A Literacia Digital e a Cibersegurança:

Contributos para o estudo dos comportamentos ciberseguros

Ivo Manuel Botelho Teixeira

Dissertação

de Mestrado em Gestão e Curadoria da Informação

Ivo Manuel Botelho Teixeira, A Literacia Digital e a Cibersegurança: Contributos para o estudo dos comportamentos ciberseguros, 2022

Março de 2022

A Literacia Digital e a Cibersegurança:

Contributos para o estudo dos comportamentos ciberseguros

Ivo Manuel Botelho Teixeira

Dissertação

de Mestrado em Gestão e Curadoria da Informação

Orientadora: Professora Doutora Paula Alexandra Ochôa de Carvalho Telo

dezembro, 2021

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão e Curadoria da Informação, realizada sob a orientação científica da Professora Doutora Paula Alexandra Ochôa de Carvalho Telo.

DECLARAÇÃO

Declaro que esta Dissertação é o resultado da minha investigação pessoal e independente. O seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto, nas notas e na bibliografia.

O candidato,

Ivo Manuel Botelho Teixeira

Lisboa, 29 de novembro de 2021

Declaro que esta Dissertação se encontra em condições de ser apreciada pelo júri a designar.

A orientadora,

Paula Alexandra Oliveira da Costa Tavares

Lisboa, 29 de novembro de 2021

Aos meus pais e irmão, pelo seu apoio, amor e carinho

Agradecimentos

Eis um dos maiores desafios da minha vida que, com muito esforço, altos e baixos, posso afirmar que o ultrapassei graças a muita gente que sempre acreditou em mim desde o início.

Começo por agradecer a todas as pessoas que colaboraram com esta dissertação, à Professora Doutora Manuela Aparício por ter sido a primeira professora a receber-me enquanto orientadora, e à Secretaria Regional da Cultura, Ciência e Transição Digital pela sua colaboração neste estudo.

Em segundo lugar, agradeço à minha família e ao meu lado mais especial, os meus pais. É de admirar todo o apoio que estes dois me deram, principalmente, na tentativa, mesmo sem saber como, de me motivarem dia para dia, aturando as minhas birras e desabafos até ao fim. O meu especial obrigado e espero poder continuar a dar mais alegrias na vida. Um outro elemento, o qual não me poderia esquecer, é o meu irmão. O meu único irmão, que também sendo o meu melhor amigo foi uma peça, mesmo que despercebida, importante nesta longa caminhada. Ao meu mano, o meu obrigado.

Em terceiro lugar, quero agradecer à Carine, Micaela, Catarina e restante turma e corpo docente do mestrado pelo espírito de trabalho e de amizade que pude experienciar e que levo para a vida. Agradeço a todos os meus amigos, em especial da ilha de São Jorge, nos Açores, com os quais cresci e vivi uma grande parte da minha vida e que são, certamente, muito importantes para que possa continuar a sorrir e a fazer sorrir, como tanto me conhecem.

Por último e não menos importante, um agradecimento especial à Professora Doutora Paula Ochôa por me ter acompanhado e dado a mão na maior parte deste trabalho, pela sua constante preocupação em não desistir e, principalmente, acreditar em mim.

Porque nunca é demais agradecer, a todos o meu muitíssimo obrigado!

Literacia Digital e Cibersegurança: Contributos para o estudo dos comportamentos ciberseguro.

Ivo Manuel Botelho Teixeira

Resumo

Os utilizadores do Mundo Digital podem ter diferentes comportamentos no uso da internet como, também, no próprio dispositivo que o liga a esse Mundo. Esses comportamentos podem não ser os mais corretos e seguros, tendo, por consequência, repercussões na experiência do utilizador, como por exemplo, ver o seu sistema de informação pessoal ou o seu dispositivo eletrónico alvo de um cibercrime. Este tema tem vindo a ser explorado em diversas áreas científicas como a Ciência da Informação, a Gestão de Sistemas de Informação e, até mesmo, a Gestão e Curadoria de Informação. Esta dissertação nasce pelo interesse em dar um contributo para o estudo dos comportamentos ciberseguros na Região Autónoma dos Açores, visto que o nível de literacia digital das pessoas desta região encontra-se abaixo do nível nacional. A questão de investigação deste estudo visa perceber qual o impacto da literacia digital e da cibersegurança na Região Autónoma dos Açores. Pretende-se assim, estudar as competências, habilidades e atitudes dos açorianos, tanto no meio digital como na sua segurança em concreto.

A metodologia aplicada neste estudo tem por base uma abordagem metodológica mista, aplicando um método quantitativo e um método qualitativo. O primeiro, é um estudo empírico através de um inquérito online a indivíduos residentes nos Açores, sendo que, posteriormente, é aplicada a metodologia de grupo focal, reunindo 5 pessoas de perfis semelhantes com o fim de perceber, numa forma de debate, opiniões, ideias e experiências sobre várias questões relacionadas com a literacia digital e cibersegurança e possíveis soluções para as gerações futuras.

As conclusões apontam para a inexistência de capacidade crítica sobre a informação que é retirada da internet, expondo assim um grande risco de transmissão da informação falsa, vírus ou fraudes e criação de conhecimento inválido, tornando necessário um reforço dos comportamentos ciberseguros por parte dos açorianos. A capacidade de proteção da identidade digital dos açorianos é ainda deficiente, pelo que

se recomenda a criação de estratégias regionais através do Plano Nacional de Leitura e o Centro Nacional de Cibersegurança, a valorização dos clubes de informática públicos e a aplicação dos videojogos em contextos escolares ou em outros contextos pedagógicos.

Espera-se ter contribuído para um maior entendimento sobre este tema, possibilitando o desenvolvimento de melhores políticas públicas a aplicar na região.

