INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

IoT (Internet of Things)

Podemos confiar?

Tomás Manuel Raposo Pereira Félix

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Orientador: Professor Doutor Paulo André Reis Duarte Branco

Presidente: Professor Doutor Pedro Ramos dos Santos Brandão

Arguente: Professor Doutor Filipe Montez Coelho Madeira

Março, 2022

ISTEC

Instituto Superior de Tecnologias Avançadas

Campus Académico do Lumiar, Lisboa

Dissertação
Mestrado em Informática

Por Tomás Félix

Dissertação de Mestrado, apresentada para cumprimento dos requisitos necessários à obtenção do grau de mestre em Informática, realizada sob a orientação científica do Professor Doutor Paulo André Reis Duarte Branco.

Lisboa, 2022

Índice

Índice de Figuras

Abreviaturas e Siglas

DLT - Tecnologia de Ledger Distribuído

DOS - *Denial of Service*

DDoS (*Distributed Denial of Service*)

DVR - Digital Video Recorder

HTTP - Hypertext Transfer Protocol

IoT - Internet of Things

LAN - Rede de área local

LTE- Long Term Evolution

M2M- Machine to Machine

NAS - Network-attached storage

VLAN - Virtual LAN

XSS - Cross-Site Scripting

Resumo

A IoT (Internet of Things), consiste num conjunto de vários tipos de software e de hardware que comunicam entre si (M2M), tendo o número de dispositivos aumentado, significativamente, nos últimos anos.

Com a IoT é feito o tratamento de dados de sensores, como por exemplo, por sensores de luz, CO2, de presença, entre outros. Dependendo da informação dos sensores, o sistema pode causar a realização de uma ação, desde ativar motores, a notificar o administrador do sistema.

Num mundo conectado entre si pela Internet, a confiança que existe na IoT pode diminuir devido à falta de segurança e de privacidade.

O principal foco desta dissertação é analisar se os utilizadores de IoT têm confiança na plataforma, olhando principalmente para a segurança e para a privacidade, tendo como metodologia a análise de documentos e a realização de um questionário, a vários utilizadores de dispositivos de IoT.

Nesta dissertação, foi criado um questionário, para tentar perceber o nível de confiança que as pessoas têm na IoT. No total, 84 pessoas responderam ao questionário. Podemos concluir com o questionário, que a maioria dos utilizadores tem receios sobre os dispositivos IoT. Os pontos que mais interferem com a confiança, de acordo com o questionário, são a segurança, a privacidade e a transparência que a marca induz no produto IoT.

Palavras-chave: Dispositivos, IoT, Privacidade, Segurança, Confiança

Abstract

The IoT (Internet of Things) consists of various types of software and hardware that communicate with each other (M2M), and the number of devices has increased significantly in recent years.

With IoT, sensor data is processed, for example, by light, CO2, and presence sensors, among others. Depending on the information from the sensors, the system can cause an action to be performed, from activating motors to notifying the system administrator.

In a world connected through the Internet, the trust in the IoT can diminish due to a lack of security and privacy.

The main focus of this dissertation is to analyze whether IoT users trust the platform, looking mainly at security and privacy, with the methodology of analyzing documents and conducting a questionnaire to several users of IoT devices.

In this dissertation, a questionnaire was created to try to understand the level of trust people have in the IoT. In total, 84 people answered the questionnaire. We can conclude from the questionnaire that most users fear IoT devices. According to the questionnaire, the points that most interfere with trust are security, privacy and the brand's transparency in the IoT product.
Keywords: Devices, IoT, Privacy, Security, Trust

Introdução

Contextualização do Tema

A IoT (*Internet of Things*, em português "Internet das Coisas") é um conceito, onde os dispositivos do dia-a-dia comunicam entre si. A Internet das Coisas permite ajudar as pessoas a viver e a trabalhar de forma mais inteligente, bem como a obter controlo total sobre as suas vidas. Para além de oferecer dispositivos inteligentes para automatizar casas, a IoT é essencial para os negócios. Esta fornece às empresas uma visão, em tempo real, sobre como os seus sistemas realmente funcionam, fornecendo informações sobre tudo, desde o desempenho das máquinas até à cadeia de fornecimento e operações logísticas (Gillis, 2020).

Nos últimos anos, a IoT tornou-se uma das tecnologias mais importantes do século XXI. Agora que podemos ligar objetos do quotidiano à Internet, através de dispositivos incorporados, é possível uma comunicação, sem falhas, entre pessoas, processos e coisas.

Através da computação de baixo custo, da *cloud*, *da big data*, dos *analytics* e das tecnologias móveis, os objetos físicos podem partilhar e recolher dados com um mínimo de intervenção humana. Neste mundo hiperligado, os sistemas digitais podem registar, monitorizar e ajustar cada interação entre as coisas ligadas. O mundo físico encontra o mundo digital - e eles cooperam (Oracle, 2021).

A IoT permite a existência de oportunidades e ligações virtualmente infinitas, muitas das quais nem sequer conseguimos pensar ou compreender. Não é difícil ver como nem porquê a Internet das Coisas é um tema tão importante hoje em dia; permite abrir certamente a porta a muitas oportunidades, mas também a muitos desafios. A segurança da *Internet of Things* é uma grande questão, que é muitas vezes levantada. Com milhares de milhões de dispositivos ligados entre si, o que podem as pessoas fazer, para garantir que a sua informação permaneça segura (Morgan, 2017)?

Tudo o que está ligado à Internet pode sofrer ataques informáticos, e os dispositivos IoT não são exceção a esta regra.

Há também a questão da vigilância. Se todos os objetos estiverem conectados entre si,

existe o potencial para a observação sem controlo dos utilizadores. Por exemplo, se um frigorífico ligado rastreia a utilização e o consumo de alimentos, os restaurantes e takeaways podem ser dirigidos a pessoas que não possuem alimentos no frigorífico (Burgess, 2018).

"No futuro, serviços inteligentes poderão utilizar a [Internet das coisas] para identificação, vigilância, monitorização, localização, e direcionamento para recrutamento ou para obter

acesso a redes ou credenciais de utilizadores", afirmou James Clapper, o diretor da inteligência nacional dos EUA em 2016, sendo documentado no jornal The Guardian (Ackerman & Thielman, 2016).

Objetivos

O objetivo deste estudo, passa por discutir e analisar problemas comuns na IoT, tais como palavras-passe fracas, previsíveis ou codificadas, interfaces inseguras, falta de mecanismos de atualização segura e bots, tendo como fim encontrar algumas soluções para a segurança e privacidade dos dispositivos e para o nível de confiança que os utilizadores têm.

Este estudo tem, também, como objetivos identificar o nível de confiança dos utilizadores na utilização da tecnologia IoT, identificar qual ou quais os problemas de segurança mais afetam os utilizadores, bem como as características de privacidade que os utilizadores consideram mais notáveis.

Estrutura da dissertação

A presente dissertação encontra-se estruturada em seis capítulos. O primeiro corresponde à introdução, onde está presente uma breve descrição do tema abordado e os objetivos desta dissertação. Segue-se o segundo capítulo, respeitante à Metodologia de Trabalho, onde está descrito o quadro metodológico adotado na investigação, tal como as diversas etapas realizadas na sua elaboração. O terceiro capítulo é composto pelo Enquadramento teórico, onde se analisa o quadro conceptual, inerente à Internet das Coisas, e o estado da arte desta problemática. O quarto capítulo designa-se Desenvolvimento do Estudo, onde é descrito como o questionário foi elaborado e a quem se aplica. De modo a analisar os dados recolhidos no formulário, existe um quinto capítulo específico para esse mesmo efeito, intitulado Análise dos Resultados. Por último, o sexto capítulo contempla as Conclusões deste estudo, tal como os trabalhos futuros a realizar posteriormente.

Metodologia de Trabalho

Para a realização deste trabalho, analisou-se qual seria a melhor metodologia a ser utilizada, sendo que se determinou que a mais adequada seria a metodologia quantitativa.

A investigação quantitativa utiliza números e métodos estatísticos. Tende a basear-se em medições numéricas de aspetos específicos dos fenómenos, abstrai-se de casos particulares para procurar uma descrição geral ou testar hipóteses causais e procura medições e análises que são facilmente replicáveis por outros investigadores (Thomas, 2011).

Esta metodologia será utilizada devido à grande evolução e alteração da área da IoT, utilizando assim uma metodologia quantitativa, sendo esta baseada num questionário online a diferentes utilizadores de IoT.

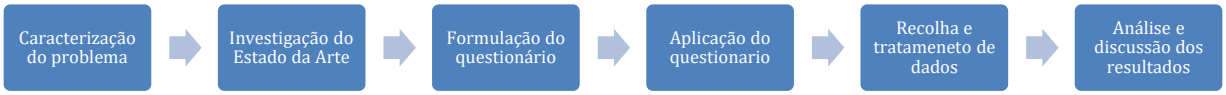

Figura 1 – Infográfico descrevendo as fases da metodologia

No primeiro passo do método científico (caracterização do problema) é onde se identificam as perguntas e as suas características. As questões identificadas neste trabalho são "Qual o nível de confiança dos utilizadores na utilização da tecnologia IoT?" e "Do ponto de vista do utilizador, quais são os problemas de segurança que mais afetam as plataformas de IoT e o seu uso?".

No capítulo investigação do estado da arte, debruçar-nos-emos sobre investigações e trabalhos semelhantes já realizados, que poderão dar o mote para a investigação a realizar. Neste trabalho, esta etapa foca-se na investigação de trabalhos realizados nas áreas da Confiança na IoT.

O subcapítulo Formulação do questionário será desenvolvido a partir do estado da arte. Serão formuladas questões que permitam perceber o nível de confiança que um utilizador IoT tem sobre os dispositivos e os problemas de segurança que o utilizador mais sofreu.

Depois do formulário criado no ponto anterior, e da sua partilha por vários meios digitais, os dados recebidos serão tratados com o método adequado para o tipo de pergunta que foi realizada ao utilizador de IoT.

Com os dados recolhidos, iremos neste ponto perceber se o trabalho é válido e definir recomendações para trabalhos futuros. Os resultados obtidos deverão contribuir para a comunidade científica.

Enquadramento teórico

Neste capítulo iremos apresentar o que é a IoT e os seus métodos de funcionamento, como também o conceito de confiança na IoT e alguns dos problemas de segurança no IoT.

Primeiro iremos observar em que consistem e o que são os dispositivos IoT, procurando perceber a metodologia nos dispositivos IoT, onde se aplicam e onde as pessoas terão mais interação com estes equipamentos.

A Internet of Things (IoT)

A Internet das Coisas, ou IoT, refere-se aos milhares de milhões de dispositivos físicos em todo o mundo que estão agora ligados à Internet, todos eles colecionando e partilhando dados. Através da utilização de chips de computador mais baratos e da ubiquidade das redes sem fios é possível transformar qualquer coisa, desde algo tão pequeno como um comprimido, até algo tão grande como um avião, numa parte da Internet das Coisas. Ligar todos estes diferentes objetos e adicionar-lhes sensores acrescenta um nível de inteligência digital a dispositivos que de outra forma seriam "ignorantes", permitindo-lhes comunicar dados em tempo real sem envolver um ser humano. A Internet das Coisas está a tornar o tecido do mundo à nossa volta mais inteligente e mais reativo, fundindo os universos digital e físico (Ranger, 2020).

Uma "coisa" ou objeto na Internet das coisas pode ser uma pessoa com um implante de monitor cardíaco, um animal de quinta com um biochip, um automóvel com sensores incorporados para alertar o condutor quando a pressão dos pneus é baixa, ou qualquer outro objeto natural, ou feito pelo homem a quem possa ser atribuído um endereço de Protocolo Internet (IP) e que seja capaz de transferir dados através de uma rede.

Cada vez mais, as organizações de uma variedade de indústrias estão a utilizar a IoT para operar mais eficientemente, compreender melhor os clientes para conseguirem prestar-lhes um melhor serviço, melhorar a tomada de decisões e aumentar o valor do negócio (Gillis, 2020).

A IoT tem como objetivo facilitar o dia-a-dia, como também permite descobrir falhas que possam existir no sistema e, principalmente, aumentar o conforto do utilizador (Ccg, 2018).

Segundo Drew W. (2016), as principais vantagens da Internet das Coisas são:

- **Automação -** A automação conduz à uniformidade das tarefas, qualidade do serviço e controlo das tarefas do dia-a-dia sem intervenção humana. A comunicação máquina-a-máquina, também ajuda a manter a transparência ao longo de todo o processo.

- **Eficiência -** A interação máquina-a-máquina, proporciona uma maior eficiência, permitindo que as pessoas se concentrem noutros trabalhos.

- **Redução de custos -** Para além da utilização ótima da energia e dos recursos, a IoT ajuda a aliviar os problemas associados a estrangulamentos, avarias e danos no sistema.

- **Comunicação -** A IoT permite que os dispositivos físicos permaneçam ligados e se comuniquem melhor, o que cria um maior controlo de qualidade.

- **Acesso instantâneo a dados -** Mais informação disponível ajuda a simplificar o processo de tomada de decisões, tornando a vida mais fácil de gerir.

Apesar de apresentar muitas vantagens, a *Internet of Things* também possui desvantagens na sua utilização. Bhagat (2019) declarou que algumas dessas desvantagens são:

- **Complexidade** - Com a IoT, há probabilidades de fracasso. Supondo, uma pessoa e o seu amigo receberam uma mensagem de que o pacote de leite guardado no frigorífico deles expirou. Assim, neste caso, ambos irão comprar um pacote de leite. Haverá dois pacotes que resultarão em desperdício de dinheiro. Isto torna todo o processo um pouco complicado. Para tornar este processo um tanto mais fácil, seria uma opção sensata registar ou ligar, apenas um dos seus números, com o dispositivo ativado por IoT.

- **Compatibilidade -** Existem milhões e biliões de dispositivos que estão ligados entre si no ecossistema da IoT, no entanto, todos os dispositivos são construídos por diferentes fabricantes, o que levanta a questão da compatibilidade na marcação e monitorização. É difícil convencer todos os fabricantes a construírem dispositivos que concordem com uma norma comum. Embora o Bluetooth possa ligar dispositivos diferentes, podem surgir problemas de compatibilidade, mesmo que os dispositivos da Internet das coisas estejam a dominar o mundo.

- **Privacidade ou Segurança -** Há um risco de perda de privacidade, nos dados que estão a ser transmitidos através de dispositivos IoT. É preciso ver como os dados estão a ser encriptados. Devido ao rápido crescimento da IoT, esta está a enfrentar problemas de segurança e privacidade.

- **Diminuição de Empregos -** A IoT está em expansão em todo o mundo e isso pode resultar na substituição de empregos monótonos e inseguros, despedindo profissionais não qualificados. Tudo isto, pode criar problemas de desemprego na sociedade. Com a Internet das coisas, as atividades diárias estão a ser automatizadas e naturalmente, haverá menos requisitos para os recursos humanos. Assim, o domínio de novas formas de trabalho aumentará ou estabilizará as hipóteses de empregabilidade de uma pessoa.

- **A Tecnologia Toma o Controlo da Vida -** A IoT teve impacto na vida de quase todos os indivíduos de todas as formas possíveis. Seja a geração mais velha ou mesmo a mais nova, todos são viciados em tecnologia, para as suas atividades do dia a dia. Com a ajuda da Internet das coisas, esta dependência tornar-se-á ainda maior nas rotinas diárias. Nenhuma aplicação está livre de falhas, e existem alguns problemas em cada aplicação técnica. Confiar em dispositivos de IoT pode criar problemas, em caso de não funcionamento, ou de colapso de uma infraestrutura de IoT.

A IoT já se tornou uma enorme parte da vida quotidiana, embora nem sempre o percebamos. À medida que a tecnologia continua a crescer e a desenvolver-se, o mesmo acontecerá com a utilização da Internet das coisas, para muitas das nossas interações básicas. Cabe-nos a nós decidir em quanto da nossa vida diária estamos dispostos a ser controlados pela tecnologia. Se for feita corretamente, porém, adaptar-se-á automaticamente às nossas necessidades e beneficiará a sociedade como um todo.

Dispositivos IoT

Os dispositivos IoT podem ser definidos como: dispositivos/ objetos que se comunicam entre si, para auxiliar as pessoas diariamente (Moloni, 2020).

Os dispositivos IoT com que o utilizador tem mais interação, são os equipamentos que geralmente temos em casa, como por exemplo, termostatos inteligentes, campainhas, lâmpadas, máquinas de café, máquinas de lavar roupa e assistentes virtuais (Tutida, 2021; Ccg, 2018).

Cada pessoa, no futuro, deverá ter em média sete dispositivos IoT, sendo que o número de equipamentos que existem no mundo, deve superar os 55 mil milhões (Magno, 2019).

A IoT estende a conectividade à Internet, para além dos dispositivos padrão, tais como desktop, portáteis, smartphones e tablets, e a qualquer gama de dispositivos físicos e objetos do dia-a-dia, tradicionalmente sem conectividade à Internet. Incorporados na tecnologia, estes dispositivos podem comunicar e interagir através da Internet. Podem também ser monitorizados e controlados remotamente.

Os dispositivos ligados fazem parte de um ecossistema, em que cada dispositivo fala com outros dispositivos relacionados, num ambiente para automatizar tarefas domésticas e industriais. Podem comunicar dados de sensores aos utilizadores, empresas e outras entidades interessadas (Posey & Shea, 2021).

