de atingir um objetivo específico.
Koreshoff, Robertson e Leong (2013)	*Internet of Things* refere-se a uma visão mais ampla, na qual "coisas" são objetos, lugares, ambientes do quotidiano. Todas essas "coisas" estão interligadas umas às outras pela Internet.

Para Asplund (2016), as perceções gerais sobre a IoT estão associadas a todos os produtos do consumidor, tais como, automação nas casas e veículos conectados. Este autor adotou como definição da IoT, que a mesma inclui todos os tipos de dispositivos

[1] *Peer-to-Peer* – é uma rede que consiste em nós interconectados ("*peers*") partilharem recursos entre si sem o uso de um sistema centralizado (exemplo de um servidor).

ligados, sejam produtos de consumo, equipamentos médicos ou sistemas de controlo industrial.

Para se tentar resumir os diferentes conceitos desta temática, Atzori (2010) classifica as principais áreas de pesquisa, tipos de aplicação e oferece uma visão mais complexa da IoT. A Figura 1 é o exemplo disso, sendo a IoT compreendida como um paradigma computacional formado pela sobreposição de visões orientadas às coisas, à Internet e à semântica.

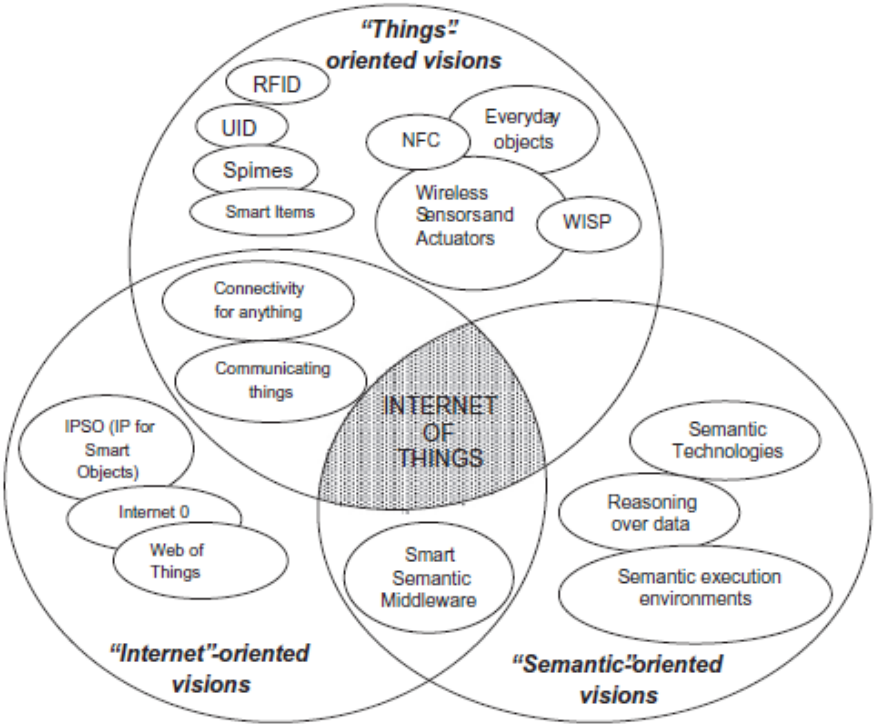


Figura 1 – Paradigma da Internet of Things (Atzori, 2010)

O problema da sobreposição das visões feita por Atzori é que ela inclui as tecnologias e parece preocupar-se pouco com os utilizadores dessas tecnologias. É possível que o autor imagine que questões relacionadas às interfaces ou ao *design* possam ser incluídas nas categorias de 'visão orientada às coisas", mas é mais difícil perceber a criação de padrões, legislação sobre a privacidade ou o direito à informação para que possam ser incluídas nessa mesma categoria. Ainda assim, a ideia de um paradigma computacional parece ser uma boa partida para a tecnologia em desenvolvimento.

Segundo Singer (2012), como definição operacional da IoT, esta, é considerada como um paradigma computacional com implicações profundas no relacionamento entre Homens e objetos. Uma definição que reúna diversos fatores, como a criação de uma rede

global, padronização e identidade dos objetos, é bastante ampla e delimita a IoT pelo o que ela faz: ligar objetos dotados da capacidade de agirem por conta própria, com ou sem supervisão humana.

Em suma, não existe uma única definição para o conceito *Internet of Things*, mas todas as que existem encaminham-se para o mesmo propósito.

2.4. Aplicações da *Internet of Things* (IoT)

O conceito de *Internet of Things*, com a sua visão de objetos conectados à Internet de várias formas, tem impulsionado o papel das Tecnologias de Informação e Comunicação (TIC), como facilitador da inovação numa variedade de mercados de aplicações.

Na Figura 2 é apresentada uma imagem ilustrativa das áreas onde pode ser aplicada a IoT.

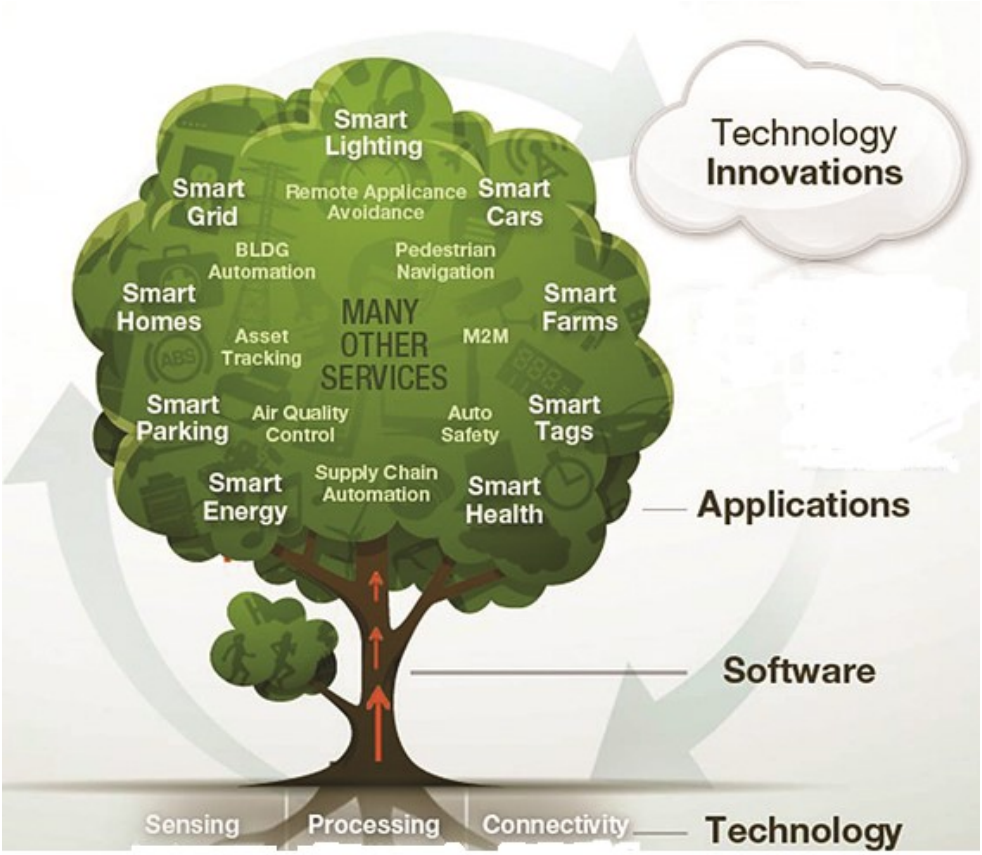


Figura 2 – Setores de atividade onde pode ser aplicada a IoT.[2]

[2] Fonte: Imagem retirada do endereço: http://itersnews.com/?attachment_id=58125

Para se atingir a inovação tecnológica nos mercados emergentes, começa-se na base pela tecnologia, que engloba sensores, processadores e conectividade de forma a que haja comunicação entre esses componentes. Seguidamente surge o *software* desenvolvido à medida das necessidades na tecnologia IoT e, consequentemente nas suas aplicações.

Os setores de atividade onde as soluções IoT podem oferecer vantagens competitivas em relação às soluções atualmente adotadas, no sentido de ajustar as suas estratégias e os seus modelos de negócio são:

- **Domótica** – Casas e edifícios inteligentes.

  Com o desenvolvimento das novas tecnologias, os edifícios com soluções IoT avançadas podem contribuir para a melhoria da eficiência energética, assim como contribuir para a melhoria do conforto e satisfação das populações, em particular no âmbito residencial e empresarial. O impacto traduz-se em termos económicos (redução dos custos operacionais) como ambientais (reduzindo as emissões poluentes inerentes aos edifícios, contribuindo assim para a redução de gases com efeito de estufa) e na sustentabilidade energética associada aos edíficios.

  Neste contexto, os sensores assumem um papel crucial e de base (cf. Figura 1), uma vez que permitem monitorizar o consumo de recursos, e na deteção das necessidades dos utilizadores. Tal cenário integra vários subsistemas diferentes e, portanto, requer um alto nível de padronização para assegurar a sua interoperabilidade. A capacidade de argumentar de forma distribuída e cooperativa também é necessária para garantir que as decisões tomadas sobre os recursos que estejam sob controlo (por exemplo, ligar/desligar a iluminação e aquecimento) satisfaçam as necessidades e expectativas dos utilizadores (Miorandi *et al.*, 2012).

- ***Smart cities*** – Cidades inteligentes, incluindo controlo de acessos, tráfego, pessoas e infraestruturas.

  O conceito de cidade inteligente (*smart city*) consiste numa visão de integração entre diversas tecnologias de informação, com o objetivo de gerir os ativos das cidades da forma mais inovadora possível (Coelho, 2017).

  Ao ser implementada uma infraestrutura de comunicação avançada e serviços inovadores numa cidade, é possível otimizar o uso de infraestruturas físicas da cidade (como por exemplo, redes rodoviárias e rede elétrica) mantendo a qualidade de vida para os seus habitantes.

As tecnologias de IoT podem encontrar uma série de aplicações diversas em cidades inteligentes, em que podem ser usadas para fornecer sistemas avançados de controlo de tráfego. Através da IoT, é possível monitorizar o tráfego de automóveis nas grandes cidades ou rodovias e implementar serviços que ofereçam rotas alternativas no sentido de evitar congestionamentos. Nesta perspectiva, os veículos devem ser entendidos como representando "objetos inteligentes". Além disso, o sistema de dispositivos de estacionamento inteligente, baseado em tecnologias RFID e sensores, permite a monitorização de lugares de estacionamento disponíveis e fornecem aos utilizadores opções de estacionamento de forma automática, melhorando assim a mobilidade na área urbana. Através de sensores pode também monitorizar-se o fluxo de tráfego de veículos nas rodovias e recuperar informações agregadas, como a velocidade média de circulação e o número de veículos. Ademais, os sensores com capacidade para detetar os níveis de poluição do ar, permitem recuperar informações de poluição atmosférica, como o nível de dióxido de carbono e partilhar essas informações às entidades de saúde (Miorandi *et al.*, 2012).

O controlo inteligente da iluminação pública é um fator importante para as autarquias, visto que esta é uma grande fonte de consumos energéticos, pelo que é pertinente encontrar soluções para uma gestão eficiente. Uma solução que ligue e desligue a iluminação automaticamente quando não é necessário ao utilizador (através do uso de sensores de movimento), ou que ative a iluminação quando fica escuro e a desligue quando amanhece ou quando está mau tempo (sensores de iluminação e de chuva, em vez de temporizadores) é algo de muito atrativo para entidades que tenham a seu cargo a gestão de iluminação pública (Coelho, 2017).

- ***Smart grids*** – Leitura automática dos contadores de eletricidade, água, gás e diversos serviços associados.

As redes inteligentes são redes elétricas que integram contadores inteligentes (que quantificam e partilham automaticamente a energia consumida às entidades comercializadoras), aparelhos domésticos inteligentes e infraestruturas de energias renováveis. Este conceito também se extendeu ao nível da distribuição do gás e da água (Coelho, 2017).

Este tipo de rede é concebida como uma rede elétrica capaz de fornecer energia de maneira controlada e inteligente, desde os pontos da sua geração até aos

consumidores finais, que são considerados parte integrante da rede, pois podem modificar os seus padrões de compra e comportamento de acordo com as informações recebidas, incentivos e desincentivos (Siano, 2014).

As *smart grids* têm várias funcionalidades desde a comunicação automática de leituras de contadores, aumento de potência, contabilização da produção local de energia (através de painéis solares e fontes renováveis) em que ao contabilizar a energia, o consumidor pode vender à rede e descontar essa energia fornecida na sua conta global.

- **Saúde** – Monitorização e alarmes de dispositivos médicos aplicados em doentes.

A medicina representa uma das áreas de aplicação promissora dos conceitos da IoT. Existem diversas aplicações que consistem na monitorização remota de pacientes em tempo real, a fim de reduzir as necessidades de hospitalização, melhorando assim a qualidade de vida do paciente e, ao mesmo tempo, reduzindo os custos de saúde. Outras aplicações estão relacionadas com a localização do paciente, por exemplo, pacientes afetados pela doença de Alzheimer (Miragliotta *et al*., 2012).

Os pacientes podem transportar sensores médicos para monitorizar diversos parâmetros, tais como, a temperatura corporal, a pressão arterial, a atividade respiratória. Outros sensores são usados para recolher dados para monitorizar as atividades dos pacientes nos seus ambientes quotidianos. Esta informação é agregada localmente e transfere para sistemas centrais médicos, que podem realizar monitorização remota avançada obtendo ações de resposta rápida sempre que seja necessário. A interligação de tais sensores heterogéneos pode fornecer uma visão abrangente dos parâmetros de saúde, desencadeando uma intervenção da equipa médica após a deteção de condições que possam levar à deterioração da saúde, realizando assim cuidados preventivos.

Outro setor de aplicação relevante relaciona-se com soluções pessoais de saúde e bem-estar. O uso de sensores portáteis aliados a aplicações adequadas, que funcionam em dispositivos informáticos pessoais, permite que as pessoas acompanhem as suas atividades diárias (passos dados, calorias queimadas, exercícios realizados), fornecendo sugestões para melhorar o seu estilo de vida e prevenir o aparecimento de problemas de saúde (Miorandi *et al.*, 2012).

- ***Fitness*** – Comunicação de *gadgets* de fitness (relógios, pulseiras, medidores) com sistemas centrais.

Há vários anos que existem dispositivos para fazer o controlo dos treinos, do exercício físico e dos parâmetros relevantes para o corpo, sendo o mais comum o do batimento cardíaco. Seguem-se alguns exemplos:

- Dispositivos de monitorização e registo de pulsação (pulseiras, bandas de peito, *t-shirts*), para controlo da forma, da sáude e do esforço;
- Dispositivos de monitorização de passos (caminhada, corrida);
- Dispositivos de monitorização de braçadas de natação;
- Relógios de esforço, para medir e registar o esforço em ginásio;
- Sensores de parâmetros biológicos diversos para registo das sessões de treino.

Para além da utilização lúdica, existe um potencial de utilização deste tipo de sistemas no desporto de alta competição, que utiliza meios cada vez mais sofisticados no sentido de melhorar os indicadores de performance (Coelho, 2017).

- **Retalho** – A susbtituição dos códigos de barras por *tags* ativas ou passivas.
- **Logística** – A utilização de dispositivos de IoT para localização, controlo de stocks, distribuição.

No retalho e na logística tornou-se importante o uso de identificadores para manter o controlo de todos os produtos. Após a generalização dos códigos de barras em todo o mundo, tem-se feito a substituição destes por tecnologias de RFID.

Assim, num mundo cada vez mais digital, ter um determinado artigo bem identificado e conectado a redes de comunicação, faz com que seja possível controlar melhor o processo de comercialização do mesmo, fornecendo intantaneamente a sua localização, com vantagens para fornecedores e clientes. Desta forma, facilita o controlo operacional de todo o processo e agiliza tarefas, ao nível de controlo de stocks e disponibilidade dos produtos (Coelho, 2017).

A tecnologia RFID e *Near-Field Comunication* (NFC) para controlo de processos logísticos são das tecnologias de comunicação mais poderosas para manter a eficiência das operações. Pelo facto de se saber a informação relativa aos

produtos em tempo útil faz com que todas as organizações intervenientes no processo possam responder mais rapidamente aos seus mercados e permitam um controlo de stock eficiente, trazendo assim vantagens competitivas para as organizações e clientes. Com este tipo de aplicações, o tempo de entrega do produto ao cliente final diminui e traz vantagens competitivas para as organizações (Atzori *et al*., 2010).

- **Agricultura** – Controlo de animais, controlo de colheitas, alarmística e monitorização variada.

A implementação de um sistema de medição e controlo do ambiente de produção numa estufa é um exemplo de aplicação de tecnologia IoT na agricultura. Os sinais críticos de temperatura, incisão e solo são recolhidos em tempo real no processo de produção agrícola, que pode ser transmitido através da tecnologia de comunicação de rede sem fios, através de *Machine to Machine* (M2M) como plataforma de suporte. Ao obter dados em tempo real do ambiente de produção agrícola pode usar-se os serviços de mensagens curtas (SMS), *web* ou o protocolo de aplicação sem fios (WAP), de modo a que o sistema central possa dominar as informações para a organização da produção (Zhao *et al*., 2010).

Os exemplos de utilização no setor agrícola, onde são aplicadas as novas tecnologias são:

- Controlo de Animais – obter informação em tempo real sobre a localização e a saúde dos animais;
- Monitorização de solos – na medição de temperatura e humidade;
- Controlo de regas – sistemas de regas otimizados de acordo com as condições climatéricas.

- **Indústria**

Desde o aparecimento da Internet, a interconexão entre computadores tornou-se uma realidade. A Internet móvel alcançou a comunicação e o contacto entre pessoas em grandes distâncias. Ambos mudaram a forma como as pessoas interagem, sendo que, a Internet e a Internet móvel rapidamente se infiltraram e influenciaram os sistemas industriais modernos. A estratégia da Indústria 4.0 consiste em fazer mais uso da Internet e da *Internet of Things* nas interações entre humanos e máquinas, permitindo a fabricação inteligente e a produção da quarta

revolução. Como a capacidade de computação e a capacidade de armazenamento de dispositivos móveis inteligentes aumentam, terminais móveis e aplicações móveis serão usados num futuro próximo para projetar, fabricar e gerir o processo de industrialização. As aplicações de terminais móveis inteligentes na indústria podem facilmente controlar e monitorizar processos inteligentes em fábricas (Zhou *et al*., 2016).

A IoT pode encontrar aplicações na indústria, por exemplo, gerir uma frota de carros numa organização. A IoT ajuda a monitorizar o seu desempenho ambiental, processar os dados para determinar e escolher o que precisa de manutenção (Khan *et al*., 2012).

O conceito de fábrica "inteligente" significa que é possível melhorar significativamente a produção e otimização dos recursos, reduzindo o ciclo de armazenamento e distribuição da produção (Wan *et al.*, 2015).

- **Ambiente** – Monitorização ambiental.

A tecnologia IoT pode ser inserida em aplicações de monitorização ambiental. Neste caso, o papel-chave é desempenhado pela capacidade de detetar, de forma distribuída, fenómenos e processos naturais, como por exemplo, temperatura, velocidade do vento, precipitação, altura dos rios, bem como integrar tais dados em aplicações globais. O processamento da informação em tempo real, juntamente com a capacidade de um grande número de dispositivos a comunicarem-se entre eles, fornece uma plataforma sólida para detetar e monitorizar anomalias que possam colocar em perigo a vida humana e animal. A vasta implementação de dispositivos pode permitir o acesso a áreas críticas, pelo que a presença de operadores humanos pode não representar uma opção viável (por exemplo, nas áreas vulcânicas, abismos oceânicos, áreas remotas), de onde a informação detetada pode ser comunicada a um ponto de decisão para detetar condições anómalas.

Nesta perspectiva, as tecnologias IoT podem permitir o desenvolvimento de uma nova geração de sistemas de monitorização e suporte à decisão, proporcionando capacidades em tempo real em relação às soluções atuais. Outro caso, em que a capacidade de deteção dos dispositivos IoT suporta a segurança ambiental é representada pela deteção de incêndio. Quando um conjunto de

sensores deteta a possível presença de fogo (por exemplo, através de sensores de temperatura), é gerado um alarme e enviado diretamente para entidades competentes, reduzindo o tempo de intervenção dos bombeiros (explorando os recursos de comunicação avançados da plataforma IoT), juntamente com outros parâmetros que são úteis na tomada de decisões e suporte, como a descrição da área sujeita ao fogo, a possível presença de pessoas e materiais inflamáveis. Claramente, a resposta rápida tem como objetivo salvaguardar as vidas humanas e respetivos bens.

Outros cenários relacionados com a proteção civil podem beneficiar com as tecnologias IoT (terramoto, tsunami), pelo que a capacidade de aceder a dados metereológicos em tempo real em áreas de grande escala possibilita a implementação de estratégias de coordenação eficientes entre as equipas de resgate, melhorando os mecanismos de prevenção de sinistros (Miorandi *et al.*, 2012).

- **Segurança** – Vigilância, alarmística, deteção de eventos.

A vigilância de forma a garantir a segurança de pessoas e bens tornou-se numa necessidade para edifícios empresariais, centros comerciais, fábricas, parques de estacionamento e muitos outros locais públicos. As tecnologias habilitadas para a IoT podem ser usadas para melhorar o desempenho das soluções atuais, fornecendo alternativas mais baratas e menos invasivas à implementação generalizada de câmaras, preservando ao mesmo tempo a privacidade dos utilizadores. Com a tecnologia IoT é possível criar sistemas de alerta rápidos e eficientes. A identificação pessoal por meio de tecnologia RFID ou tecnologias similares também é uma opção. Não obstante, é necessário adotar mecanismos e regulamentos para preservar a privacidade dos indivíduos. As tecnologias IoT podem oferecer alto nível de flexibilidade, capaz de lidar com políticas de acesso (por exemplo, para diferentes áreas de edifícios) que podem mudar ao longo do tempo devido a mudanças logísticas e/ou a mudanças no papel do utilizador e/ou de acordo com informações contextuais (por exemplo, algumas áreas não acessíveis num determinado dia devido a obras de renovação em curso). Também neste mercado, as vantagens são em termos de funcionalidades aprimoradas, com melhor aceitação do utilizador através da redução do uso de câmaras, custos

operacionais reduzidos e maior flexibilidade num ambiente em mudança (Miorandi *et al.*, 2012).

- **Localização** – De crianças, idosos, animais.