Palavras-chave: Literacia digital; Cibersegurança; Comportamento Informacional; Comportamento Ciberseguro; Região Autónoma dos Açores.

Digital Literacy and Cybersecurity: Contributions to the study of cyber-safe behaviors.

Ivo Manuel Botelho Teixeira

Abstract

Users of the Digital World may have different behaviors in the use of the Internet, as well as on the device that connects it to that World. Such behavior may not be the most correct and secure, resulting in repercussions on the user experience, such as seeing your personal information system or your electronic device that is the target of a cybercrime. This theme has been explored in several scientific areas such as Information Science, Information Systems Management and even Information Management and Curation. This dissertation is born out of interest in contributing to the study of cyber-insurance behaviors in the Autonomous Region of the Azores, since the level of digital literacy of people in this region is below the national level. The research question of this study aims to understand the impact of digital literacy and cybersecurity in the Autonomous Region of the Azores. Thus, it is intended to study the competences, skills, and attitudes of the Azoreans, both in the digital environment and in their specific security.

The methodology applied in this study is based on a mixed methodological approach, applying a quantitative method and a qualitative method. The first is an empirical study through an online survey of individuals residing in the Azores, and subsequently, the focus group methodology is applied, bringing together 5 people from similar profiles to understand, in a form of debate, opinions, ideas and experiences on various issues related to digital literacy and cybersecurity and possible solutions for future generations.

The conclusions of the study point to the lack of critical capacity on the information that is taken from the Internet, thus exposing a great risk of transmission of false information, viruses or fraud and creation of invalid knowledge, making it necessary to reinforce cyber-safe behaviors on the part of the Azoreans. The ability to protect the digital identity of Azoreans is still deficient, so it is recommended the creation of regional strategies through the National Reading Plan and the National Cybersecurity Center, the

valorization of public computer clubs and the application of video games in school contexts or in other pedagogical contexts.

It is expected to have contributed to a greater understanding on this topic, enabling the development of better public policies to be applied in the region.

Keywords: *Digital literacy; Cybersecurity; Informational Behavior; Cybersecurity Behavior; Autonomous Region of the Azores.*

Lista de Abreviaturas

ALA	***American Library Association***
SCONUL	***Society of College, National and University Libraries***
CILIP	***Chartered Institute of Library and Information Professionals***
LD	**Literacia Digital**
LI	**Literacia Informacional**
LC	***Locus of Control***
TA	***Technology Awareness***
CAE	***Cyber-Attack Experiences***
SE	***Self-Eficaccy***
I	***Impulsivity***
KC	***Knowledge of Cybersecurity***
FG	***Focus Group***
P.1	**Participante 1**
P.2	**Participante 2**
P.3	**Participante 3**
P.4	**Participante 4**
P.5	**Participante 5**

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Índice Geral

1. Introdução

A utilização da Internet tem vindo a ser cada vez mais generalizada no contexto quotidiano do ser humano, e a cibersegurança, por sua vez, também tem feito parte da experiência de cada indivíduo que entre em contato com o Mundo digital. O conceito de cibersegurança toma como base, técnicas e comportamentos que são aplicados pelo indivíduo ao nível da sua segurança digital (Howard, 2018). Estes comportamentos podem ser positivos ou negativos, acabando por haver, posteriormente, repercussões aquando a obtenção, gestão e disseminação de informação pelo indivíduo (Howard, 2018). Uma utilização segura da Internet parte, geralmente, do comportamento do próprio indivíduo. Deste modo, um comportamento ciberseguro requer certas e determinadas variantes que podem ir para além da literacia digital do indivíduo, sendo necessária a procura por um maior conhecimento sobre os processos de aprendizagem, resultando numa melhor aplicação de mecanismos de segurança digital (Addae et al., 2019).

Olhando para o território português, variáveis como a idade e as habilitações literárias têm apresentado algum impacto quanto à forma como é utilizada a Internet e, consequentemente, como é exercida a cibersegurança. Primeiramente, importa referir que, quanto à utilização de um computador, em 2017, registou-se uma maior utilização de um computador por parte de indivíduos com idades compreendidas entre os 16 e os 24 anos, enquanto que o grupo etário que menos utilizava um computador integra os indivíduos com idades entre os 65 e 74 anos (PORDATA, 2020a). A partir destes dados, importa referir que, em 2020 e com o surgir da pandemia Covid 19, verificou-se que o grupo etário que mais utilizava a Internet eram indivíduos com idades compreendidas entre os 16 e 24 anos (99,5% do total de indivíduos), enquanto que o grupo etário que menos utilizava a Internet integrava os indivíduos com idades entre os 65 e 74 anos (39% do total de indivíduos) (PORDATA, 2020a). Contudo, em relação aos anos 2019 e 2020, houve um crescimento do uso do computador e internet por parte de indivíduos com 16 ou mais anos, em proporção, de 3%.

No que toca ao nível de escolaridade, em 2020, registou-se que os indivíduos que mais utilizavam a Internet eram os que detinham o ensino superior completo (98,7%), enquanto que os indivíduos que menos utilizavam a Internet eram indivíduos que

detinham apenas o ensino básico completo (56,3%) (PORDATA, 2020b). Neste caso, entre os anos 2019 e 2020, houve um crescimento do uso da internet nos três níveis de escolaridade, sendo que o crescimento mais significativo foi em indivíduos com 16 ou mais anos que detêm o ensino básico de escolaridade com um aumento, em proporção, de 2,1%.