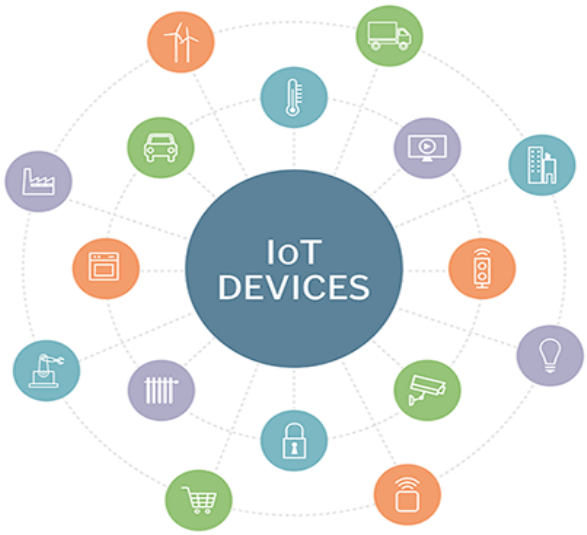

Figura 2 - Várias aplicações de dispositivo IoT. Imagem retirada de (Saini, 2019).

Existem muitos tipos de dispositivos IoT no mercado, sendo descritos por Seal (2020), os seguintes, dos mais conhecidos e usados:

- **Dispositivos "inteligentes" para uso doméstico** - Estes são dispositivos centrados no consumidor, concebidos para ajudar a automatizar funções domésticas e podem incluir coisas

como altifalantes inteligentes (Amazon Echo, Google Home, etc.), frigoríficos, luzes com Wi-Fi, fechaduras eletrónicas e entre muitos outros dispositivos. Segundo o Statista (2020), o mercado de dispositivos "casa inteligente" foi projetado para atingir 23,328 mil milhões de dólares em 2020, o que o torna um importante contribuinte para o mercado global de dispositivos IoT.

- **Sensores industriais** - Os fabricantes podem utilizar equipamento de sensores ligados à Internet, para recolher dados sobre a fábrica e para monitorizar linhas de montagem para potenciais problemas. Os sensores IoT podem ajudar a melhorar a visibilidade operacional, a programação da manutenção, a logística, a monitorização dos equipamentos e a taxa de consumo para recursos específicos.

- **Automóveis Inteligentes** – Automóveis e camiões de todos os tamanhos começam a ver cada vez mais a funcionalidade da IoT como parte de um esforço contínuo para criar veículos com autocondução. Segundo Geske (2020), "O investimento na indústria automóvel autónoma atingiu mais de 100 mil milhões de dólares", enquanto vários fabricantes de automóveis concorrem, para serem a primeira empresa a lançar um automóvel com condução autónoma.

- **Câmaras Inteligentes** - Tanto proprietários privados como empresas estão a começar a investir cada vez mais em câmaras ligadas à Internet, que podem ser controladas remotamente e armazenar as suas gravações em locais seguros e protegidos fora do local. Algumas câmaras inteligentes IoT podem utilizar software que ajuda a reconhecer intrusos e armas, bem como a enviar alertas se um for detetado.

- **Robôs de Fabrico** - As linhas de montagem estão a ver uma quantidade crescente de automatização ligada à Internet. Os robôs de fabrico com capacidades IoT podem ser controlados e programados remotamente, permitindo aos fabricantes controlar, remotamente, as suas linhas de montagem e mudar as filas de produção, sempre que quiserem.

- **Dispositivos/ Equipamentos de Saúde** - Desde relógios inteligentes que monitorizam o ritmo cardíaco, a dispositivos hospitalares, a tecnologia IoT tem ajudado a revolucionar os cuidados de saúde e o fitness, facilitando a recolha de informações vitais de saúde. Os dados recolhidos podem ser utilizados para ajudar as pessoas a acompanhar o progresso em direção aos

seus objetivos de saúde e aptidão física, ou para gerar alertas para os prestadores de cuidados de saúde numa emergência.

Por muito úteis que sejam os dispositivos da Internet das Coisas, existem preocupações em relação aos mesmos. A maior preocupação com os dispositivos IoT, na maioria das empresas, é tipicamente a sua segurança. Outras preocupações, incluem estrangulamentos na conectividade, regulamentação governamental e conseguir a adesão dentro da organização, para a adoção de novos dispositivos IoT.

Metodologias de IoT

A metodologia do sistema depende do fabricante do ecossistema. A IoT não é uma tecnologia única; é antes uma aglomeração de várias tecnologias que trabalham em conjunto (Sethi & Sarangi, 2017).

Em grande parte, os ecossistemas IoT são divididos em três partes, sendo elas:

- **Camada de perceção** - esta camada é constituída pelos sensores, que são responsáveis por medir e detetar informações sobre o ambiente que o rodeia;

- **Camada de rede** - esta camada é responsável por conectar todos os dispositivos IoT, servidores e dispositivos de rede. Esta camada é responsável por transmitir e processar os dados sensoriais. Esta camada pode ser apenas local ou mundial com a utilização de serviços *cloud*.

- **Camada de aplicação** - esta camada é responsável pela prestação de serviços específicos da aplicação para o utilizador. Define várias aplicações nas quais a IoT pode ser implantada, por exemplo, casas inteligentes, cidades inteligentes e saúde inteligente.

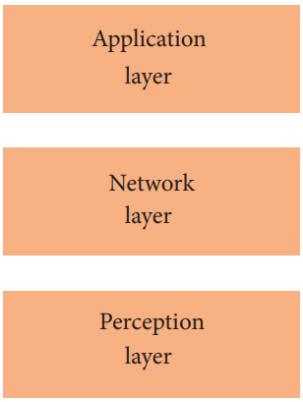

Figura 3 - Ilustração das camadas de IoT. Imagem retirada de (Sethi & Sarangi, 2017)

Outra arquitetura proposta por Yan, Zhang, & Vasilakos (2014), é inspirada nas camadas de processamento do cérebro humano. Esta é inspirada na inteligência e habilidade dos seres humanos para pensar, sentir, recordar, tomar decisões e reagir ao ambiente físico, podendo afirmar-se que esta arquitetura pode ser dividida em três partes, sendo elas:

- A primeira é o cérebro humano, que é análogo ao processamento e unidade de gestão de dados ou o *data center*;

- A segunda parte é a coluna vertebral, que é análoga à rede distribuída de nós de processamento de dados e *gateways* inteligentes;

- A terceira é a rede de nervos, que corresponde aos componentes de rede e sensores.

Para poder montar um sistema IoT é, normalmente, necessário um servidor que processe os dados e que se denomina de *gateway*. A *gateway* faz a ligação entre a camada de rede e a camada de aplicação. Se a camada de aplicação se encontra na *cloud*, a *gateway* faz um túnel entre a rede local e a *cloud*.

A *gateway* atua como um proxy para o domínio de deteção e domínio de rede para as "coisas" que lhe estão ligadas. As *gateways* IoT são bastante distintas, de aplicação para aplicação, para vários requisitos. No entanto, as características comuns são amplamente discutidas e listadas abaixo:

- **Interfaces múltiplas** - “Coisas inteligentes" podem ligar-se a uma *gateway* IoT através de vários tipos de tecnologias (Zigbee, Bluetooth, WiFi, etc.), tendo também vários métodos para se ligar à rede pública (2G/3G, LTE, LAN, etc.). Quantas e que tipos de interfaces uma *gateway* IoT devem suportar, dependem dos requisitos de aplicação, das estratégias de operação e das soluções de implementação relacionadas.

- **Conversão de protocolos** - Há duas situações, em que uma porta de acesso de IoT precisa de executar a conversão do protocolo. Uma é quando a comunicação ocorre entre diferentes protocolos de domínio de deteção (por exemplo, entre Zigbee e Bluetooth), a outra é quando a comunicação ocorre entre um protocolo de domínio de deteção e um protocolo de domínio de rede (por exemplo, entre Zigbee e 3G).

- **Capacidade de gestão -** Em primeiro lugar, uma *gateway* IoT, em si, precisa de ser gerida por servidores IoT *back-end*, como gestão de assinaturas, gestão de autoridade, gestão de estado, gestão de mobilidade, etc. Em segundo lugar, "coisas inteligentes" ligadas a uma *gateway* também precisam de ser geridas pela *gateway* correspondente. A *gateway* pode ter capacidades para identificar, controlar, diagnosticar, configurar e manter estas "coisas inteligentes".

Resumindo, o objetivo da *gateway* IoT é fazer a ponte entre várias redes de domínio de deteção (por exemplo, rede de área pessoal, rede de veículos e rede doméstica), com redes públicas de comunicação (tanto fixas como móveis) ou Internet, estabelecer com a heterogeneidade entre estas várias redes, reforçando a gestão tanto da própria *gateway* IoT (Hao Chen, Xueqin Jia, & Heng Li, 2011).

Confiança na IoT

A confiança desempenha um papel crucial na nossa vida social. A nossa vida social é caracterizada pelas relações de confiança que temos, como por exemplo, confiança nos familiares e amigos, nos pares, nas chefias e equipas, nos produtos e marcas adquiridos, entre outros. A confiança entre as pessoas, pode ser vista como uma componente-chave para facilitar a coordenação e cooperação para benefício mútuo. A confiança social é o produto de experiências passadas e de uma perceção de confiança. Modificamos e atualizamos, constantemente, a nossa confiança noutras pessoas com base nos nossos sentimentos, em resposta às circunstâncias em mudança. Muitas vezes, a confiança é criada e apoiada por um quadro legal, especialmente em ambientes empresariais, ou quando estão envolvidas questões financeiras. O quadro garante que

o mau comportamento pode ser punido com ações legais, e aumenta o incentivo para iniciar uma relação de confiança (Yan & Holtmanns , 2007).

A confiança refere-se à vontade que um indivíduo tem de ser vulnerável a outros indivíduos, e à expectativa de que um parceiro não se comporte de forma oportunista, mesmo quando tal comportamento não pode ser detetado. Parece haver um consenso na literatura, de que a confiança é um estado psicológico que está ligado a afetos/ emoções individuais (Eddleston et al., 2010).

A confiança dos utilizadores nos dispositivos e serviços da Internet das Coisas é essencial, para o sucesso e longevidade da Internet das coisas. Køien (2011) investigou a confiança num ambiente de IoT com considerável profundidade, apresentando uma visão multifacetada da confiança em software, hardware, dispositivos e serviços: transitividade e reflexividade, aspetos psicológicos de risco e avaliação de risco, desconfiança, engano, retaliação e altruísmo, reputações, associação e marcas, e cérebro humano. Køien (2011) salientou que, é óbvio que não se pode confiar, plenamente, em nenhum dos componentes da IoT (por exemplo, software, hardware, comunicações, etc.), mas tal não significa que os seres humanos não possam, ou não devam, confiar nos serviços da IoT. A manipulação humana de riscos, ameaças e oportunidades não está isenta de falhas, mas a utilização de dispositivos de proxy de confiança e a confiança que temos em marcas e empresas reconhecidas, permitir-nos-á confiar em muitos serviços sem demasiada hesitação (Køien, 2011).

Segundo Yan et al. (2014) a confiança é um conceito que é influenciado por vários parâmetros, sendo os mais relevantes a segurança do sistema e a segurança do utilizador. Contudo, a confiança é mais do que segurança e, de acordo com Michler et al. (2019), a confiança pode ser, também, medida pelos seguintes tópicos:

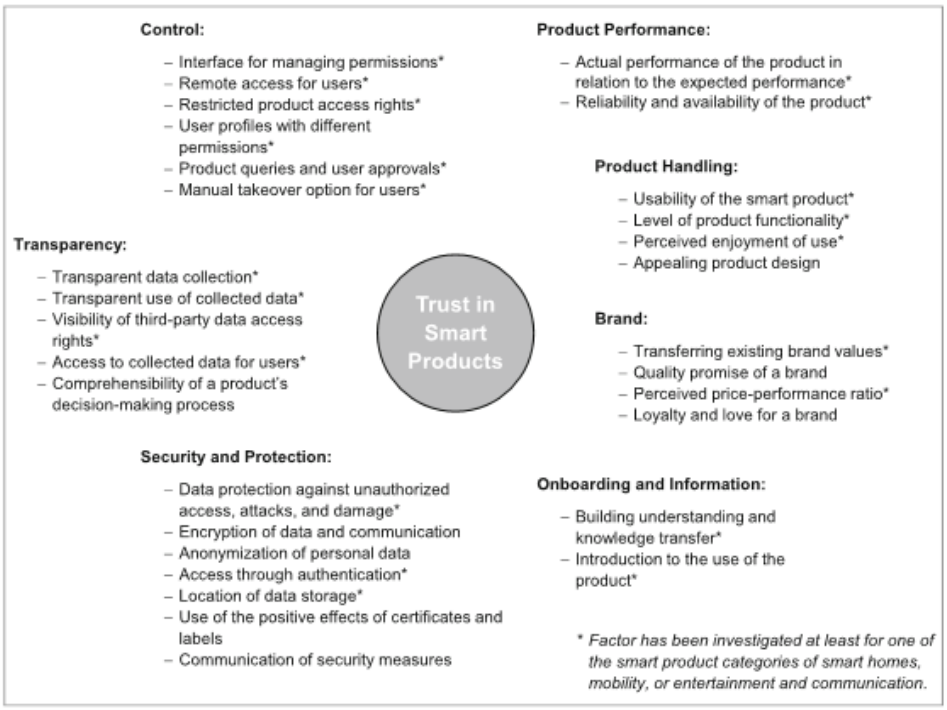

Figura 4 - Imagem retirada de Michler (2019) que sumariza os elementos que conferem confiança na IoT

Controlo

O nível de confiança, depende do controlo que o produto inteligente tem, sobre a nossa informação e o seu nível de autonomia.

De acordo com a National Institute of Standards and Technology (2018), o controlo também está relacionado com a percentagem do equipamento que pertence ao utilizador, e do que ele pode fazer com ele. Os dispositivos ao tornarem-se caixas pretas, torna-se difícil perceber o funcionamento do equipamento. Depende assim, das informações que o dispositivo tem ao seu redor, como da Internet, o que ele pode fazer com essa informação e se nós (utilizadores) podemos alterar ou escrever o estado do dispositivo ou qualquer outra informação a que o aparelho tem acesso.

Um utilizador para ter confiança num dispositivo, espera que tenha sempre controlo sobre as ações do mesmo. A sensação de controlo pode ser aumentada, tendo disponível uma interface que

permita analisar o que o ecossistema está a fazer, e qual o estado dos dispositivos, sendo que a utilização da plataforma será utilizada por utilizadores mais avançados.

O controlo percetível sobre o encontro dum serviço é a quantidade de influência que um cliente tem sobre o processo ou resultado. O controlo facilita um padrão de consumo mais previsível. Por exemplo, no contexto dos serviços financeiros, ter controlo significa que um consumidor pode automatizar pagamentos de faturas, para reduzir os custos de atrasos de pagamento ou agendar transações a serem executadas, quando um instrumento financeiro atinge um determinado ponto de preço ou taxa de juro. Um maior controlo do utilizador aumenta a confiança na tecnologia, reduzindo a incerteza do consumidor sobre o resultado das transações (Johnson et al., 2008).

Os dispositivos têm que ter um sistema que permita definir quem tem acesso a informação e as ações possíveis do dispositivo, tendo também a possibilidade de criar e definir as permissões.

Os utilizadores de *Smart Homes*, por exemplo, gostam da capacidade de ligar o aquecimento à distância no seu regresso a casa. Estas opções remotas podem diminuir os potenciais efeitos negativos na confiança e levar a uma maior credibilidade, permitindo um controlo contínuo (Brush et al., 2011). Por exemplo, os carros autónomos sem volantes e pedais de travão proporcionam aos utilizadores possibilidades muito limitadas de intervir se o carro avariar, ou se hackers atacarem os seus sistemas informáticos. A perda de poder percebida é o sentimento (potencial) dos utilizadores de que uma inovação reduz a sua liberdade de escolha ou de ação, e faz com que percam o controlo e a autonomia (Schweitzer & den Hende, 2016).

Quando combinado com ignorância e negligência, o risco de colocar informação pessoal em mãos erradas é muito real. Para contrariar a perda de controlo e a desconfiança associada, os produtos inteligentes devem pedir também a aprovação em decisões importantes (Janne et al., 2017).

Transparência

A transparência é um ponto importante, pois refere-se à privacidade, tal como ao método de funcionamento do dispositivo.

Um fabricante, ao fornecer transparência sobre o seu produto está a criar confiança e credibilidade sobre o utilizador do produto. Especialmente em dispositivos que tomam iniciativa.

A privacidade é um ponto muito importante, meramente do ponto de vista do tratamento e recolha de dados. A questão da privacidade entra mais em questão, quando um dispositivo comunica com servidores externos, sendo para guardar dados como para processamento, como por exemplo, assistentes digitais.

Nas empresas que fornecem o serviço de processamento e armazenamento dos dados do utilizador, torna-se uma questão moral guardar os dados sem os vender a terceiros. Sendo que grande parte das empresas o que faz, é tratar os dados e vender publicidade ao utilizador, dependendo das ações que ele tenha feito.

De acordo com Weber (2013), não é apenas a Internet em geral, mas também a transparência da IOT, que é um problema chave na gestão dos dispositivos. Os mecanismos transparentes são centrais, para estruturas externas e internas de mercados e organizações. Normalmente, estão em conformidade com os seguintes cinco elementos:

- Disponibilidade de uma organização ou de uma instituição, com poder suficiente para influenciar a gestão dos recursos na sociedade;

- Existência de informação publicamente fiável, ou seja, normas de qualidade substantivas relacionadas com a informação, permitir efeitos de influência baseados nas escolhas das pessoas;

- Definição do destinatário como componente essencial para a perceção de informação e transparência;

- Disponibilidade de informação suficiente, incluindo o estabelecimento de requisitos de informação, direitos de acesso à informação e procedimentos de divulgação;

- Observação da informação num espaço de tempo (visibilidade da informação).