A implementação de sistemas de localização de pessoas e bens pode ser extremamente útil, no entanto, pode gerar questões de conflito, como perda de privacidade, pelo que é perentório criarem-se sistemas regulados.

Existe um conjunto de casos de interesse, quando se fala em localização de pessoas e bens:

- Localização de uma criança em tempo real, sabendo-se num sistema de informação reservado onde está;
- Localização de idosos, veículos, montanhistas, criminosos, animais de estimação.

Há várias estratégias de implementação de sistemas de localização. As mais eficazes consistem no recurso a sistemas GPS, combinadas com a localização através das redes móveis e redes *wi-fi* (sistemas de localização também disponível nos *smartphones*) (Coelho, 2017).

- **Aeronáutica** - Monitorização e controlo de manutenção de equipamentos, deteção de falhas em tempo real.

A utilização de aeronaves não tripuladas desenvolveu-se bastante nos últimos anos, quer a nível militar como civil. Existem variadas soluções de *drones* com diferentes tamanhos, capacidades e tecnologias de controlo. A mais habitual é aquela que usa rádio para controlo e monitorização. Associado à utilização dos *drones,* com a aplicação da tecnologia IoT surgem diversas aplicações, como gestão de tráfego e entrega de encomendas (Coelho, 2017).

Outra função que a *Internet of Things* pode ter é: ajudar a melhorar a segurança e a proteção de produtos e serviços, protegendo-os da falsificação. A indústria da aviação, por exemplo, pode estar ameaçada pelo problema de peças suspeitas não aprovadas (SUP). Uma SUP é uma peça de aeronave que não tem garantia de atender aos requisitos de uma peça de aeronave aprovada (por exemplo, falsificações, que não estão em conformidade com as restrições de qualidade rígidas da indústria da aviação). Assim, as SUPs violam seriamente os padrões de

segurança de uma aeronave. Mas com a IoT, usando etiquetas RFID ligadas a peças de aeronaves, pode trazer segurança e proteção às mesmas. Outra área de aplicação emergente que forma a base para redes de sensores é a monitorização da aeronave usando dispositivos inteligentes com capacidades de deteção disponíveis dentro e fora da cabine, conectados aos sistemas de monitorização da aeronave (Sundmaeker *et al*., 2010).

- ***Wearables*** – Roupa, sapatos, óculos inteligentes, pulseiras, relógios.

  Os acessórios inteligentes já entraram no mercado há alguns anos e já ganharam o seu espaço de utilidade para um conjunto de funções específicas.

  Os primeiros *wearables,* para programadores de *wearables,* foram realizados em Sao Francisco em março de 2014 e foram recebidos com grande entusiasmo, com mais de 1000 pessoas presentes num evento de três dias. Com a introdução do Google Glass, Epson Moverio (óculos inteligentes) Pebble e Fitbit (relógios inteligentes), os *wearables* certamente atraíram a atenção de muitos consumidores e organizações. Enquanto alguns destes *wearables* têm principalmente uma única função, como monitorização da saúde e exibição de mensagens, outros assumem a integração de múltiplas funções no mesmo dispositivo. O relógio BASIS (relógio inteligente) é um exemplo disso, pois tem várias funções, como de tempo, *fitness* e monitorização de saúde num único dispositivo. De acordo com um relatório de mercado publicado pela *Transparency Market Research*, "Mercado de Tecnologia *Wearable* - Cenário Global, Tendências, Análise da Indústria, Tamanho, Partilha e Previsão, 2012-2018", espera-se que o mercado global de tecnologia *wearable* cresça de 750 milhões de dólares em 2012 para 5,8 biliões de dólares em 2018, sendo que irá haver cada vez mais dispositivos deste tipo (Wei, 2014).

2.5. Segurança, Privacidade e Confiança na *Internet of Things* (IoT)

2.5.1. Segurança

Um dos principais desafios que deve ser superado de modo a assegurar uma boa integração da *Internet of Things* (IoT) no quotidiano é a segurança. As arquiteturas de IoT devem lidar com uma população estimada de biliões de objetos, que vão interagir entre eles e com outras entidades, como seres humanos ou realidades virtuais. Todas essas

interações devem ser garantidas de forma a proteger a informação e o fornecimento de serviços de todos os componentes relevantes e limitar o número de incidentes que podem afetar toda a IoT. No entanto, proteger a IoT é uma tarefa complexa e difícil. O número de situações de vulnerabilidades pode tornar-se assombroso, uma vez que a conectividade global ("aceder a qualquer um") e a acessibilidade ("acesso de qualquer maneira, a qualquer momento") são princípios fundamentais da IoT. As ameaças que podem afetar as entidades IoT são numerosas, como atributos que visam vários canais de comunicação, ameaças físicas, falha de serviços, construção de identidades (Roman *et al.,* 2013).

A complexidade inerente da IoT, onde múltiplas entidades heterogéneas localizadas em contextos diferentes podem trocar informações entre si, complica ainda mais o projeto e a implementação de mecanismos de segurança eficientes, interoperáveis e escaláveis.

A segurança desempenha assim um papel fundamental para proteger a IoT contra ataques e *malware* (Roman *et al.*, 2013). Tradicionalmente, a segurança significa criptografia, comunicação segura e garantias de privacidade. No entanto, a segurança na IoT abrange uma gama mais ampla de tarefas, incluindo a confidencialidade dos dados, disponibilidade de serviços, integridade, anti-*malware*, integridade da informação, proteção de privacidade, controlo de acessos (Keoh *et al.,* 2014).

O sucesso da IoT depende da padronização de segurança em vários níveis, o que proporciona interoperabilidade, compatibilidade, confiabilidade e eficácia segura das operações numa escala global (Li *et al.,* 2016).

Para enfrentar os desafios de segurança na IoT, analisaram-se os problemas de segurança na IoT com base numa arquitetura de quatro camadas (Li *et al.,* 2016).

Os serviços residem em diferentes camadas da IoT, tais como: camada de deteção, camada de rede, camada de serviços e camada de aplicação-interface. A aplicação baseada em serviços dependerá fortemente da arquitetura da IoT. A camada de deteção é integrada com componentes finais da IoT para detetar e adquirir a informação de dispositivos; A camada de rede é a infraestrutura para suportar ligações sem fios ou com fios entre as coisas; A camada de serviços é para fornecer e gerir serviços requeridos pelos utilizadores ou aplicações; A camada de aplicação-interface consiste em métodos de interação entre utilizadores ou aplicações.

2.5.2. Privacidade

Como referido anteriormente, a IoT pode ser aplicada em diferentes áreas, tais como: monitorização remota de pacientes, controlo de consumo de energia, controlo de tráfego, sistema de estacionamento inteligente, gestão de inventário, cadeia de produção, proteção civil. Para todas as áreas, os utilizadores exigem a proteção das suas informações pessoais relacionadas com os seus movimentos, hábitos e interações com outras pessoas. Todavia, a privacidade de cada indivíduo deve ser garantida (Sicari *et al.*, 2015).

Na literatura, encontram-se diferentes abordagens sobre a privacidade.

Evans e Eyers (2012) propõem uma etiquetagem de dados para gerir a privacidade na IoT, usando técnicas tiradas do controlo de fluxo de informações, os dados representam eventos de rede e podem ser marcados com várias propriedades de privacidade; essas *tags* permitem ao sistema argumentar sobre os fluxos de dados e preservar a privacidade dos indivíduos. A exploração de etiquetagem dentro de nós de sensores que sejam restritos a recursos pode não ser uma solução viável, porque as *tags* podem ser muito grandes em relação ao tamanho e sensibilidade dos dados e gerar uma sobrecarga excessiva. Desta forma e para este caso, não se adequa para a IoT.

Huang *et al.,* (2012) propõem um protocolo de controlo de acessos resguardado pela privacidade, em que o controlo é feito por utilizadores, com base em políticas de privacidade de anonimato compatíveis com o contexto em causa. Os mecanismos de proteção de privacidade são investigados, na medida em que os utilizadores podem controlar quais os dados pessoais que estão a ser recolhidos e acedidos, quem está a recolher e a aceder a esses dados, e quando isso acontece.

Cao *et al.*, (2011) apresentam um esquema de dados denominado CASTLE (*Continuously Anonymizing STreaming cLustEring*) que é baseado em *Cluster*[3] de modo a garantir o anonimato e as restrições no atraso dos fluxos de dados, aumentando assim as técnicas de preservação da privacidade, concebidos para conjuntos de dados estáticos e não para produtos contínuos, ilimitados e fluxos transitórios.

A abordagem seguinte consiste em dividir em duas categorias os mecanismos tradicionais de privacidade: acesso discricionário e acesso limitado. O primeiro aborda os

[3] *Cluster* - é um grupo de servidores e outros recursos que atuam como um único sistema e permitem uma alta disponibilidade e, em alguns casos, balanceamento de carga e processamento paralelo.

riscos mínimos de privacidade, a fim de evitar a divulgação ou a clonagem de dados confidenciais, enquanto que o outro visa limitar o acesso de segurança para evitar ataques maliciosos não autorizados (Yang & Fang, 2011).

Para Wang e Wen (2011) deve ser realizada uma análise ao risco da privacidade quando um nome de domínio estático é atribuído a um nó específico da IoT. Os autores propõem um DNS (*Domain Name System*) com proteção de privacidade para dispositivos inteligentes, que pode autenticar a identidade original dos utilizadores e rejeitar o acesso ao dispositivo inteligente quando for ilegal.

Alcaide *et al.*, (2013) apresentam um protocolo de autenticação anónima, totalmente descentralizado para as aplicações de IoT, destinado à preservação da privacidade. Essa proposta é baseada num sistema de credenciais onde diferentes visualizações da mesma credencial não podem ser vinculadas entre si, evitando assim que as chaves de geração sejam descobertas. O sistema define duas funções possíveis: os utilizadores, que representam os nós que originam a recolha dos dados e os dados, que são responsáveis por reunir os dados dos utilizadores autorizados. Os utilizadores podem autenticar-se anonimamente desde que comprovem possuir um acesso válido anónimo.

Outra das abordagens referidas é que a partir das técnicas de preservação de dados de privacidade e de *data mining*[4] minimiza-se a probabilidade da divulgação de dados sensíveis e a análise de conteúdo sensível. Para os autores, o problema de consciencialização da privacidade do utilizador é abordado, propondo um esquema de gestão de privacidade que permite ao utilizador estimar o risco de partilhar dados confidenciais. Também visam desenvolver um sistema de deteção de sensibilidade robusto, capaz de quantificar o conteúdo de privacidade da informação (Ukil *et al.*, 2014).

A avaliação dos requisitos da privacidade dos dados, fornecida por diferentes fontes, é referido por Sicari *et al.*, (2014) e define uma arquitetura em camadas para a IoT, a fim de estimar a qualidade dos dados e o nível de segurança e privacidade. Além disso, essa arquitetura define um dado para fornecer serviços, que integra dados de diferentes fontes, de acordo com as necessidades do cliente.

[4] *Data Mining* – é um processo de computação de modo a descobrir padrões em grandes conjuntos de dados, que envolvem métodos na interseção de sistemas de aprendizagem, estatística e bases de dados. (São aplicados métodos inteligentes para extrair padrões de dados)

Em suma, o requisito da privacidade na IoT é atualmente coberto, mas parcialmente e há um amplo espaço de questões de pesquisa a serem investigadas, referentes à necessidade de definir políticas de privacidade a partir de um modelo bem definido e o desenvolvimento correspondente, lidando com a escalabilidade e o ambiente dinâmico que caracteriza os cenários da IoT. Na verdade, a captura de requisitos de privacidade nos estágios iniciais é essencial para criar confiança suficiente e facilitar a adoção de novos sistemas de IoT.

2.5.3. Confiança

O conceito de confiança é usado em vários contextos e com diferentes significados. A confiança é um termo complexo no qual não existe consenso definitivo na literatura científica, embora a sua importância seja amplamente reconhecida. O problema principal com muitas abordagens para a definição de confiança é que não se presta ao estabelecimento de métricas e metodologias de avaliação. Além disso, a satisfação dos requisitos de confiança está estritamente relacionada com os problemas de gestão de identidade e controlo de acessos (Sicari *et al.*, 2015).

O protocolo de gestão de confiança para a IoT proposto por Bao e Chen (2012) é distribuído, baseado em encontros e em atividades. Ou seja, ao existirem dois nós que entram em contacto um com o outro ou envolvidos numa interação mútua podem avaliar-se diretamente e trocar a avaliação de confiança entre si. Os parâmetros de referência para a avaliação de confiança são: honestidade, cooperação e interesse da comunidade. Portanto, esse protocolo de gestão de confiança dinâmico é capaz de ajustar adequadamente a melhor configuração de parâmetros de confiança em resposta a ambientes em constante mudança de modo a maximizar o desempenho da aplicação.

Existe um foco importante na avaliação do nível de confiança por parte de entidades da IoT. Assume-se que a maioria dos objetos inteligentes são dispositivos humanos ou relacionados com os humanos, por isso são frequentemente expostos a áreas públicas e comunicam-se através de redes sem fio, estando vulneráveis a ataques maliciosos (Bao & Chen, 2012).

Os objetos inteligentes têm características heterogéneas e precisam de trabalhar e de cooperar em conjunto, no sentido de evitar quebrar a funcionalidade básica da IoT por meio de ataques relacionados com a confiança (Bao & Chen, 2012).

Uma abordagem semelhante para fornecer uma avaliação de confiabilidade é mencionada por Nitti *et al.,* (2012) na chamada *Social Internet of Things* (SIoT). Este paradigma decorre da integração dos conceitos de redes sociais na IoT, devido ao facto dos objetos pertencentes à infraestrutura da IoT serem capazes de estabelecer relações sociais de maneira autónoma em relação aos seus proprietários. O desafio abordado por estes autores é construir um mecanismo de confiança baseado em reputação para a SIoT, que pode efetivamente lidar com certos tipos de comportamentos maliciosos destinados a enganar outros nós, a fim de impulsionar o uso de serviços e a entrega de informações apenas para nós confiáveis.

A confiança é um conceito muito complicado que é influenciado por muitas propriedades mensuráveis e não mensuráveis. Está fortemente relacionado com a segurança, pois garantir a segurança de um sistema e a segurança do utilizador é uma necessidade de ganhar confiança. No entanto, a confiança é mais do que a segurança. Relaciona não apenas a segurança, mas também muitos outros fatores, tais como: bondade, força, confiabilidade, disponibilidade, habilidade ou outros caracteres de uma entidade. O termo "confiança" abrange um âmbito maior do que a segurança, por isso é mais complicado e difícil de estabelecer, garantir, manter, gerir a confiança do que a segurança (Yang *et al*., 2015).

2.6. Riscos e Ameaças na IoT

Existem diversos riscos associados à tecnologia IoT, sendo o mais grave o que tem consequências diretas em algo que também é uma das funcionalidades mais poderosas da tecnologia: a capacidade de controlar objetos físicos. Ter a capacidade de controlar remotamente qualquer tipo de sistema, seja industrial, centrais elétricas, componentes de veículos ou aeronaves tem riscos físicos para as pessoas e bens (Coelho, 2017).

Por outro lado, ao colocar na Internet meios e formas de como aceder remotamente a determinados dispositivos, leva a potenciais intrusões e roubo de dados de vários tipos, desde o acesso indevido a imagens e videos, credenciais, dados bancários.

Para Coelho (2017) existe um conjunto de riscos associados ao uso de IoT, sendo eles:

- Acesso a dados pessoais ou corporativos não autorizados, comprometendo a privacidade;
- Acesso a sistemas internos críticos, a partir de uma rede IoT comprometida;

- Intrusão em redes internas (domésticas ou empresariais) e a partir daí o roubo de identidade ou de dados privados;
- Acesso indevido ao controlo de objetos, incluindo sensores e atuadores, causando ações não pretendidas pelos donos do sistema;
- Alteração ou eliminação de dados;
- Ligação indevida de dispositivos não autorizados em rede;
- Inibição do funcionamento do sistema.

As ameaças na IoT estão geralmente associadas às vulnerabilidades de segurança, porque cada elemento na própria tecnologia IoT integra vários componentes para configurar um serviço específico. É difícil manter a segurança no ambiente IoT porque existem várias entidades envolvidas, como fornecedor de dispositivos, fornecedor de comunicação e rede, programador de serviços, programador de APIs, fornecedores de plataformas e proprietários de dados (Yang *et al*., 2015).

Quando se passa de redes empresariais para redes criadas a partir de uma mistura de dispositivos finais (dispositivos portáteis, dispositivos embutidos, sensores isolados), junto com computadores no centro de operações, enfrentam-se dois problemas de segurança: novos ataques que vão aparecendo e as antigas estratégias de defesa não são mais válidas. Sendo estas consideradas como ameaças emergentes (Asplund, 2016).

Capítulo 3 – Investigação Empírica

3.1. Apresentação da investigação

A presente investigação visa, principalmente, compreender como é que os estudantes universitários percecionam a IoT e que expectativas têm sobre esta tecnologia. Pretende-se saber também que importância os estudantes universitários atribuem à IoT e que aplicações lhe associam. Esta pesquisa engloba duas fases: a primeira é exploratória – onde utilizamos o método de entrevistas e o uso de uma ferramenta de *text mining*, como o Leximancer, para recolher os dados essenciais para o levantamento dos principais indicadores que envolvem a temática – e, a segunda, é inferencial – onde construimos e desenvolvemos um questionário, com os indicadores obtidos na primeira fase, de modo a analisarmos os objetivos específicos a responder.

3.2. Fase exploratória

3.2.1. Objetivos

Nesta primeira fase da presente investigação, foi realizado um estudo de índole mais qualitativa, tendo por base cinco entrevistas - seguindo um guião previamente elaborado (cf. Apêndice A), para se fazer um levantamento dos principais indicadores sobre a temática da *Internet of Things* (IoT). Pretendeu-se determinar as perceções e expectativas sobre a IoT, analisar a confiança na mesma, riscos e ameaças associadas, verificar as principais aplicações de IoT, vantagens e desvantagens, áreas em que a IoT é útil, assim como a importância na mesma na sociedade. Este levantamento de indicadores foi fundamental para a construção do questionário, na fase inferencial.

3.2.2. Entrevistas

As entrevistas são um método de recolha de dados qualitativo, devendo existir um planeamento prévio, cabendo ao investigador determinar quais as questões específicas a abordar, assim como, a escolha do entrevistado, o local, o modo e o momento para a sua realização (Belei *et al*., 2008).

A entrevista é considerada um modo de interação entre duas pessoas ou mais. Trata-se de uma conversa dirigida a um objetivo específico, que não é a satisfação da conversa

em si, mas obter a informação desejada para atingir esse mesmo objetivo (Fraser & Gondim, 2004).

Segundo Fraser e Gondim (2004), a entrevista como técnica de pesquisa qualitativa pode ter algumas vantagens, sendo elas:

- favorecer a relação intersubjetiva do entrevistador com o entrevistado, e, por meio das trocas verbais e não verbais que se estabelecem neste contexto de interação, permitir uma melhor compreensão dos significados, dos valores e das opiniões dos atores envolvidos a respeito de situações e vivências pessoais.
- flexibilização na condução do processo de pesquisa e na avaliação dos seus resultados, visto que o entrevistado tem um papel ativo na construção da interpretação do investigador. Esta é uma modalidade de triangulação (confiabilidade), pois, em vez do investigador tirar as suas próprias conclusões apenas da interpretação do que o entrevistado diz, ele concede a este último a oportunidade de legitimá-la. Este é um dos aspetos que caracteriza a entrevista como um texto negociado.

As entrevistas são importantes fontes de informação para a pesquisa qualitativa, porque os investigadores podem obter o entendimento pessoal e os sentimentos dos entrevistados em relação às questões colocadas através do processo de diálogo. O principal objetivo da pesquisa qualitativa é reunir uma compreensão profunda das questões (Tu, 2018).

Neste estudo foi usado o tipo de entrevista estruturada, que é um modelo representado por um guião de questões previamente estabelecidas (cf. Apêndice A), destacando as principais perguntas que deverão ser feitas a cada entrevistado. Ao utilizarmos esse modelo, desenvolveu-se uma entrevista mais uniforme para todos os entrevistados.

As entrevistas variaram quanto à sua duração, tendo durado em média entre 20 a 30 minutos. Foram realizadas presencialmente e em sala privada.

3.2.3. Método

3.2.3.1. Amostra

A amostra foi de conveniência, sendo constituída por cinco participantes de forma individual, um individuo do sexo feminino e quatro do sexo masculino, pertencentes e

não pertencentes ao ISCTE. A sua seleção obedeceu aos seguintes critérios: serem especialistas da área da IoT e a sua participação ser voluntária.

3.2.3.2. Guião de Entrevistas

Para a realização das entrevistas foi criado um guião (cf. Apêndice A). Nele estão todas as questões realizadas aos entrevistados, que foram aplicadas com alguma flexibilidade, pelo facto de deixar-se, tanto quanto possível, os entrevistados discorrerem sobre o assunto, mas a investigadora é que fazia as questões pela ordem pretendida. Os entrevistados foram informados sobre o objetivo do trabalho, assim como, que poderiam desistir em qualquer momento, se assim o desejassem, recordando-se que a sua participação era voluntária, e que as suas respostas seriam tratadas de forma anónima e confidencial, e somente no âmbito científico da investigação em curso.

Recordamos as principais questões abordadas no guião:

a) O que é para si a Internet of Things? Que perceções tem sobre a mesma? b) Que expectativas tem sobre a IoT? c) Que vantagens/desvantagens a IoT pode ter na sociedade? d) Que ameaças e riscos vislumbra com o uso da IoT? e) Na sua opinião qual a importância da IoT na sociedade? f) Na sua opinião quais são as áreas onde a IoT está mais implementada? g) Que atividades profissionais pensa que mais podem usufruir com a adoção da IoT?

3.2.3.3. Técnica de Análise de Dados

Os dados foram analisados através do Leximancer, um *software* de *text mining* utilizado para analisar o conteúdo de documentos textuais. Este levantamento de indicadores foi fundamental para a construção de um questionário, na fase seguinte.

3.2.4. Resultados

Com base na análise de contexto, distinguimos dois tipos de grupos. O primeiro grupo é chamado de perceções, que consiste na visão proveniente dos especialistas sobre o significado de *Internet of Things*. O segundo grupo atender às expectativas dos especialistas em IoT sobre essa tecnologia. Os dois grupos juntam-se quanto à

importância de ver que impacto a IoT pode ter na vida das pessoas e na sociedade em geral. Utilizamos o Leximancer para analisar as respostas dos entrevistados, de modo a processar o texto e encontrar todos os conceitos e temas possíveis. Em seguida, analisamos e removemos os que não são significativos para esses grupos.