Em 2019, foram feitas algumas inferências pelo Centro Nacional de Cibersegurança, com base em dados do Eurostat, em que o uso da Internet para fins pessoais, num modo geral, é feita por indivíduos com idades entre os 25 e 34 anos e os indivíduos que detêm o ensino superior têm tendência em reconhecer melhor sobre terem sofrido algum incidente de segurança na utilização da Internet para fins pessoais do que os indivíduos com idades compreendidas entre os 64 e os 74 anos, a par dos indivíduos que não possuem estudos superiores (Centro Nacional de Cibersegurança, 2020). Serve de contexto para esta problemática a situação atual de pandemia, em que houve evidentemente a exposição de várias fragilidades das sociedades modernas quanto às tecnologias de informação, mostrando ser claro o papel fulcral das redes sociais na disseminação de desinformação e campanhas de "*phishing*" (Carreiras et al., 2020). Neste caso, pôde-se constatar que os cibercriminosos têm a tendência de explorar os receios dos indivíduos e, desta forma, incentiva-os a certos e determinados comportamentos como por exemplo, a instalação de uma aplicação para o acompanhamento da evolução de casos de COVID-19 no concelho onde reside ou trabalha mas que, no entanto, é um sistema de *malware* (Carreiras et al., 2020).

Perante esta situação, emerge a preocupação quanto à competência digital dos açorianos, bem como, porventura, ao seu comportamento ciberseguro, sendo que, em 2019, a proporção de indivíduos com idade entre 16 e 74 anos com competências digitais ao nível básico ou acima de básico, na Região Autónoma dos Açores é de 43%, estando a 8.8 valores percentuais abaixo do nível nacional, 9.1% abaixo de Portugal Continental e 3.7% abaixo da Região Autónoma da Madeira (INE, 2019).

Neste sentido é colocada a seguinte questão de partida da investigação: "Qual o impacto da literacia digital e da cibersegurança na Região Autónoma dos Açores?". Reforçando o problema inerente ao nível de literacia digital da Região, o principal objetivo deste estudo visa contribuir para o estudo dos comportamentos ciberseguros

dos açorianos, contribuindo, também, para um maior entendimento sobre a literacia digital da população açoriana, ao incentivo na criação de novas políticas pedagógicas e valorização da literacia digital, e compreender o impacto que a literacia digital e a cibersegurança têm na população açoriana através do estudo do nível de proficiência digital.

A estrutura desta dissertação está dividida em cinco capítulos, sendo eles o Estado da Arte (Capítulo 2), o Modelo Conceptual de Análise (Capítulo 3), a Metodologia (Capítulo 4), a Literacia Digital e Cibersegurança na Região Autónoma dos Açores (Capítulo 5), e Conclusões (Capítulo 6).

O capítulo do "Estado da Arte" apresenta a revisão de literatura com base em produção científica sobre o tema em causa. A realização do enquadramento teórico-conceptual é feita através de uma revisão de literatura sobre aspetos que fossem relacionados com os temas "Literacia Digital" e "Cibersegurança", começando por explorar conceitos como o Comportamento Informacional, o Fosso Digital, e os Comportamentos Ciberseguros. Para que tal acontecesse, recorreu-se à procura de informação em diversas fontes, tendo sido o Google Scholar a mais utilizada. Foram também utilizadas outras fontes como a b-on e a ResearchGate, como forma de chegar a mais informação que pudesse não ser encontrada no Google Scholar. Como estrutura desta revisão, o capítulo foi dividido em dois subcapítulos, sendo que o primeiro subcapítulo é sobre Comportamento Informacional, onde são discutidos os termos de literacia digital, literacia informacional, comparando e discutindo os seus conceitos, e o fosso digital como um conceito consequente do termos anteriores. O segundo subcapítulo é sobre a Cibersegurança, onde são discutidos os temas do comportamento ciberseguro e o *malware*.

O capítulo do "Modelo Conceptual de Análise" foi concebido para tentar compreender vários fatores que pudessem levar ao que se entende por comportamento ciberseguro, ou seja, é criado um modelo com base em várias variáveis de podem ser relacionadas com a variável dependente, sendo ela, o comportamento ciberseguro e, por fim, utilizar esse modelo como uma ferramenta de análise e sustentação aos métodos de investigação do estudo. Este modelo teve como base o *Theory of planned*

behavior de Icek Ajzen e complemento de várias variáveis referentes a vários estudos sobre a temática.

O capítulo da "Metodologia" é onde se expõe a metodologia "quant-qual", isto é, uma abordagem metodológica mista, sendo baseada, primeiramente, num estudo empírico a partir de inquéritos fundamentados no Quadro Europeu de Referência para a Competência Digital, desenvolvido pelo Laboratório de Conteúdos Digitais do CIDTFF (Departamento de Educação e Psicologia da Universidade de Aveiro), e, em segunda instância, pelo debate em formato *focus group* como complemento qualitativo, onde se irá retirar com maior detalhe informações sobre as temáticas a abordar, através de opiniões, experiências e ideias dos participantes. No final são descritas as contribuições do grupo focal para o estudo.

No capítulo "Literacia Digital e Cibersegurança na Região Autónoma" é sintetizado os resultados referentes à metodologia mista utilizada, onde são feitas algumas interpretações desses resultados, bem como algumas recomendações para a problemática em questão. Por fim, o capítulo das "Conclusões" é baseado numa num conjunto de limitações e propostas de estudos futuros.