A nível do sistema, as especificações técnicas dos dispositivos devem ser igualmente transparentes, de modo que as características de recolha, armazenamento e transferência de dados possam ser auditadas e responsabilizadas. Decisões de conceção, devem ser tomadas com consciência dos riscos potenciais, e devem ser envidados esforços para os mitigar. Princípios tais como, privacidade por conceção e por defeito, que incorporam tais valores ao longo de todo o processo de desenvolvimento, podem formar uma parte chave. As organizações que adquirem dispositivos IoT, devem ser capazes de determinar e comunicar que dados são recolhidos e partilhados, como isso cria valor, e quem beneficia dos dados.

Ao considerar o sistema na sua totalidade desde o início, tendo em conta a posição e os benefícios para todas as partes interessadas, incluindo cidadãos, organizações do sector público, e fornecedores de tecnologia comercial, os potenciais riscos de privacidade e segurança podem ser identificados com antecedência, e as escolhas apropriadas podem ser feitas. Aplicar abordagens, como a privacidade, desde o design não é apenas uma boa prática para proteger a privacidade, mas incentiva uma maior eficiência, evitando problemas evitáveis que podem exigir correções caras, por exemplo, a criação de um novo software, hardware ou políticas (Jacobs et al., 2020).

Performance do produto

Um dispositivo inteligente tem de ser capaz de realizar as tarefas que necessita, sempre da mesma maneira. O utilizador espera que o produto seja estável e que cumpra as suas expectativas. Por exemplo, se o utilizador espera que uma ação ocorra automaticamente, como ligar o ar condicionado antes que o utilizador chegue a casa, e o evento não acontece, o utilizador vai ficar preocupado/ chateado com o dispositivo. Isto cria uma falta de confiança no dispositivo, o que pode levar à sua troca.

Quantas mais vezes o utilizador tiver de utilizar o dispositivo, a sua utilização irá tornar-se cada vez mais rápida. Por exemplo, um utilizador espera que ao carregar no interruptor, a luz acenda quase instantaneamente, mas dependendo da metodologia do ecossistema, ao carregar no interruptor, a lâmpada pode demorar a acender mais do que esperado, o que pode causar preocupações e incertezas, sobre o que pode estar a acontecer. Esta espera, para um novo utilizador, pode ser preocupante, pois pode ficar a carregar no botão à espera de que algo aconteça, por isso é aconselhado mostrar ao utilizador que algo vai acontecer (Alam, 2018).

Diferentes previsões têm reportado a disponibilidade de milhares de milhões de dispositivos ligados nos próximos anos. Desta forma, as aplicações inteligentes terão de lidar, normalmente, com milhares de dispositivos.

As preocupações consideravelmente superiores de desempenho e escalabilidade são a chave, para qualquer implantação bem-sucedida da IoT. Além disso, as diferentes escolhas arquitetónicas e de implantação de sistemas IoT afetam a escalabilidade, e é possível tomar decisões em tempo real, num ambiente composto por milhares de sensores. Por conseguinte, a compreensão dos *tradeoffs* envolvidos no planeamento e na implementação de diferentes componentes de software, de um cenário específico sobre diferentes infraestruturas *cloud*, requer uma cuidadosa consideração do desempenho e da escalabilidade (Zyrianoff et al., 2019).

Cruz et al. (2018) propuseram métricas qualitativas e quantitativas e avaliaram o desempenho de várias plataformas IoT. Das 11 plataformas inicialmente analisadas pela abordagem qualitativa, cinco foram selecionadas para a análise de desempenho. No entanto, uma vez que adotaram uma abordagem genérica, os autores não se debruçaram sobre as especificidades de cada plataforma, e não avaliaram de forma diferente as infraestruturas de implantação.

Usabilidade do Produto

Um produto não deve ser complicado de utilizar pelo utilizador, como também a informação disponibilizada pelo dispositivo deve ser de fácil compreensão. O equipamento tem de ser fácil de utilizar e configurar, mas também deve ter funções e definições mais avançadas para um utilizador mais avançado, de modo a fornecer uma configuração mais específica para cada situação. Se o dispositivo tiver uma instalação (configuração inicial) agradável e se se conseguir integrar mais facilmente no ecossistema já presente, o utilizador ficará mais satisfeito com o mesmo.

Dependendo da função e das funcionalidades de um produto, a sua simplicidade é um fator importante. Por exemplo, um termostato inteligente tem de ter uma forma fácil e cómoda de alterar a temperatura, para que seja fácil para um utilizador alterar a temperatura no painel, tal como é no smartphone.

Os sistemas são fáceis de aprender quando são eficientes de utilizar, não sujeitos a erros, e satisfatórios na utilização. A usabilidade traz muitos benefícios, que incluem maior produtividade, melhor qualidade de trabalho, maior satisfação do utilizador, reduções nos custos de apoio e formação e maior satisfação do utilizador (Jokela, 2003). O dispositivo IoT é esperado que funcione 24/7 sem falhas, e que trabalhe como previsto da mesma forma todas as vezes (Michler, Decker, & Stummer, 2019).

A usabilidade tem sido cada vez mais reconhecida como uma dimensão de qualidade crucial, para arbitrar o sucesso dos sistemas interativos. De acordo com Baharuddin et al.(2013), a usabilidade é a competência que um produto tem para ser compreendido, aprendido, operado e atrativo para os utilizadores, quando estes estão habituados a atingir determinados objetivos com eficácia em ambientes específicos, sendo que a usabilidade de um produto é, habitualmente, validada através das suas interfaces.

Até à data, não existem dimensões de usabilidade definidas ou diretrizes, especificamente destinadas aos dispositivos de IoT. As diretrizes disponíveis destinam-se, particularmente, a aplicações e sistemas baseados em ambiente de trabalho e na web. A IoT tende a utilizar aplicações móveis, para além de aplicações baseadas na Web e de desktop, devido à sua natureza

de mobilidade. Para assegurar que os sistemas satisfazem o seu desempenho de qualidade esperado, foram introduzidas no passado várias diretrizes de usabilidade (Thomas et al., 2016).

De acordo com (Thomas et al., 2016) a usabilidade pode ser divida em 4 categorias, sendo elas:

- **Flexibilidade**

Dado que a IoT consiste em dispositivos interligados, é pertinente que todos eles funcionem para realização da especificação dos utilizadores. É esperado que haja consistência na funcionalidade, para permitir que os utilizadores destes sistemas ou dispositivos se tornem familiarizados com comandos funcionais importantes. A adoção de normas de usabilidade é importante, pois ajudaria a evitar complicações na navegação da interface de utilizador dos dispositivos IoT.

- **Operabilidade**

Como a IoT consiste em componentes heterogéneos interligados, é pertinente que todos eles funcionem no sentido de alcançar a especificação dos utilizadores. Espera-se que haja consistência na funcionalidade, para permitir que os utilizadores destes sistemas ou dispositivos se familiarizem com comandos funcionais importantes. A adoção de normas de usabilidade importantes, ajuda a evitar complicações na navegação das interfaces nos dispositivos de IoT.

- **Capacidade de aprendizagem**

De acordo com Thomas et al. (2016), a facilidade de aprendizagem de um dado sistema, é uma característica de qualidade importante que todo o sistema deve possuir. Para alcançar esta característica, o sistema deve ter tarefas que satisfaçam o modo de vida dos utilizadores. Assegura que termos técnicos falsos, elementos ou ícones que não são familiares ao utilizador são mínimos, estes princípios asseguram que não há uma interpretação errada da funcionalidade para que os utilizadores não se percam. Espera-se que um sistema ou componente IoT previna conclusões erradas, conteúdos irrelevantes, e minimize a utilização de comandos complexos, permitindo o mínimo possível de ações ou funções para executar uma tarefa. Tarefas complexas dificultam a aprendizagem e aumentam a possibilidade de erros.

- **Acessibilidade**

Espera-se geralmente, que cada sistema funcione de forma consistente em termos de funcionalidade, pois tal permite ao utilizador familiarizar-se com a composição fundamental básica do sistema. A funcionalidade descreve a qualidade de um sistema IoT a ser concebido, desenvolvido e implantado para servir bem os seus objetivos na duração prescrita para o qual foi fabricado. Tendo em conta a natureza dinâmica do nosso ambiente, espera-se que todos os sistemas e dispositivos da Internet das coisas sejam fáceis de aprender com base no ambiente de implementação. Para conseguir facilidade de utilização e aprendizagem, os sistemas ou dispositivos de Internet sem fios, devem estar isentos de termos técnicos ou comandos ambíguos, que não sejam amplamente conhecidos pelos utilizadores. Tal destina-se a evitar interpretações erradas da funcionalidade, que possam levar a danos adversos.

Marca

A marca é um aspeto muito importante na IoT devido às políticas que ela tem, tal como o apoio que dá aos clientes. Se uma empresa, no passado, conseguiu criar um produto bom e agradável, é provável que no futuro também crie um bom produto com uma longa vida de apoio e atualizações.

A questão da marca possui mais influência na altura da compra, e principalmente se o utilizador já tiver produtos da mesma marca. O que o utilizador pensa sobre a marca terá impacto no produto, principalmente, se anteriormente a marca não teve um produto de qualidade, ou não serviu o seu propósito, danificando a relação entre o utilizador e a marca.

De acordo com Michler, Decker, e Stummer (2019), um consumidor prefere um produto de marca em vez de um produto de marca branca no que toca a produtos de tecnologia. Quanto mais produtos de qualidade e que tenham boa fiabilidade no futuro, o consumidor terá mais interesse na gama de produtos da marca e será mais fácil a adoção de novos dispositivos.

Um aspeto importante sobre as marcas e os ecossistemas criados pelos produtos e das interações entre eles, é que um utilizador terá mais probabilidade de comprar um produto que se configure e interaja com facilidade com os outros produtos já existentes.

Almeida & Mendes (2021) recomendaram que as pessoas não comprassem produtos de marca branca ou de marcas menos conhecidas. As marcas mais conhecidas, em princípio, estão mais atentas aos problemas dos dispositivos IoT. Mesmo assim poderá haver problemas de segurança, bem como outras complicações.

Onboarding

Bauer (2015) definiu, a partir de um estudo de 2010, que o *onboarding* podia ser dividido em quatro aspetos:

- ***Compliance* (conformidade do produto) -** Para que um produto seja *compliance*, este terá de ser anunciado ao utilizador de forma justa. O utilizador ao comprar o dispositivo espera que ele faça, pelo menos, o que foi dito na embalagem e na publicidade, como também que tenha tudo o que o utilizador precisa para utilizar o dispositivo. Por exemplo, se um utilizador comprar um interruptor inteligente, este irá esperar que o mesmo funcione como um interruptor 'básico'.

- ***Clarification* (compreensão) -** Um produto tem de ser claro desde o manual de instruções até à sua configuração. O utilizador tem que perceber logo na primeira utilização o que o dispositivo faz e como o faz.

- ***Culture* (cultura) -** Neste ponto, *culture* refere-se ao entendimento da metodologia de funcionamento de um produto, e de como este se pode integrar num ecossistema, sendo que a cultura em si também terá um impacto na confiança, desde a existência da tradução para a língua materna do utilizador e como o dispositivo vai ser utilizado.

- ***Connection* (relacionamento) -** O relacionamento com o produto é constituído pelo mecanismo de suporte, seja ele com a empresa ou em fóruns. O relacionamento entre o fabricante e o utilizador é importante, pois um produto inteligente terá mais funcionalidades que podem ser difíceis de compreender pelo utilizador.

Segurança

Michler et al. (2019, p.10) afirmou que "*Users expect services and product use to be secure*.", traduzindo para o português, "Os utilizadores esperam que os serviços e a utilização do produto sejam seguros", isto significa que para o utilizador ter confiança no produto, é necessário que a empresa mostre algum cuidado com a segurança do produto e do serviço. Isto inclui a capacidade de deteção de eventos fora do comum, como também a proteção de dados. Se a empresa que

desenvolve o produto tiver boas medidas de seguranças ativas contra ataques, a confiança do utilizador sobre o produto aumenta (Kumar, 2015).

Os peritos em cibersegurança advertem que a IoT é uma das tecnologias mais vulneráveis, e esperam ataques mais direcionados a infraestruturas existentes e emergentes, por exemplo, roubo de dados, danos físicos, ataque DDoS (*Distributed Denial of Service*), resgates para casas inteligentes ou carros inteligentes, entre outos.

Figura 5 - Desafios da segurança. Imagem retirada de Farhan et al. (2018)

Quatro das chaves de segurança IoT, referidas por Farhan et al. (2018), e que podem ser visualizadas na figura 5, são:

- **Confiança e integridade dos dados:** isto significa que pode assegurar que os dados não tenham mudado, desde o momento em que foi detetada até chegar ao destino final. Envolve também a verificação dos dados e validar o certificado de verificação.

- **Triliões de pontos de vulnerabilidade:** com cada dispositivo que se junta ao ecossistema IoT, representa um aumento potencial de riscos. Isto leva a questões: quão confiante pode uma organização estar com os dados recolhidos e a integridade dos dados enviados? Como assegurar que os dados não tenham sido interferidos ou comprometidos?

- **Proteção de dados:** trata-se de um mecanismo legal necessário para ser concebido para proteger e controlar os dados individuais e organizacionais, recolhidos por sensores ou aplicações e armazenados para fazer parte de um sistema de arquivo.

- **Privacidade dos dados:** significa proteger os dados da exposição no ambiente IoT. Por exemplo, qualquer ambiente lógico ou físico pode receber um endereço único e a capacidade de comunicar automaticamente através da rede.

Problemas de segurança no IoT

Aprofundando o assunto de segurança, iremos ver, de seguida, onde o utilizador pode ser mais afetado nos aspetos de segurança, e o que é possível fazer para resolver estes mesmos problemas.

Como já vimos neste documento, a IoT trouxe oportunidades interessantes tanto para consumidores, quanto para empresas, mas veio junto com uma vasta coleção de novos desafios de segurança. As tecnologias de IoT são incorporadas e estendem o ecossistema da Internet e, como consequência, herdam todos os problemas de segurança relacionados à Internet e apresentam novos problemas específicos.

Aldowah (2020), especifica que mais de 70% dos dispositivos IoT têm um conjunto de vulnerabilidades derivadas a partir de interfaces Web inseguras, estas podendo ser causadas por encriptação fraca no transporte, falta de autenticação e proteção inadequada do software.

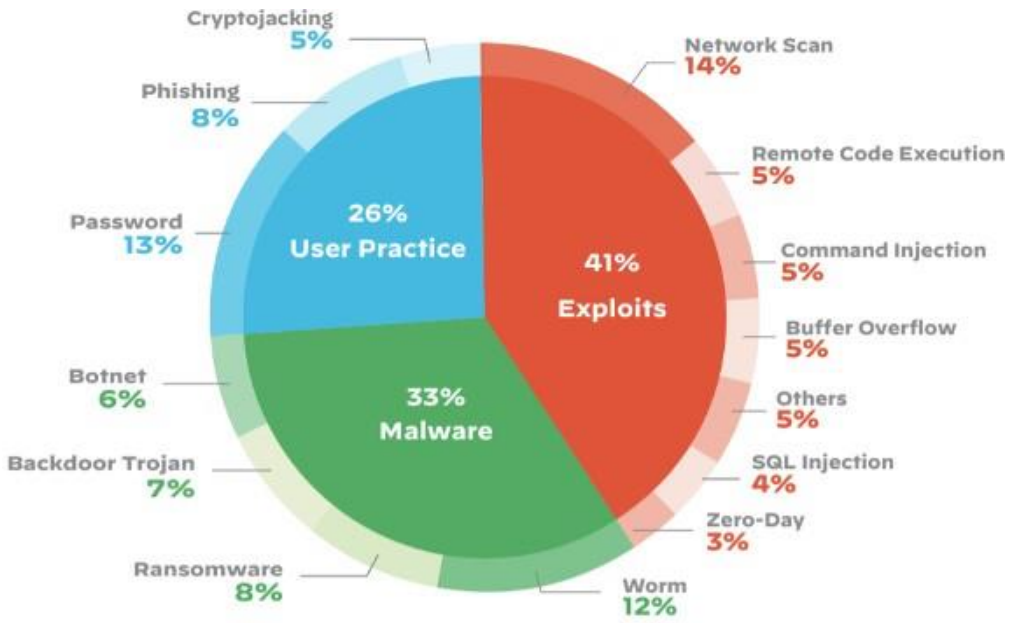

Figura 6 - Imagem retirada do papel de UNIT 42 (2020) que refere os diversos ataques que os dispositivos IoT sofrem

No estudo feito por UNIT 42 (2020), ao verificar vários dispositivos IoT, concluiu-se que 41% destes estavam comprometidos por falhas no sistema, 33% eram causados por *malware* e que 26% eram causados por más práticas dos utilizadores. UNIT 42 afirma que estes 4 passos podem reduzir os riscos de ataque, sendo eles:

- O utilizador conhecer os riscos envolvidos;
- Corrigir erros de segurança em impressoras e outros dispositivos fáceis de corrigir;
- Segmentar a rede informática em várias seções (VLAN);
- Habilitar a monitorização ativa da rede.

Desta forma, é necessário também que o utilizador conheça algumas das falhas de segurança, como por exemplo, *Phishing*, password *cracking* ou um vírus, e também que saiba como é suposto o dispositivo funcionar, como por exemplo, o motivo da lentidão do dispositivo e a falta de resposta do dispositivo IoT. O utilizador do dispositivo IoT tem também de saber que ao ter palavras-passes fracas (por exemplo só números ou nomes comuns), ou a repetição de passwords por vários equipamentos, pode tornar o dispositivo mais vulnerável a ataques.