3.2.4.1. Perceções sobre a IoT

A Figura 3 mostra o mapa conceitual elaborado pelo Leximancer, onde os temas são apresentados em círculos que agrupam conceitos. Verifica-se que os conceitos mais relevantes são os Dispositivos e IoT, seguidos de Internet, Dados, Áreas, Rede e Equipamento. Em destaque está o termo Dispositivos, que é um dos temas com mais conceitos associados. Os dispositivos estão conectados aos conceitos de Internet, dados, áreas, sensores e, estes, por sua vez, ao conceito rede. A esfera rede está ligada aos conceitos IoT e equipamento.

Pelo que a IoT é percepcionada como uma rede de equipamentos que, através de sensores, se conectam a dispositivos com ligação à Internet com o intuito de comunicarem entre si. Os dispositivos estão conectados à Internet, podendo identificar-se na rede através de sensores. Os dispositivos têm capacidade de recolher informações através de dados. Eles estão presentes em várias áreas. Os dispositivos podem ser controlados a partir de um único equipamento, desde que estejam ligados a uma rede.

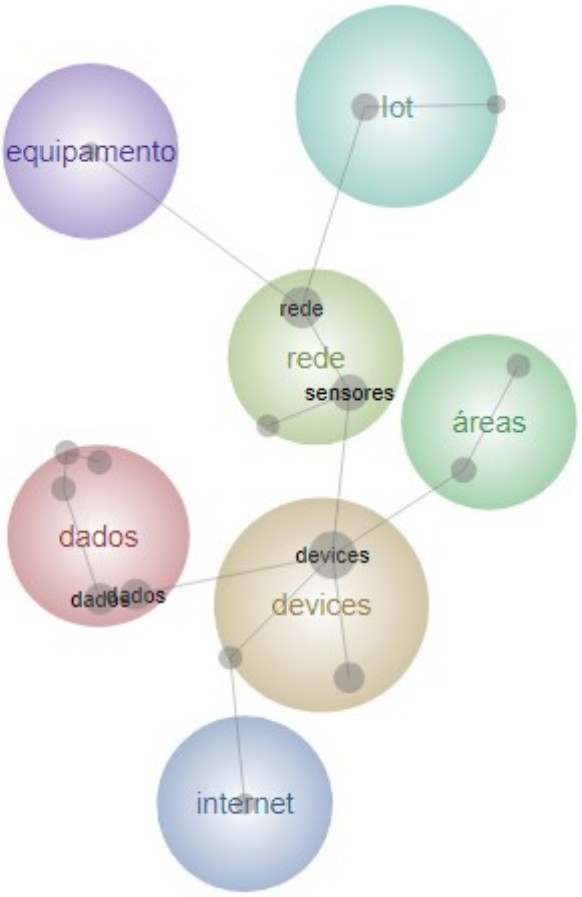


Figura 3 – Perceções sobre a IoT

3.2.4.2. Expectativas sobre a IoT

A Figura 4 mostra que as esferas nucleares se focam nos dispositivos, temas vida e tecnologia, seguido por casa, permite, coisas, interessantes. Em destaque está o termo dispositivos, como o maior tema pelo facto de ter mais conceitos associados. Dispositivos é um conceito que está ligado a problemas e, estes, por sua vez, à IoT. A esfera dispositivos interseta com a esfera vida, isso significa que elas estão interrelacionadas. Os dispositivos também estão conectados às pessoas, e, elas, por sua vez à casa. Os dispositivos estão conectados à tecnologia e à esfera permite. A tecnologia está ligada à esfera interessante que, por sua vez, se liga às coisas. Assim, as expectativas sobre a IoT são: os dispositivos são importantes porque podem permitir que as pessoas em casa tenham uma melhor qualidade de vida, usem a tecnologia para fazer coisas interessantes. Mas, por outro lado, a IoT pode ter problemas com esses dispositivos caso apresentem vulnerabilidades.

Figura 4 – Expectativas sobre a IoT

Foram elaborados outros gráficos no Leximancer referentes a outras questões realizadas nas entrevistas, que podem ser consultados no Apêndice A1. Mas foi dada mais importância às duas questões anteriores, pelo facto de abordarem as perceções e as expectativas que se tem sobre a *Internet of Things.*

No âmbito deste estudo exploratório, desenvolvemos um artigo (cf. Anexo 1) que foi aceite na Conferência **ICERI2018** *11th annual International Conference of Education, Research and Innovation* denominado *Perceptions and Expectations of college students about Internet of Things?* (Vasconcelos & Oliveira, 2018). [Aguarda Publicação - à data da entrega deste trabalho]

3.3. Fase Inferencial

3.3.1. Objetivos

Tendo em conta os resultados obtidos na fase exploratória, traçamos os seguintes objetivos:

- Determinar as perceções dos estudantes universitários sobre a IoT
- Verificar as expectativas dos estudantes universitários face à IoT

- Analisar a confiança que os estudantes universitários têm na IoT
- Determinar os riscos e ameaças associadas à IoT
- Verificar as principais áreas de aplicação da IoT
- Determinar as áreas em que a IoT é útil

3.3.2. Método

3.3.2.1. Amostra

A amostra foi aleatória, e a seleção dos participantes obedeceu aos seguintes critérios: a) ter idade igual ou superior a 17 anos; b) serem estudantes universitários; c) a participação ser voluntária e anónima. Contámos com 232 participantes, dos quais 82 (35.3%) são do género feminino e 150 (64.7%) do género masculino.

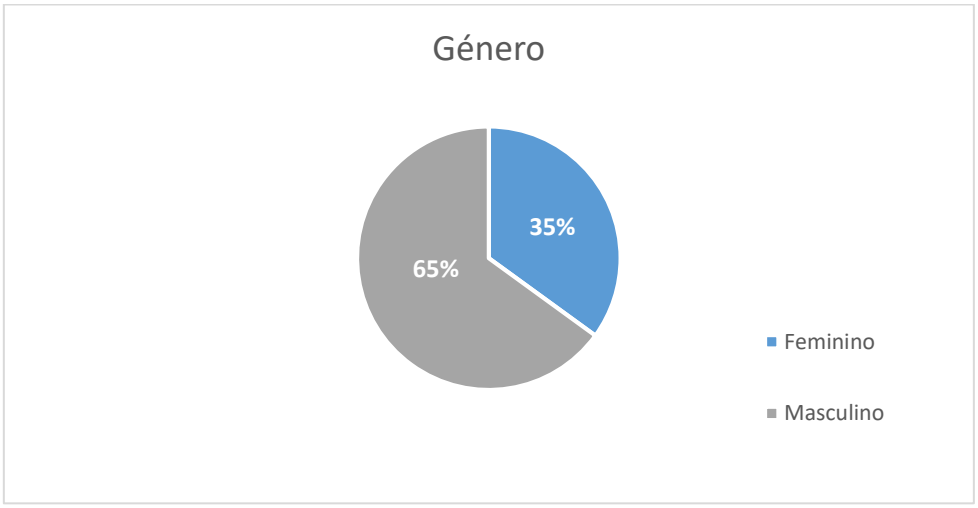


Figura 5 – Gráfico relativo ao género

A idade foi recodificada em quatro grupos. O grupo até aos 20 anos (N=39) representa 17% da população inquirida. O grupo que está entre os 20 e os 30 anos (N=124) representa mais de metade da população (53%). Dos 30 aos 40 anos (N=48) é o grupo de idades que representa 21% da população. O grupo que tem mais de 40 anos (N=21) representa 9% da população, sendo o menos frequente. Desta forma conclui-se que a maioria dos inquiridos neste estudo têm idades compreendidas entre 20 e 30 anos.

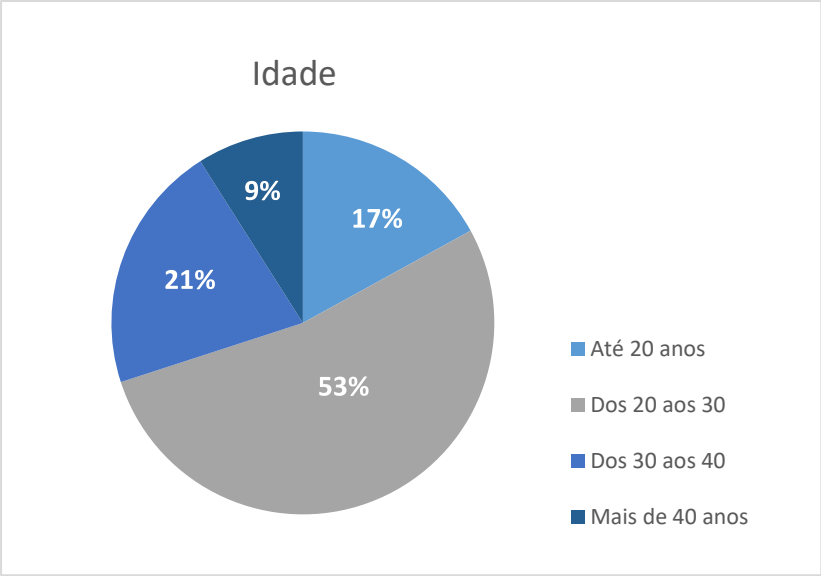


Figura 6 – Gráfico relativo à idade

O ano foi recodificado em quatro grupos. Através do gráfico abaixo, verifica-se que os participantes deste estudo (N=117) frequentam todos os anos escolares. Os estudantes do 1º ano (N=19) representam 16,2% da população inquirida. Alunos de 2º ano (N=51) representam 43,6% dos participantes inquiridos. Alunos de 3º ano (N=26) têm 22, 2% e para anos superiores ao 3º ano (N=21) representam 17,9% da população. Em resumo, o grupo de participantes que tem mais representatividade são estudantes do 2º ano.

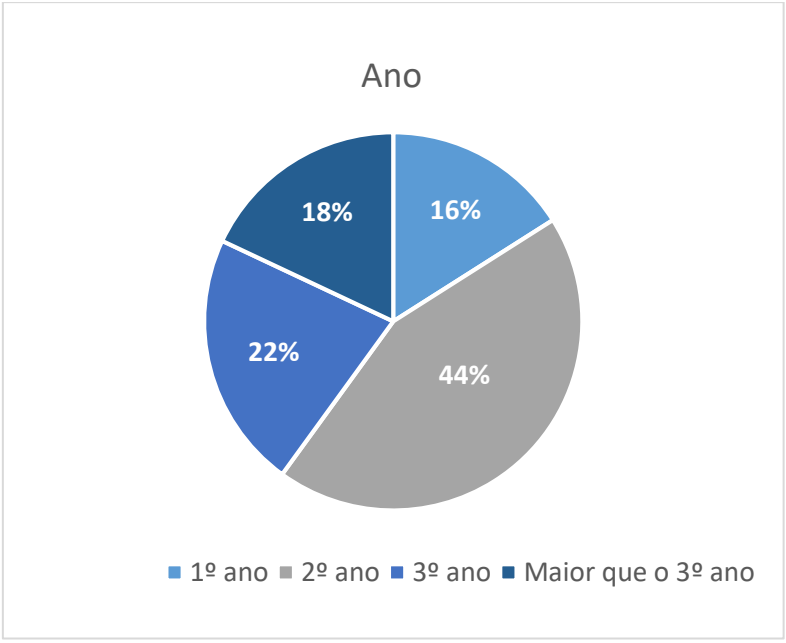


Figura 7 – Gráfico relativo ao ano frequentado

Em relação ao tipo de curso que os estudantes universitários frequentam (N=232), verifica-se o seguinte: na Licenciatura (N=106) estão 45,7% dos participantes, no Mestrado (N=94) estão 40,5% da população inquirida, o Doutoramento (N=22) é frequentado por 9,5% dos inquiridos e para o Tipo Outro (N=10) estão inseridos 4,3% dos participantes neste estudo.

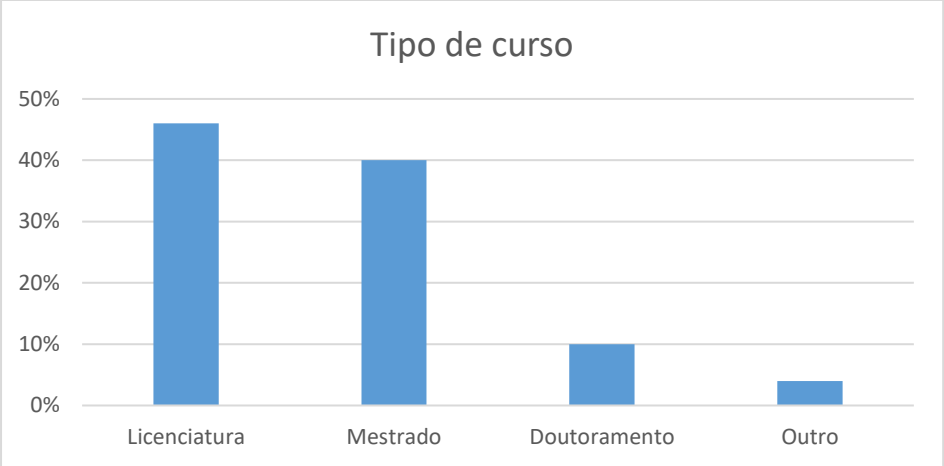


Figura 8 – Gráfico relativo ao tipo de curso

Em relação à Universidade/Instituição de Ensino Superior que os participantes deste estudo frequentam (N=117), pode constatar-se que a maioria (60%) dos inquiridos frequenta o ISCTE-Instituto Universitário de Lisboa, seguido de Outras (25%) - onde foram agrupadas as universidades com pouca adesão de estudantes, de seguida a Universidade de Lisboa (10%) e o Instituto Politécnico de Leiria com 5%.

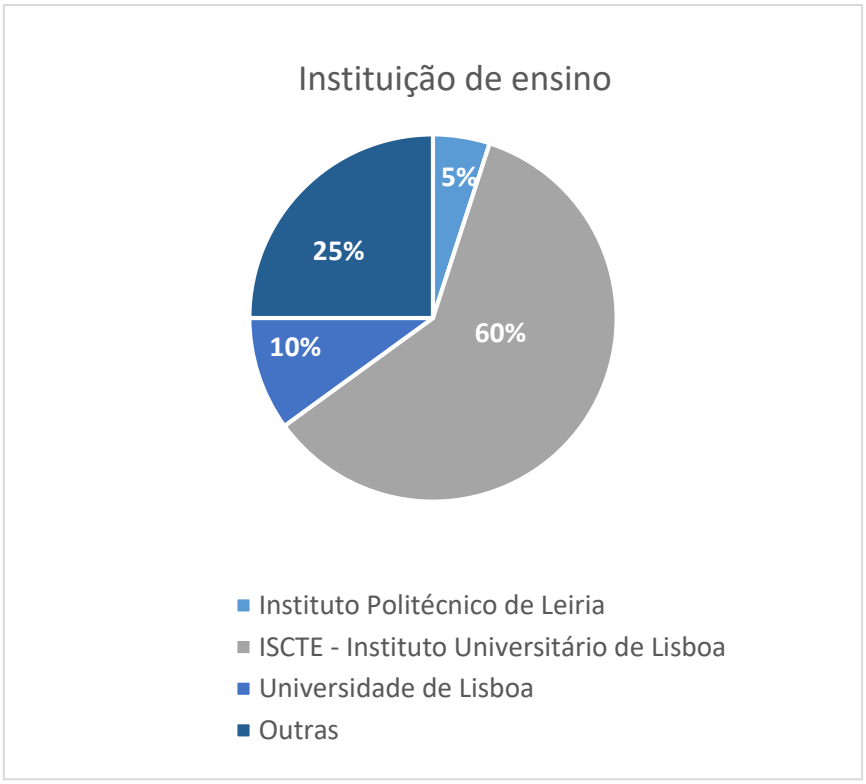


Figura 9 – Gráfico relativo à instituição de ensino

3.3.2.2. Questionário

O questionário foi elaborado através da plataforma *online* do Qualtrics, tendo este sido construído para divulgação via redes sociais, email e outros meios de comunicação para chegar a todos que fossem estudantes universitários. Na folha de apresentação, encontrava-se descrito o objetivo do estudo, as questões de ética, como a confidencialidade dos dados, a participação ter que ser voluntária, tendo os participantes sempre a possibilidade de desistirem do preenchimento se assim o pretendessem.

O questionário (cf. Apêndice B) teve duas partes, uma que corresponde aos dados sociodemográficos da população inquirida, onde se pretendeu recolher informações relativas à idade, ao género, ao curso, tipo de curso, ano e à instituição de ensino dos participantes. A segunda parte agrupou um conjunto de sete questões, sendo que a maioria eram constituídas por vários itens ou indicadores provenientes de resultados obtidos na fase exploratória. Estas questões estão de acordo com os objetivos de investigação, e podem resumir-se a: Indique o que significa para si a IoT; O que espera em relação à IoT; Até que ponto considera que a IoT é confiável; Até que ponto concorda com determinadas afirmações associadas à IoT; Quais as principais áreas de aplicação da IoT; Para que áreas

académicas/profissionais pode ser útil a IoT e Qual a importância que atribui à IoT na sociedade.

A maioria dos indicadores é acompanhada por uma escala de tipo Likert (5 pontos), de 1 (Nada confiável/Discordo totalmente) a 5 (Muito confiável/Concordo totalmente).

3.3.2.3. Técnicas de Análise de Dados

Foram utilizadas as seguintes técnicas no tratamento de dados:

a) Análises de estatística descritiva, através da frequência, média, desvio-padrão e percentagem de resposta;
b) Análises fatoriais em componentes principais (ACPs);
c) Análises de correlações, para verificar os tipos de associações entre as dimensões encontradas (que derivaram dos componentes, ou fatores, extraídos das ACPs e interpretados).

3.3.3. Resultados

Iremos de seguida interpretar os resultados obtidos, de acordo com cada um dos objetivos propostos:

3.3.3.1. Determinar as perceções dos estudantes universitários sobre a IoT

De modo a *determinar as perceções dos estudantes universitários sobre a Internet of Things(IoT)*, foram utilizados os dados recolhidos na pergunta sete da parte II do questionário (cf. Apêndice B). Nesta pergunta os estudantes classificaram em função da sua concordância, com uma escala de 1 (Discordo totalmente) a 5 (Concordo totalmente), uma série de afirmações relativas às perceções sobre a IoT.

Verificou-se que a maioria dos participantes concordou com grande parte das afirmações, destacando-se os itens Coisas a comunicarem com outras coisas (M[5]=4,21); Conjunto de dispositivos (sem serem computadores) ligados à Internet (M=4,13); Geração da informação através da comunicação entre objetos (M=4,00); Sensores a comunicarem com aplicações e sistemas (M=4,06); Sistemas de aparelhos que podem comunicar à distância-*online* (M=4,01); Variados objetos ligados (sem fio) à Internet e

[5] M= Média

entre si (M=4,01); Máquinas com inteligência e capacidade para comunicarem entre si (M=3,91); Captação e manipulação de dados em tempo real (M=3,89).

Com a intenção de averiguar as perceções relativas à IoT, realizou-se uma análise fatorial de componentes principais (ACP) com os itens da questão sete. Esta ACP permitiu-nos identificar as dimensões centrais nas perceções dos estudantes universitários sobre a IoT (Tabela 2). Foram identificados cinco componentes, que correspondem às dimensões: Dispositivos interligados, Rede de sensores, Máquinas inteligentes, Potencial e Autonomia.

O primeiro componente (36,7% de variância total explicada, com alfa de Cronbach $\alpha = 0,816$) agrupa os itens referentes aos dispositivos interligados.

O segundo componente (7,09% de variância total explicada, com alfa de Cronbach $\alpha = 0,825$) agrupa os itens que pertencem à rede de sensores.

O terceiro componente (6,01% de variância total explicada, com alfa de Cronbach $\alpha = 0,731$) agrupa os itens que se referem a máquinas inteligentes.

O quarto componente (4,79% de variância total explicada, com alfa de Cronbach $\alpha = 0,624$) agrupa os itens referentes ao potencial da *Internet of Things.*

O quinto componente (4,69% de variância total explicada, com alfa de Cronbach $\alpha = 0,524$) agrupa os itens referentes à autonomia da *Internet of Things.* Este componente podia não ter sido considerado, dado que o alfa é mais baixo.

Para verificar a consistência interna de cada um dos componentes obtidos, em cada ACP, realizaram-se testes de fiabilidade, para medir a consistência interna de cada componente, recorrendo ao indicador alfa de Cronbach – que varia entre 0 e 1, e quanto mais próximo de 1, maior é a consistência interna do componente considerado, isto é, mais forte é a associação entre os itens que o constituem.

Tabela 2 – ACP – Determinar as perceções sobre a IoT

	Componentes				
	Dispositivos interligados	Rede de sensores	Máquinas inteligentes	Poten-cial	Auto-nomia
Conjunto de dispositivos (sem ser computadores) ligados à Internet	,738	-,006	,116	-,038	-,003
Deriva da facilidade que existe em ligar-se algo à internet	,672	,146	,010	,281	-,115

	Componentes				
	Dispositivos interligados	Rede de sensores	Máquinas inteligentes	Poten-cial	Auto-nomia
Geração de informação, através da comunicação entre objetos	,619	,298	,123	,204	,277
Forma de comunicar e transferir dados sem intervenção humana	,580	,393	,017	,138	,190
Coisas a comunicarem com outras coisas	,563	,394	,078	,040	,366
Forma de interação de sistemas que vai além do que temos nos computadores	,527	,345	,401	,296	-,022
Identificação única de objetos	,500	,233	,316	-,168	,050
Sensores a comunicarem com aplicações e sistemas	,302	,774	,164	,262	,223
Redes (inteligentes, de robots, wireless, sensores sem fio)	,160	,704	,221	,292	,094
Tem origem na ubiquidade da internet (ou estar ao mesmo tempo em todos os lugares)	,177	,685	,255	-,038	,165
Sistema de aparelhos que podem comunicar à distância, online	,454	,579	,139	,281	,018
Objetos inteligentes	,151	,396	,680	,204	,054
Machine learning (sistema capaz de analisar grandes quantidades de dados, e encontrar ou gerar padrões específicos)	,048	,095	,662	,138	-,021
Máquinas com inteligência e capacidade para comunicarem entre si	,143	,260	,646	,040	,362
Indústria 4.0 (4ª revolução industrial)	,171	-,053	,588	,296	,460
Sistema virtual baseado em protocolos de comunicação padronizados	,267	,368	,410	-,168	-,223
Não há limites, consegue-se fazer quase tudo	,300	,067	,255	,735	,154
Tudo o que se relaciona com computação pode ser aplicado em coisas	-,008	,432	,101	,665	,209
Autonomia de sistemas (reduzida necessidade de seres humanos)	,023	,170	,064	,147	,824
Captação e manipulação de dados em tempo real	,441	,250	,183	,142	,468
Valores próprios	8,447	1,631	1,383	1,103	1,080
Variância explicada (%)	36,72	7,091	6,014	4,795	4,695
Percentagem acumulada	36,72	43,81	49,83	54,62	59,32
Alfa de Cronbach (α)	0,816	0,825	0,731	0,624	0,524

Nota: Resultado da ACP: matriz após rotação varimax, com normalização Kaiser, convergente em 11 iterações. Medida KMO =0,836; Teste de Bartlett = 982,497; Significância = 0,000

3.3.3.2. Verificar as expectativas dos estudantes universitários face à IoT

De forma a responder ao segundo objetivo*, verificar as expectativas dos estudantes universitários face à IoT,* foram utilizados os dados recolhidos na pergunta oito da parte II do questionário (cf. Apêndice B). Nesta pergunta os estudantes classificaram em função da sua concordância, com uma escala de 1 (Discordo totalmente) a 5 (Concordo totalmente), uma série de afirmações relativas às expectativas perante a IoT.