2. Estado da Arte

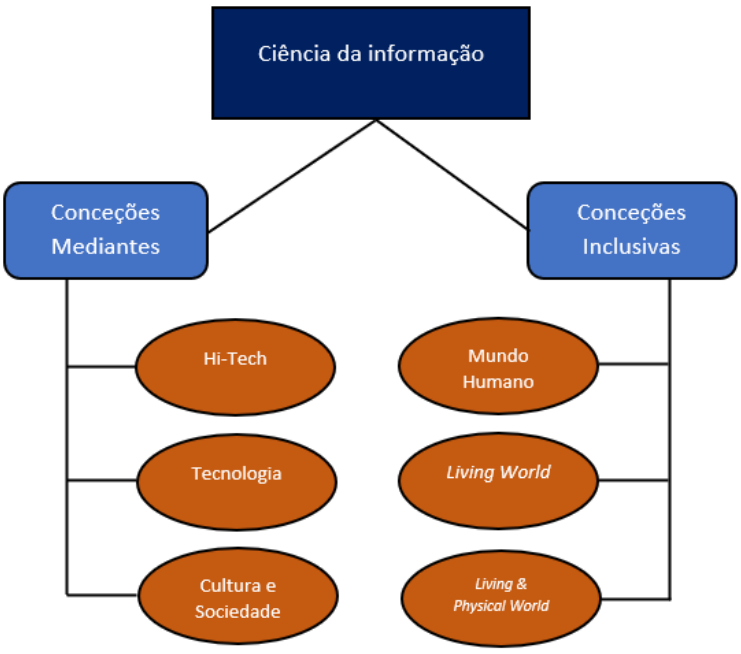
A ciência da informação tem vindo a estar cada vez mais presente na comunidade científica, dada a sua interdisciplinaridade. O termo pode parecer simples, mas o seu entendimento vai para além de ser uma matéria objetiva, ou seja, é uma definição multidimensional e bastante abrangente, em constante mudança (Zins, 2007). Segundo Borko, (1968), no seu artigo "*Information science: What is it?"*, a ciência da informação é a disciplina que estuda as propriedades e comportamentos da informação, tendo em conta o conhecimento relacionado com a origem, coleção, organização, armazenamento, interpretação, transmissão, transformação, e utilização da informação. Contudo, Chaim Zins (2007) aponta que a ciência da informação é um campo científico onde engloba os conceitos de "documentação", a "informação", o "conhecimento" e a "mensagem da informação", indo além de uma só interpretação quanto ao próprio conceito de "Ciência da Informação". O mesmo autor, desconstrói a definição de "Ciência da Informação" em seis diferentes dimensões, cujas podem ser agrupadas em dois grupos, sendo eles: o grupo das conceções mediantes e o grupo das conceções inclusivas. No primeiro, inserem-se as dimensões cujas conceções são baseadas na racionalidade, ou seja, são focadas na exploração de aspetos relacionados com o conhecimento humano (Zins, 2007). No outro grupo, inserem-se as dimensões cujas conceções são baseadas na racionalidade da ciência da informação como um campo genérico no seu termo(Zins, 2007).

No grupo das conceções mediantes, inserem-se a conceção de ciência da informação no domínio do "Hi-tech"; a conceção de ciência da informação no domínio da tecnologia; e a mesma conceção, mas no domínio da cultura e sociedade (Zins, 2007). No domínio do "Hi-tech", a ciência da informação é baseada em aspetos relacionados com tecnologias com base em computadores; no domínio da tecnologia, a ciência da informação é baseada em aspetos relacionados com a implementação de todos os tipos de tecnologia da informação; e, por fim, o domínio da cultura e sociedade, a ciência da informação tem por base aspetos relacionados com as sociedades humanas (Zins, 2007).

No Grupo das conceções inclusivas, inserem-se a conceção de ciência da informação nos domínios do Mundo Humano, do *"Living World"*, e do "*Living & Physical Worlds"*. No domínio do Mundo Humano, a ciência da informação é regida por aspetos

que estão relacionados com o "reino humano", ou seja, pelas interações entre humanos e informação e todos os mecanismos que se regem nessas interações; no domínio do "*Living World*", a ciência da informação rege-se por aspetos relacionado com a vivência no mundo, ou seja, aplica-se aos conceitos de comunidade e grupos de indivíduos, sendo estes contextos de ambientes em que a informação passa a ser um fator de vivência dos mesmos; por fim no domínio do "*Living & Physical Worlds*", a ciência da informação toma por base todos os tipos de organismos biotecnológicos, humanos e não humanos, e todos os objetos físicos, isto é, por exemplo, a relação que existe entre a informação e os reinos das plantas e animais, ou às organizações e aplicações humanas (Zins, 2007). Contudo, todos os seis domínios tomam partido do conceito principal que é a "Ciência da Informação", mas que para Zins (2007), o domínio da cultura e sociedade é o modelo representativo da ciência da informação contemporânea.

Figura 1: Conceitos de Ciência da Informação.
Fonte: Conceptions of information science (Zins, 2007)



2.1. O Comportamento Informacional

O estudo e valorização dos comportamentos informacionais deram-se após a grande Guerra (1946) numa conferência realizada em duas partes, em Londres, sendo a primeira chamada de *Royal Society Scientific Information* e a segunda de *British Commonwealth Official Scientific Conference.* Nesta conferência tornou-se evidente que se precisava de dar uma maior importância aos serviços de informação científica para que houvesse um maior desenvolvimento da ciência (Shaw, 1948). Neste sentido, a *Royal Society* convocou uma conferência com bibliotecas, sociedades e instituições responsáveis por publicar, abstração, serviço de informação com o intuito de aperfeiçoarem os métodos já existentes de recolha, indexação e distribuição de literatura científica (Shaw, 1948).

Nas décadas de 1970 e 1980 começaram a surgir estudos sobre o comportamento informacional por parte do público em geral (Case, 2006). Nos inícios do século XXI, já com a *World Wide Web* a disseminar-se no quotidiano do ser humano, começou a surgir uma exponencial mudança no modo como as pessoas procuravam por informação, ou seja, segundo Donald Case (2006) constatou-se que as pessoas, na generalidade, começaram a utilizar a internet como fonte de informação, ao invés da comunicação social recorrente, como a televisão e a rádio. O mesmo autor refere ainda o significado de "*intra-individual information behavior*", em que o utilizador apresenta padrões de necessidade em procurar informação, o contexto da informação e, ainda, a seleção de fontes nos vários contextos diários dos indivíduos (Case, 2006).