Para que a rede e os dispositivos IoT estejam protegidos, os dispositivos que se encontrem conectados à mesma rede, devem ter todas as atualizações feitas, sendo que tendo mesmo apenas um dispositivo desatualizado na rede pode comprometer os outros equipamentos.

Se uma empresa deixa de atualizar um certo produto, coloca-se o problema da atualização, pois o fornecedor já não oferece apoio a esse dispositivo. Nesta situação, o utilizador apenas tem duas hipóteses: ou desfaz-se do dispositivo e compra um novo, ou mantém o dispositivo desatualizado, confiando apenas na firewall e antivírus do sistema para o proteger, o que pode causar um problema de segurança no futuro.

Se os dispositivos IoT não tiverem um método fácil ou automático de fazer as atualizações, significa que provavelmente irão ficar com o software que veio de origem, o que pode causar uma falha de segurança no futuro (Atac & Akleylek, 2019).

Alguns dos dispositivos IoT têm a possibilidade de efetuar atualizações a partir do ar (WiFi), tornando essas atualizações mais fáceis. Se esta função for mal desenvolvida pode criar problemas de segurança (Carroll, 2016).

A segmentação da rede depende muito do router que a infraestrutura tem, pois, grande parte dos utilizadores usa o que o fornecedor de Internet (ISP) fornece. Sendo assim, em certos casos, não é possível dividir a rede. Se o utilizador pretender dividir a rede, terá de comprar um router para servir de intermediário (Karamanos, 2012).

Se o router tiver capacidade de criação de VLAN, não significa que quem o instalou o tenha configurado, caindo assim a responsabilidade da configuração para o 'administrador da rede'/utilizador. Este pode não perceber como se realiza a configuração, ou pode não se importar com o assunto, podendo isto causar uma falha de segurança.

A importância das VLAN é iminente no aspeto dos IoT, pois permite a separação da rede, por exemplo uma câmara IP não pode comunicar diretamente com um dispositivo que esteja na rede, como por exemplo, um computador, tendo o computador de aceder à câmara a partir do router ou a partir de um serviço que esteja disponível na rede (Payne & Abegaz, 2018).

Um passo importante é ter uma firewall ativa na rede e a existência de antivírus nos dispositivos, ou até mesmo no router. Sendo que os dispositivos IoT de fraca capacidade computacional podem não ter um antivírus, ou este ser fraco, isto torna-os vulneráveis. Um antivírus é muito importante, pois um vírus pode instalar-se no sistema sem ninguém notar.

Grande parte dos utilizadores, em média, utiliza o antivírus que o sistema traz, pois é o mais fácil de utilizar (Zhang et al., 2014).

Pelos pontos de defesa dados pela UNIT 42 (2020), se um utilizador tiver um destes pontos implementados, podemos chegar à conclusão que saberá, no mínimo, de alguns dos problemas de segurança. O utilizador, ao ter cuidado, pode evitar grande parte dos ataques, por exemplo, a passwords, *Phishing*, Vírus (*worm, ransomware*).

Almeida & Mendes (2021) realizaram um estudo em que chegaram à conclusão que dos 15 dispositivos testados, foram detetadas 50 vulnerabilidade nos dispositivos IoT. Descobriram também que os dispositivos enviam informação para 528 servidores em 13 países. Grande parte dos dispositivos testados enviava informações para servidores e certa parte enviava-a sem os dados serem encriptados.

De seguida iremos falar de alguns ataques mais comuns disposto por UNIT 42 (2020).

Malware

O termo *malware* vem da combinação de duas palavras: malicioso e software, e este é utilizado para indicar qualquer software não desejado. Foi definido, em geral, como qualquer código adicionado, alterado ou removido de um sistema de software a fim de intencionalmente causar danos ou subverter a função pretendida do sistema. O termo vírus, foi definido como um termo genérico que engloba Vírus, Trojans, Spywares e outros códigos intrusivos.

Um *malware* é caracterizado pela capacidade de replicação, propagação, auto-execução e corrupção do computador ou sistema. A corrupção do sistema informático pode afetar a confidencialidade da informação, integridade e negação de serviços. A replicação é uma

característica importante para a maioria dos *malwares*, uma vez que assegura a sua existência. Em alguns casos de *malware* incessante, a replicação torna difícil a exaustão dos recursos informáticos (por exemplo disco, RAM).

A propriedade de invisibilidade é utilizada por muitos tipos de *malware* para evitar serem detetados por *anti-malware*. Pode ser feito por uma de técnicas polimórficas ou metamórficas.

A forma comum de infetar um sistema (dados ou executáveis ficheiros, registos de arranque de unidades de disco ou rede exaustiva largura de banda) é a transferência de *malware* de um dispositivo poluído para outro não infetado, utilizando o sistema de ficheiros local ou de rede. O *malware* faz uso de vulnerabilidades do sistema operativo e bugs de software. Inicia o seu ciclo de vida no mesmo sistema ou remotamente a partir de outro sistema (A.Saeed et al., 2013).

Botnet

Botnet é uma rede de computadores comprometidos, sendo denominadas de *Bots*, sob o controlo remoto de um operador humano chamado *Botmaster*. O termo *Bot* deriva da palavra "Robot". Semelhante aos robôs, os *bots* são concebidos para executar algumas funções pré-definidas de forma automatizada. Por outras palavras, os *bots* são programas de software que funcionam num computador anfitrião permitindo ao *botmaster* controlar as ações do anfitrião remotamente. Os *botnets* representam uma ameaça significativa e crescente contra a cibersegurança, uma vez que fornecem uma plataforma distribuída para muitos cibercrimes, tais como ataques de Negação Distribuída de Serviço (DDoS) contra alvos críticos, disseminação de *malware*, *phishing*, e fraude por clique. A deteção de *botnets* tem sido um tema de investigação importante nos últimos anos. Os investigadores têm proposto várias abordagens de deteção de *botnet*, para combater a ameaça de *botnet* contra a cibersegurança. As abordagens de deteção de redes de *bots* é divididas em quatro classes: baseada na assinatura digital, baseada na anomalia, baseada no DNS e baseada na mineração (Feily et al., 2009).

Ransomware

A palavra "ransomware", e o fenómeno associado, apareceram por volta do ano 2005. Iluminou uma classe específica de *malwares* que exigem um pagamento em troca de uma funcionalidade roubada. A maioria dos “ransomwares" difundidos fazem um uso intensivo da encriptação de ficheiros como meio de extorsão. Basicamente, encriptam vários ficheiros nos discos rígidos das vítimas antes de pedir um resgate para que os ficheiros sejam desencriptados. Os meios de comunicação relacionados com a segurança e alguns vendedores de antivírus, rapidamente classificaram este "novo" tipo de vírus como uma grande ameaça para o mundo

informático (Gazet, 2008).

Os criminosos podem desligar o aquecimento no Inverno, provocando o congelamento e o rebentamento dos canos. Ou, podem desligar o seu ar condicionado no Verão, destruindo o equipamento até que o resgate seja pago (Heffelfinger, 2020).

Phishing

Phishing é uma tentativa de um indivíduo ou grupo, para solicitar informações pessoais de utilizadores insuspeitos, empregando técnicas de engenharia social. Os e-mails de *phishing* são criados para aparecerem como se tivessem sido enviados por uma organização legítima ou por um indivíduo conhecido. Estas mensagens de correio eletrónico tentam, frequentemente, induzir os utilizadores a clicar num link que levará o utilizador a um website fraudulento que pareça legítimo. O utilizador pode então ser solicitado a fornecer informações pessoais, tais como nomes de utilizador de contas e palavras-passe, que podem expô-los ainda mais a futuros compromissos. Além disso, estes sites fraudulentos podem conter código malicioso (CISA, 2020).

Utilizando técnicas de engenharia social, é possível adquirir informação sensível fraudulentamente, como nomes de utilizador e palavras-passe, tentando enganar os utilizadores de websites populares, enviando-lhes por e-mail, ou outros meios, versões falsas de sites a fim de fornecerem as suas credenciais. Isto pode parecer fácil de evitar, mas os avanços na comunidade de *phishing* estão tornando os esquemas de *phishing* cada vez mais difíceis de identificar do ponto de vista das vítimas. O termo *phishing* tem evoluído de um e-mail mal construído, em cópias quase perfeitas de websites inteiros para enganar os utilizadores a fornecer informações pessoais (Vayansky & Kumar, 2018).

Man-In-The-Middle Attack

Um ataque de homem no meio é um tipo de ataque de espionagem, em que os atacantes interrompem uma conversa existente ou transferência de dados. Depois de se inserirem no "meio" da transferência, os atacantes fingem ser ambos participantes legítimos. Isto permite que um atacante intercete informações e dados de qualquer das partes, ao mesmo tempo que envia ligações maliciosas ou outras informações a ambos os participantes legítimos de uma forma que pode não ser detetada até ser demasiado tarde.

Pode-se pensar neste tipo de ataque como semelhante ao jogo do “telefone estragado”, em que as palavras de uma pessoa são transportadas de participante para participante, até que tenham mudado no momento em que chegam à pessoa final. Num ataque de homem no meio, o participante do meio manipula a conversa desconhecida para qualquer dos dois participantes

legítimos, agindo para recuperar informações confidenciais e de outra forma, causar danos (Veracode, 2014).

O objetivo deste ataque é o de recolher informação do utilizador, por exemplo, certificações de login, dados de interesse e números do cartão de crédito. Os alvos são normalmente os clientes de aplicações financeiras, empresas de serviços *cloud*, locais de negócios baseados na web e outros locais onde é necessário iniciar sessão. As informações obtidas durante um ataque poderiam ser utilizadas para muitos fins, incluindo fraude, mudança ilegal de palavras de contas. Além disso, pode ser utilizado para ganhar conhecimento sobre a rede e os procedimentos de uma empresa (Mallik, 2019).

Denial-of-service attack

Um ataque de Negação de Serviço é um ataque que pode ser utilizado para influenciar a ligação à rede, tornando-a inacessível aos utilizadores a que se destina. Um ataque DoS é realizado inundando o alvo com tráfego, ou enviando-lhe informações para desencadear um crash. É um dos métodos mais populares de ciberataque na segurança da rede. As vítimas de ataques de DoS são frequentemente os servidores web de organizações de alto perfil (Liang et al., 2016).

As vítimas de ataques DoS têm, frequentemente, como alvo, servidores web de organizações de alto perfil, tais como bancos, comércio e empresas de meios de comunicação, ou organizações governamentais e comerciais. Embora os ataques de DoS não resultem tipicamente no roubo ou perda de informação significativa ou outros bens, podem custar à vítima muito tempo e dinheiro para lidar com eles (*Palo Alto Networks*).

Uma variante do DOS é o DDOS (Distributed Denial of Service Attacks). Um ataque Distributed Denial of Service (DDoS) usa um conjunto de computadores, para lançar um ataque coordenado DoS contra um ou mais alvos. Utilizando tecnologia cliente/ servidor, o atacante é capaz de multiplicar, significativamente, a eficácia da Negação de Serviço, aproveitando os recursos de múltiplos computadores cúmplices involuntários que servem como plataformas de ataque. Tipicamente, um programa mestre é instalado num computador utilizando uma conta roubada. O programa mestre, num determinado momento, comunica então com qualquer número de programas "agentes", instalados em computadores em qualquer parte da Internet. Os agentes, quando recebem o comando, iniciam o ataque. Utilizando tecnologia cliente/ servidor, o programa mestre pode iniciar centenas, ou mesmo milhares de programas de agentes em segundos (Weiler, 2002).

SQL Injection attack

A injeção SQL é um tipo de ataque de injeção, que torna possível executar instruções SQL maliciosas. Estas instruções controlam um servidor de base de dados por detrás de uma aplicação web. Os atacantes podem usar as vulnerabilidades de SQL *injection* para contornar as medidas de segurança da aplicação. Podem contornar a autenticação e autorização de uma página web ou aplicação web e recuperar o conteúdo de toda a base de dados SQL. Podem também usar SQL *Injection* para adicionar, modificar e apagar registos na base de dados (acunetix, 2020).

SQL Injection é um ataque que permite aos hackers executar código malicioso num sistema, sendo uma das mais comuns a Injeção SQL. Esta vulnerabilidade permite, geralmente, que o hacker veja partes do website geradas dinamicamente não destinadas a ser exibidas dessa forma, ou simplesmente aceder à base de dados do website. Esta vulnerabilidade é, provavelmente, uma das mais perigosas, uma vez que existem muitos tipos diferentes de *Injection*, e proteger um website contra todos eles pode ser bastante desafiante, e deixar um hacker executar uma *Injection* pode destruir empresas, especialmente as que mantêm dados sensíveis (Shiaeles et al., 2019).

Zero-Day Attack

Se um hacker conseguir explorar a vulnerabilidade antes que os criadores de software possam encontrar uma solução, essa exploração torna-se conhecida como um ataque de dia zero.

As vulnerabilidades de dia zero podem assumir quase qualquer forma, porque podem manifestar-se como qualquer tipo de vulnerabilidade de software mais ampla. Por exemplo, podem tomar a forma de encriptação de dados em falta, injeção de SQL, buffer *overflows*, autorizações em falta, algoritmos quebrados, redireccionamento de URLs, bugs, ou problemas com a segurança de palavra-passe.

Isto torna as vulnerabilidades de dia zero difíceis de encontrar proactivamente, o que de certa forma é uma boa notícia, porque também significa que os hackers terão dificuldade em encontrá-las. Mas também significa que é difícil proteger-se contra estas vulnerabilidades de forma eficaz (*Check Point Software, 2021*).

Uma vez corrigida a falha ou descoberta, o ataque já não se chama *zero-day*. Estes ataques raramente são descobertos de imediato. De facto, muitas vezes levam, não apenas dias, mas sim, meses, e por vezes anos, até que um programador saiba da vulnerabilidade que levou a um ataque (FireEye, 2015).

Cross-Site Scripting

Ataques de Cross-Site Scripting, abreviado XSS, juntam-se a uma categoria de vulnerabilidades da web, em que o servidor confia e não verifica, minuciosamente, a entrada do utilizador em aplicações HTTP. Na ausência de validação de entrada, os pedidos criados podem conter pedaços de código malicioso, que podem potencialmente, ser executados no browser de outros clientes desconhecidos.

Normalmente, as vulnerabilidades XSS levam à execução de código malicioso no lado do cliente, mas a vulnerabilidade reside no lado do servidor, representado por uma aplicação Web menos segura no dispositivo de alojamento. As atenuações dos ataques XSS têm de ocorrer no servidor, uma vez que a própria aplicação web facilita os ataques que ocorrem, não o navegador dos clientes. O XSS representa uma percentagem bastante pequena de ataques, embora a grande maioria dos dispositivos IoT que temos observado exponha geralmente um serviço HTTP.

Os tipos de dispositivos com tentativas de XSS observadas contra eles são sistemas de monitorização IP (seja câmara ou DVR), e NAS (Network Attached Storage). Os atacantes que aproveitam as explorações XSS para comprometer os dispositivos IoT, geralmente, dependem de uma fase inicial de sondagem, onde é analisada a possibilidade de executar o código injetado no pedido HTTP (Moldovan et al., 2020).

IoT com *Blockchain*

Problemas de escalabilidade e segurança que surgem, devido ao número excessivo de objetos IoT na rede. O modelo servidor/ cliente exige que todos os dispositivos sejam ligados e autenticados através do servidor, o que cria um único ponto de falha. Portanto, mover o sistema IoT para o caminho descentralizado pode ser a decisão certa. Um dos sistemas de descentralização populares é a Blockchain. A Blockchain é uma tecnologia poderosa que descentraliza os processos de computação e gestão que podem resolver muitos dos problemas da IoT, especialmente a segurança. Este documento fornece uma visão geral da integração da cadeia de bloqueio com o Blockchain, destacando os benefícios e desafios da integração (Atlam et al., 2018).

Blockchain é um sistema de registo de informação, de uma forma que torna difícil ou mesmo impossível (aos dias de hoje) mudar, piratear ou enganar o sistema.

A Blockchain é essencialmente um livro-razão digital de transações, que é duplicado e distribuído por toda a rede de sistemas informáticos na Blockchain. Cada bloco da cadeia contém

um número de transações, e sempre que uma nova transação ocorre na cadeia de bloqueio, um registo dessa transação é adicionado ao livro-razão de cada participante. A base de dados descentralizada gerida por múltiplos participantes é conhecida como Tecnologia de Ledger Distribuído (DLT).

Isto significa que se um bloco de uma cadeia fosse alterado, seria imediatamente visível que tinha sido adulterado. Se os hackers quisessem corromper um sistema de blockchain, teriam de alterar cada bloco da cadeia, através de todas as versões distribuídas da cadeia (Euromoney, 2020).

A blockchain tem muitas características que a tornam muito atrativa, para a IOT resolver muitos dos seus problemas. As características da cadeia de bloqueio incluem: Imutabilidade; Descentralização; Anonimato; Melhor Segurança; Aumento da Capacidade.

Não há dúvida de que a integração da cadeia de bloqueios teria muitas vantagens. No entanto, a tecnologia da blockchain não é um modelo perfeito, pois tem as suas próprias falhas e desafios. Estes desafios podem ser resumidos da seguinte forma: escalabilidade; poder e tempo de processamento; armazenamento; falta de competências; legal e de conformidade; nomeação e descoberta (Atlam et al., 2018).

Se, no entanto, houver necessidade de incluir *blockchain* no IoT para aumentar a segurança, há questões a serem ultrapassadas. Uma delas é o processamento da *blockchain*, sendo que este requer uma grande quantidade de computação. Muitos dispositivos IoT não têm a potência necessária. As blockchains são vulneráveis se um grupo controlar mais de 50% da taxa de *hashrate*.