Verificou-se que a maioria dos participantes concordou com grande parte das afirmações, destacando-se os itens Evolução e Inovação Tecnológica (M=4,26); Utilidade (M=4,22); Automação de certas atividades diárias (p.e., tarefas rotineiras no trabalho e em casa) com M=4,17; Fácil acesso e controlo à distância (p.e., através de um telemóvel) a várias coisas, sistemas ou dispositivos (M=4,17); É um mundo de oportunidades, onde muitas coisas se podem explorar (M=4,16); Poupança de tempo na realização de certas tarefas (p. e., controlo de temperatura, eletrodomésticos ligarem-se automaticamente e o trabalho estar feito quando a pessoa chega a casa) com M=4,15; Facilitação do uso de equipamentos (p.e., frigoríficos autorregulados, aspiradores autónomos, dispensadores de ração para animais, controlar um candeeiro por telemóvel, abrir e fechar janelas automaticamente) com M=4,17 e Facilitação na obtenção de vários dados (tráfego, dados meteorológicos, validação de bilhetes dos transportes públicos) também com média de 4,15.

Para averiguar as expectativas relativas à IoT, realizou-se uma análise fatorial de componentes principais (ACP) com os itens desta questão. Esta ACP permitiu-nos identificar as dimensões centrais das expectativas dos estudantes universitários sobre a IoT (Tabela 3). Foram identificados seis componentes, que correspondem às dimensões: Facilidade Tecnológica, Oportunidades, Privacidade e Segurança, Confiabilidade, Usabilidade e Comunicação.

O primeiro componente (31,3% de variância total explicada, com alfa de Cronbach $\alpha = 0,913$) agrupa os itens referentes à Facilidade Tecnológica.

O segundo componente (8,86 % de variância total explicada, com alfa de Cronbach $\alpha = 0,505$) agrupa os itens que pertencem às Oportunidades.

O terceiro componente (8,39 % de variância total explicada, com alfa de Cronbach $\alpha = 0,771$) agrupa os itens que se referem à Privacidade e Segurança.

O quarto componente (6,90 % de variância total explicada, com alfa de Cronbach $\alpha = 0,689$) agrupa os itens referentes à Confiabilidade.

O quinto componente (4,89 % de variância total explicada, com alfa de Cronbach $\alpha = 0,773$) agrupa os itens referentes à Usabilidade.

O sexto componente (4,38 % de variância total explicada, com alfa de Cronbach $\alpha = 0,574$) agrupa os itens referentes à Comunicação.

Tabela 3 – ACP – Expectativas face à IoT

	Componentes					
	Facilidade Tecnológica	Oportu-nidades	Privacidade e Segurança	Confia-bilidade	Usabi-lidade	Comu-nicação
Fácil acesso e controlo à distância (p.e., através de um telemóvel) a várias coisas, sistemas ou dispositivos	,748	-,101	,109	-,018	,076	,221
Poupança de tempo na realização de certas tarefas (p. e., controlo de temperatura, eletrodomésticos ligarem-se automaticamente e o trabalho estar feito quando a pessoa chega a casa)	,746	-,030	-,069	,201	-,035	,004
Facilitação do uso de equipamentos (p.e., frigoríficos autorregulados, aspiradores autónomos, dispensadores de ração para animais, controlar um candeeiro por telemóvel, abrir e fechar janelas automaticamente)	,724	,079	,013	,000	,151	,239
Evolução e inovação tecnológica	,701	,331	,078	,048	,078	-,058
Novas formas de interação humano-máquina (p.e., mais interfaces tácteis e sistemas de realidade aumentada)	,673	,149	,074	,097	,060	,346
Usar a tecnologia para melhorar o desempenho e garantir melhores resultados	,645	,352	-,192	,065	,136	,199
Automação de certas atividades diárias (p.e., tarefas rotineiras no trabalho e em casa)	,639	,143	,077	,011	,273	-,161
Facilitação na obtenção de vários dados (tráfego, dados meteorológicos, validação de bilhetes dos transportes públicos)	,639	,113	,169	,150	-,028	,163

	Componentes					
	Facilidade Tecnológica	Oportu-nidades	Privacidade e Segurança	Confia-bilidade	Usabi-lidade	Comu-nicação
Maior eficiência dos processos	,636	,468	-,041	,127	,146	,133
Redução do tempo e custos energéticos	,624	,104	-,084	,354	,014	-,151
É um mundo de oportunidades,onde muitas coisas se podem explorar	,622	,523	,061	-,062	,160	-,042
Utilidade	,613	,440	-,080	,138	,140	-,062
Maior responsabilidade no uso da tecnologia	,229	,644	,215	,300	-,077	,062
Gerar mais/novos empregos	,108	,628	-,092	,040	,087	,275
Impactos e vulnerabilidades de segurança	,119	,113	,876	-,081	,037	-,042
Invasão de privacidade	,134	-,010	,871	-,026	-,017	-,187
Perda da identidade e da individualidade	-,212	-,109	,705	,201	,035	,311
Libertar o ser humano para a capacidade de raciocínio, abstração e inteligência	,022	,146	,014	,774	,154	,046
Tecnologia confiável	,208	-,048	,033	,735	,161	,209
Tecnologia aliada do ser humano	,239	,485	,005	,600	,006	,047
Ajudar a alcançar o bem-estar com aplicações de vestuário e de refeições inteligentes	-,027	,156	,039	,098	,866	,079
Aplicações móveis de controlo (p.e., de sono, nutrição, peso)	,251	,038	-,033	,205	,777	,010
Aumento da inteligência artificial (com máquinas inteligentes)	,449	-,192	,069	,004	,588	,324
Acesso rápido à informação	,190	,163	,011	,043	,235	,714
Ter uma conetividade segura, fiável e abrangente	,117	,208	-,094	,422	-,072	,655
Valores próprios	7,828	2,216	2,099	1,727	1,224	1,097
Variância explicada (%)	31,31	8,866	8,395	6,907	4,898	4,387
Percentagem acumulada	31,31	40,17	48,57	55,47	60,37	64,76
Alfa de Cronbach (α)	0,913	0,505	0,771	0,689	0,773	0,574
Nota: Resultado da ACP: matriz após rotação Varimax, com normalização Kaiser, convergente em 7 iterações. Medida KMO=0,838; Teste de Bartlett=1356,777; Significância = 0,000						

3.3.3.3. Analisar a confiança que os estudantes universitários têm na IoT

De forma a responder ao terceiro objetivo*, analisar a confiança que os estudantes universitários têm na IoT,* foram utilizados os dados recolhidos na pergunta nove da parte II do questionário (cf. Apêndice B). Nesta pergunta os estudantes classificaram em função da sua confiança, com uma escala de 1 (Nada Confiável) a 5 (Muito Confiável), uma série de afirmações relativas à confiança na IoT.

Neste caso, os participantes classificaram as afirmações como sendo moderadamente confiáveis, porque a média é superior ao valor 3 (Indiferente), mas não chega efetivamente ao 4 (Confiável), dando destaque sobretudo nos itens: Usabilidade (M=3,91); Complexidade da tecnologia (M=3,77); Gestão dos sistemas de informação envolvidos (M=3,67); Domínio dos equipamentos conectados (M=3,64); Localização geográfica (M=3,62) e Disponibilidade dos dados (M=3,58). De referir também, que os participantes consideraram pouco confiável a privacidade dos dados (M=2,68) e a confidencialidade dos dados (M=2,84).

Realizou-se também uma ACP, com os itens da questão nove, para identificar as dimensões centrais da confiança dos estudantes universitários face à IoT (Tabela 4). Foram identificados quatro componentes, que correspondem às dimensões: Conformidade, Segurança, Fiabilidade e Complexidade.

O primeiro componente (34,5 % de variância total explicada, com alfa de Cronbach $\alpha = 0,807$) agrupa os itens referentes à Conformidade.

O segundo componente (10,3 % de variância total explicada, com alfa de Cronbach $\alpha = 0,786$) agrupa os itens que pertencem à Segurança.

O terceiro componente (10,1 % de variância total explicada, com alfa de Cronbach $\alpha = 0,679$) agrupa os itens que se referem à Fiabilidade.

O quarto componente (7,36 % de variância total explicada, com alfa de Cronbach $\alpha = 0,647$) agrupa os itens referentes à Complexidade.

Tabela 4 – ACP – Confiança na IoT

	Componentes			
	Conformidade	Segurança	Fiabilidade	Complexidade
Auditorias	,782	,152	,037	,146
Ambiente (dependência em relação a condições ambientais)	,719	,101	,102	,072
As coisas funcionarem conforme o previsto	,700	,289	,033	,176
Autenticação em aplicações	,666	,248	,217	,281
Gestão dos sistemas de informação envolvidos	,649	,076	,247	,016
Privacidade dos dados	,137	,911	-,014	,027
Confidencialidade dos dados	,283	,812	,163	-,010
Integridade dos dados	,184	,628	,293	,126
Integridade física das pessoas	,038	-,045	,826	-,077
Usabilidade	,086	,139	,764	,204
Fiabilidade	,280	,321	,543	,182
Pessoas envolvidas no(s) processo(s)	,281	,240	,476	,114
Domínio sobre os equipamentos conectados	,112	,062	,108	,832
Complexidade da tecnologia	,237	,031	,096	,807
Valores próprios	4,843	1,445	1,420	1,031
Variância explicada (%)	34,58	10,32	10,14	7,366
Percentagem acumulada	34,58	44,91	55,05	62,41
Alfa de Cronbach (α)	0,807	0,786	0,679	0,647
Nota: Resultado da ACP: matriz após rotação Varimax, com normalização Kaiser, convergente em 5 iterações. Medida KMO=0,813; Teste de Bartlett=540,815; Significância = 0,000				

3.3.3.4. Determinar os riscos e ameaças associados à IoT

De forma a responder ao quarto objetivo*, determinar os riscos e ameaças que os estudantes universitários associam à IoT,* foram utilizados os dados recolhidos na pergunta dez da parte II do questionário (cf. Apêndice B). Nesta pergunta os estudantes classificaram em função da sua concordância, com uma escala de 1 (Discordo totalmente)

a 5 (Concordo totalmente), uma série de afirmações relativas aos riscos e ameaças que podem existir na IoT.

Os estudantes classificaram as afirmações de uma forma discordante e com tendência a não saberem o que responder (Não concordo nem discordo) porque a média está próxima de 3, para os itens: Perda de controlo das máquinas (M=2,99); Acesso indevido ao controlo de objetos (M=2,97); Intrusão em redes internas (domésticas ou empresariais (M=2,93); Acesso a dados pessoais ou corporativos não autorizados (M=2,89) e Inibição do funcionamento do sistema M=2,86. Em alguns casos a média chegou mesmo ao 3, nas afirmações: Fatores ambientais (naturais e humanos) com M=3,00; Ligação indevida de dispositivos não autorizados na rede (M=3,04) e Privacidade dos indivíduos e dados (M=3,03). De referir que o item mais discordante é Ausência de encriptação na transmissão dos dados com M=2,59.

Com o intuito de averiguar os riscos e ameaças associados à IoT, realizou-se uma análise fatorial de componentes principais (ACP) com os itens da questão dez. Esta ACP permitiu-nos identificar as dimensões centrais dos riscos e ameaças possíveis na IoT (Tabela 5). Foram identificados dois componentes, que correspondem às dimensões: Dados e redes, assim como Segurança.

O primeiro componente (49,5 % de variância total explicada, com alfa de Cronbach $\alpha = 0,886$) agrupa os itens referentes aos dados e redes.

O segundo componente (11,8 % de variância total explicada, com alfa de Cronbach $\alpha = 0,834$) agrupa os itens que pertencem à segurança.

Tabela 5 – ACP – Riscos e Ameaças na IoT

	Componentes	
	Dados e redes	Segurança
Acesso a dados pessoais ou corporativos não autorizados	,900	,013
Acesso indevido ao controlo de objetos	,841	,184
Alteração ou eliminação de dados	,781	,344
Intrusão em redes internas (domésticas ou empresariais)	,706	,401
Ausência de encriptação na transmissão dos dados	,612	,345
Interface web insegura	,571	,493
Privacidade dos indivíduos e dados	,131	,794
Perda de liberdade	,132	,785

	Componentes	
	Dados e redes	Segurança
Serviços de rede inseguros	,465	,675
Fraca segurança física dos equipamentos	,145	,669
Fracos mecanismos de autenticação e autorização	,360	,596
Perda de controlo das máquinas	,362	,571
Valores próprios	5,941	1,425
Variância explicada (%)	49,51	11,87
Percentagem acumulada	49,51	61,38
Alfa de Cronbach (α)	0,886	0,834
Nota: Resultado da ACP: matriz após rotação Varimax, com normalização Kaiser, convergente em 3 iterações. Medida KMO=0,887; Teste de Bartlett=574,428; Significância = 0,000		

3.3.3.5. Verificar as principais áreas de aplicação da IoT

De forma a responder ao quinto objetivo*, verificar as principais áreas de aplicação da IoT,* foram utilizados os dados recolhidos na pergunta 11 da parte II do questionário (cf. Apêndice B). Nesta pergunta os estudantes classificaram em função da sua concordância, com uma escala de 1 (Discordo totalmente) a 5 (Concordo totalmente), uma série de itens relativos às principais áreas de aplicação da IoT.

Os participantes (N=92) concordaram na sua maioria com os itens expostos. Damos destaque, como principais áreas de aplicação da IoT, a: Casas e edifícios inteligentes (domótica) com M=4,47; Cidades inteligentes (*smart cities*) com média de 4,47; Infraestruturas inteligentes (M=4,32); Indústria (M=4,25); Leitura automática dos contadores de eletricidade, água, gás e diversos serviços associados (*smart grids*) com M=4,25; Veículos inteligentes (M=4,18).

De referir que, para este caso houve poucas discordâncias e alguns itens estão muito próximos do valor 4 (Concordo), sendo eles: Localização (M=3,97); Aeronáutica (M=3,96); Ambiente (M=3,96); *Wearables* (M=3,90); Etiquetas inteligentes (3,89). (cf. Tabela 22, Apêndice C).

3.3.3.6. Determinar as áreas em que a IoT é útil

De forma a responder ao sexto objetivo*, determinar as áreas em que a IoT é útil,* foram utilizados os dados recolhidos na pergunta 12 da parte II do questionário (cf. Apêndice

B). Nesta pergunta os estudantes classificaram em função da sua concordância, com uma escala de 1 (Discordo totalmente) a 5 (Concordo totalmente), uma série de itens relativos às áreas em que a IoT pode ser útil.

Os participantes (N=92) concordaram moderadamente com os itens expostos. Damos destaque a: Engenharia Mecânica (M=4,20); Empresas/Empresários(as) com M=4,16; Engenharia Civil (M=4,06); Profissionais de Saúde (M=4,03). Seguem-se as áreas em que a IoT pode ser útil com valores aproximados de 4 (Concordo) em: Estudantes (M=3,95) e Motoristas (M=3,71). Alguns itens foram classificados com incerteza na resposta (Não concordo nem discordo) porque a tendência é estar próxima do valor 3: Informática (M=3,38); Industriais (M=3,16); Profissionais Governamentais (M=3,51). E para a área de Psicologia, os estudantes consideram que a IoT seja pouco útil (M=1,99). (cf. Tabela 23, Apêndice C).

3.3.3.7. Criação de índices relativos às ACPs

A criação de índices (compósitos) serve para posteriormente se criarem as correlações entre os diferentes componentes das ACPs. De seguida é apresentado um resumo das médias e desvio-padrão, sendo que as tabelas de frequência associadas a cada índice encontram-se no Apêndice D.

Tabela 6 – Índices dos componentes da ACP relativos às perceções sobre a IoT

Componentes	N	Média	Desvio-Padrão
Dispositivos interligados	117	3,79	0,683
Redes de sensores	117	3,91	0,732
Máquinas inteligentes	117	3,71	0,713
Potencial	117	3,14	1,00
Autonomia	117	3,73	0,797

Tabela 7 – Índices dos componentes da ACP relativos às expectativas face à IoT

Componentes	N	Média	Desvio-Padrão
Facilidade Tecnológica	117	4,11	0,520
Oportunidades	117	3,51	0,867
Privacidade e Segurança	117	3,25	0,917
Confiabilidade	117	3,41	0,703
Usabilidade	117	3,65	0,825
Comunicação	117	3,67	0,788

Tabela 8 – Índices dos componentes da ACP relativos à confiança na IoT

Componentes	N	Média	Desvio-Padrão
Conformidade	117	3,56	0,617
Segurança	117	2,94	0,848
Fiabilidade	117	3,58	0,593
Complexidade	117	3,70	0,695

Tabela 9 – Índices dos componentes da ACP relativos aos riscos e ameaças da IoT

Componentes	N	Média	Desvio-Padrão
Dados e rede	92	2,84	0,861
Segurança	92	2,89	0,793

3.3.4. Análise de correlações

Para compreendermos as associações mais significativas entre as dimensões encontradas, com base nos componentes determinados (a partir das ACPs), foram feitas análises de correlações. Em todas as análises que iremos interpretar, indicamos as associações estatisticamente significativas, de acordo com o coeficiente de Pearson, assim como o grau de significância de cada correlação – indicado pela probabilidade p associada, tendo em conta que: * significa que $p<0,050$; ** $p<0,010$; *** $p<0,001$.

Todas as tabelas de correlações encontram-se no Apêndice E, sendo indicado em cada análise, a tabela associada que pode ser consultada.

3.3.4.1. Correlações entre Dispositivos interligados, Redes de sensores, Máquinas inteligentes, Potencial e Autonomia

As correlações entre as dimensões Dispositivos interligados, Rede de sensores e Máquinas inteligentes, Potencial e Autonomia são moderadas a fortes (entre 0,403 e 0,666), de acordo com o coeficiente de Pearson (cf. Tabela 41, no Apêndice E).

Podemos observar as correlações Dispositivos interligados e Rede de sensores ($0,666^{***}$), Dispositivos interligados e Máquinas inteligentes ($0,533^{***}$), Dispositivos interligados e Potencial ($0,461^{***}$), que significam que, à medida que os alunos associam às perceções da IoT itens relacionados com Dispositivos interligados, também os identificam em relação a Rede de sensores, Máquinas inteligentes e Potencial.

De destacar também, as correlações Redes de sensores com Máquinas inteligentes ($0,592^{***}$), Redes de sensores e Potencial ($0,504^{**}$), Redes de sensores e Autonomia ($0,487^{***}$), que à medida que os alunos associam às perceções da IoT itens relacionados com Rede de sensores, também os reconhecem em relação a Máquinas inteligentes, Potencial e Autonomia.

3.3.4.2. Correlações entre Facilidade tecnológica, Oportunidades, Privacidade e Segurança, Confiabilidade, Usabilidade e Comunicação

As correlações entre as dimensões Facilidade Tecnológica, Oportunidades, Privacidade e Segurança, Confiabilidade, Usabilidade e Comunicação, são moderadas e algumas tendem a ser fracas mas têm significância de acordo com o coeficiente de Pearson (cf. Tabela 42, no Apêndice E).

Existem correlações entre Facilidade tecnológica e Oportunidades ($0,463^{***}$), Facilidade tecnológica e Usabilidade ($0,408^{***}$), Comunicação e Facilidade tecnológica ($0,362^{***}$), isto significa que, à medida que os estudantes associam às expectativas da IoT itens relacionados com a Facilidade tecnológica, também os reconhecem em relação a Oportunidades, Usabilidade e Comunicação. Outras correlações existentes como: Oportunidades e Confiabilidade ($0,401^{***}$), Confiabilidade e Comunicação ($0,425^{***}$), significam que os alunos ao associarem Confiabilidade às expectativas, também lhe associam Oportunidades e Comunicação. De referir que não existe correlação com a dimensão Privacidade e Segurança.

3.3.4.3. Correlações entre Conformidade, Segurança, Fiabilidade e Complexidade

As correlações entre as dimensões Conformidade, Segurança, Fiabilidade e Complexidade, são moderadas e significativas de acordo com o coeficiente de Pearson (cf. Tabela 43, no Apêndice E).

Existem correlações entre Conformidade e Segurança (0,488***), Conformidade e Fiabilidade (0,433***), Conformidade e Complexidade (0,401***), isto significa que, à medida que os estudantes associam à confiança da IoT itens relacionados com a Conformidade, também os identificam em relação à Fiabilidade e Complexidade. Em relação à Segurança e Fiabilidade (0,395***) existe uma correlação significativa, ou seja, os alunos quando escolheram itens relacionados com a confiança na IoT, estas duas dimensões estavam incluídas.

3.3.4.4. Correlações entre Dados e rede com Segurança

As correlações das dimensões Dados e rede com Segurança é forte (cf. Tabela 44, no Apêndice E).

Verificamos que há correlação forte entre as dimensões Dados e rede com Segurança (0,661***). Isto quer dizer que, os estudantes quando concordam com os itens relacionados com Dados e rede como sendo pertencentes a riscos e a ameaças na IoT, também os identificam em relação à Segurança.

3.3.4.5. Correlações entre todas as dimensões

As correlações entre todas as dimensões são, na sua maioria moderadas, mas existem casos onde as correlações são fracas mas são significativas, de acordo com o coeficiente de Pearson (cf. Tabela 45, no Apêndice E).