Importa enfatizar que o conceito de *Comportamento Informacional*, neste estudo, refere-se ao comportamento informacional por parte do ser humano e não, como o próprio nome indica, sobre o comportamento da informação (Fernandes, 2020). Este conceito está intrinsecamente relacionado com os métodos que cada individuo utiliza para bem de procurar e encontrar a informação que necessita, podendo ser denominado, desta forma, uma ação etnográfica perante a utilização de sistemas (digitais ou analógicos) de informação (T. Wilson, 2000).

Contudo, Wilson (2000) exibe, como forma de conceptualização, quatro definições descritas na tabela abaixo:

Tabela 1: Definições de Comportamento Informacional por Wilson (2000).

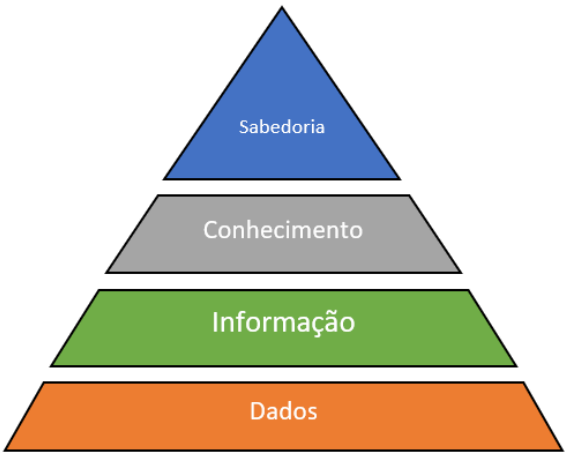
"Information Behavior"	Comportamento humano em relação com as fontes e canais de informação, desde a comunicação face-a-face com outros indivíduos à receção de informação através da televisão ou rádio.
"Information Seeking Behavior"	Ação propositada em procurar informação para um determinado objetivo, seja através da procura em sistemas de informação manuais (bibliotecas), ou digitais (internet).
"Information Searching Behavior"	Termo específico que retrata o comportamento ao nível micro do indivíduo na procura por informação. Este tipo de comportamento consiste em interações computacionais como clicar em *links* ou aplicar uma estratégia de procura booleana para determinar um certo tipo de informação.
"Information Use Behavior"	Atos físicos e mentais resultantes da incorporação de informação na base do conhecimento do indivíduo.

Neste sentido, é possível definir mais quatro conceitos dentro desta temática, sendo eles: *dados*, *informação*, *conhecimento* e *sabedoria.* A definição de *dados* é basicamente caracterizada por dados "crus", ou seja, simplesmente dados sem significância e que são inseridos e lidos pela máquina de modo a conseguir-se dar significado e forma aos dados (Bellinger et al., 2004). Depois de serem estruturados é, então, criada a *informação,* sendo construídos significados e conexões relacionais que

tanto podem ser úteis ou não ao utilizador da máquina (Bellinger et al., 2004). O *conhecimento* é designado pela coleção de informação útil, sendo um determinante de todo o processo de estruturação e seleção de dados, dado o lugar a uma coletânea de informação útil para corresponder à transformação e criação de conhecimento do utilizador (Bellinger et al., 2004). Por fim, segundo Bellinger et al. (2004), a *sabedoria* "*is an extrapolative and non-deterministic, non-probabilistic process.*", ou seja, é um conceito que vai para além do entendimento de conhecimento, levando o ser humano a desenvolver os seus níveis de consciência e, especificamente, os tipos de programação humana, como a programação moral, códigos éticos, etc. Dá ao indivíduo um entendimento melhor ao conhecimento previamente adquirido.

Quando se fala em "utilizador" fala-se no indivíduo que utiliza a máquina que processa toda esta hierarquia, estando na base os dados e no cimo a sabedoria.

Figura 2: Hierarquia do Comportamento Informacional Humano.
Fonte: Elaboração própria.



2.1.1. Literacia digital

O termo *Literacia Digital* (LD) é mencionado por Hwang e Kuo (2015) como sendo a capacidade de se conseguir obter e gerir informação através da Internet. Este termo, segundo os mesmos autores, nasce da necessidade que o indivíduo moderno tem pela informação com o fim de produzir resultados ou solucionar problemas tanto em contextos pessoais, como laborais ou académicos. Deste modo, segundo Loureiro e

Rocha (2012), pressupõe-se que um indivíduo digitalmente literado é capaz de aceder e recolher informação em contextos digitais; de manusear informação para uso futuro; gerir a informação de múltiplas fontes; criar conhecimento e recrear nova informação; e, comunicar a informação.

Este indivíduo é considerado como um ser que procura constantemente por informação e, neste caso, compete ao mesmo que detenha uma *consciência tecnológica* (CT), isto é, que tenha o interesse em adquirir novos conhecimentos sobre o uso das tecnologias e as suas respetivas estratégias de manuseamento para bem de as usufruir da melhor forma possível, como por exemplo utilizar um dispositivo tecnológico ou aceder à Internet (Alshboul, 2017). Neste sentido, o conceito de *literacia digital*, também pode ser denominado de "*digital skills"*, ou *competência digital,* referindo-se a diversos tipos de habilidades relacionadas com o conhecimento do mundo digital, designadamente, a competências necessárias para operar sistemas digitais e para manusear conteúdo online da Internet (Dodel & Mesch, 2018).