O *hashrate* é uma medida da potência computacional, por segundo, utilizada na exploração do blockchain. De uma forma simplificada, é a velocidade da exploração mineira. É medida em unidades de hash/ segundo, o que significa quantos cálculos por segundo podem ser efetuados. As máquinas com uma alta potência de *hash* são altamente eficientes, e podem processar muitos dados num único segundo. A distribuição global de nós numa típica blockchain torna isto muito difícil. Mas o poder de processamento de uma blockchain no IoT doméstica pode ser mais facilmente *hackeado*.

A segurança da IOT continuará a evoluir à medida que os regulamentos relacionados com o seu desenvolvimento e utilização continuarem a sua marcha em frente. No entanto, a possibilidade de um sistema de segurança de uma blockchain da Internet de alta velocidade é algo que pode ter um grande potencial (IEEE Innovation at Work , 2020).

Em conclusão podemos ver na imagem (nº7) os pontos onde a confiança do utilizador é exercida sobre IoT, sendo todos eles importantes para assegurar a confiança do utilizador.

Pontos focais da confiança no IoT

Concluindo dos capítulos anteriores é possível a construção de um gráfico (*Figura 7*), que exprima os pontos fulcrais para que seja possível haver confiança no IoT.

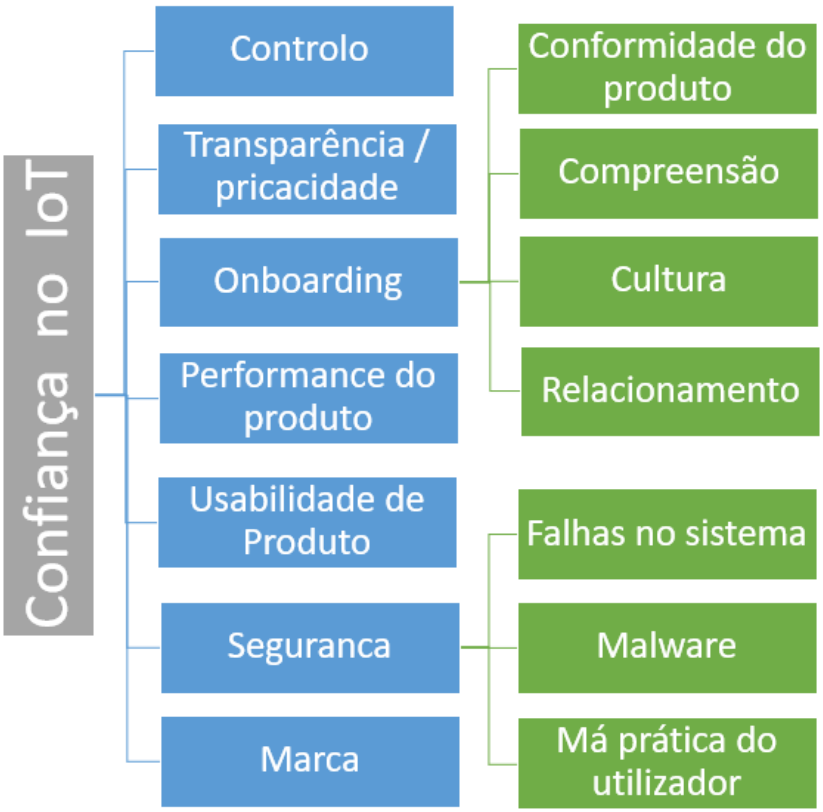

Figura 7 - Diagrama que sumariza os pontos onde a confiança é criada

Desenvolvimento do estudo

Recolhendo a informação agregada no capítulo anterior (estado da arte) e da figura final desse capítulo (Figura 7), foi criado um questionário com 18 perguntas que fossem ao encontro de cada capítulo. Destas questões, algumas foram colocadas sob a forma de afirmação, em que o inquirido deveria mostrar o seu grau de concordância com as mesmas, para estas utilizou-se uma escala de Likert. Além destas perguntas, foram também solicitadas algumas informações pessoais, qual a idade, se tem dispositivos IoT, quantas vezes usa a Internet e qual a sua profissão. Não foi pedido mais nenhum método de identificação, para aumentar a anonimidade de quem respondeu ao questionário. O questionário aplicou-se a pessoas que possuíam, ou não, dispositivos IoT, que entendessem a língua portuguesa, sendo que este foi desenvolvido somente em português.

O questionário foi criado a partir da plataforma Google, utilizando a ferramenta de formulário. Este formulário online teve o seu principal foco nos pontos referidos anteriormente no capítulo do estado da arte, sendo estes: Controlo, Transparência/privacidade, Performance do produto, Usabilidade do Produto, Marca, Onboarding, Segurança.

Depois de criado o questionário, na plataforma online Google Forms, foi gerado um link. Esse link foi partilhado com os contactos pessoais e profissionais do investigador, sendo solicitado que, sempre que possível, o mesmo fosse partilhado com outras pessoas, tratando-se assim de uma amostra não probabilística com técnica de *snowball*. O formulário foi disponibilizado durante um prazo de 4 meses tendo sido obtidas 84 respostas consideradas como válidas.

As questões feitas e as suas hipóteses de respostas encontram-se no apêndice 1 (Formulário).

O questionário foi dividido em 6 capítulos, sendo eles:

- **Introdução**

Nesta seção existe uma pequena introdução sobre para que é o estudo, o que é a IoT e o que consiste um dispositivo IoT.

- **Informações pessoais**

Neste capítulo fizemos perguntas sobre alguns aspetos pessoais, de modo a ter informações que pudessem influenciar as perguntas do capítulo seguinte. Tentando sempre que possível fazer perguntas específicas para que, quem responde ao questionário, tenha sempre assegurada a sua anonimidade, sendo assim mais difícil identificar quem respondeu ao questionário.

- **Confiança**

Nesta seção serão questionados os pontos realçados e elencados no Enquadramento Teórico.

Para tornar o questionário mais fácil e abrangente para as pessoas que não possuem dispositivos IoT, e para que estes consigam entender as questões, foram realizadas perguntas semelhantes, mas adaptadas para essas mesmas.

A performance do produto varia consoante o dispositivo e o trabalho a ser realizado, sendo assim, este tópico não foi abordado no questionário.

- **Segurança**

Neste capítulo do formulário iremos questionar se as pessoas consideram que os seus dispositivos IoT estão protegidos contra-ataques e/ ou, se já sofreram algum ataque de segurança.

Nesta seção tentamos observar se os utilizadores têm alguns dos pontos referidos no capítulo sobre segurança ou no relatório feito por UNIT 42 (2020) implementados, para aumentar a segurança dos dispositivos IoT.

- **Conclusão**

Neste Capítulo, iremos perguntar a quem realizou o questionário, se as perguntas foram bem concebidas e o que se pode fazer para melhorar o questionário. Estas perguntas serão realizadas de maneira a descobrir se as questões do formulário foram bem colocadas e/ ou se existe alguma maneira de as melhorar. Este campo terá influência nos trabalhos futuros.

- **Mensagem Final**

Terminaremos o questionário com uma fase de agradecimento por ter respondido, assegurando que os dados serão tratados com o maior respeito e só serão utilizados nesta dissertação.

Análise dos resultados

Informações sobre as pessoas que responderam ao questionário

No total foram recolhidos um total de 84 questionários. dos quais 62 tinham pelo menos 1 dispositivo IoT, sendo assim 73,8% de todos os questionários. 63,1% das pessoas responderam

que tinham entre 1 a 5 dispositivos. 7,1% afirmou que tinha entre 6 e 13 dispositivos e 3,6% disse que tinha mais de 14.

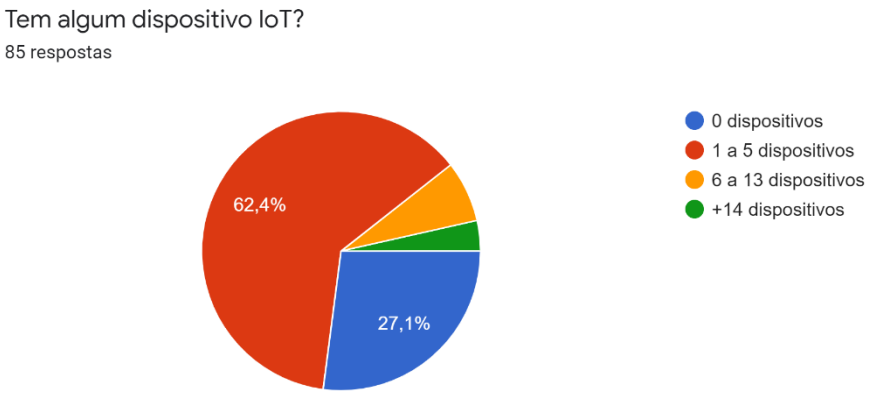

Figura 8 - Gráfico que demonstra o número de pessoas que têm dispositivos IoT que responderam ao questionário

Todas as pessoas que responderam a este questionário usam a Internet pelo menos 1 hora por semana, sendo que 91,7% usa diariamente. Os sujeitos que responderam a este questionário têm, em média, 46 anos.

Pergunta 1.1

Devido ao facto de existirem pessoas sem dispositivos IoT a responder ao questionário, o mesmo teve de ser dividido em duas partes semelhantes. Em comparação com os dois gráficos, representados nas figuras 9 e 10, é possível identificar que as pessoas que não tem dispositivos responderam mais vezes que discordam parcialmente e discordam totalmente, do que as pessoas que já têm um dispositivo.

Na amostra de pessoas que não têm dispositivos IoT, podemos verificar um receio acerca do controlo. Pelo contrário, na amostra das pessoas que já possuem um dispositivo IoT, sentem que têm controlo. Mesmo assim, ainda existe uma grande percentagem de pessoas que sentem que não tem controlo total.

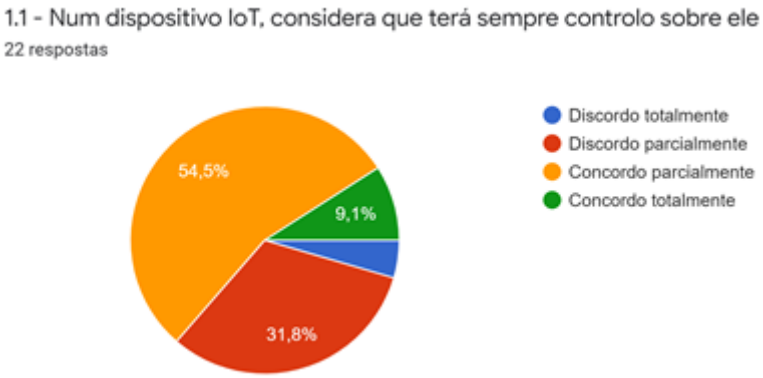

Figura 9 - Diagrama que reflete se os utilizadores que não tem dispositivos IoT sentem que vão ter controlo sobre o produto

Figura 10 - Diagrama que reflete se os utilizadores que têm dispositivos IoT sentem que têm controlo sobre o produto

Verificando agora para o agregado dos dois gráficos, podemos observar que continuamos com uma grande percentagem de pessoas que responderam que concordam parcialmente, especificamente 48,8%, num total de 41 pessoas. Podemos verificar que, em grande parte, as pessoas consideram que têm controle sobre o dispositivo, e que a maioria sente receios de não conseguir controlar o dispositivo.

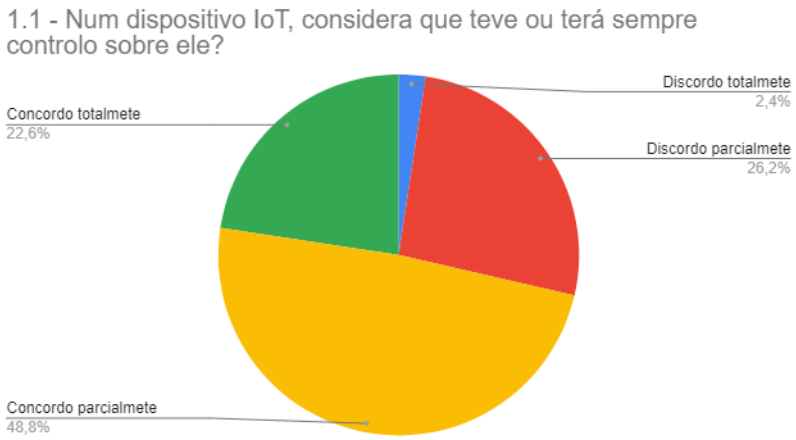

Figura 11 - Diagrama que reflete se os utilizadores sentem que têm ou vão ter controlo sobre os dispositivos.

Pergunta 1.2

Nesta pergunta tenta-se entender se as pessoas conseguem definir quem tem acesso ao dispositivo, verificando-se que 27,4% das pessoas consideram que conseguem definir totalmente quem tem acesso ao dispositivo. 47,6% das pessoas que responderam o questionário, concordam parcialmente, o que quer dizer que consideram que conseguem definir o acesso, no entanto, apresentam alguma dificuldade. Porém, este ponto pode variar dependendo dos dispositivos que as pessoas conhecem, sendo que nem todos se configuram da mesma forma.

Cerca de 3,6% pessoas consideram que não conseguem definir quem tem acesso ao dispositivo. Esta percentagem, em comparação com a percentagem de pessoas que concordam parcialmente ou totalmente, é muito pequena.

Num universo de 84 pessoas, 75,9% responderam que em princípio conseguiam configurar quem tem acesso ao dispositivo. Desta forma, é possível concluir que a maioria considera que consegue configurar quem tem acesso aos dispositivos IoT.

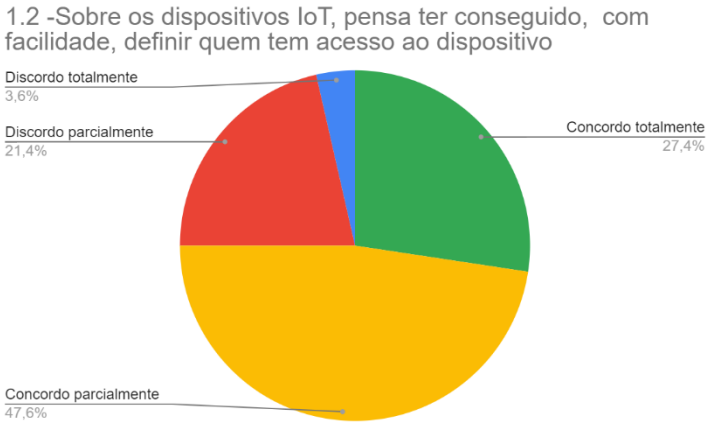

Figura 12 - Diagrama que reflete se as pessoas conseguem definir quem tem controlo sobre os dispositivos

Pergunta 1.3

Mais de metade (63,6%) dos inquiridos sem dispositivos IoT responderam que concordam parcialmente que os fabricantes dizem o que fazem com a informação. Pelo contrário, as pessoas que referiram que tinham pelo menos um dispositivo - cerca de 70,9% - afirmaram que discordam.

Figura 13 - Gráfico que mostra se as pessoas sem dispositivos acham se os fabricantes dizem o que fazem com as informações recolhidas

Figura 14 - Gráfico que mostra se as pessoas com dispositivos IoT acham se os fabricantes dizem o que fazem com as informações recolhidas

No total, 34,5% dos entrevistados concordam parcialmente sobre o que as empresas fazem com os dados recolhidos e 39,3% acredita que não dizem com clareza o que fazem com a informação. Existem mais pessoas que discordam totalmente (21,4%), do que as que concordam totalmente (4,8%).

Figura 15 - Diagrama que reflete se os fabricantes de dispositivos IoT dizem com clareza o que fazem com os dados recolhidos

Deste modo, é possível afirmar que os fabricantes de dispositivos IoT não dizem com clareza o que fazem com as informações recolhidas.

Pergunta 1.4

Neste ponto, questionamos as pessoas acerca do seu conhecimento sobre onde estão guardados os dados recolhidos pelo dispositivo. Sendo que as pessoas que não têm dispositivos IoT não podem responder a esta pergunta, perguntamos, em alternativa, se consideram importante saber onde ficam guardadas as informações recolhidas.

Na amostra de pessoas que têm mais de um dispositivo, 74,4% disseram que não sabiam onde os dados estavam guardados. Apenas 16,1% disseram que sabiam onde estes eram guardados. 6,5% das pessoas que responderam, disseram que não era importante para eles saber onde ficam guardados.

Figura 16 - Gráfico que reflete se as pessoas que responderam ao questionário que tem dispositivos sabem onde estão guardados os dados dos dispositivos

Quanto às pessoas que não têm nenhum dispositivo IoT, quase a totalidade (90,9%), disseram que é importante saber onde ficam guardados os dados recolhidos.

Figura 17 - Diagrama que reflete se as pessoas sem dispositivos IoT pensam que é importante saber onde os dados ficam guardados

Ambos os gráficos indicam que existe uma necessidade de o utilizador saber onde ficam guardados os dados recolhidos.

Pergunta 1.5

Nesta pergunta, ambos os grupos (com e sem dispositivos), consideram que é importante que a privacidade seja respeitada. 75% das pessoas que responderam, disseram que concordavam totalmente, e 25% disseram que concordavam parcialmente.

Ninguém que tenha respondido ao questionário, afirmou que não era importante a privacidade no IoT.

Sendo assim, a maioria dos inquiridos - 63 pessoas (75%) - responderam que concordavam, totalmente, com a questão da privacidade nos dispositivos IoT, tornando assim a privacidade um ponto importante para a confiança das pessoas na IoT.