De destacar algumas correlações mais fortes pela sua significância, sendo elas: Rede de sensores com Facilidade tecnológica (0,500***), Potencial com Conformidade (0,451***), Facilidade tecnológica com Máquinas inteligentes (0,453***), Confiabilidade com Segurança (0,479***), Segurança com Máquinas inteligentes (0,369***), Fiabilidade com Confiabilidade (0,441***), Dados e rede com Privacidade e segurança (0,361***).

Verificamos que existem correlações entre as diferentes dimensões, que juntam as perceções e as expectativas sobre a IoT, as perceções e a confiança na IoT, expectativas e a confiança na IoT, assim como, expectativas e riscos e/ou ameaças na IoT.

Capítulo 4 – Discussão dos Resultados

Esta investigação teve como objetivo genérico compreender como é que os estudantes universitários percecionam a *Internet of Things*, que expectativas lhe atribuem, que confiança e que aplicações lhe associam.

Os objetivos que foram delineados (cf. Alínea 3.3.1) foram verificados. De forma a facilitar a leitura dos resultados nesta discussão, é indicado no início de cada parágrafo, o objetivo que se está a abordar e os respetivos resultados obtidos.

Determinar as perceções dos estudantes universitários sobre a IoT

Os estudantes universitários percecionam a IoT como sendo: Coisas a comunicarem com outras coisas, Conjunto de dispositivos (sem serem computadores) ligados à Internet, Geração da informação através da comunicação entre objetos, Sensores a comunicarem com aplicações e sistemas, Sistemas de aparelhos que podem comunicar à distância-*online*, Variados objetos ligados (sem fio) à Internet e entre si, Máquinas com inteligência e capacidade para comunicarem entre si e Captação e manipulação de dados em tempo real. Algumas destas perceções concordam com as perceções que outros autores têm sobre a *Internet of Things* (cf. Tabela 1), nomeadamente: coisas a comunicarem com outras coisas, dispositivos ligados à Internet, variados objetos ligados à Internet e entre si.

Para Asplund (2016), no estudo que fez, em relação às perceções gerais sobre a IoT, refere que algumas pessoas não tinham ouvido o termo anteriormente, mas a maioria considerou estar associado com produtos do consumidor como automação residencial e veículos ligados.

Verificar as expectativas dos estudantes universitários face à IoT

As expectativas dos estudantes universitários face à IoT estão relacionadas com os itens: Evolução e Inovação Tecnológica; Utilidade; Automação de certas atividades diárias (p.e., tarefas rotineiras no trabalho e em casa); Fácil acesso e controlo à distância (p.e., através de um telemóvel) a várias coisas, sistemas ou dispositivos; É um mundo de oportunidades, onde muitas coisas se podem explorar; Poupança de tempo na realização de certas tarefas (p. e., controlo de temperatura, eletrodomésticos ligarem-se automaticamente e o trabalho estar feito quando a pessoa chega a casa); Facilitação do uso de equipamentos (p.e., frigoríficos autorregulados, aspiradores autónomos, dispensadores de ração para animais, controlar um candeeiro por telemóvel, abrir e fechar

janelas automaticamente) e Facilitação na obtenção de vários dados (tráfego, dados meteorológicos, validação de bilhetes dos transportes públicos).

Em suma, tudo o que os estudantes possam beneficiar com a IoT e que esta tecnologia os ajude no seu dia-a-dia.

Para Skaržauskienė e Kalinauskas (2015), o potencial que existe na IoT é excelente e as expectativas relacionadas com a tecnologia também é muito alta. E nesse âmbito, o setor empresarial apresenta interesse no desenvolvimento da IoT. Os serviços devem seguir a infraestrutura tecnológica e, se forem bem sucedidos, mais áreas da vida quotidiana tornar-se-ão domínios de aplicação para ambientes "inteligentes". A IoT pode influenciar a qualidade de vida e a produtividade do trabalho, quer seja individualmente, em comunidades e/ou empresas, contribuindo para o desenvolvimento das regiões.

Analisar a confiança que os estudantes universitários têm na IoT

Os estudantes consideram itens como a Usabilidade, Complexidade da tecnologia, Gestão dos sistemas de informação envolvidos, Domínio dos equipamentos conectados, Localização geográfica e Disponibilidade dos dados moderadamente confiáveis. De referir também, que os participantes consideraram a IoT pouco confiável a nível da privacidade dos dados e da confidencialidade dos dados. Eles têm alguma incerteza se a tecnologia IoT será confiável, porque as respostas tenderam para a opção central (Indiferente).

Geralmente, a confiança está associada à segurança e à privacidade. No entanto, a confiança é mais do que a segurança. Relaciona não apenas a segurança, mas também outros fatores, tais como: conformidade, fiabilidade, confiabilidade, disponibilidade, habilidade. O termo “confiança” abrange um âmbito maior do que a segurança, por isso é mais complicado e difícil de estabelecer, garantir, manter, gerir a confiança do que a segurança (Yan *et al*., 2014).

Determinar os riscos e ameaças associadas à IoT

A maioria dos estudantes universitários teve dúvidas a responder a este objetivo tendo optado pela opção central (Não concordo nem discordo) mas a tendência foi para discordarem dos itens apresentados. Logo, deduz-se que consideram um risco e ameaça determinados itens, tais como: Ausência de encriptação na transmissão dos dados e Acesso a dados pessoais ou corporativos não autorizados.

Para Abomhara e Koien (2015), o crescimento exponencial da IoT levou a maiores riscos de segurança e privacidade. Muitos desses riscos são atribuidos a vulnerabilidades de dispositivos que surgem por *hackers* no cibercrime e no uso indevido dos sistemas.

Verificar as principais áreas de aplicação da IoT

Os participantes deste estudo consideram como principais áreas de aplicação da IoT as seguintes: Casas e edifícios inteligentes (domótica), Cidades inteligentes (*smart cities*), Infraestruturas inteligentes, Indústria, Leitura automática dos contadores de eletricidade, água, gás e diversos serviços associados (*smart grids*) e Veículos inteligentes. De seguida estão a Localização, a Aeronáutica, Ambiente, *Wearables* e Etiquetas inteligentes.

Segundo Miorandi *et al*. (2012) também consideram a aplicação da IoT em *smart homes* e *smart cities*, monitorização do ambiente, mas também acrescenta que nos cuidados de saúde tem aplicabilidade. Gubbi *et al*. (2013) mencionam no seu estudo *smart homes*, *smart cities*, ambiente e acrescentam que a IoT tem aplicabilidade na agricultura e transportes.

Determinar as áreas em que a IoT é útil

Os estudantes universitários consideraram como principais áreas em que a IoT é útil, as seguintes: Engenharia Mecânica, em Empresas/Empresários, na Engenharia Civil, Profissionais de saúde, Estudantes, Motoristas. Eles consideram que para a área de Psicologia a IoT seja pouco útil.

Em suma, através dos resultados obtidos nesta investigação foi possível compreender as perceções e expectativas dos estudantes universitários sobre a *Internet of Things* , bem como que confiança esta lhes desperta e que áreas e aplicações lhe associam.

Capítulo 5 – Conclusões

O termo *Internet of Things* refere-se, geralmente, a cenários nos quais a conetividade de rede e a capacidade de computação se estendem a objetos, sensores e itens comuns que normalmente não são considerados computadores, permitindo que esses dispositivos gerem, troquem e consumam dados com intervenção humana mínima. No entanto, não existe uma definição universal única (Rose *et al*., 2015).

Miragliotta *et al*. (2012) consideram que existem várias definições sobre a *Internet of Things*, demonstrando que há um grande interesse neste assunto. No entanto, na literatura encontra-se uma complexidade significativa na compreensão do real significado da *Internet of Things* e, também a nível de implicações sociais, económicas e técnicas na implementação da IoT.

Do ponto de vista conceitual, a IoT é baseada em três pilares, relacionados com a capacidade de objetos inteligentes de: ser identificável (qualquer coisa se identifica), comunicar (qualquer coisa se comunica) e interagir (qualquer coisa interage), entre si, construindo redes de objetos interconectados, com utilizadores finais ou outras entidades na rede (Miorandi *et al*., 2012).

Para Sicari (2015), a disseminação de serviços de IoT requer níveis de segurança e privacidade que devem ser garantidos. Mas ainda há uma visão unificada de como garantir isso, porque o ambiente é muito heterogéneo, envolvendo diferentes tecnologias e padrões de comunicação. As soluções devem ser desenhadas para garantir: confidencialidade, controlo de acessos e privacidade para utilizadores e coisas, confiabilidade entre dispositivos e utilizadores, assim como, conformidade com políticas de segurança e privacidade bem definidas.

Com esta investigação, verificou-se que as perceções e as expectativas que os estudantes universitários têm sobre a IoT são significativas, destacando os fatores Dispositivos interligados, Rede de sensores, Máquinas inteligentes, Potencial e Autonomia nas perceções e, fatores como Facilidade Tecnológica, Oportunidades, Privacidade e Segurança, Confiabilidade, Usabilidade e Comunicação para as expectativas. De referir, que surgiram algumas incertezas em relação à IoT ser uma tecnologia confiável e se podia ter riscos e ameaças associadas.

Em relação às áreas de aplicação, os estudantes universitários destacaram as Casas e edifícios inteligentes (domótica) e Cidades inteligentes (*smart cities*). As áreas académicas/profissionais onde a IoT é considerada útil pelos estudantes universitários são: Engenharia Mecânica, em Empresas/Empresários, na Engenharia Civil, Profissionais de saúde, Estudantes e Motoristas.

Este trabalho contribui para aprofundar mais a temática da *Internet of Things*, saber até que ponto os estudantes universitários têm conhecimento sobre a mesma, alertar as instituições académicas e público/privadas para analisarem os seus processos e estarem de acordo com esta tecnologia emergente. Caso estejam na vanguarda, podem organizar *workshops* para os alunos que ainda não conheçam bem esta temática.

Os resultados que obtivemos são importantes e significativos relativamente às perceções e expectativas que os estudantes universitários têm sobre a IoT. Encontraram-se algumas limitações ao nível da dimensão da amostra, pelo facto de ter havido desistências no preenchimento do questionário. Os participantes que efetivamente responderam à totalidade das questões foram 92. Uma amostra de maior dimensão poderia reforçar os resultados e conclusões.

A *Internet of Things* revolucionará a vida das pessoas em geral e, a partir do momento em que todos entenderem essa tecnologia e apostarem em soluções globais para o mercado, tornarão a vida mais fácil para todas as pessoas e organizações. Ali (2015) refere que a *Internet of Things* faz parte do grupo das tecnologias disruptivas adotada em muitas áreas da vida quotidiana. A partir daqui, espera-se que outros estudos possam ser realizados, com outras populações, e a nível global. Os caminhos estão abertos para serem descobertos, como os benefícios e o impacto que a tecnologia IoT pode ter na vida das pessoas e na sociedade.

Bibliografia

Abomhara, M., & Koien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. doi:10.13052/jcsm2245-1439.414

Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. *Computer Security,* 37, 111-123.

Ali, F. (2015). Teaching The Internet of Things Concepts. *Proceedings of the WESE'15: Workshop on Embedded and Cyber-Physical Systems Education - WESE'15*, 1–6. doi:10.1145/2832920.2832930

Araujo, M. (2017). IoT – Internet das Coisas: motivação, benefícios e segurança. Consultado em dezembro 2017. Disponível em: http://www.afrikatec.com.br/iot-internet-das-coisas-motivacao-beneficios-e-seguranca

Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal. Consultado em dezembro de 2017. Disponivel em http://www.rfidjournal.com/articles/view?4986.

Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access*, *4*, 2130–2138. doi:10.1109/ACCESS.2016.2560919

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: a survey. *Computer Networks*, 54(15), 2787–2805. doi: 10.1016/j.comnet.2010.05.010

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), *3rd International Conference on Recent Trends in Network Security and Applications (CNSA'10*), Chennai, India. pp. 420-429.

Bao, F., & Chen, I. (2012). Dynamic trust management for internet of things applications. *Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT '*12, USA, San Jose, pp. 1-6.

Bao, F., & Chen, I. (2012). Trust management for the internet of things and its application to service composition. *13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, WoWMoM 2012, San Francisco, CA, United States, pp. 1-6

Belei, R. A., Gimeniz-Paschoal, S. R., Nascimento, E. N., & Matsumoto, P. H. V. R. (2008). O uso de entrevista, observação e videogravação em pesquisa qualitativa. *Cadernos de Educação - FaE/PPGE/UFPel Pelotas*, *30*, 187–199. doi: 10.5935/1415-2762.20140009

Cao, J., Carminati, B., Ferrari, E., & Tan, K.L. (2011). CASTLE: continuously anonymizing data streams*, IEEE Transactions on Dependable and Secure Computing*, 8, 337-352.

Coelho, P. (2017). *Internet das Coisas – Introdução Prática*. FCA. Lisboa.

Evans, D., & Eyers, D. (2012). Efficient data tagging for managing privacy in the internet of things, *2012 IEEE International Conference on Green Computing and Communications*, Besancon, pp. 244-248.

Fraser, M. T. D., & Gondim, S. M. G. (2004). Da fala do outro ao texto negociado: discussões sobre a entrevista na pesquisa qualitativa. *Paidéia (Ribeirão Preto)*, *14*(28), 139–152.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Huang X., Fu R., Chen B., Zhang T., & Roscoe A. (2012). User interactive internet of things privacy preserved access control. *7th International Conference for Internet Technology and Secured Transactions, ICITST 2012*, London, pp. 597-602.

Intel. The Internet of Things (IoT) Starts with Intel Inside. Consultado em dezembro 2017. Disponivel em https://www.intel.com/content/www/us/en/internet-of-things/overview.html

ITU (2005). Internet reports —The internet of things Consultado em outubro 2018. Disponível em https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

Keoh, S., Kumar, S., & Tschofenig, H. (2014), Securing the Internet of Things: A Standardization Perspective*, IEEE Internet of Things Journal,* 3 (1), pp. 265-275

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 257–260. doi:10.1109/FIT.2012.53

Koreshoff, T. L., Robertson, T., & Leong, T. W. (2013). P335-Koreshoff. *Internet of Things: A Review of Literature and Products*, 335–344.

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. *Internet Research*. 26, 337-359.

Li, S., Xu, L. Da., & Zhao., S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17, 243-259.

Mattern, F., & Floerkemeier, C. (2010). From the internet of computers to the internet of things. *Communications of the ACM*, 6462, 242–259. doi:10.1007/978-3-642-17226-7

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10, 1497-1516.

Miragliotta, G., Perego, A., & Tumino, A. (2012). Internet of Things: Smart Present or Smart Future? Department of Management, Economics and Industrial Engineering, Politecnico Di Milano.

Nitti, M., Girau, R., Atzori, L., Iera, A., & Morabito, G. (2012). A subjective model for trustworthiness evaluation in the social internet of things, *2012 IEEE 23rd International Symposium on Pearsonal Indoor and Mobile Radio Communications*, PIMRC, Australia, Sydney, pp. 18-23.

Press, G. (2014). Internet of Things By The Numbers: Market Estimates And Forecasts. Consultado em dezembro 2017. Disponível em https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#3d636621b919

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. doi:10.1016/j.comnet.2012.12.018

Rose, K., Eldridge, S., & Lyman, C. (2015). The internet of things: an overview. Internet Society, (October), 53.

SAS. Internet of Things (IoT). What it is and why it matters. Consultado em dezembro 2017. Disponível em https://www.sas.com/pt_br/insights/big-data/internet-das-coisas.html.

Siano, P. (2014). Demand response and smart grids - A survey. *Renewable and Sustainable Energy Reviews*, 30, 461-478.

Sicari, S., Cappiello, C., Pellegrini, F.D., Miorandi, D., & Coen-Porisini, A. (2014). A security-and quality-aware system architecture for internet of things. *Inf. Syst. Frontiers*, 18, 665-677.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.

Singer, T. (2012). *Tudo Conectado: Conceitos e Representações Da Internet Das Coisas*, 15. doi:10.1590/1981-5344/2356

Skaržauskienė, A., & Kalinauskas, M. (2015). The internet of things: when reality meets expectations. *International Journal of Innovation and Learning*, *17*(2), 262–274.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). *Vision and Challenges for Realising the Internet of Things Cluster of european research project on Internet of Things*. doi:10.2759/26127

Tan, L., & Wang, N. (2010). Future Internet: The Internet of Things, *3rd International Conference on Advanced Computer Theory and engineering (ICACTE)*, pp. 376–380. doi:10.1109/ICACTE.2010.5579543

Tu, M. International Journal of Logistics Management, The an exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management - a mixed research approach for Authors an exploratory study of Internet of Things (IoT) adoption. *International Journal of Logistics Management*, 11–2016.

Ukil A., Bandyopadhyay S., & Pal. A. (2014). Iot-privacy: To be private or not to be private. *2014 IEEE Conference on Computer Communications Workshops* (INFOCOM WKSHPS), Toronto, ON, pp. 123-124.

Vasconcelos, C., & Oliveira, A. (2018). Perceptions and Expectations of college students about Internet of Things? In *ICERI2018 11th annual International Conference of Education, Research and Innovation*.

Wan, J., Cai, H., & Zhou, K. (2015). Industrie 4.0: Enabling technologies. *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things*, pp. 135-140.

Wang Y., & Wen Q. (2011). A privacy enhanced dns scheme for the internet of things, *IET International Conference on Communication Technology and Application*, ICCTA 2011, Beijing, China. pp. 699-702.

Wei, J. (2014). How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine*, 3, 53-56.

Yan, Z., Zhang, P., & Vasilakos, A. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, 42, 120-134.

Yang J., & Fang, B. (2011). Security model and key technologies for the internet of things, J. *China Universities Posts Telecommun*, 18, 109-112.

Yang, J., Lee, H., Park, M., & Eom, J. (2015). Security Threats on National Defense ICT based on IoT. *Advanced Science and Technology Letters*, 97, 94-98.

Zhao, J. C., Zhang, J. F., Feng, Y., & Guo, J. X. (2010). The study and application of the IOT technology in agriculture. *2010 3rd International Conference on Computer Science and Information Technology*, pp. 462-465.

Zhou, K., Liu, T., & Zhou, L. (2016). Industry 4.0: Towards future industrial opportunities and challenges. *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2015*, 2147–2152. doi:10.1109/FSKD.2015.7382284

Apêndice A – Guião de Entrevistas

O objetivo do trabalho consiste em saber as perceções e expectativas que os estudantes universitários têm sobre a Internet of Things. Para esta entrevista, a sua participação é voluntária e pode desistir em qualquer momento, se assim o desejar. As suas respostas são tratadas de forma anónima e confidencial, e somente no âmbito científico da investigação em curso. Seguem as questões:

1. O que é para si a Internet of Things? Que perceções tem sobre a mesma?
2. Quantos anos de experiência tem na área da IoT?
3. Trabalha diariamente com esta tecnologia? Se sim, em que aplicações?
4. Como se sente relativamente à fiabilidade da IoT?
5. Em que medida a adoção da IoT no quotidiano tem impacto na privacidade dos individuos?
6. Que expectativas tem sobre a IoT?
7. Que vantagens/desvantagens a IoT pode ter na sociedade?
8. Que oportunidades pode contribuir para a sociedade?
9. Que ameças e riscos vislumbra com o uso da IoT?
10. Na sua opinião qual a importância da IoT na sociedade?
11. A sociedade pode confiar na IoT?
12. A IoT tem limitações? Quais?
13. Na sua opinião quais são as áreas onde a IoT está mais implementada?
14. Quais são os beneficios que a IoT pode trazer para as universidades de uma forma geral e em particular para os estudantes?
15. Que atividades profissionais pensa que mais podem usufruir com a adoção da IoT?

Apêndice A1 – Gráficos de Leximancer

Questão 2: Quantos anos de experiência tem na área da IoT?

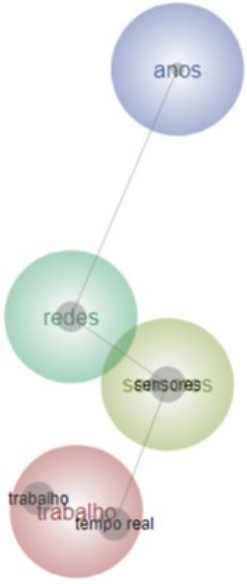


Figura 10 – Anos de experiência na área da IoT

Questão 3: Trabalha diariamente com esta tecnologia? Se sim, em que aplicações?

Figura 11 – Estado atual com a IoT

Questão 4: Como se sente relativamente à fiabilidade da IoT?

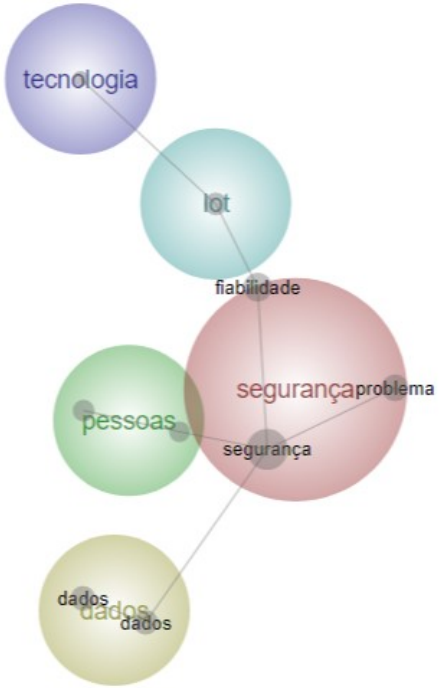


Figura 12 – Fiabilidade da IoT

Questão 5: Em que medida a adoção da IoT no quotidiano tem impacto na privacidade dos indivíduos?

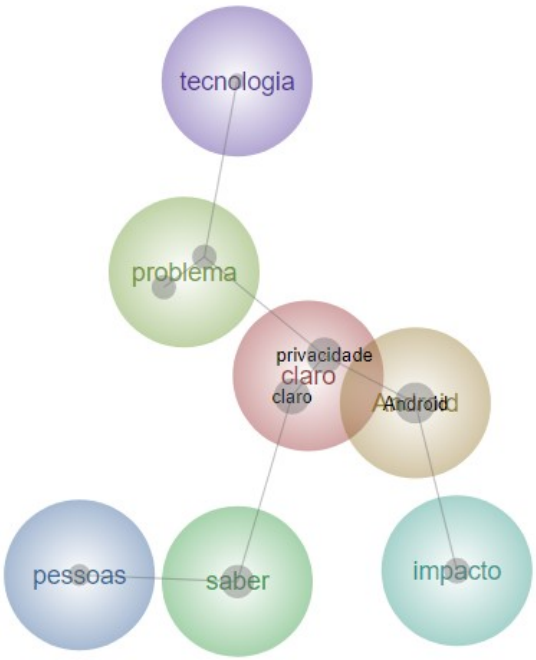


Figura 13 – Adoção da IoT com impacto na privacidade dos indivíduos

Questão 8: Que oportunidades pode contribuir para a sociedade?