Figura 3: Conceptualização de Literacia Digital
Fonte: Elaboração própria

Segundo Ramos e Faria (2012), o conceito de Literacia Digital contém algumas dimensões que podem definir melhor a sua conceptualização, a par de um termo que os próprios autores definem como *literacia informacional* (LI). Neste sentido, fala-se das dimensões: *Aprendizagem transformativa*; *Problemática intergeracional*; *Inevitabilidade; Dependências*. No que toca ao significado da *Aprendizagem transformativa*, os autores referem que a LD é uma das bases transformadoras da pedagogia do ser humano, considerando que só existirá literacia digital quando os indivíduos transformam as suas práticas laborais e/ou pessoais para um conceito digital (Ramos & Faria, 2012). Contudo, esta transformação implica que a literacia digital

consiga abranger os adultos e, até mesmo, os idosos para que possa haver um desenvolvimento pessoal e integração social em qualquer contexto social, surgindo deste modo a *Problemática intergeracional* (Ramos e Faria, 2012).

Tende-se a afirmar cada vez mais que o uso das tecnologias é indispensável para as gerações futuras, seja para o seu sucesso escolar e académico como para o seu sucesso profissional, tornando o conceito da *literacia digital* como sendo inevitável (*Inevitabilidade*) para as suas vidas (Ramos e Faria, 2012). Porém, existem algumas desvantagens e limitações quanto ao uso das tecnologias. Neste sentido, Ramos e Faria (2012) referem que as tecnologias podem provocar impacto negativo em relação ao utilizador, tocando em vários domínio como: a ansiedade, resultante do excesso de informação, gerando assim, impotência de suportar toda a informação; problemas cognitivos através do excesso de informação, pela "sobrecarga decorrente da acumulação de tarefas que as tecnologias acabam por desencadear" (Ramos e Faria, 2012). Existem outros tipos de características decorrentes do excesso de informação circunstante na *Internet*, como por exemplo: "a fragmentação, a superficialidade, o imediatismo, e por vezes a incorreção (…)" (Ramos e Faria, 2012), tornando-se, desta forma, necessário que o utilizador da *Internet* tenha competências ao nível da pesquisa, análise e seleção, sendo esta última de teor crítico. Neste contexto, é designado outro conceito, sendo ele a *literacia informacional* (LI).

2.1.2. Literacia Informacional

O termo *literacia informacional* começou a ser discutido nos anos 70 por Paul Zurkowski, caracterizando as pessoas que possuíam literacia informacional como sendo pessoas que treinaram na aplicação de recursos informacionais no seu trabalho, aprendendo desta forma técnicas e habilidades com ferramentas de informação em larga escala, bem como *"primary sources in molding information-solutions to their problems."* (Behrens, 1994).

Nos finais da década de 80 e com a disseminação de novas tecnologias de informação pela sociedade, Patricia Breivik's, apontou que a questão da literacia informacional é um processo de aprendizagem, especificamente, como competência essencial para uma aprendizagem a longo prazo (Marcum, 2002) e, deste modo, *"in*

order to improve undergraduate education, it would became vital for libraries to integrate fully with the learning process." (Behrens, 1994). Após uma década, o conceito foi redefinido pela mesma autora de forma a abranger novas tendências tais como: a aprendizagem baseada em recursos; "*undergraduate research*"; serviços de aprendizagem; aprendizagem por inquérito; e, aprendizagem por resolução de problemas (Marcum, 2002).

Em 1989, a *American Library Association* (ALA) elaborou um relatório em que dava ênfase à importância de se adquirir literacia informacional, salientando que apenas podia ser adquirido através de um novo modelo de aprendizagem. A ALA define que para se ser *"information literade"*, uma pessoa tem que ser capaz de identificar a informação necessária, bem como a habilidade de encontrar, avaliar e usar efetivamente a informação pretendida (Behrens, 1994).

De acordo com Behrens (1994, p.315):

> *"Ultimately, information literate people are those who have learned how to learn. They know how to learn because they know how knowledge is organized, how to find information, and how to use information in such a way that others can learn from them. They are people prepared for lifelong learning, because they can always find the information needed for any task or decision at hand."* (Behrens, 1994).

Para a *Society of College, National and University Libraries* (SCONUL), *"information literade people"* tendem a demonstrar um conhecimento sobre como garantem, usam, gerem, sintetizam e criam informação de forma ética, desenvolvendo habilidades sobre a informação de forma eficaz (SCONUL, 2011). Neste sentido, desenvolver *"information literade people"* é um processo contínuo e holístico. A SCONUL define a LI através de um modelo chamado *"Seven Pillars of Information Litaracy"*, desenvolvido em 1999 mas que os seus conceitos básicos ainda são válidos atualmente (SCONUL, 2011). Este modelo define o âmago das habilidades e competências, e as atitudes e comportamentos da literacia digital no desenvolvimento de uma maior educação (SCONUL, 2011). Estes pilares são os seguintes: Identificação, isto é, ser-se capaz de identificar a necessidade pessoal por informação; Alcançar, através do acesso de conhecimento corrente e identificação de falhas; Planear, isto é, conseguir contruir estratégias para localizar informação; Agrupar, ou seja, localizar e

aceder dados e informação necessária; Avaliar, através da revisão, comparação e avaliação da informação no processo de pesquisa; Gerir, organizando eticamente a informação; e Apresentar, aplicando o conhecimento adquirido, expondo resultados de pesquisa, sintetizando informação para se criar conhecimento e, por fim, disseminando em diversas maneiras (SCONUL, 2011).

Segundo a *Chartered Institute of Library and Information Professionals* (CILIP), a LI é caracterizada como a habilidade de pensar criticamente e balancear julgamentos sobre qualquer informação que se encontre e use (Landøy et al., 2020). O mesmo grupo aponta que a LI capacita o indivíduo em obter e expressar visões informadas, sendo o seu papel principal o reforço da democracia e o compromisso cívico (Landøy et al., 2020). Para a CILIP, os *media*, também, têm um papel fundamental na medida em que são um importante pré-requisito para fomentar um acesso igualitário à informação e conhecimento, através de uma promoção independente, livre e plural (Landøy et al., 2020).