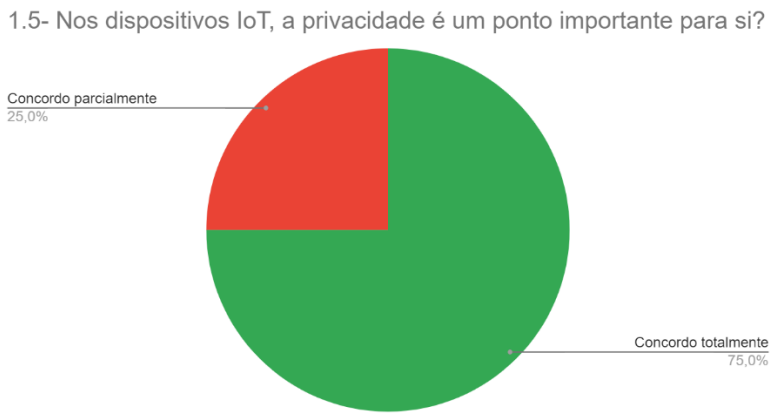

Figura 18 - Gráfico que sumaria se as pessoas que responderam ao questionário afirmam se a privacidade é importante para elas nos dispositivos IoT

Pergunta 1.6

Esta pergunta foi apenas destinada a pessoas com dispositivos IoT. Das 62 pessoas com dispositivos IoT, 30,6% achou que os equipamentos eram fáceis de utilizar e 58,1% afirmaram

que os dispositivos são, parcialmente, fáceis de utilizar, ou seja, a maioria respondeu positivamente.

Das 62 pessoas (com dispositivos IoT) que responderam ao questionário, apenas 7 (11,3%) disseram que os dispositivos eram difíceis, ou parcialmente difíceis, de usar. Verifica-se assim, que para as pessoas com dispositivos IoT, estes equipamentos não oferecem dificuldades na sua utilização.

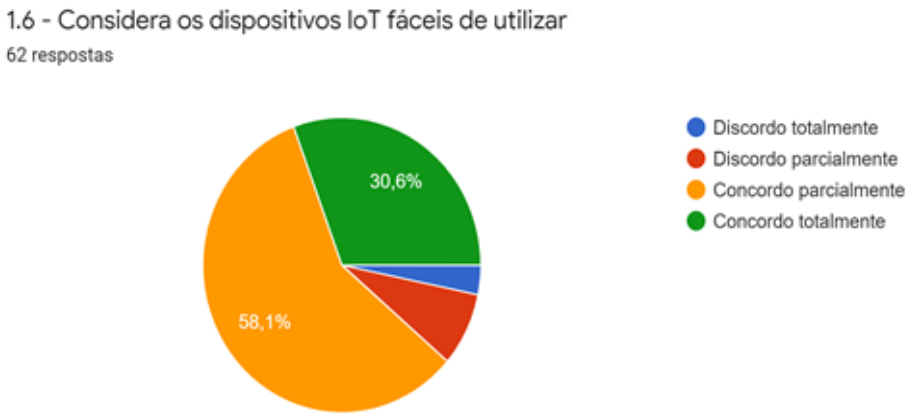

Figura 19 - Diagrama que reflete se as pessoas consideram *que os dispositivos IoT são fáceis de usar*

Pergunta 1.7

Esta pergunta foi mostrada para pessoas com e sem dispositivos IoT. Para ambos os grupos, as respostas foram muito semelhantes.

No que concerne aos inquiridos que possuem dispositivos IoT, 51,6% manifestaram uma concordância total, em relação ao facto da marca ser um aspeto importante na confiança do produto, e 38,7% das respostas concordam parcialmente. Desta forma, é possível verificar que a maioria das pessoas concorda que a marca é um aspeto importante na confiança do produto.

Verifica-se que, para a larga maioria dos inquiridos, a confiança na marca traduz-se numa confiança nos produtos oferecidos. Com efeito, apesar do enorme crescimento da oferta que existe de dispositivos IoT, muitos deles de marca denominada “branca”, os utilizadores continuam a ter uma preocupação pela escolha de marcas já estabelecidas, e que ofereçam uma maior segurança.

Figura 20 - Gráfico que mostra se a marca é um aspeto importante para as pessoas com dispositivos IoT

As pessoas que não têm dispositivos IoT, 31,8% responderam que concordam totalmente que a marca influencia a confiança nos produtos inteligentes. A maioria (54,5%) respondeu que concordava parcialmente.

Figura 21 - Diagrama que demonstra se a marca é um ponto importante para as pessoas sem dispositivos IoT

Somando as respostas dos entrevistados que têm e os que não tem dispositivos IoT, chegamos à conclusão de que 46,4% concordam na totalidade, e que 42,9% concordam parcialmente que a confiança é afetada pela marca.

Das pessoas que responderam ao questionário, apenas 10,7% disseram que discordam, sendo que 8,3% das 84 pessoas disseram que discordam parcialmente.

Portanto, é possível atestar que a marca se apresenta como um aspeto importante na confiança do produto.

Figu–a 22 - Gráfico que soma as pessoas com e sem dispositivos IoT e que demonstra se a marca e um ponto importante

Pergunta 1.8

Nesta questão, todas as pessoas afirmaram que conheciam, pelo menos, uma marca de dispositivos IoT. Dos respondentes ao questionário, 72 pessoas (85,7%) reconheceram o Google como uma marca de dispositivos IoT. Sessenta pessoas (71,4%) responderam que reconheciam a Microsoft e 58 pessoas (69%) responderam que reconheciam a Huawei como fabricante de dispositivos de IoT.

A Amazon foi reconhecida por 47 pessoas (55,9%) e a Cisco por 30 pessoas (35,7%). Quem selecionou IBM, 23 pessoas (27,3%), ou Oracle, 17 pessoas (20,2%), também selecionou outras marcas (Google, Microsoft, Huawei, Amazon, Cisco, IBM, Oracle).

Verifica-se assim, que cada inquirido reconhece pelo menos uma marca de dispositivos IoT.

Esta pergunta também demostrou que, se uma empresa que se foca mais a aplicar os seus dispositivos IoT noutras empresas, observamos que o utilizador comum não a reconhece como fabricante de equipamentos IoT.

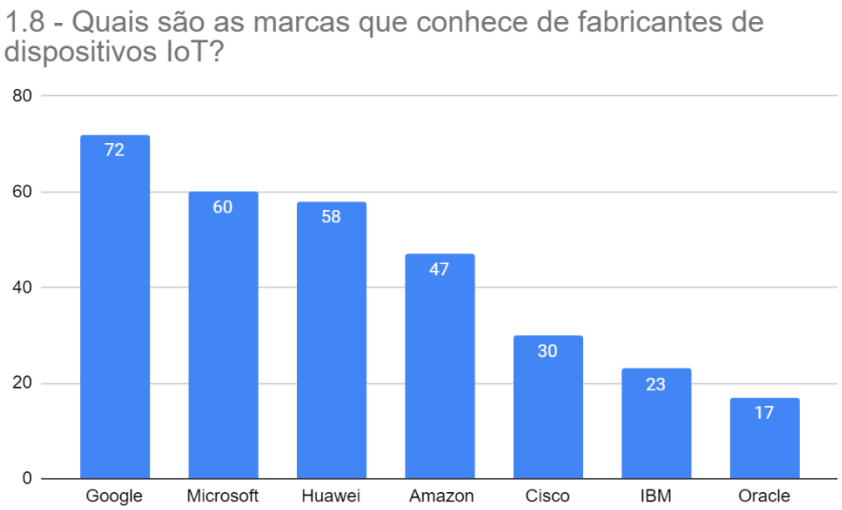

Figura 23 - Gráfico que demonstra quais são as marcas que as pessoas reconhecem mais

Pergunta 1.9

Esta pergunta foi apenas colocada a pessoas que têm pelo menos 1 dispositivo IoT, das quais 61,3% responderam que achavam parcialmente fácil de instalar e 24,2% achou que era fácil de compreender e executar a instalação. Apenas 14,5% responderam que a instalação foi parcialmente difícil. Verifica-se, assim, que os fabricantes de IoT têm tido uma, cada vez maior, preocupação em desenvolver métodos instalação de dispositivos facilitada. Algumas pessoas tiveram dificuldades a instalar dispositivos, provavelmente, devido à vasta diferença que existe nos produtos, pois nem todos os fabricantes utilizam o mesmo método de instalação.

Figura 24 - Diagrama que mostra a facilidade de compreensão e execução da instalação de dispositivos IoT, de entre as pessoas que têm estes equipamentos.

Pergunta 1.10

Nesta pergunta é questionado o nível de customização inicial que o utilizador prefere. Apenas 10,7% das pessoas responderam que queriam o mínimo necessário para que o dispositivo trabalhasse. Trinta e cinco pessoas (47,6%) disseram que preferiam o mínimo necessário para a instalação e algumas opções pré-definidas. As restantes 41,7% responderam que, além das hipóteses anteriormente referidas, também preferiam que houvesse algumas opções extra. Verifica-se, assim, que a maioria dos utilizadores de dispositivos IoT preocupa-se com o nível de personalização dos equipamentos que utiliza.

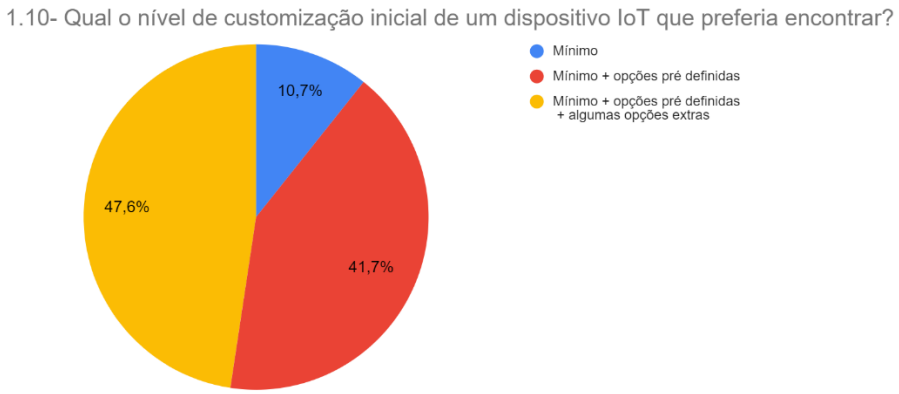

Figura 25 - Diagrama que reflete o nível de customização inicial que o utilizador prefere

Pergunta 1.11

Esta pergunta foi apenas apresentada a pessoas com pelo menos um dispositivo IoT.

Das 62 pessoas, 9,7% responderam que concordam que a publicidade (anúncios, caixa do produto, sites de venda) representa as funcionalidades do produto.

E 51,6% concordam, parcialmente, que a publicidade reflete o produto, já 29% discordam parcialmente e 9,7% discordam totalmente.

Desta maneira, é possível definir que a publicidade (anúncios, caixa do produto, sites de venda) representa claramente os produtos IoT. Esta pergunta é importante, pois analisa o que o utilizador pensou antes de comprar, para a maioria das respostas recolhidas é possível observar que a publicidade que foi feita ao produto, condizia com as funcionalidades do produto.

Figura 26 -Gráfico que mostra se a publicidade representa bem o produto

Pergunta 1.12

Esta pergunta foi feita a pessoas com e sem dispositivos IoT. 15,5% das pessoas que responderam ao questionário disseram que confiam nos dispositivos IoT. A maioria (78,6%) disse que tem receios ou não confia totalmente nos produtos inteligentes. Por último, 6% dizem que não confiam nos dispositivos IoT.

De acordo com estas percentagens, é possível verificar que a maioria das pessoas tem receios na confiança dos dispositivos IoT. Assim, verifica-se que as pessoas querem adotar as tecnologias IoT, mas não sabem como os sistemas funcionam, nem quais são os pontos fracos dos ecossistemas. Este receio existe, particularmente, para as primeiras adoções de um dispositivo IoT, mesmo tendo esse utilizador anteriormente comprado um dispositivo inteligente.

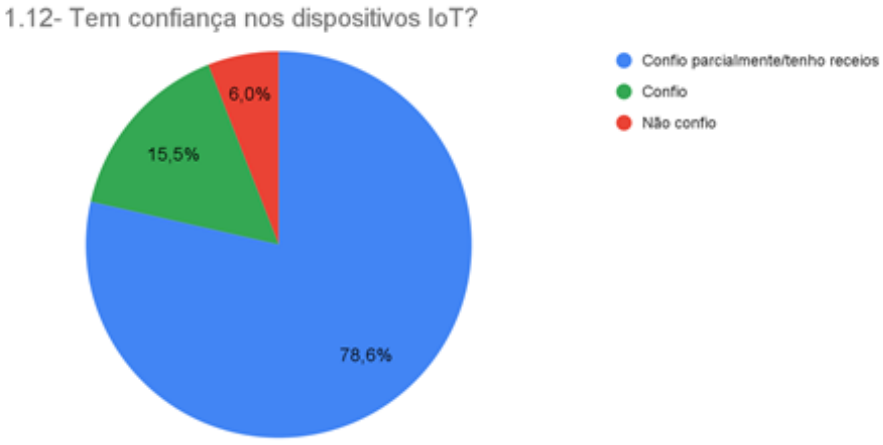

Figura 27 - Diagrama que reflete se as pessoas que responderam ao questionário confiam nos dispositivos IoT

Pergunta 2.1

Nesta pergunta, questionámos os inquiridos se já tinham sofrido um ataque informático. Das 84 pessoas, a maioria (82,1%), disseram que não tinham sofrido nenhum ataque informático e 17,9% (15 pessoas) responderam que já tinham sofrido um ataque.

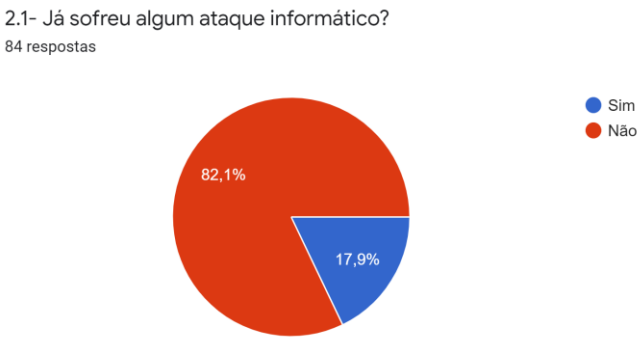

Figura 28 - Diagrama que representa a percentagem de utilizadores que sofreram algum ataque informático

Das 15 pessoas que responderam que tinham sido atacadas, uma não especificou o ataque que tinha sofrido, seis sofreram um ataque de vírus, quatro sofreram ataques que envolvem os cartões bancários, duas ataques através de e-mails e duas sofreram encriptação de ficheiros.

Grande parte dos ataques referidos pode comprometer dispositivos IoT, a rede informática ou até o ecossistema de produtos inteligentes. Apesar disso, verificou-se que a maioria dos inquiridos refere não ter sofrido qualquer tipo de ataque informático. O que poderá ser levar a duas suposições, ou as pessoas tiveram cuidado ao usar os dispositivos, ou então foram atacadas e não tiveram a perceção de que foram atacadas.

Pergunta 2.2

Neste ponto, perguntámos às pessoas se consideravam ter palavras-passe fortes e diferentes para cada plataforma.

A maioria (64,3%) respondeu que tinha palavras-passe fortes e diferentes. As restantes 35,7% disseram que tinham palavras-passes fracas e semelhantes.

De tal forma, é possível concluir que a maioria afirma que tem palavras-passe diferentes e consideradas fortes. Esta pergunta demonstra que as pessoas entrevistadas pensam ter palavas-passes fortes, apesar de uma boa parte ter respondido que não, podendo ter as palavras-passes

repetidas em vários sites ou palavas-passes fracas. Por sua vez, os inquiridos que responderam que tinham palavras-passes diferente e fortes, podem ter um conceito de palavra-passe forte enviesado.

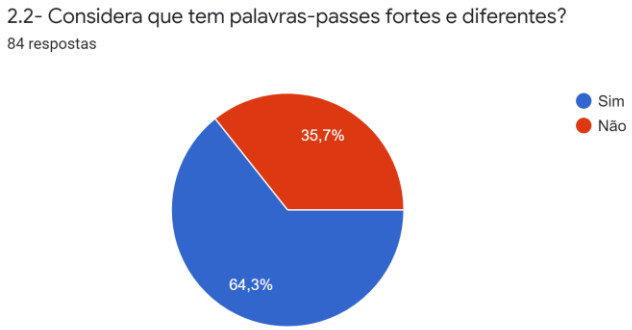

Figura 29 - Gráfico que mostra se o utilizador acha que tem palavra-passe fortes e diferentes

Pergunta 2.3

Certos dispositivos trazem palavras-passe pré-definidas, sendo a intenção desta pergunta saber se os inquiridos, ao comprar tais dispositivos, alteram a palavra-passe do equipamento. A maioria das pessoas (60,7%) respondeu que alterava sempre as palavras-passe originais. 35,7% das pessoas responderam que às vezes mudavam as passwords. Apenas 3 pessoas (3,6%) responderam que nunca mudavam as palavras-passe.

Deste modo, é possível concluir que a maioria das pessoas se preocupa em mudar a palavra-passe original, podendo levar a um aumento na segurança dos equipamentos.