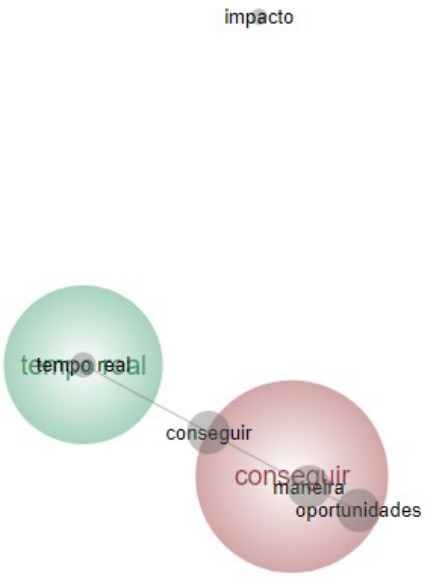


Figura 14 – Oportunidades da IoT para a sociedade

Questão 9: Que ameaças e riscos vislumbra com o uso da IoT?

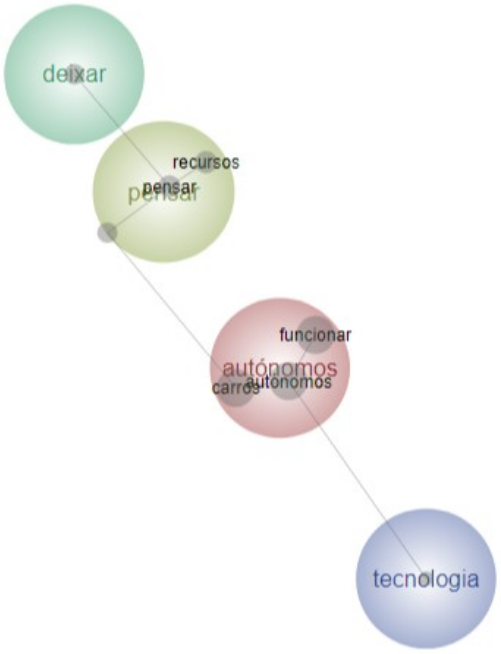


Figura 15 – Ameaças e riscos com o uso da IoT

Questão 10: Na sua opinião qual a importância da IoT na sociedade?

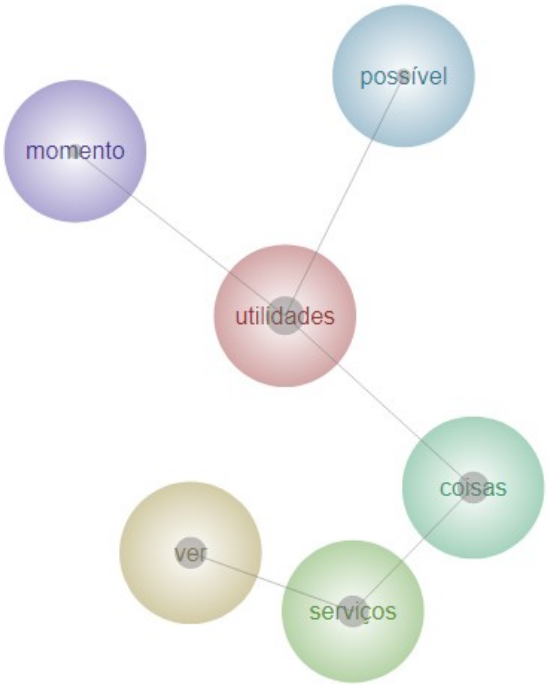


Figura 16 – Importância da IoT na sociedade

Questão 11: A sociedade pode confiar na IoT?

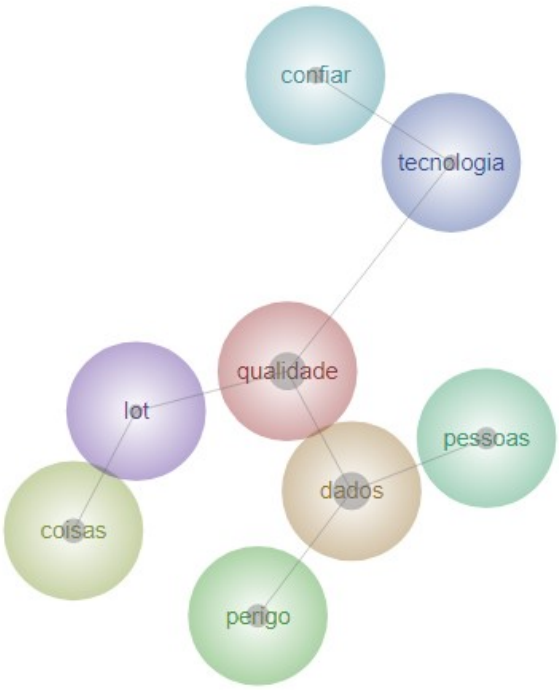


Figura 17 – Confiança na IoT

Questão 12: A IoT tem limitações? Quais?

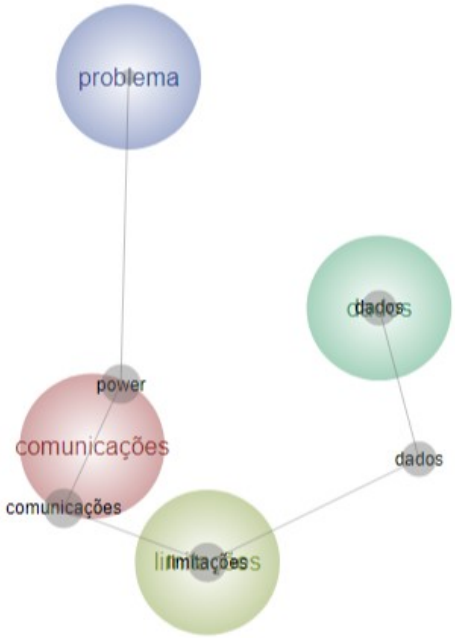


Figura 18 – Limitações da IoT

Questão 13: Na sua opinião quais são as áreas onde a IoT está mais implementada?

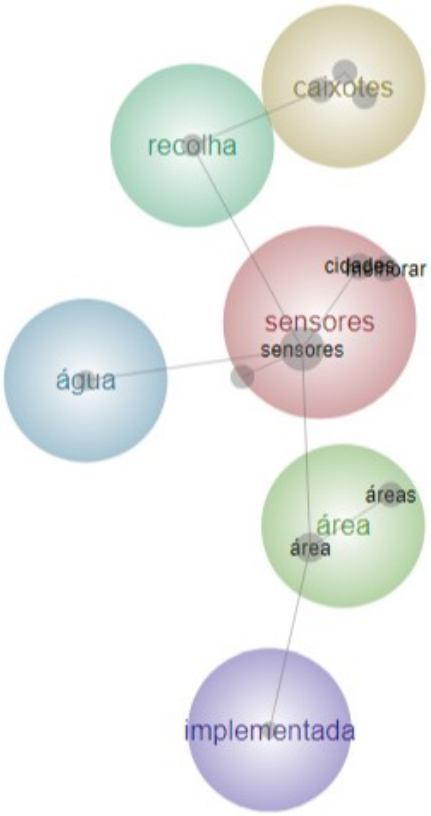


Figura 19 – Áreas onde a IoT está mais implementada

Questão 14: Quais são os beneficios que a IoT pode trazer para as universidades de uma forma geral e em particular para os estudantes?

Figura 20 – Beneficios da IoT para universidades e estudantes

Questão 15: Que atividades profissionais pensa que mais podem usufruir com a adoção da IoT?

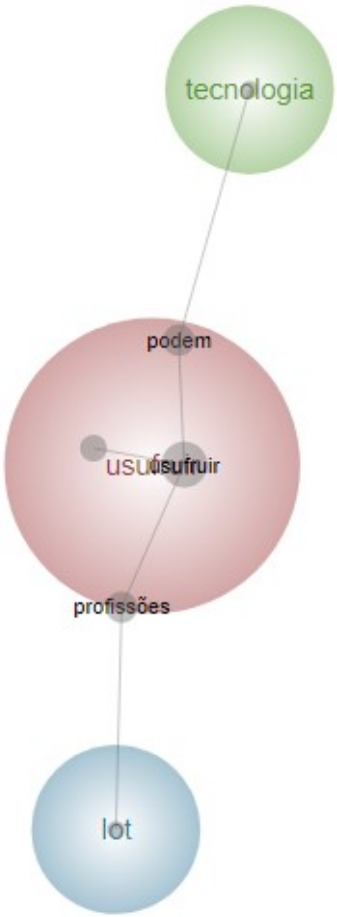


Figura 21 – Atividades profissionais que possam usufruir com a IoT

Apêndice B – Questionário

O presente estudo insere-se numa dissertação de Mestrado em Gestão de Sistemas de Informação, que visa avaliar as perceções e expectativas que os universitários têm sobre a *Internet of Things* (Internet das Coisas).

Neste sentido, pedimos a sua atenção para responder de forma o mais sincera e espontânea quanto possível, às questões que em seguida colocamos, selecionando as respostas que lhe parecerem mais adequadas.
Os dados do presente questionário são para uso exclusivo na investigação, pelo que se garante a absoluta confidencialidade e anonimato dos participantes.

O tempo de preenchimento do questionário é de cerca de 10 minutos. A sua participação é voluntária, pelo que poderá desistir do questionário a qualquer momento, se assim o desejar.

Agradecemos muito pela sua disponibilidade em colaborar com este estudo!

Nota: Se tiver qualquer questão ou posteriormente pretender ter informação sobre os resultados obtidos, pode contactar-nos através do e-mail: carvs@iscte-iul.pt

Neste questionário vamos referirmo-nos a *Internet of Things*, ou Internet das Coisas, usando o termo abreviado IoT.

Q1. * Idade:

Q2. * Sexo:

Feminino ☐ Masculino ☐

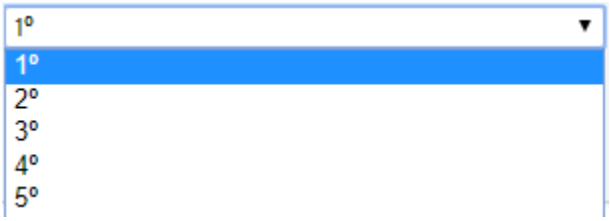
Q3. * Qual é o seu curso?

Q4. * Que tipo de curso frequenta?

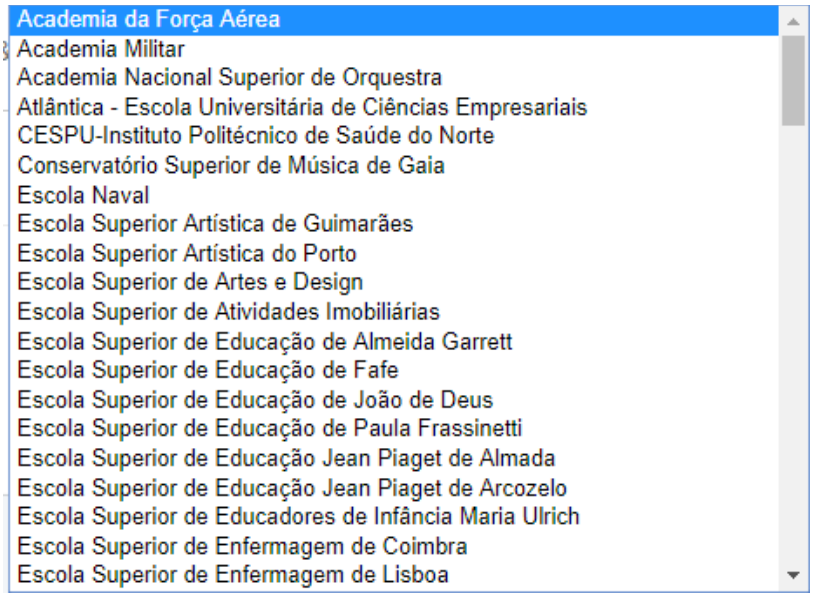
Licenciatura ▼
- Licenciatura
- Mestrado
- Doutoramento
- Outro

Q4a. * Que outro tipo de curso frequenta?

Q5. Que ano frequenta?



Q6. Qual é a Universidade/Instituição de Ensino Superior que frequenta?



Q7. * De acordo com a escala abaixo, indique o que significa para si a IoT:

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
	1	2	3	4	5
Autonomia de sistemas (reduzida necessidade de seres humanos)					
Captação e manipulação de dados em tempo real					
Coisas a comunicarem com outras Coisas					
Conjunto de dispositivos (sem ser computadores) ligados à Internet					
Deriva da facilidade que existe em ligar-se algo à internet					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Forma de comunicar e transferir dados sem intervenção humana					
Forma de interação de sistemas que vai além do que temos nos omputadores					
Geração de informação através da comunicação entre objetos					
Identificação única de objetos					
Indústria 4.0 (4ª revolução industrial)					
Máquinas com inteligência e capacidade para comunicarem entre si					
Machine learning (sistema capaz de analisar uma grandes quantidades de dados e encontrar ou gerar padrões específicos)					
Não há limites, consegue-se fazer quase tudo					
Novo paradigma de interligação de dispositivos					
Objetos inteligentes					
Permite que pessoas e coisas/objectos se conectem a qualquer momento e, em qualquer lugar, recorrendo a uma rede e a um serviço					
Redes (inteligentes, de robots, wireless e sensores sem fio)					
Sensores a comunicarem com aplicações e sistemas					
Sistema de aparelhos que podemos comunicar à distância, online					
Sistema que interliga dispositivos de computação					
Tem origem na ubiquidade da internet (ou estar ao mesmo tempo em todos os lugares)					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Tudo o que se relaciona com computação pode ser aplicado em coisas					
Tudo ligado em rede					
Variados objetos ligados (sem fio) à Internet e entre si					

Q8. * O que espera em relação à IoT?

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
	1	2	3	4	5
Acesso rápido à informação					
Ajudar a alcançar o bem-estar com aplicações de vestuário e de refeições inteligentes					
Aplicações móveis de controlo (por exemplo, de sono, nutrição, peso)					
Aumento da inteligência artificial (com máquinas inteligentes)					
Automação de certas atividades diárias (por exemplo, tarefas rotineiras no trabalho e em casa)					
Crescimento exponencial desta tecnologia (com mais dispositivos ligados à Internet do que pessoas)					
É um mundo de oportunidades, onde muitas coisas se podem explorar					
Evolução e Inovação tecnológica					
Fácil acesso e controlo à distância (p.e., através de um telemóvel) a várias coisas, sistemas ou dispositivos					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Facilitação do uso de equipamentos (por exemplo, frigoríficos autoregulados, aspiradores autónomos, dispensadores de ração para animais, controlar um candeeiro por telemovel, abrir e fechar janelas automaticamente					
Facilitação na obtenção de vários dados (tráfego, estações de recolha de dados metereológicoas, validação de bilhetes dos transportes públicos)					
Flexibilidade na adaptação de recursos (máquinas e humanos) consoante a necessidade					
Gerar mais/novos empregos					
Invasão de privacidade					
Impactos e vunerabilidades de segurança					
Libertar o ser humano para a capacidade de raciocionio, abstração e inteligência					
Maior eficiência nos processos					
Maior responsabilidade no uso da tecnologia					
Melhor otimização dos recursos para as soluções IoT					
Melhor qualidade de vida das pessoas					
Não saber o que a IoT vai trazer à sociedade					
Novas formas de interação humano-máquina (por exemplo, mais interfaces tácteis e sistemas de realidade aumentada)					
Oportunidades de negócio					
Perda da identidade e da individualidade					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Poupança de tempo na realização de certas tarefas (por exemplo, controlo de temperatura, eletrodomésticos ligarem-se automaticamente e o trabalho estar feito quando a pessoa chega a casa)					
Redução do tempo e custos					
Soluções IoT permitem aumentar as receitas de empresas/entidades fornecedoras					
Tecnologia confiável					
Tecnologia aliada do ser humano					
Ter uma conetividade segura, fiável e abrangente					
Usar a tecnologia para melhorar o desempenho e garantir melhores resultados					
Utilidade					

Q9. * Até que ponto considera que a IoT é confiável a nível de:

	Nada Confiável	Pouco Confiável	Indiferente	Confiável	Muito Confiável
	1	2	3	4	5
Ambiente (dependência em relação a condições ambientais)					
As coisas funcionarem conforme o previsto					
Auditorias					
Autenticação em aplicações					
Complexidade da tecnologia					
Confidencialidade dos dados					
Disponibilidade dos dados					
Domínio sobre os equipamentos conectados					
Fiabilidade					
Gestão dos sistemas de informação envolvidos					
Integridade dos dados					
Integridade física das pessoas					

	Nada Confiável	Pouco Confiável	Indiferente	Confiável	Muito Confiável
	1	2	3	4	5
Localização geográfica					
Pessoas envolvidas no(s) processo(s)					
Privacidade dos dados					
Situações que impliquem risco (por exemplo, formas de utilização dos dados, possíveis hackers, falhas na informação, etc.)					
Usabilidade					

Q10. * Até que ponto concorda com as seguintes afirmações associadas à IoT?

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
	1	2	3	4	5
Acesso a dados pessoais ou corporativos não autorizados					
Acesso indevido ao controlo de objetos					
Alteração ou eliminação de dados					
Atualizações de software inseguras					
Ausência de encriptação na transmissão dos dados					
Configuração insuficiente					
Fraca segurança física dos equipamentos					
Fracos mecanismos de autenticação e autorização					
Fatores ambientais (naturais e humanos)					
Inibição do funcionamento do sistema					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Interface web insegura					
Interface na *Cloud* insegura					
Interface com dispositivos móveis insegura					
Intrusão em redes internas (domésticas ou empresariais)					
Ligação indevida de dispositivos não autorizados na rede					
Perda de controlo das máquinas					
Perda de liberdade					
Privacidade dos indivíduos e dados					
Serviços de rede inseguros					

Q11. * Quais as principais áreas de aplicação da IoT?

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
	1	2	3	4	5
Aeronáutica					
Agricultura					
Ambiente					
Arquitectura					
Casas e edificios inteligentes (Domótica)					
Cidades inteligentes					
Etiquetas inteligentes					
Fitness					
Indústria					
Infraestruturas inteligentes					
Leitura automática dos contadores de eletricidade, água, gás e diversos serviços associados (*smart grids*)					
Localização					

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
Logística					
Roupas inteligentes					
Retalho					
Saúde					
Segurança					
Transportes					
Uso pessoal/doméstico					
Veículos inteligentes					
Wearables					

Q12. * Para que áreas académicas/profissionais pode ser útil a IoT?

	Discordo totalmente	Discordo	Não Concordo Nem Discordo	Concordo	Concordo totalmente
	1	2	3	4	5
Arquitectura					
Engenharia Civil					
Engenharia Mecânica					
Estudantes					
Empresas/Empresários(as)					
Industriais					
Informática					
Motoristas					
Professores					
Profissionais da Informação/ Comunicação					
Profissionais Governamentais					
Profissionais de Saúde					
Profissionais de Segurança					
Psicologia					

Q13. * Em suma, e em breves palavras, qual a importância que atribui à IoT na sociedade?

Apêndice C – ACPs

Objetivo 1 - Determinar as perceções dos estudantes universitários sobre a *Internet of Things*

Tabela 10 – KMO e Teste de Bartlett's da ACP das perceções sobre a IoT

KMO e Teste de Bartlett's		
KMO		,836
Teste de Bartlett's	Qui-Quadrado Aprox.	982,497
	Grau de liberdade	190
	Sig.	,000

Tabela 11 – Variância total explicada da ACP das perceções sobre a IoT

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	7,344	36,722	36,722	3,346	16,728	16,728
2	1,517	7,583	44,304	3,145	15,724	32,452
3	1,363	6,814	51,118	2,400	12,000	44,452
4	1,078	5,390	56,508	1,732	8,658	53,110
5	1,031	5,156	61,664	1,711	8,554	61,664
6	,885	4,425	66,089			
7	,866	4,328	70,417			
8	,796	3,978	74,395			
9	,723	3,615	78,011			
10	,670	3,351	81,361			
11	,612	3,058	84,420			
12	,543	2,713	87,133			
13	,507	2,533	89,666			
14	,405	2,027	91,692			
15	,383	1,916	93,608			
16	,349	1,743	95,352			
17	,296	1,482	96,834			
18	,263	1,313	98,147			
19	,221	1,105	99,252			
20	,150	,748	100,000			

Método de Extração: Análise de components principais

Tabela 12 – Matriz de componentes da ACP das perceções sobre a IoT

Matriz de Componentes					
Componentes	1	2	3	4	5
1	,574	,574	,435	,277	,275
2	-,676	-,061	,596	,366	,225
3	,177	-,189	,037	,664	-,701
4	,315	-,653	-,140	,348	,578
5	,290	-,453	,659	-,477	-,222
Método de Extração: Análise de componentes principais. Método de rotação: Varimax e normalização de Kaiser.					

Objetivo 2 – Verificar as expectativas dos estudantes universitários sobre a *Internet of Things*

Tabela 13 – KMO e Teste de Bartlett's da ACP das expectativas sobre a IoT

KMO e Teste de Bartlett's		
KMO		,838
Teste de Bartlett's	Qui-Quadrado Aprox.	1356,777
	Grau de liberdade	300
	Sig.	,000

Tabela 14 – Variância total explicada da ACP das expectativas sobre a IoT

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	7,828	31,311	31,311	5,930	23,719	23,719
2	2,216	8,866	40,176	2,229	8,916	32,634
3	2,099	8,395	48,571	2,215	8,858	41,493
4	1,727	6,907	55,478	2,114	8,455	49,948
5	1,224	4,898	60,376	2,025	8,100	58,048
6	1,097	4,387	64,763	1,679	6,715	64,763
7	,856	3,423	68,186			
8	,843	3,372	71,558			
9	,825	3,299	74,858			
10	,706	2,825	77,683			
11	,663	2,653	80,336			
12	,618	2,473	82,809			
13	,583	2,334	85,143			
14	,550	2,202	87,345			
15	,458	1,833	89,178			

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
16	,401	1,603	90,781			
17	,347	1,386	92,168			
18	,331	1,323	93,491			
19	,302	1,207	94,698			
20	,277	1,109	95,806			
21	,273	1,093	96,900			
22	,238	,950	97,850			
23	,195	,781	98,631			
24	,179	,714	99,345			
25	,164	,655	100,000			

Método de Extração: Análise de components principais

Tabela 15 – Matriz de componentes da ACP das expectativas sobre a IoT

Matriz de Componentes						
Componentes	1	2	3	4	5	6
1	,826	,371	,042	,271	,249	,207
2	,076	-,116	,973	-,152	,009	-,108
3	-,476	,112	,201	,663	,285	,447
4	,044	-,487	-,099	-,303	,797	,153
5	-,197	,481	-,001	,060	,465	-,715
6	-,212	,606	,045	-,608	,069	,460
Método de Extração: Análise de componentes principais. Método de rotação: Varimax e normalização de Kaiser.						