Enquanto um dos grandes problemas da *literacia digital* é a falta de formação, o conceito de *literacia informacional* tem como problema a superficialidade e uso instrumental das tecnologias (Ramos & Faria, 2012). Ora, a LI apresenta, segundo os autores Ramos e Faria (2012), várias dimensões que a descrevem como conceito, sendo elas: *competências investigativas; pensamento estratégico; pensamento crítico; pensamento criativo; resolução de problemas*. Estas dimensões podem ser desenvolvidas em três determinados contextos, como: a família, sendo o primeiro agente social do indivíduo, onde são inculcados valores que podem ou não acompanhar o indivíduo durante a sua vida; a escola, onde a criança começa a desenvolver capacidades emocionais e cognitivas através do convívio com outras crianças e, até mesmo, durante as aulas; a biblioteca, sendo um local de grande influência literária, fazendo com que o indivíduo pratique, use, e desenvolva a sua *literacia informacional* (Ramos e Faria, 2012).

A *literacia informacional* corresponde a uma visão sobre a informação como sendo uma ferramenta para atuar perante o mundo, dando uma escolha mais correta sobre uma multiplicidade de questões que testam o conhecimento atual (Jones-Jang et al., 2021). Por outras palavras, este conceito pode ser definido como um esquema

intelectual para compreender, encontrar, avaliar e usar a informação (Jones-Jang et al., 2021). Contudo, o termo *literacia informacional* pode ser, por vezes, confundido por *instrução bibliotecária*, limitando o seu verdadeiro significado que vai muito para além do próprio, ou seja, o sentido lato do termo vai ao encontro de um conjunto de esforços entre bibliotecários, especialistas de *media*, tecnologistas e educadores na criação de um conjunto de elementos complementares, sendo eles a "*media literacy", "digital literacy", "news literacy"* e "*critical thinking"* (Head et al., 2020).

De acordo com Head et al. (2020, p.8):

> "*Taken together, information literacy is an integrated set of skills, knowledge, practices, and dispositions that prepares students to discover, interpret, and create information ethically while gaining a critical understanding of how information systems interact to produce and circulate news, information, and knowledge"* (Head et al., 2020).

2.1.3. O Fosso Digital

O conceito de "*digital divide",* ou *fosso digital*, foi desenvolvido nos anos 90, no sentido de descrever a discrepância crescente quanto ao acesso e às competências do uso de tecnologias de informação (Kyriakidou et al., 2011). Numa visão geral, o *fosso digital* permanece evidente em todos os países, principalmente devido a desvantagens sociais e pelas poucas infraestruturas digitais, podendo levar a um impacto negativo em questões económicas ou até mesmo sociais (Kyriakidou et al., 2011). Para Debb et al. (2020), o *fosso digital* tende a ser um problema com mais evidência a nível geracional, isto é, os indivíduos mais novos são cada vez mais os detentores de conhecimento sobre o uso das tecnologias e, por outro lado, os mais velhos com menor conhecimento. Os indivíduos mais novos são considerados como *nativos digitais*, isto é, que nasceram num mundo tecnológico e os indivíduos mais velhos, sendo denominados de *imigrantes digitais*, são indivíduos que tiveram de se adaptar ao mundo tecnológico (Debb et al., 2020). Porém, a idade não explica por completo a literacia digital do indivíduo, nem o fosso digital. A experiência no uso de tecnologias digitais tende a ser mais essencial do que a idade do indivíduo. Outras dinâmicas como as atitudes do indivíduo, o acesso à

tecnologia, proficiência e razões de uso, também, são essenciais para se entender o comportamento do fosso digital na sociedade (Debb et al., 2020).

Para além das dinâmicas supramencionadas, a sociedade motiva o crescimento do fosso digital através das tendências digitais geradas pela mesma. Estas tendências são, geralmente, explicadas pelo que a sociedade prefere quanto às tecnologias (Kianpour et al., 2019). O indivíduo, porém, dependendo dos recursos que detém, acompanha ou não a evolução das tendências sociais no ramo tecnológico, acabando, por vezes por não acompanhar e, assim, fazer parte do *fosso digital.* Este caso apresenta alguma complexidade teórica, visto que o comportamento do indivíduo no mundo digital pode partir do grupo social em que o indivíduo está inserido como, também, pode partir do interesse do próprio (Kianpour et al., 2019).

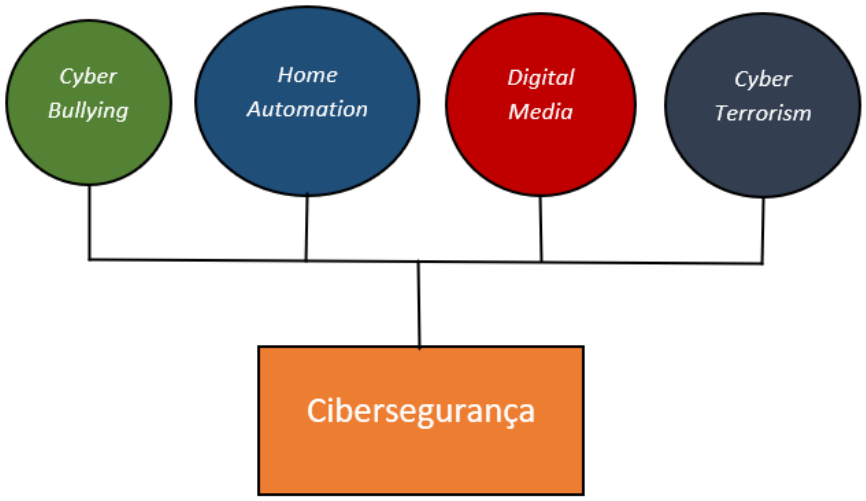
2.3. A Cibersegurança

O termo *cibersegurança* (CS) está intrinsecamente relacionado com a segurança do indivíduo no mundo digital, ou seja, corresponde às diversas práticas e comportamentos ligados à monitorização da atividade e segurança dos dados (Correia et al., 2016). Deste modo pode-se designar CS como sendo uma organização e coleção de recursos, métodos e disposições usadas para proteger o mundo digital de ocorrências que possam comprometer direitos de propriedade (Craigen et al., 2014).