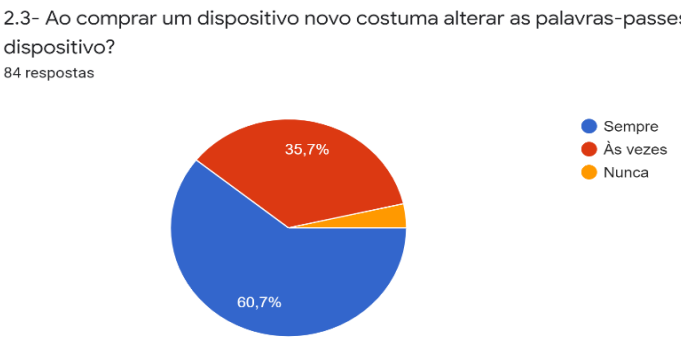

Figura 30 - Diagrama mostra se o utilizador costuma mudar as palavras-passes *que vem pré-definidas*

Pergunta 2.4

Nesta pergunta tentámos entender se os utilizadores de IoT fazem as atualizações a dispositivos, que não as fazem automaticamente. De tal forma, foram obtidos os seguintes resultados: 23,8% responderam que não costumam fazer as atualizações automáticas, a maioria (51,2%) disseram que faziam apenas quando estas surgiam, 29.8% responderam que faziam atualizações aos dispositivos quando se lembravam e 23,8% tinham contestado que só as fazem quando encontram problemas.

Verifica-se assim que a maioria, dos inquiridos, preocupa-se em fazer atualizações aos dispositivos. Este é um ponto importante para a segurança no IoT, podemos assim observar que as pessoas se preocupam em fazer as atualizações, promovendo o aumento na segurança destes dispositivos.

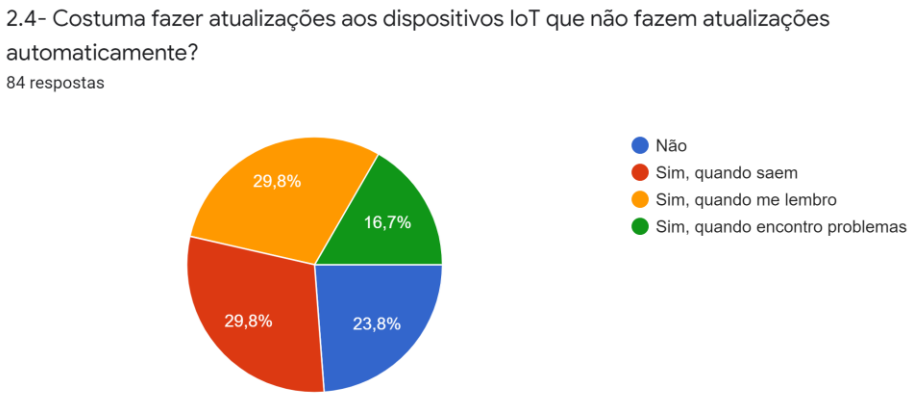

Figura 31 - Gráfico que mostra quando é que o utilizador faz atualizações aos dispositivos que o não fazem automaticamente

Pergunta 2.5

Nesta questão, a maioria (51,2%) dos inquiridos disseram que não sabiam o que é uma VLAN (Virtual LAN). Responderam que não sabem criar uma VLAN 26,2% dos inquiridos, e 14,3% consideram que não é necessário a criação de VLAN. Apenas 8,3% dos inquiridos responderam que tinham criado uma VLAN.

Podemos afirmar, deste modo, que a maioria das pessoas não sabe o que são VLAN, ou desconhece o seu potencial de segurança, particularmente no uso de dispositivos IoT. Posto isto, a responsabilidade poderá recair sobre o fornecedor de Internet, que poderá não apenas divulgar o que são VLAN, mas também configurá-las para os seus clientes.

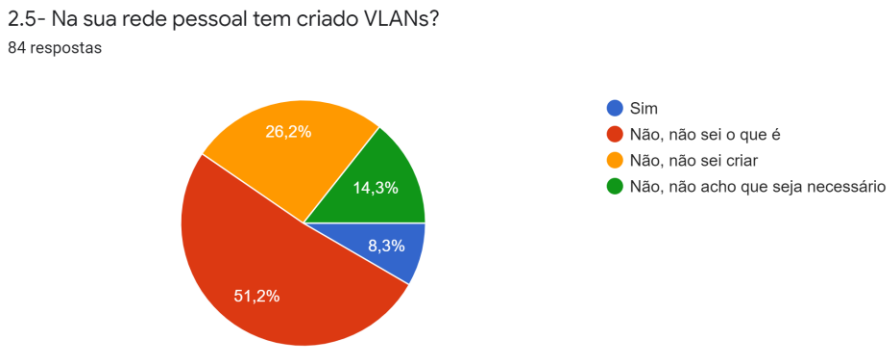

Figura 32 - Diagrama que demonstra se as pessoas têm VLAN criadas na rede pessoal

Pergunta 2.6

A maioria das pessoas (67,9%) responderam que não têm um router além do fornecido pelo fornecedor de Internet. O restante (32,1%) responderam que tinham pelo menos um router além do fornecido pelo fornecedor de Internet.

Observa-se assim que a segurança implementada na rede pessoal é prestada a partir do router instalado pelo fornecedor de Internet. Quanto mais configurações o router tiver, maior será o nível de customização.

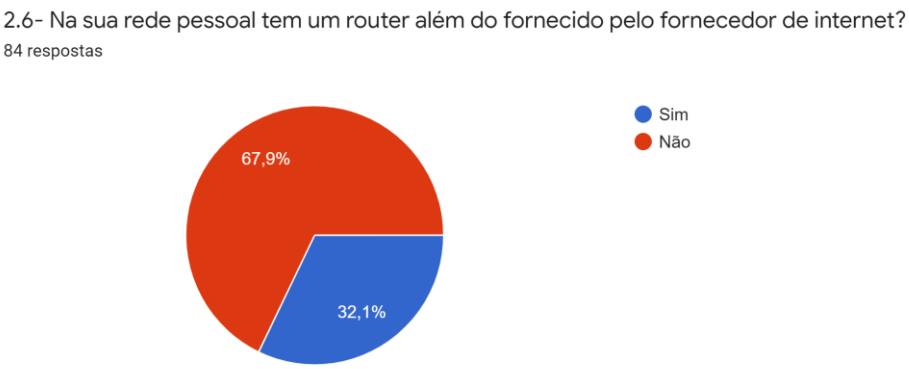

Figura 33 - Gráfico que mostra se as pessoas têm um router além do que foi fornecido pelo fornecedor de Internet

Resumo do capítulo

Nesta secção iremos agregar as informações recolhidas anteriormente referidas.

Nas perguntas 1.1 e 1.2 questionámos os inquiridos, sobre o nível de controlo que consideram que têm sobre os dispositivos. A maioria que respondeu ao questionário, concorda parcialmente que achava que tinha controlo, e que conseguia definir quem tem acesso ao dispositivo inteligente.

Da pergunta 1.3 à 1.5, tencionámos obter a opinião dos inquiridos sobre os aspetos de transparência e privacidade. De acordo com as respostas recolhidas, as pessoas dizem que não sabem o que os fabricantes fazem com a informação recolhida e não sabem onde ficam guardados.

A maioria dos inquiridos respondeu que os dispositivos IoT eram fáceis de utilizar, sendo assim os produtos tem uma usabilidade acessível.

As perguntas 1.7 e 1.8 tiveram a finalidade de verificar o que os utilizadores pensam sobre as marcas que fabricam dispositivos IoT. Neste caso, a maioria dos inquiridos respondeu que a marca é um aspeto importante no aspeto do IoT.

Da pergunta 1.9 a 1.11, os inquiridos foram questionados sobre o *onboarding*, tendo respondido que os dispositivos foram fáceis de instalar e que a publicidade (anúncios, caixa do produto, sites de venda) representa, parcialmente bem, as funcionalidades dos dispositivos IoT. Foi possível verificar também, que a maioria das pessoas desejam que os dispositivos IoT tenham um grande número de definições iniciais.

As perguntas da seção 2 foram realizadas de forma a obter informações sobre métodos de prevenção de segurança, e o que as pessoas têm implementado nos seus dispositivos IoT.

Verificou-se que a maioria das pessoas afirma que tem palavras-passes fortes e diferentes e que fazem atualizações recomendadas aos sistemas informáticos.

Observou-se, também, que metade dos inquiridos não sabe o que é um VLAN e 26,6% não sabe como esta e cria na rede pessoal. Grande parte das pessoas respondeu que, na rede pessoal, tem apenas o router fornecido pelo fornecedor de Internet.

Para além disso, a maioria dos inquiridos afirmou não ter sofrido nenhum ataque informático.

Por último, verificou-se que mais de metade dos inquiridos responderam que tinham receio sobre os dispositivos IoT.

Conclusão e trabalhos futuros

Esta dissertação procurou apurar em que medida os utilizadores de dispositivos IoT confiam nos dispositivos IoT e as principais preocupações face a esta tecnologia. Teve, também, como objetivo analisar alguns dos problemas de segurança na IoT.

No futuro haverá cada vez mais dispositivos IoT. Estes dispositivos irão estar ao nosso redor, fazendo cada vez mais parte das nossas vidas. Os equipamentos IoT variam desde tomadas, sensores de temperatura, carros, a cidades inteiras. Como as vantagens da IoT aparentam superar as desvantagens, ou pontos fracos, o número de equipamentos IoT terá tendência a aumentar.

Do mesmo modo, conforme verificado no enquadramento teórico, o nível de confiança do utilizador depende dos seguintes pontos: controlo do dispositivo, Transparência/ Privacidade, *Onboarding*, Performance do produto, Segurança, Marca, elementos estes que procurámos aferir através dos inquéritos por questionário realizados no estudo. Estes pontos foram descritos no estado da arte; onde foi descrito que a segurança e a privacidade eram os mais importantes, mas tendo também outros pontos que influenciam a confiança na IoT.

A tecnologia IoT tem vários problemas, sendo eles principalmente a nível de segurança. Estes problemas irão estar sempre presentes, mas ao logo do tempo podem ser mitigados. Espera-se que grande parte dos problemas sejam resolvidos pelos fabricantes de IoT à medida que a tecnologia irá evoluir.

Os problemas de segurança que mais afetam as plataformas de IoT são as falhas no sistema, o *malware*, ou a má prática do utilizador. Para diminuir estas e outras falhas de segurança é aconselhado aos utilizadores da IoT conhecer os riscos envolvidos, corrigir erros de segurança em impressoras e outros dispositivos, segmentar a rede informática em várias seções (VLAN) e habilitar a monitorização ativa da rede.

Nesta dissertação procedeu-se à elaboração de um Inquérito por questionário com 18 perguntas, que foi distribuído por vários métodos digitais (e-mail e redes sociais). Obteve-se um conjunto de 84 respondentes. A maioria dos inquiridos afirmou ter receio sobre os dispositivos IoT, mas considerou que tem controlo sobre os mesmos.

Tendo por base a investigação realizada, procurar-se-á dar resposta às questões de investigação que nortearam este trabalho e que aqui relembramos:

1. Qual o nível de confiança dos utilizadores na utilização da tecnologia IoT?
2. Do ponto de vista do utilizador, quais são os problemas de segurança que mais afetam as plataformas de IoT e a sua utilização?

Quanto à primeira questão, um dos factos mais importantes para os utilizadores que responderam ao questionário foi a questão sobre a marca e o que o fabricante faz com os dados e onde os guarda. Ao longo do questionário observou-se uma tendência de que o utilizador de IoT quer saber o que se passa por detrás das "cortinas". As pessoas querem saber como os dispositivos IoT interagem com o mundo físico e com a Internet.

Chegou-se também à conclusão de que o utilizador diz que os dispositivos IoT são fáceis de instalar e de usar.

Assim, verifica-se que genericamente os utilizadores confiam na tecnologia, apesar de a recearem, tendo essencialmente como referência a questão da marca por detrás do dispositivo.

Verificámos que os pontos que mais afetam o nível de confiança do utilizador nos dispositivos IoT são a segurança e a privacidade, sendo os mesmos pontos idênticos com investigações anteriores que relatam os mesmos pontos.

Quanto à segunda questão, existem vários elementos a ter em consideração.

Na segunda parte do questionário foram realizadas perguntas sobre medidas de segurança que os utilizadores têm implementado nos dispositivos IoT e na rede pessoal. A maioria dos inquiridos afirmou no questionário que fazem as atualizações nos sistemas, que têm palavras-passes fortes e diferentes.

Foi possível observar-se também, que mais de metade das pessoas inquiridas não tem um segundo router na rede pessoal e que não tem VLAN criadas na rede pessoal. Além disso, a maioria afirmou que não sofreu nenhum ataque informático, e os que sofrem podiam pôr em causa o ecossistema IoT.

De acordo com os resultados obtidos no questionário, podemos aferir que as pessoas têm receios nos dispositivos IoT e que o fabricante do dispositivo tem um grande efeito na confiança do produto.

Tendo os dispositivos IoT vários problemas de segurança, não foi possível identificar qual o problema de segurança que mais afeta o utilizador. Olhamos então para soluções que previnam os ataques. Como os dipositivos IoT podem ter várias falhas de segurança temos de implementar políticas de segurança sobre o equipamento e o ecossistema que o engloba. A maioria dos utilizadores de dipositivos IoT implementa o mínimo de segurança (mudar de password e fazer atualizações aos dipositivos), deixando o resto da implementação de segurança para o fornecedor de Internet. A maioria das pessoas responderam que não sofreram ataques informáticos. Verificámos assim que grande parte das pessoas, não tem implementadas todas as medidas de segurança recomendadas por investigações anteriores. Isto pode causar um aumento de falhas de segurança nos ecossistemas IoT como em toda a rede informática, afetando assim todos os

dipositivos. Todos os ataques informáticos são detestados por todos os utilizadores de IoT devido a causarem perturbações nos serviços. Qualquer seja o nível do ataque informático, este irá causar distúrbios e diminuição de confiança nos dispositivos IoT. Os ataques informáticos não são previsíveis e podem acontecer a qualquer utilizador, sendo a única forma de mitigar essa probabilidade de ataque é tendo medidas implementadas, que consigam prevenir tais distúrbios.

Limitações do trabalho

Uma das limitações deste trabalho, deveu-se à dificuldade em obter uma amostra mais significativa, mesmo tendo sido o questionário partilhado por vários meios, o método poderá ser repensado em investigações futuras.

Outra limitação desta dissertação, prendeu-se com um pequeno grupo de pessoas que sentiu dificuldades em responder ao questionário, apesar deste ter sido pensado e criado para que fosse acessível para todos. Observou-se que para certo tipo de pessoas teria sido útil que as perguntas fossem mais esclarecedoras. Uma validação do questionário, com um pré-teste realizado a especialistas poderia ter resolvido esta questão, contudo, as limitações de tempo inerentes à investigação e à situação pandémica que atravessamos não permitiram esta pré-testagem.

Propostas de trabalhos futuros

Para trabalhos futuros pretende-se questionar sobre apenas um tipo de dispositivo IoT, como por exemplo lâmpadas ou aspiradores inteligentes. Tende-se apenas a questionar um só tipo de dispositivos para tornar o questionário mais fácil de responder e relacionar as perguntas com o dipositivo IoT.

No final do questionário foi feita uma pergunta, de resposta não obrigatória, sobre que pode ser melhorado, das 84 pessoas que responderam ao questionário 22 responderam a esta pergunta. As respostas a esta pergunta podem ser divididas em 2 grupos:

- O primeiro grupo afirmou que o questionário devia ter sido mais esclarecedor para o utilizador comum. Podendo incluir exemplos de situações onde a questão se aplica, procurando, assim, tornar o questionário mais revelante para utilizadores que não conheçam alguns conceitos, ou tenham dificuldade em compreender algumas perguntas.

Mesmo existindo na introdução do questionário, uma explicação da sigla IoT houve pessoas que responderam a esta pergunta que o questionário devia ter um glossário, provavelmente para outros termos utilizados no questionário.

- O segundo grupo dissertou sobre o que pode ser melhorado nos dispositivos IoT. Os pontos a melhorar no IoT, de acordo com quem respondeu a esta pergunta são: a segurança, a privacidade, as medidas de segurança, para além das palavas-passe, e a clareza e cumprimento das regras impostas pela lei.

Em suma, e para concluir, foi possível verificar que, a confiança no uso da tecnologia IoT, depende, principalmente, da segurança e privacidade dos dispositivos. Os fabricantes de IoT têm que melhorar a segurança e a privacidade, tendo também em conta a apresentação de modos para melhorar a segurança, a privacidade e como são tratados os dados recolhidos.

O fornecedor de Internet também tem um papel importante no IoT no que toca à segurança, particularmente no que se refere à configuração da rede, dos seus clientes, para que esta seja segura para todos os dipositivos.

Referências Bibliográficas

A.Saeed, I., Selamat, A., & M. A. Abuagoub, A. (2013). A survey on malware and malware detection systems. International Journal of Computer Applications, 67(16), 25–31. https://doi.org/10.5120/11480-7108

Ackerman, S., & Thielman, S. (2016, February 9). US intelligence chief: We might use the Internet of things to spy on you. The Guardian. Retrieved September 22, 2021, from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Acunetix. (2020, September 10). What is sql INJECTION (SQLI) and how to prevent attacks. Acunetix. Retrieved September 15, 2021, from https://www.acunetix.com/websitesecurity/sql-injection/.

Alam, T. (2018). A Reliable Communication Framework and Its Use in Internet of Things (IoT). Islamic University of Medina. Retrieved September 22, 2021, from https://www.researchgate.net/publication/325645304_A_Reliable_Communication_Framework_and_Its_Use_in_Internet_of_Things_IoT.

Aldowah, H., Ul Rehman, S., & Umar, I. (2020). Trust in iot systems: A vision on the current issues, challenges, and recommended solutions. Advances on Smart and Soft Computing, 329-339. doi:10.1007/978-981-15-6048-4_29

Almeida, J., & Mendes, P. (2021). Piratas em casa. In Proteste (Vol. 437, Ser. Setembro, pp. 27–29). essay, Deco Proteste.