Objetivo 3 - Analisar o grau de confiança que os estudantes universitários têm com a IoT

Tabela 16 – KMO e Teste de Bartlett's da ACP da confiança na IoT

KMO e Teste de Bartlett's		
KMO		,813
Teste de Bartlett's	Qui-Quadrado Aprox.	540,815
	Grau de Liberdade	91
	Sig.	,000

Tabela 17 – Variância total explicada da ACP da confiança na IoT

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	4,843	34,589	34,589	2,852	20,370	20,370

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
2	1,445	10,321	44,910	2,256	16,113	36,483
3	1,420	10,142	55,052	2,041	14,580	51,063
4	1,031	7,366	62,418	1,590	11,356	62,418
5	,820	5,859	68,277			
6	,799	5,707	73,984			
7	,679	4,851	78,835			
8	,632	4,512	83,347			
9	,545	3,893	87,241			
10	,493	3,523	90,764			
11	,408	2,912	93,676			
12	,374	2,674	96,350			
13	,299	2,137	98,488			
14	,212	1,512	100,000			

Método de Extração: Análise de componentes principais

Tabela 18 – Matriz de componentes da ACP relativa à confiança na IoT

Matriz de componentes				
Componentes	1	2	3	4
1	,672	,510	,428	,323
2	-,028	-,701	,488	,519
3	-,506	,272	,738	-,355
4	-,540	,417	-,184	,707
Método de Extração: Análise de componentes principais Método de Rotação: Varimax com normalização Kaiser				

Objetivo 4 - Determinar os riscos e ameaças associados à IoT

Tabela 19 – KMO e Teste de Bartlett's da ACP dos riscos e ameaças na IoT

KMO e Teste de Bartlett's		
KMO		,887
Teste de Bartlett's	Qui-Quadrado Aprox.	574,428
	Grau de Liberdade	66
	Sig.	,000

Tabela 20 – Variância total explicada da ACP dos riscos e ameaças associados à IoT

Variância Total Explicada						
Componentes	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**	**Valores Próprios**	**% Variância Explicada**	**% Cumulativa**
1	5,941	49,512	49,512	3,860	32,163	32,163
2	1,425	11,874	61,386	3,507	29,223	61,386
3	,895	7,458	68,844			
4	,722	6,018	74,862			
5	,604	5,031	79,893			
6	,534	4,448	84,340			
7	,452	3,764	88,105			
8	,371	3,089	91,194			
9	,350	2,916	94,110			
10	,281	2,339	96,449			
11	,252	2,097	98,547			
12	,174	1,453	100,000			

Método de Extração: Análise de componentes principais

Tabela 21 – Matriz de componentes da ACP relativa à confiança na IoT

Matriz de Componentes		
Componentes	1	2
1	,734	,679
2	,679	,734
Método de Extração: Análise de componentes principais Método de Rotação: Varimax com normalização Kaiser.		

Objetivo 5 - Verificar as principais áreas de aplicação da IoT

Tabela 22 – Tabela de frequência das principais áreas de aplicação da IoT

		Aeronáutica	Agricultura	Ambiente	Arquitectura	Casas e edifícios inteligentes (domótica)	Cidades inteligentes (*smart cities)*
N	Valido	92	92	92	92	92	92
	Em falta	140	140	140	140	140	140
Média		3,96	3,83	3,96	3,54	4,47	4,47
Mediana		4,00	4,00	4,00	4,00	5,00	5,00
Moda		4	4	4	4	5	5
Desvio-Padrão		,876	1,065	,837	1,010	,687	,718
Mínimo		1	1	2	1	2	2
Máximo		5	5	5	5	5	5

Continuação da tabela 22

	Fitness	Etiquetas inteligentes	Indústria	Infraestruturas inteligentes	Leitura automática dos contadores de eletricidade, água, gás e diversos serviços associados (*smart grids*)	Localização
N Válido	92	92	92	92	92	92
N Em falta	140	140	140	140	140	140
Média	3,82	3,89	4,25	4,32	4,25	3,97
Mediana	4,00	4,00	4,00	4,00	4,00	4,00
Moda	4	4	5	5	4	4
Desvio-Padrão	,994	1,043	,750	,755	,765	,999
Mínimo	1	1	2	2	2	1
Máximo	5	5	5	5	5	5

		Localização	Logística	Roupas inteligentes	Retalho	Saúde	Segurança
N	Válido	92	92	92	92	92	92
	Em falta	140	140	140	140	140	140
Média		3,97	4,12	3,32	3,58	4,15	3,84
Mediana		4,00	4,00	3,00	4,00	4,00	4,00
Moda		4	4	4	4	5	4
Desvio-Padrão		,999	,837	1,204	1,061	,901	1,009
Mínimo		1	1	1	1	1	1
Máximo		5	5	5	5	5	5

		Transportes	Uso pessoal/ doméstico	Veículos inteligentes	*Wearables*
N	Válido	92	92	92	92
	Em falta	140	140	140	140
Média		4,10	4,10	4,18	3,90
Mediana		4,00	4,00	4,00	4,00
Moda		4	4	4	5

Desvio-Padrão	,813	,799	,864	,995
Mínimo	1	2	1	1
Máximo	5	5	5	5

Objetivo 6: Determinar as áreas em que a IoT é útil

Tabela 23 – Tabela de frequência das principais áreas em que a IoT é útil

		Arquitectura	Engenharia Civil	Engenharia Mecânica	Estudantes	Industriais	Empresas/ Empresários(as)
N	Válido	92	92	92	92	92	92
	Em falta	140	140	140	140	140	140
Média		2,55	4,05	4,20	3,95	3,16	4,16
Mediana		4,00	4,00	4,00	4,00	4,00	4,00
Moda		4	4	4	4	4	4
Desvio-Padrão		10,752	,817	,745	,843	10,792	,788
Mínimo		-99	1	2	1	-99	2
Máximo		5	5	5	5	5	5

		Informática	Motoristas	Professores	Profissionais da Informação/Comunicação
N	Válido	92	92	92	92
	Em falta	140	140	140	140
Média		3,38	3,71	2,58	2,91
Mediana		5,00	4,00	4,00	4,00
Moda		5	4	4	4
Desvio-Padrão		10,810	,896	10,752	10,778
Mínimo		-99	1	-99	-99
Máximo		5	5	5	5
		Profissionais Governamentais	Profissionais de Saúde	Profissionais de Segurança	Psicologia
N	Válido	92	92	92	92
	Em falta	140	140	140	140
Média		3,51	4,03	2,92	1,99
Mediana		4,00	4,00	4,00	3,00
Moda		4	4	4	3
Desvio-Padrão		,943	1,032	10,790	10,703
Mínimo		1	1	-99	-99

Máximo	5	5	5	5

Apêndice D – Tabelas de frequência dos índices das ACPs

Objetivo 1 - Perceções sobre a IoT

Tabela 24 – Tabela de frequência para o índice de Dispositivos interligados

		Frequência	Percentagem Válida
Válido	1,00	2	1,7
	2,00	1	,9
	2,50	1	,9
	2,75	1	,9
	3,00	7	6,0
	3,25	7	6,0
	3,50	17	14,5
	3,75	15	12,8
	4,00	31	26,5
	4,25	8	6,8
	4,50	5	4,3
	4,75	6	5,1
	5,00	16	13,7
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 25 – Tabela de frequência para o índice do componente Redes de sensores

		Frequência	Percentagem Válida
Válido	1,00	2	1,7
	2,00	1	,9
	2,50	1	,9
	2,75	1	,9
	3,00	7	6,0
	3,25	7	6,0
	3,50	17	14,5
	3,75	15	12,8
	4,00	31	26,5
	4,25	8	6,8
	4,50	5	4,3
	4,75	6	5,1
	5,00	16	13,7

	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 26 – Tabela de frequência para o índice do componente Máquinas inteligentes

		Frequência	Percentagem Válida
Válido	1,00	1	,9
	1,60	1	,9
	2,00	1	,9
	2,20	2	1,7
	2,40	1	,9
	2,60	2	1,7
	2,80	5	4,3
	3,00	4	3,4
	3,20	6	5,1
	3,40	17	14,5
	3,60	18	15,4
	3,80	15	12,8
	4,00	14	12,0
	4,20	9	7,7
	4,40	3	2,6
	4,60	8	6,8
	4,80	4	3,4
	5,00	6	5,1
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 27 – Tabela de frequência para o índice do componente Potencial

		Frequência	Percentagem Válida
Válido	1,00	5	4,3
	1,50	5	4,3
	2,00	8	6,8
	2,50	24	20,5
	3,00	24	20,5
	3,50	18	15,4
	4,00	19	16,2
	4,50	3	2,6
	5,00	11	9,4
	Total	117	100,0

Em falta	Sistema	115	
Total		232	

Tabela 28 – Tabela de frequência para o índice do componente Autonomia

		Frequência	Percentagem Válida
Válido	1,00	2	1,7
	1,50	1	,9
	2,00	2	1,7
	2,50	5	4,3
	3,00	19	16,2
	3,50	20	17,1
	4,00	41	35,0
	4,50	17	14,5
	5,00	10	8,5
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Objetivo 2 - Expectativas sobre a IoT

Tabela 29 – Tabela de frequência para o índice de Facilidade tecnológica

		Frequência	Percentagem Válida
Válido	2,92	1	,9
	3,00	5	4,3
	3,08	2	1,7
	3,17	1	,9
	3,25	1	,9
	3,50	2	1,7
	3,58	5	4,3
	3,67	5	4,3
	3,75	4	3,4
	3,83	6	5,1
	3,92	9	7,7
	4,00	21	17,9
	4,08	1	,9
	4,17	7	6,0
	4,25	6	5,1
	4,33	5	4,3

		Frequência	Percentagem Válida
	4,42	8	6,8
	4,50	1	,9
	4,58	3	2,6
	4,67	4	3,4
	4,75	4	3,4
	4,83	6	5,1
	4,92	3	2,6
	5,00	7	6,0
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 30 – Tabela de frequência para o índice do componente Oportunidades

		Frequência	Percentagem Válida
Válido	1,00	1	,9
	1,50	3	2,6
	2,00	4	3,4
	2,50	13	11,1
	3,00	24	20,5
	3,50	21	17,9
	4,00	30	25,6
	4,50	11	9,4
	5,00	10	8,5
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 31 – Tabela de frequência para o índice de Privacidade e Segurança

		Frequência	Percentagem Válida
Válido	1,00	3	2,6
	1,33	3	2,6
	1,67	5	4,3
	2,00	4	3,4
	2,33	8	6,8
	2,67	8	6,8
	3,00	20	17,1
	3,33	15	12,8
	3,67	17	14,5

		Frequência	Percentagem Válida
	4,00	19	16,2
	4,33	6	5,1
	4,67	6	5,1
	5,00	3	2,6
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 32 – Tabela de frequência para o índice do componente Confiabilidade

		Frequência	Percentagem Válida
Válido	2,00	5	4,3
	2,33	7	6,0
	2,67	9	7,7
	3,00	23	19,7
	3,33	22	18,8
	3,67	20	17,1
	4,00	17	14,5
	4,33	5	4,3
	4,67	4	3,4
	5,00	5	4,3
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 33 – Tabela de frequência para o índice do componente Usabilidade

		Frequência	Percentagem Válida
Válido	1,00	2	1,7
	1,33	1	,9
	1,67	1	,9
	2,00	3	2,6
	2,33	2	1,7
	2,67	5	4,3
	3,00	13	11,1
	3,33	14	12,0
	3,67	24	20,5
	4,00	30	25,6
	4,33	5	4,3
	4,67	6	5,1
	5,00	11	9,4

		Frequência	Percentagem Válida
	Total	117	100,0
Missing	System	115	
Total		232	

Tabela 34 – Tabela de frequência para o índice do componente Comunicação

		Frequência	Percentagem Válida
Válido	1,50	2	1,7
	2,00	4	3,4
	2,50	10	8,5
	3,00	17	14,5
	3,50	21	17,9
	4,00	33	28,2
	4,50	25	21,4
	5,00	5	4,3
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Objetivo 3 - Confiança na IoT

Tabela 35 – Tabela de frequência para o índice do componente Conformidade

		Frequência	Percentagem Válida
Válido	1,20	1	,9
	2,00	2	1,7
	2,40	3	2,6
	2,60	1	,9
	2,80	5	4,3
	3,00	16	13,7
	3,20	8	6,8
	3,40	9	7,7
	3,60	22	18,8
	3,80	14	12,0
	4,00	20	17,1
	4,20	6	5,1
	4,40	3	2,6
	4,60	2	1,7
	4,80	4	3,4
	5,00	1	,9

		Frequência	Percentagem Válida
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 36 – Tabela de frequência para o índice do componente Segurança

		Frequência	Percentagem Válida
Válido	1,00	2	1,7
	1,33	4	3,4
	1,67	1	,9
	2,00	18	15,4
	2,33	11	9,4
	2,67	18	15,4
	3,00	20	17,1
	3,33	8	6,8
	3,67	10	8,5
	4,00	18	15,4
	4,33	6	5,1
	5,00	1	,9
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Tabela 37 – Tabela de frequência para o índice do componente Fiabilidade

		Frequência	Percentagem Válida
Válido	1,75	1	,9
	2,00	2	1,7
	2,25	1	,9
	2,50	1	,9
	2,75	2	1,7
	3,00	21	17,9
	3,25	15	12,8
	3,50	17	14,5
	3,75	17	14,5
	4,00	21	17,9
	4,25	9	7,7
	4,50	6	5,1
	4,75	3	2,6
	5,00	1	,9
	Total	117	100,0

		Frequência	Percentagem Válida
Em falta	Sistema	115	
Total		232	

Tabela 38 – Tabela de frequência para o índice do componente Complexidade

		Frequência	Percentagem Válida
Válido	1,50	1	,9
	2,00	5	4,3
	2,50	3	2,6
	3,00	17	14,5
	3,50	26	22,2
	4,00	47	40,2
	4,50	11	9,4
	5,00	7	6,0
	Total	117	100,0
Em falta	Sistema	115	
Total		232	

Objetivo 4 - Riscos e Ameaças na IoT

Tabela 39 – Tabela de frequência para o índice do componente Dados e rede

		Frequência	Percentagem Válida
Válido	1,00	3	3,3
	1,17	1	1,1
	1,33	3	3,3
	1,50	2	2,2
	1,67	4	4,3
	1,83	2	2,2
	2,00	5	5,4
	2,17	5	5,4
	2,33	2	2,2
	2,50	4	4,3
	2,67	4	4,3
	2,83	4	4,3
	3,00	16	17,4
	3,17	8	8,7
	3,33	7	7,6
	3,50	4	4,3
	3,67	6	6,5

		Frequência	Percentagem Válida
	3,83	1	1,1
	4,00	7	7,6
	4,17	1	1,1
	4,50	2	2,2
	4,67	1	1,1
	Total	92	100,0
Em falta	Sistema	140	
Total		232	

Tabela 40 – Tabela de frequência para o índice do componente Segurança

		Frequência	Percentagem Válida
Válido	1,00	1	1,1
	1,17	1	1,1
	1,33	2	2,2
	1,67	2	2,2
	1,83	3	3,3
	2,00	7	7,6
	2,17	3	3,3
	2,33	10	10,9
	2,50	5	5,4
	2,67	4	4,3
	2,83	7	7,6
	3,00	14	15,2
	3,17	3	3,3
	3,33	5	5,4
	3,50	4	4,3
	3,67	3	3,3
	3,83	6	6,5
	4,00	8	8,7
	4,17	2	2,2
	4,33	1	1,1
	4,67	1	1,1
	Total	92	100,0
Em falta	Sistema	140	
Total		232	

Apêndice E – Correlações

Tabela 41 – Correlações entre Dispositivos interligados, Redes de sensores, Máquinas inteligentes, Potencial e Autonomia

Correlações						
		Dimensão Dispositivos interligados	Dimensão Redes de sensores	Dimensão Máquinas inteligentes	Dimensão Potencial	Dimensão Autonomia
Dimensão Dispositivos interligados	Correlação de Pearson	1	,666***	,533***	,461***	,471***
	Sig. (bicaudal)		,000	,000	,000	,000
	N	117	117	117	117	117
Dimensão Redes de sensores	Correlação de Pearson	,666***	1	,592***	,504***	,487***
	Sig. (bicaudal)	,000		,000	,000	,000
	N	117	117	117	117	117
Dimensão Máquinas inteligentes	Correlação de Pearson	,533***	,592***	1	,494***	,442***
	Sig. (bicaudal)	,000	,000		,000	,000
	N	117	117	117	117	117
Dimensão Potencial	Correlação de Pearson	,461***	,504***	,494***	1	,403***
	Sig. (bicaudal)	,000	,000	,000		,000
	N	117	117	117	117	117
Dimensão Autonomia	Correlação de Pearson	,471***	,487***	,442***	,403***	1
	Sig. (bicaudal)	,000	,000	,000	,000	
	N	117	117	117	117	117
*p<0,050; **p<0,010; ***p<0,001						

Tabela 42 – Correlações entre Facilidade tecnológica, Oportunidades, Privacidade e Segurança, Confiabilidade, Usabilidade e Comunicação

Correlações							
		Dimensão Facilidade Tecnológica	Dimensão Oportunidades	Dimensão Privacidade e Segurança	Dimensão Confiabilidade	Dimensão Usabilidade	Dimensão Comunicação
Dimensão Facilidade Tecnológica	Correlação de Pearson	1	,463***	,043	,380***	,408***	,362***
	Sig. (bicaudal)		,000	,643	,000	,000	,000
	N	117	117	117	117	117	117
Dimensão Oportunidades	Correlação de Pearson	,463***	1	,068	,401***	,145	,324***
	Sig. (bicaudal)	,000		,466	,000	,119	,000
	N	117	117	117	117	117	117
Dimensão Privacidade e Segurança	Correlação de Pearson	,043	,068	1	,057	,062	,004
	Sig. (bicaudal)	,643	,466		,539	,508	,969
	N	117	117	117	117	117	117
Dimensão Confiabilidade	Correlação de Pearson	,380***	,401***	,057	1	,299**	,425***
	Sig. (bicaudal)	,000	,000	,539		,001	,000
	N	117	117	117	117	117	117
Dimensão Usabilidade	Correlação de Pearson	,408***	,145	,062	,299**	1	,302**
	Sig. (bicaudal)	,000	,119	,508	,001		,001
	N	117	117	117	117	117	117
Dimensão Comunicação	Correlação de Pearson	,362***	,324***	,004	,425***	,302**	1
	Sig. (bicaudal)	,000	,000	,969	,000	,001	
	N	117	117	117	117	117	117
*p<0,050; **p<0,010; ***p<0,001							

Tabela 43 – Correlações Conformidade, Segurança, Fiabilidade e Complexidade

Correlações					
		Dimensão Conformidade	Dimensão Segurança	Dimensão Fiabilidade	Dimensão Complexidade
Dimensão Conformidade	Correlação de Pearson	1	,488***	,433***	,401***
	Sig. (bicaudal)		,000	,000	,000
	N	117	117	117	117
Dimensão Segurança	Correlação de Pearson	,488***	1	,395***	,191*
	Sig. (bicaudal)	,000		,000	,039
	N	117	117	117	117
Dimensão Fiabilidade	Correlação de Pearson	,433***	,395***	1	,286**
	Sig. (bicaudal)	,000	,000		,002
	N	117	117	117	117
Dimensão Complexidade	Correlação de Pearson	,401***	,191*	,286**	1
	Sig. (bicaudal)	,000	,039	,002	
	N	117	117	117	117
*p<0,050; **p<0,010; ***p<0,001					

Tabela 44 – Correlações entre Dados e rede com Segurança

Correlações			
		Dimensão Dados e rede	Dimensão Segurança
Dimensão Dados e rede	Correlação de Pearson	1	,661***
	Sig. (bicaudal)		,000
	N	92	92
Dimensão Segurança	Correlação de Pearson	,661***	1
	Sig. (bicaudal)	,000	
	N	92	92
*p<0,050; **p<0,010; ***p<0,001			

Tabela 45 – Correlações entre todos os índices dos componentes

Correlações						
		Dispositivos interligados	Redes de sensores	Máquinas inteligentes	Potencial	Autonomia
Dispositivos interligados	Correlação de Pearson	1	,666***	,533***	,461***	,471***
	Sig. (bicaudal)		,000	,000	,000	,000
	N	117	117	117	117	117
Redes de sensores	Correlação de Pearson	,666***	1	,592***	,504***	,487***

Correlações						
		Dispositivos interligados	Redes de sensores	Máquinas inteligentes	Potencial	Autonomia
	Sig. (bicaudal)	,000		,000	,000	,000
	N	117	117	117	117	117
Máquinas inteligentes	Correlação de Pearson	,533***	,592***	1	,494***	,442***
	Sig. (bicaudal)	,000	,000		,000	,000
	N	117	117	117	117	117
Potencial	Correlação de Pearson	,461***	,504***	,494***	1	,403***
	Sig. (bicaudal)	,000	,000	,000		,000
	N	117	117	117	117	117
Autonomia	Correlação de Pearson	,471***	,487***	,442***	,403***	1
	Sig. (bicaudal)	,000	,000	,000	,000	
	N	117	117	117	117	117
Facilidade tecnológica	Correlação de Pearson	,482***	,500***	,453***	,339***	,383***
	Sig. (bicaudal)	,000	,000	,000	,000	,000
	N	117	117	117	117	117
Oportunidades	Correlação de Pearson	,253**	,289**	,296**	,280**	,148
	Sig. (bicaudal)	,006	,002	,001	,002	,111
	N	117	117	117	117	117
Privacidade e Segurança	Correlação de Pearson	,191*	,077	,139	,170	,028
	Sig. (bicaudal)	,039	,408	,134	,067	,762
	N	117	117	117	117	117
Confiabilidade	Correlação de Pearson	,269**	,272**	,407***	,319***	,209*
	Sig. (bicaudal)	,003	,003	,000	,000	,024
	N	117	117	117	117	117
Usabilidade	Correlação de Pearson	,313**	,295**	,472***	,348***	,320***

Correlações						
		Dispositivos interligados	Redes de sensores	Máquinas inteligentes	Potencial	Autonomia
	Sig. (bicaudal)	,001	,001	,000	,000	,000
	N	117	117	117	117	117
Comunicação	Correlação de Pearson	,252**	,161	,397**	,351**	,142
	Sig. (bicaudal)	,006	,083	,000	,000	,127
	N	117	117	117	117	117
Conformidade	Correlação de Pearson	,268**	,238**	,329***	,451***	,159
	Sig. (bicaudal)	,003	,010	,000	,000	,086
	N	117	117	117	117	117
Segurança	Correlação de Pearson	,210*	,130	,369***	,316**	,122
	Sig. (bicaudal)	,023	,161	,000	,001	,189
	N	117	117	117	117	117
Fiabilidade	Correlação de Pearson	,246**	,264**	,398***	,275**	,252**
	Sig. (bicaudal)	,007	,004	,000	,003	,006
	N	117	117	117	117	117
Complexidade	Correlação de Pearson	,244**	,247**	,273**	,296**	,101
	Sig. (bicaudal)	,008	,007	,003	,001	,278
	N	117	117	117	117	117
Dados e Rede	Correlação de Pearson	-,036	-,045	-,133	-,016	-,013
	Sig. (bicaudal)	,731	,673	,207	,883	,902
	N	92	92	92	92	92
Segurança	Coeficiente de Pearson	-,080	-,111	-,274**	-,081	,014
	Sig. (bicaudal)	,448	,292	,008	,441	,897
	N	92	92	92	92	92

Continuação da tabela

		Facilidade Tecnologica	Oportunidades	Privaci-Dade e segurança	Confiabilidade	Usabili-dade	Comunicação
Dispositivos interligados	Correlação de Pearson	,482***	,253**	,191*	,269**	,313**	,252**
	Sig. (bicaudal)	,000	,006	,039	,003	,001	,006
	N	117	117	117	117	117	117
Redes de sensores	Correlação de Pearson	,500***	,289**	,077	,272**	,295**	,161
	Sig. (bicaudal)	,000	,002	,408	,003	,001	,083
	N	117	117	117	117	117	117
Máquinas inteligentes	Correlação de Pearson	,453***	,296**	,139	,407***	,472***	,397***
	Sig. (bicaudal)	,000	,001	,134	,000	,000	,000
	N	117	117	117	117	117	117
Potencial	Correlação de Pearson	,339***	,280**	,170	,319***	,348***	,351***
	Sig. (bicaudal)	,000	,002	,067	,000	,000	,000
	N	117	117	117	117	117	117
Autonomia	Correlação de Pearson	,383***	,148	,028	,209*	,320***	,142
	Sig. (bicaudal)	,000	,111	,762	,024	,000	,127
	N	117	117	117	117	117	117
Facilidade tecnológica	Correlação de Pearson	1	,463***	,043	,380***	,408***	,362***
	Sig. (bicaudal)		,000	,643	,000	,000	,000
	N	117	117	117	117	117	117
Oportunidades	Correlação de Pearson	,463***	1	,068	,401***	,145	,324***
	Sig. (bicaudal)	,000		,466	,000	,119	,000
	N	117	117	117	117	117	117
Privacidade e Segurança	Correlação de Pearson	,043	,068	1	,057	,062	,004
	Sig. (bicaudal)	,643	,466		,539	,508	,969
	N	117	117	117	117	117	117

		Facilidade Tecnologica	Oportunidades	Privaci-Dade e segurança	Confiabilidade	Usabili-dade	Comunicação
Confiabilidade	Correlação de Pearson	,380***	,401***	,057	1	,299**	,425***
	Sig. (bicaudal)	,000	,000	,539		,001	,000
	N	117	117	117	117	117	117
Usabilidade	Correlação de Pearson	,408***	,145	,062	,299**	1	,302**
	Sig. (bicaudal)	,000	,119	,508	,001		,001
	N	117	117	117	117	117	117
Comunicação	Correlação de Pearson	,362***	,324***	,004	,425***	,302**	1
	Sig. (bicaudal)	,000	,000	,969	,000	,001	
	N	117	117	117	117	117	117
Conformidade	Correlação de Pearson	,450***	,321***	,081	,396***	,245**	,297**
	Sig. (bicaudal)	,000	,000	,388	,000	,008	,001
	N	117	117	117	117	117	117
Segurança	Correlação de Pearson	,275**	,317***	,006	,479***	,378***	,432***
	Sig. (bicaudal)	,003	,000	,951	,000	,000	,000
	N	117	117	117	117	117	117
Fiabilidade	Correlação de Pearson	,398***	,153	-,128	,441***	,331***	,281**
	Sig. (bicaudal)	,000	,100	,168	,000	,000	,002
	N	117	117	117	117	117	117
Complexidade	Correlação de Pearson	,376***	,296**	,152	,363***	,178	,233*
	Sig. (bicaudal)	,000	,001	,102	,000	,055	,012
	N	117	117	117	117	117	117
Dados e Rede	Correlação de Pearson	-,093	-,120	,361***	-,124	-,071	-,251*
	Sig. (bicaudal)	,380	,254	,000	,241	,503	,016
	N	92	92	92	92	92	92

		Facilidade Tecnologica	Oportunidades	Privaci-Dade e segurança	Confiabilidade	Usabili-dade	Comunicação
Segurança	Correlação de Pearson	-,157	-,086	,296**	-,242*	-,099	-,299**
	Sig. (bicaudal)	,135	,416	,004	,020	,350	,004
	N	92	92	92	92	92	92

Continuação da tabela

		Conformidade	Segurança	Fiabilidade	Complexidade	Dados e rede	Segurança
Dispositivos interligados	Correlação de Pearson	,268**	,210*	,246**	,244**	-,036	-,080
	Sig. (bicaudal)	,003	,023	,007	,008	,731	,448
	N	117	117	117	117	92	92
Rede de sensores	Correlação de Pearson	,238**	,130	,264**	,247**	-,045	-,111
	Sig. (bicaudal)	,010	,161	,004	,007	,673	,292
	N	117	117	117	117	92	92
Máquinas inteligentes	Correlação de Pearson	,329***	,369***	,398***	,273**	-,133	-,274**
	Sig. (bicaudal)	,000	,000	,000	,003	,207	,008
	N	117	117	117	117	92	92
Potencial	Correlação de Pearson	,451***	,316**	,275**	,296**	-,016	-,081
	Sig. (bicaudal)	,000	,001	,003	,001	,883	,441
	N	117	117	117	117	92	92
Autonomia	Correlação de Pearson	,159	,122	,252**	,101	-,013	,014
	Sig. (bicaudal)	,086	,189	,006	,278	,902	,897
	N	117	117	117	117	92	92
Facilidade tecnológica	Correlação de Pearson	,450***	,275**	,398***	,376***	-,093	-,157

		Confor-midade	Segu-rança	Fiabilidade	Complexi-dade	Dados e rede	Segurança
	Sig. (bicaudal)	,000	,003	,000	,000	,380	,135
	N	117	117	117	117	92	92
Oportunidades	Correlação de Pearson	,321***	,317***	,153	,296**	-,120	-,086
	Sig. (bicaudal)	,000	,000	,100	,001	,254	,416
	N	117	117	117	117	92	92
Privacidade e segurança	Correlação de Pearson	,081	,006	-,128	,152	,361**	,296**
	Sig. (bicaudal)	,388	,951	,168	,102	,000	,004
	N	117	117	117	117	92	92
Confiabilidade	Correlação de Pearson	,396***	,479***	,441***	,363***	-,124	-,242*
	Sig. (bicaudal)	,000	,000	,000	,000	,241	,020
	N	117	117	117	117	92	92
Usabilidade	Correlação de Pearson	,245**	,378***	,331***	,178	-,071	-,099
	Sig. (bicaudal)	,008	,000	,000	,055	,503	,350
	N	117	117	117	117	92	92
Comunicação	Correlação de Pearson	,297**	,432***	,281**	,233*	-,251*	-,299**
	Sig. (bicaudal)	,001	,000	,002	,012	,016	,004
	N	117	117	117	117	92	92
Conformidade	Correlação de Pearson	1	,488***	,433***	,401***	-,024	-,124
	Sig. (bicaudal)		,000	,000	,000	,822	,239
	N	117	117	117	117	92	92
Segurança	Correlação de Pearson	,488***	1	,395***	,191*	-,139	-,173
	Sig. (bicaudal)	,000		,000	,039	,186	,100
	N	117	117	117	117	92	92

		Confor-midade	Segu-rança	Fiabilidade	Complexi-dade	Dados e rede	Segurança
Fiabilidade	Correlação de Pearson	,433***	,395***	1	,286**	-,142	-,163
	Sig. (bicaudal)	,000	,000		,002	,176	,120
	N	117	117	117	117	92	92
Complexidade	Correlação de Pearson	,401***	,191*	,286**	1	,166	,088
	Sig. (bicaudal)	,000	,039	,002		,113	,403
	N	117	117	117	117	92	92
Dados e rede	Correlação de Pearson	-,024	-,139	-,142	,166	1	,661***
	Sig. (bicaudal)	,822	,186	,176	,113		,000
	N	92	92	92	92	92	92
Segurança	Correlação de Pearson	-,124	-,173	-,163	,088	,661***	1
	Sig. (bicaudal)	,239	,100	,120	,403	,000	
	N	92	92	92	92	92	92

*p<0,050; **p<0,010; ***p<0,001

Anexo 1 – Artigo

Perceptions and expectations of college students about the internet of things?

Catarina Vasconcelos[1], Abílio Oliveira[2]

[1]*Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal*

catarina_alexandra_vasconcelos@iscte-iul.pt

[2]*Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL, Lisboa, Portugal*

abilio.oliveira@iscte-iul.pt

Abstract

The Internet is increasingly used as a means of communication of excellence. With the increasing ease and access to virtual communication, namely through social networks, it is verified that the relationships between people have assumed new forms of expression and higher levels of importance in society. In addition to communication between people, there is also an increasing possibility of any object communicating and connecting to other objects, with a unique way of identifying, anywhere, with devices connected to the Internet, this being the essential concept of Internet of Things (IoT).

In this paper, our main goal is understand how college students represent IoT and what are their perceptions and expectations about it. From their point of view, is important to verify what is the impact

that IoT may have on their Pearsonal lives, academic performance and in society. According to the methodology adopted we performed individual interviews with a population of college students.

Data were treated through context analyses, after being transcribed and analyzed, using a typical software - Leximancer. Our findings showed that, in general, participants have an accurate perception about the Internet of Things, and how it works, and that they also have positive expectations in relation to it, considering it can be useful to our day-to-day life. Although, at the same time, they highlight the importance of being careful in terms of privacy, threats, vulnerabilities and risks associated to the internet.

Keywords: Internet of Things (IoT), college students, perceptions, expectations, vulnerabilities.

1 INTRODUCTION

The main goal of this research is based on analyzing the perceptions and expectations that college students have about the Internet of Things (IoT) and, from their point of view, what impact it may have on their Pearsonal lives, academic performance and in society.

The Internet is more and more used for the most different purposes, and this has caused a very large growth of the devices connected to it. In an initial phase, the growth of the connected entities was made by the increase of the use, more human connected results in more computers, as in more servers (Coelho, 2017).

According to (Li, Xu, & Zhao, 2015), the Internet of Things is a paradigm that is rapidly gaining ground in the scenario of wireless telecommunications. The idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones – which, through unique addressing schemes, can interact with each other and cooperate with their neighbors to reach common goals.

The technological revolution of the mobile devices, through smartphones and tablets, resulted in an additional growth in the number of devices, because it also allowed the growth among the public that already used the Internet in computers, connecting other new devices (Coelho, 2017).

The IoT will create a world where physical objects are integrated into information networks in order to provide advanced and intelligent services to humans. Trust management performs an important role in IoT for the fusion of reliable data, skilled services with context awareness, and greater privacy and security of user information. This helps people overcome their perceived uncertainty and risk and involves user acceptance and consumption in IoT services and applications (Yan *et al*., 2014).

The IoT, with his vision of objects connected to the Internet, could promote the role of ICTs as facilitators of innovation in a variety of areas and applications. In terms of application and market sectors in which IoT solutions can offer competitive advantages over current solutions, the following are identified: environmental monitoring; smart cities; smart houses/intelligent building management; health-care; security and surveillance (Miorandi *et al.*, 2012).

Currently with IoT it is possible to connect all kinds of objects in the network, resulting in an exponential increase of connected objects.

A few years ago, this concept was not very common in organizations and international institutions, but that did not undermine that more and more devices were becoming connected through the network. According to some manufacturers, in 2009 there was an increase in Internet connected devices in relation to people (in 2010 there were a total of 12.500 million objects connected to the Internet, almost twice the world population). The global trend is that more and more devices are networked. These devices fulfill different functions, such as monitoring, sensing, warning, interaction or distribution of processing. This leads analysts, consultants and manufacturers to agree: in 2020 the number of connected devices will exceed 26.000 million with an exponential growth (in 2009 the number of devices connected to the network was approximately 900 million). And this represents a very important share of IT and communications revenues in the very near future (Coelho, 2017).

The devices connected through the wireless network exceeded 16 billion in 2014, a 20% increase compared to 2013. With this trend, the number of devices will be more than double the current, with 40.9 billion expected by 2020. The growth between now and the end of the decade will come from devices like sensors and other accessories (Press, 2014).

According to the Intel organization, IoT is a robust network of devices, all integrated with software and sensors that allow them to exchange and analyze data. The IoT has been transforming the way we have lived for nearly two decades, paving a new way for innovative solutions, innovative products, efficient manufacturing, and ultimately, new and even more incredible ways to do business.

The IoT represents a solution with the potential to improve people's lives. Besides the exchange of data between machines, facilitating access to information, there is still the possibility of saving energy, safety, health, education and other aspects of everyday life.

2 METHODOLOGY

The present research aims, mainly, to understand the perceptions of college students about the Internet of Things (IoT), and what are their expectations about this technology.

In this phase, a qualitative study was carried out, based on five interviews with specialists in this field - 1 female element and 4 male elements - following a previously elaborated guide to make a survey of the core dimensions concerning the IoT. The main questions for the interviews were:

a) What is the Internet of Things for you? What perceptions do you have about this?

b) How do you feel about IoT's reliability?

c) What expectations do you have about IoT?

d) What advantages / disadvantages can IoT have in society?

e) What threats and risks do you envision using IoT?

f) In your opinion, what is the importance of IoT in society?

In the context of this paper, data were gathered from the answers to the questions a) and c) and analyzed through Leximancer, which is a text mining software used to analyze the content of textual documents.

This raising of indicators was fundamental for the construction of a questionnaire, to be used in the next phase of our current research project – being the inferential phase.

3 RESULTS

Based on the context analysis, we distinguished two types of groups. The first group is called perceptions, that consists of analyzing if college students know the meaning of Internet of Things. The second group has to meet the expectations students have about this technology. The two groups join in the importance of seeing what impact IoT can have on their Pearsonal lives, academic performance and society.

We used the Leximancer software to analyze the content of participants textual answers. Leximancer processes the text and find all the possible concepts, and themes. Then, we analyze and remove the ones that are not significant for these groups.

3.1 Perceptions about Internet of Things

Figure 1 shows the conceptual map elaborated by Leximancer, where the themes are presented in circles that group concepts. It is verified that the most relevant concepts are the Devices and IoT, followed by Internet, Data, Areas, Network and Equipment.

Highlighted is the term devices, it is one of the major themes that has more concepts associated. The devices are connected to the concepts Internet, data, areas, sensors which in turn to the network concept. The network sphere is linked to IoT concepts and equipment.

In this way, their perceptions about IoT are: IoT is a network of equipment, which through sensors connect to devices with internet connection in order to communicate with each other. The devices are connected to the Internet, being able to identify themselves in the network through sensors. The devices have ability to gather information through data. They are present in several areas. Devices can be controlled from a single equipment, provided it is connected to a network.

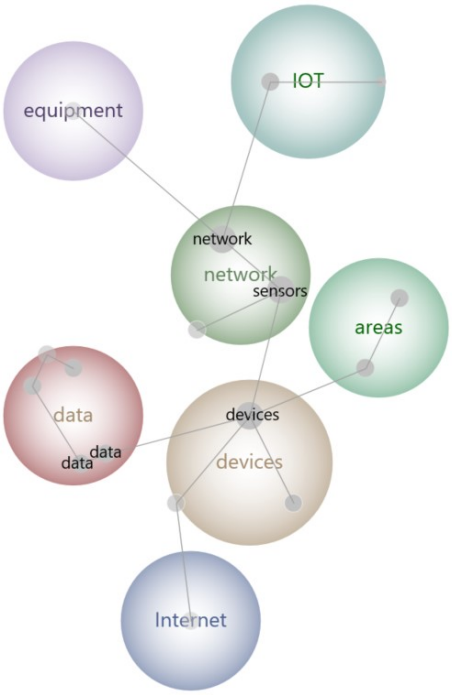


Figure 1. Perceptions about IoT

3.2 Expectations about Internet of Things

Figure 2 shows that nuclear spheres focus on devices, life and technology themes, followed by home, allows, interesting things.

Highlighted is the term devices, as the biggest theme is the subject with more associated concepts. Devices is a concept that is connected to problems which in turn to IoT. The sphere devices intersects with the sphere life, this means that they are interrelated. The devices are also connected to people, which in turn connected to the house. They are connected to technology and the sphere allows.

The technology is linked to the interesting sphere which in turn to things.

So, expectations about IoT are that: Devices are important because they can allow people at home to have a better quality of life, use technology to do interesting things. But on the other hand, IoT may have problems with these devices that have vulnerabilities.

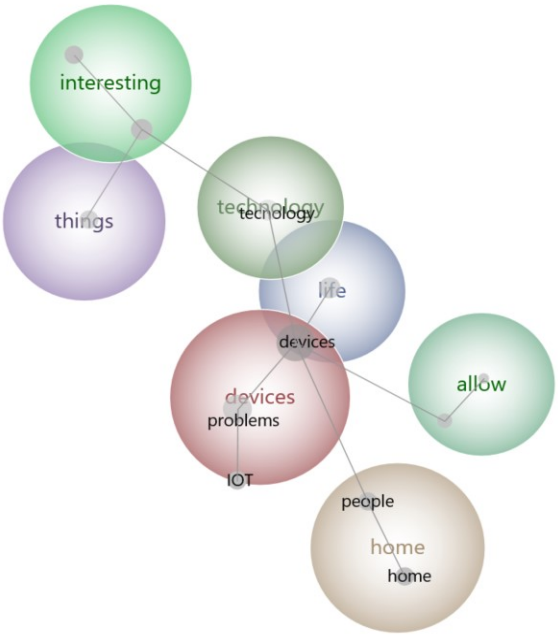


Figure 2. Expectations about IoT

4 CONCLUSIONS

For Albert Einstein, "The mind that opens to a new idea will never return to it is original size", this translates what technology can bring to the world (Albert Einstein, n.d.).

Miragliotta (Miragliotta, Perego, & Tumino, 2012) consider several definitions about the Internet of Things, demonstrating that there is a great interest in this subject. However, through the literature, there is a significant complexity in understanding the real meaning of Internet of Things and the social, economic and technical implications of IoT´s implementation.

According to our results, regarding the objective to determinate the perceptions about Internet of Things, now, it is clear this knowledge (see Figure 1), because it can tell us that the Internet of Things are all connected devices in a network in which it is possible to collect information/data, in the most different areas.

Ali (2015) refers that the Internet of Things is part of the group of the disruptive technologies and it has been adopted in many areas of everyday life.

From a conceptual point of view, the IoT is based on three pillars, related to the capability of intelligent objects to: be identifiable (anything identifies), communicate (anything communicates), and interact (anything interacts), between each other, building networks of interconnected objects, with end users or other entities in the network (Miorandi et al., 2012).

The term Internet of Things generally refers to scenarios in which network connectivity and computing capacity extend to objects, sensors, and common items that normally not considered as computers, allowing these devices to manage, exchange, and consume data with minimal human intervention. However, there is no single universal definition (Rose, Eldridge, & Lyman, 2015).

Regarding the expectations about IoT (see Figure 2), it is evident that it is an interesting technology in people's lives because this kind of devices at home allows to do interesting things. But IoT can also bring problems with these devices to the level of security and privacy, exposing system vulnerabilities.

For Sicari (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015), the dissemination of IoT services requires levels of security and privacy that must be guaranteed. But there is still a unified view of how to ensure this because the environment is so heterogeneous, involving different technologies and communication patterns. Solutions must be designed to ensure: confidentiality, access control and privacy for users

and things, reliability between devices and users, as well as compliance with defined security and privacy policies.

The Internet of Things will revolutionize people's lives in general, from the moment everyone understands this technology and bet on global solutions for the market that will make life easier for all people and organizations.

This study was important to understand the definition and expectations that one has about the Internet of Things. From here on, other avenues are open to be discovered and analyzed, such as the benefits and impact that this technology may has on people's lives and in society.

REFERENCES

Albert Einstein. Citations by Albert Einstein. Retrieved September 5, 2018, from https://citacoes.in/autores/albert-einstein/

Ali, F. (2015). Teaching The Internet of Things Concepts. *Proceedings of the WESE'15: Workshop on Embedded and Cyber-Physical Systems Education - WESE'15*, 1–6. http://doi.org/10.1145/2832920.2832930

Coelho, P. (2017). *Internet das Coisas - Introdução Prática*. FCA.

Intel. The Internet of Things (IoT). Retrieved August 5, 2018, from https://www.intel.com/content/www/us/en/internet-of-things/overview.html

Li, S., Xu, L. Da, & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. http://doi.org/10.1007/s10796-014-9492-7

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*. http://doi.org/10.1016/j.adhoc.2012.02.016

Miragliotta, G., Perego, A., & Tumino, A. (2012). Internet of Things: Smart Present or Smart Future? *Department of Management, Economics and Industrial Engineering, Politecnico Di Milano*.

Press, G. (n.d.). Internet of Things by the Numbers: Market Estimates and Forecasts. Retrieved from https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#3d636621b919

Rose, K., Eldridge, S., & Lyman, C. (2015). The internet of things: an overview. *Internet Society*, (October), 53. http://doi.org/10.1017/CBO9781107415324.004

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*. http://doi.org/10.1016/j.comnet.2014.11.008

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*. http://doi.org/10.1016/j.jnca.2014.01.014