Atac, C., & Akleylek, S. (2019). A survey on security threats and solutions in the age of iot. A Survey on Security Threats and Solutions in the Age of IoT. Retrieved September 14, 2021, from https://dergipark.org.tr/en/download/article-file/661535.

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05

Bauer, T. N. (2015, December). (Pdf) onboarding: The power of connection. Retrieved July 20, 2021, from https://www.researchgate.net/publication/286447344_Onboarding_The_power_of_connection

Baharuddin, R., Singh, D., & Razali, R. (2013). Usability dimensions for mobile applications-a review. Research Journal of Applied Sciences, Engineering and Technology `, 11(9), 2225–2231. https://doi.org/10.19026/rjaset.5.4776

Bhagat, V. (2019, June 23). What are pros and cons of Internet of Things? Let's check out! Retrieved July 20, 2021, from https://www.pixelcrayons.com/blog/what-are-pros-and-cons-of-internet-of-things/

Brush, A. J. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., & Dixon, C. (2011). Home automation in the wild. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/1978942.1979249

Burgess, M. (2018, February 16). What is the internet of things? Wired explains. Retrieved July 20, 2021, from https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

Carroll, N. (2016). Key success factors for smart and connected health software solutions. Computer, 49(11), 22–28. https://doi.org/10.1109/mc.2016.340

Ccg. (2018, March). Internet Das Coisas: EXEMPLOS, APLICAÇÕES E VANTAGENS. Retrieved July 20, 2021, from https://www.ccg.pt/internet-das-coisas-exemplos-aplicacoes-e-vantagens/

CISA. (2020). Report phishing sites. Cybersecurity and Infrastructure Security Agency CISA. Retrieved September 14, 2021, from https://us-cert.cisa.gov/report-phishing.

Check Point Software. (2021, July 26). *What is zero day attack?* Check Point Software. Retrieved September 14, 2021, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-zero-day-attack/.

Cruz, M. A. A., Rodrigues, J. J. P. C., Sangaiah, A. K., Al-Muhtadi, J., & Korotaev, V. (2018). Performance evaluation of iot middleware. Journal of Network and Computer Applications, 109, 53–65. https://doi.org/10.10*16/j.jnca.2018.02.013*

Drew W. (2016, September 30). Internet of things (iot): Pros and cons. Retrieved July 20, 2021, from https://www.keyinfo.com/pros-and-cons-of-the-internet-of-things-iot/

Eddleston, K. A., Chrisman, J. J., Steier, L. P., & Chua, J. H. (2010). Governance and trust in family firms: An introduction. Entrepreneurship Theory and Practice, 34(6), 1043–1056. https://doi.org/10.1111/j.1540-6520.2010.00412.x

Euromoney. (2020). What is blockchain? Blockchain Explained: What is blockchain? | Euromoney Learning. Retrieved September 21, 2021, from https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain.

Farhan, L., Kharel, R., Kaiwartya, O., Quiroz-Castellanos, M., Alissa, A., & Abdulsalam, M. (2018). A concise review on Internet of Things (IoT) -problems, challenges and opportunities. 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP). doi:10.1109/csndsp.2018.8471762

Feily, M., Shahrestani, A., & Ramadass, S. (2009). A survey of botnet and botnet detection. 2009 Third International Conference on Emerging Security Information, Systems and Technologies. https://doi.org/10.1109/securware.2009.48

FireEye. (2015). What is a zero-day exploit. FireEye. Retrieved September 14, 2021, from https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

Gazet, A. (2008). Comparative analysis of various ransomware virii. Journal in Computer Virology, 6(1), 77–90. https://doi.org/10.1007/s11416-008-0092-2

Geske, D. (2020, November 7). A look at the investment in self-driving cars: Who has spent the most? International Business Times. Retrieved September 22, 2021, from https://www.ibtimes.com/look-investment-self-driving-cars-who-has-spent-most-2848289.

Gillis, A. (2020, February 11). What is IoT (Internet of Things) and How Does it Work? Retrieved July 20, 2021, from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Giri Arindam Giri Haldia Institute of Technology Publication Years2017 - 2017Publication counts1Available f, A., Dutta, S., Neogy, S., Dahal, K., & Pervez, Z. (2017, October 01). Internet of things (iot): A survey on architecture, enabling technologies, applications and challenges. Retrieved July 20, 2021, from https://dl.acm.org/doi/abs/10.1145/3109761.3109768

Hao Chen, Xueqin Jia, & Heng Li. (2011). A brief introduction to iot gateway. IET International Conference on Communication Technology and Application (ICCTA 2011). doi:10.1049/cp.2011.0740

Heffelfinger, M. (2020). Prevent IoT Ransomware: Best practices from the SecurityMetrics SOC. SecurityMetrics. Retrieved September 21, 2021, from https://www.securitymetrics.com/blog/prevent-iot-ransomware-best-practices-securitymetrics-soc.

IEEE Innovation at Work . (2020, January 2). Is blockchain the solution to Iot security? IEEE Innovation at Work. Retrieved September 14, 2021, from https://innovationatwork.ieee.org/blockchain-iot-security/.

Jacobs, N., Edwards, P., Markovic, M., Cottrill, C. D., & Salt, K. (2020). Who trusts in the smart city? Transparency, governance, and the internet of things. Data & Policy, 2. https://doi.org/10.1017/dap.2020.11

Janne, L., Sami, H., & Jani, K. (2017). The false prometheus. The ORBIT Journal, 1(1), 1–13. https://doi.org/10.29297/orbit.v1i1.22

Johnson, D. S., Bardhi, F., & Dunn, D. T. (2008). Understanding how technology paradoxes affect customer satisfaction with self-service technology: The role of performance ambiguity and trust in technology. Psychology and Marketing, 25(5), 416–443. https://doi.org/10.1002/mar.20218

Jokela, T. (2003). Assessments of usability engineering processes: Experiences from experiments. 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of The. https://doi.org/10.1109/hicss.2003.1174898

Karamanos, E. (2012, March 8). Investigation of home router security. Retrieved September 14, 2021, from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A508254.

Kumar, V., Dixit, A., Javalgi, R. G., & Dass, M. (2015). Research framework, strategies, and applications of intelligent agent technologies (iats) in marketing. Journal of the Academy of Marketing Science, 44(1), 24-45. doi:10.1007/s11747-015-0426-9

Køien, G. M. (2011). Reflections on trust in devices: An informal survey of human trust in an internet-of-things context. Wireless Personal Communications, 61(3), 495–510. https://doi.org/10.1007/s11277-011-0386-4

Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016). A denial of service attack method for an iot system. 2016 8th International Conference on Information Technology in Medicine and Education (ITME). https://doi.org/10.1109/itme.2016.0087

Magno, S. (2019, January 07). CES: 55 mil MILHÕES DE dispositivos IoT em 2025. Retrieved July 20, 2021, from https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2019-01-07-ces-55-mil-milhoes-de-dispositivos-iot-em-2025/

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109. https://doi.org/10.22373/cj.v2i2.3453

Michler, O., Decker, R., & Stummer, C. (2019). To trust or not to trust smart consumer products: A literature review of trust-building factors. Management Review Quarterly, 70(3), 391-420. doi:10.1007/s11301-019-00171-8

Moldovan, F., Satmarean, P., & Oprisa, C. (2020). An analysis of http attacks on home iot devices. 2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). https://doi.org/10.1109/aqtr49680.2020.9129980

Moloni. (2020, September 13). IoT: O que é a Internet das Coisas? Retrieved July 20, 2021, from https://www.moloni.pt/blog/dicas-e-conselhos/iot-o-que-e-a-internet-das-coisas?gclid=Cj0KCQjwxdSHBhCdARIsAG6zhlUP9MyBmia-m94FWVhW8sRc1lZoa3azBObN7T-NDJzMDY3HjRBmJ2EaAhdwEALw_wcB

Morgan, J. (2017, April 20). A simple explanation of 'the internet of things'. Retrieved July 20, 2021, from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

Oracle. (2021). What is the internet of things (iot)? What Is the Internet of Things (IoT)? | Oracle Portugal. Retrieved September 21, 2021, from https://www.oracle.com/pt/internet-of-things/what-is-iot/.

Palo Alto Networks. (n.d.). What is a denial of service attack (dos) Denial-of-Service. Retrieved September 14, 2021, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

Payne , B. R., & Abegaz, T. T. (2018). Securing the Internet of Things: Best Practices for Deploying IoT Devices. Computer and Network Security Essentials, 493. https://doi.org/10.1007/978-3-319-58424-9 ,Capítulo 28

Posey, B., & Shea, S. (2021, March 22). What are IoT Devices? IoT Agenda. Retrieved September 23, 2021, from https://internetofthingsagenda.techtarget.com/definition/IoT-device.

Ranger, S. (2020, February 03). What is the Iot? Everything you need to know about the Internet of things right now. Retrieved July 20, 2021, from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Schweitzer, F., & den Hende, E. A. (2016). To be or not to be in thrall to the March of smart products. Psychology & Marketing, 33(10), 830–842. https://doi.org/10.1002/mar.20920

Saini, R. K. (2019). A survey on internet of things (iot) applications and challenges for smart healthcare and farming. Bioscience Biotechnology Research Communications, 12(4), 1194–1200. https://doi.org/10.21786/bbrc/12.4/44

Seal, A. (2020, December). What are iot devices and what should you know about them? Retrieved July 20, 2021, from https://www.vxchnge.com/blog/what-are-iot-devices

Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017, 1-25. doi:10.1155/2017/9324035

Shiaeles, S., Kolokotronis, N., & Bellini, E. (2019). Iot vulnerability data crawling and analysis. 2019 IEEE World Congress on Services (SERVICES). https://doi.org/10.1109/services.2019.00028

Statista . (2020). Smart home . Statista. Retrieved September 22, 2021, from https://www.statista.com/outlook/dmo/smart-home/united-states.

Thomas, M. O., Onyimbo, B. A., & Logeswaran, R. (2016). Usability evaluation criteria for internet of things. International Journal of Information Technology and Computer Science, 8(12), 10–18. https://doi.org/10.5815/ijitcs.2016.12.02

Thomas, R. M. (2011). Blending qualitative & quantitative research methods in theses and dissertations. SAGE distributor. ISBN-10: 0-7619-3931-8

Tutida, D. (2021, June 26). 4 exemplos de IOT no MUNDO REAL. Retrieved July 20, 2021, from https://encontreumnerd.com.br/blog/4-exemplos-de-iot

Unit 42. (2020, November 03). 2020 unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report. Retrieved July 20, 2021, from https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. Computer Fraud & Security, 2018(1), 15–20. https://doi.org/10.1016/s1361-3723(18)30007-1

Voas, J., Kuhn, R., Laplante, P., & Applebaum, S. (2018, October 17). Internet of things (iot) trust concerns (draft). Retrieved July 20, 2021, from https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft

Weber, R. H. (2013). Internet of things – governance quo vadis? Computer Law & Security Review, 29(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010

Weiler, N. (2002). Honeypots for distributed denial-of-service attacks. Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. https://doi.org/10.1109/enabl.2002.1029997

Veracode. (2014). Man in the Middle ATTACK: Tutorial & examples. Veracode. Retrieved September 21, 2021, from https://www.veracode.com/security/man-middle-attack.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for internet of things. Journal of Network and Computer Applications, 42, 120-134. doi:10.1016/j.jnca.2014.01.014

Yan, Z., & Holtmanns , S. (2007). Trust Modeling and Management: from Social Trust to Digital Trust. Trust Modeling and Management. Retrieved September 14, 2021, from http://lib.tkk.fi/Diss/2007/isbn9789512291205/article1.pdf.

Zhang, Z.-K., Cho, M. C., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). Iot security: Ongoing challenges and research opportunities. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. https://doi.org/10.1109/soca.2014.58

Zyrianoff, I., Heideker, A., Silva, D., Kleinschmidt, J., Soininen, J.-P., Salmon Cinotti, T., & Kamienski, C. (2019). Architecting and deploying iot smart applications: A performance–oriented approach. Sensors, 20(1), 84. https://doi.org/10.3390/s20010084

Apêndice 1 - Formulário

Introdução

Este questionário deverá durar em média 6 minutos.

Este questionário foi desenvolvido para a dissertação final do Mestrado de Informática do ISTEC do aluno Tomás Félix. Este formulário irá permitir obter informação, de várias pessoas, sobre o que pensam acerca de dispositivos IoT (Internet of Things). Os seus dados pessoais não serão divulgados.

O que é a IoT?

A Internet das coisas (IoT) refere-se a objetos do dia a dia, que ficam ligados entre si através da Internet. Algum destes objetos variam entre lâmpadas, carros, equipamentos de rega e semáforos. A IoT tem como objetivo facilitar, automatizar e muito mais, onde pode ser colocado em casas, fábricas, hospitais, quintas e cidades.

Informações pessoais

Pergunta	Tipo de Resposta
Qual a sua idade?	Resposta livre
Tem algum dispositivo IoT?	Esta pergunta teve 4 escolhas sendo: 0 dispositivos 1 a 5 dispositivos; 6 a 13 dispositivos; +14 dispositivos.
Quantas horas por semana usa a Internet?	Esta pergunta teve 4 escolhas sendo: Nunca ou raramente

	1 a 3 horas por semana 4 a 6 horas por semana Diariamente
Qual a sua profissão	Resposta livre

Confiança

As perguntas com a letra “a” indicam as pessoas com dispositivo IoT e a letra “b” as pessoas sem dispositivos.

Assunto	Pergunta	Tipo de resposta
Controlo	1.1 (a) - Num dispositivo IoT, considera que teve sempre controlo sobre ele 1.1 (b)- Num dispositivo IoT, considera que terá sempre controlo sobre ele	Esta pergunta tem 4 opções de resposta, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente.
	1.2 (a) -Sobre os dispositivos IoT, pensa ter conseguido, com facilidade definir quem tem acesso ao dispositivo 1.2 (b) -Sobre os dispositivos IoT, pensa que irá conseguir, com facilidade definir quem tem acesso ao dispositivo	Esta pergunta teve 4 valores, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente.

Transparência/ privacidade	1.3- Sobre os dispositivos IoT, pensa que os fabricantes dizem com clareza o que fazem com as informações que o dispositivo recolhe	Esta pergunta teve 4 valores, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente.
	1.4 (a) -Sabe onde ficam guardados os dados dos dispositivos IoT 1.4 (b)-Pensa que é importante saber onde estão guardados os dados dos dispositivos IoT	Esta pergunta teve 3 valores, sendo elas: Sim; Não; Não me interessa;
	1.5- Nos dispositivos IoT, a privacidade é um ponto importante para si	Esta pergunta tem 4 valores, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente;
Usabilidade do Produto	1.6 (a)- Considera os dispositivos IoT fáceis de utilizar	Esta pergunta tem 4 valores, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente;

Marca	1.7- Considera que a marca é um aspeto importante na confiança do produto	Esta pergunta tem 4 valores, sendo elas: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente;
	1.8- Quais são as marcas que conhece de fabricantes de dispositivos IoT	Esta pergunta tem 7 opções e um campo para acrescentar outras marcas. As marcas mostradas são: Google; Amazon; Cisco; Huawei; Microsoft; Oracle; IBM;
Onboarding	1.9 (a)- Nos dispositivos IoT, acha que a sua instalação foi fácil de compreender e executar	Tendo as seguintes opções: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente;
	1.10- Qual o nível de customização inicial de um dispositivo IoT que preferia encontrar	Tendo as seguintes opções: Mínimo; Mínimo + opções predefinidas; Mínimo + opções predefinidas + algumas opções extras;

	1.11 (a) -A publicidade (anúncios, caixa do produto, sites de venda) representa bem as funcionalidades dos produtos IoT	Resposta facultativa; Tendo as seguintes opções: Discordo totalmente; Discordo parcialmente; Concordo parcialmente; Concordo totalmente;
1.12- Tem confiança nos dispositivos IoT		Esta pergunta tem 3 escolhas, sendo: Confio; Confio parcialmente/ tenho receios; Não confio;

Segurança

Pergunta	Tipo de resposta
2.1- Já sofreu algum ataque informático? Terá também uma pergunta de detalhe caso a pessoa tenha respondido “Sim”: 2.1.1 - Se sim, descreva o ataque.	Esta pergunta tem 2 escolhas, sendo elas: Sim; Não;
2.2- Considera que tem palavras-passes fortes e diferentes?	Esta pergunta tem 2 escolhas, sendo elas: Sim; Não;
2.3- Ao comprar um dispositivo novo costuma alterar as palavras-passes que vieram com o dispositivo?	Esta pergunta tem 3 escolhas, sendo elas: Sempre; Às vezes; Nunca;

2.4- Costuma fazer atualizações aos dispositivos IoT que não fazem atualizações automaticamente	Esta pergunta tem 4 escolhas, sendo elas: Não Sim, quando saem; Sim, quando me lembro; Sim, quando encontro problemas;
2.5- Na sua rede pessoal tem criado VLAN	Esta pergunta tem 4 escolhas, sendo elas: Sim; Não, não sei o que é; Não, não sei criar; Não, não acho que seja necessário;
2.6- Na sua rede pessoal tem um router além do fornecido pelo fornecedor de Internet	Nesta pergunta a resposta pode ser sim ou não.

Conclusão

Pergunta	Tipo de Resposta
4.1- Teve dificuldades em responder ao questionário	Não tive dificuldades; Tive algumas dificuldades; Tive muitas dificuldades;
4.2- O que pode ser melhorado	Resposta livre.

Mensagem Final

A sua resposta foi registada. Obrigado pelo seu tempo. As suas respostas serão tratadas com o maior respeito e só serão utilizadas nesta dissertação.