Deste modo, existe uma panóplia de cenários que podem comprometer o bom funcionamento da CS, sendo maior parte deles ligados a ameaças a utilizadores do ciberespaço e ou organizações que estejam ligadas ao mesmo (von Solms e van Niekerk, 2013). O primeiro cenário diz respeito ao *cyber bullying* que é um conceito ligado à sociedade moderna, sendo resultado da tecnologia como ferramenta de comportamentos desviantes, isto é, comportamentos que possam dar um impacto negativo aos utilizadores do ciberespaço (von Solms e van Niekerk, 2013). O *cyber bullying*, segundo um largo consenso de literatura é definido como uma envolvência intencional, cruel e comportamentos repetitivos através de redes digitais, afetando a saúde mental e bem estar das vítimas deste (Rosa et al., 2019).

Segundo os autores von Solms e van Niekerk (2013), ainda são apontados mais três cenários que podem comprometer o bom funcionamento da cibersegurança, sendo eles: a *home automation* ou *automação de lares*, isto é, como resultado do avanço tecnológico em matéria eletrónica, como por exemplo os sistemas de segurança integrada de casas, sistemas de aquecimento de água, frigoríficos, televisões e outros eletrodomésticos que possam ter uma gestão de sistemas web, têm como consequência um aumento do risco de alguém poder obter informações de forma não autorizada, podendo causar danos nesses sistemas; o *digital media* ou *media digital*, ou seja, sistemas que sejam relacionados com a partilha de informação ou da industria de entretenimento, envolvendo partilha de filmes ilegais, música e outros tipos de media digital, podendo ser meios que possam afetar, não só a confidencialidade e integridade do conteúdo partilhado como, também, o bem estar financeiro dos detentores dos direitos desses conteúdos; por fim, o cenário do *cyber terrorismo* ou ciberterrorismo, podendo ser descrito como um ato de terrorismo através do ciberespaço capaz de comprometer ativos e sistemas de redes (físicas ou virtuais) de um país, tendo um efeito debilitante na segurança, segurança económica nacional ou segurança e saúde pública.

Figura 4: Cenários de comprometimento à cibersegurança.



2.3.1. O Comportamento ciberseguro

A experiência do indivíduo do Mundo digital pode facilmente ser alterada por causa de certas variáveis de personalidade do próprio. Segundo Whitty et al. (2015), existem indivíduos convictos de que certos acontecimentos dependem do comportamento gerado por alguém e, por outro lado, existem indivíduos que acreditam que esses acontecimentos não dependem das suas ações ou comportamentos e assim acabam por praticar comportamentos de risco na Internet. Nesta linha de pensamento, poder-se-á associar uma variável de personalidade, chamada de *impulsividade*. Este conceito está intrinsecamente relacionado com o desejo espontâneo de agir sem reflexão sobre a ação, isto é, sem se consciencializar das consequências, sendo elas positivas ou não (Aivazpour, 2019). Exemplo deste acontecimento é o facto de um indivíduo ser motivado a abrir um anúncio de forma impulsiva, pois surgiu-lhe curiosidade por ser algo que se identificava. A *impulsividade* pode ser distinguida sob duas formas: a impulsividade funcional e a impulsividade disfuncional. A primeira refere-se à fraca capacidade de processar informação em determinadas circunstâncias, enquanto que a segundo refere-se ao desejo no empenho numa determinada tarefa (Aivazpour, 2019).

Porém, ao serem aplicados comportamentos de risco neste meio, eis que os indivíduos têm uma *experiência de ciberataque*. Portanto, a experiência tida por um indivíduo de um ciberataque, sendo ele provocado por um ou vários indivíduos, com o intuito de violar o sistema de informação pessoal do próprio, pode determinar a alteração do seu comportamento em relação à sua segurança digital (Kianpour et al., 2019). Contudo, tem existido um elevado número de pessoas que se descuidam no que toca à importância que deve ser dada aos comportamentos adequados de cibersegurança, nem mesmo com o desenrolar de campanhas educacionais impostas pelo governo (Whitty et al., 2015).

2.3.2. *Malware*

Um *malware* é designado como sendo um *software* malicioso com o intuito de interromper o funcionamento normal de um dispositivo eletrónico (Quesinberry, 2016). Este software apresenta diversas categorias de ameaças, bem como diferentes

intensidades de ameaça. O *malware* mais conhecido é o Vírus, cujo é caracterizado por infetar programas no computador com código viroso, podendo ser associado roubo de dados, fornecimento de controlo do computador a hackers, e exibição de mensagens incomodativas (Quesinberry, 2016). Isto tudo possível através do acesso de anexos infetados em e-mails, dispositivos de armazenamento portáteis como uma *pen* USB ou o download de ficheiros de música pirateada (Quesinberry, 2016). Outro *malware* bastante comum é o Adware, que é caracterizado como sendo um software usado em publicidades que ocorrem durante a utilização da Internet. Este tipo de publicidade maliciosas contém um código de rastreamento de informação do indivíduo, deixando o computador lento com o download de vários anúncios, através de websites ou aplicações (Quesinberry, 2016).

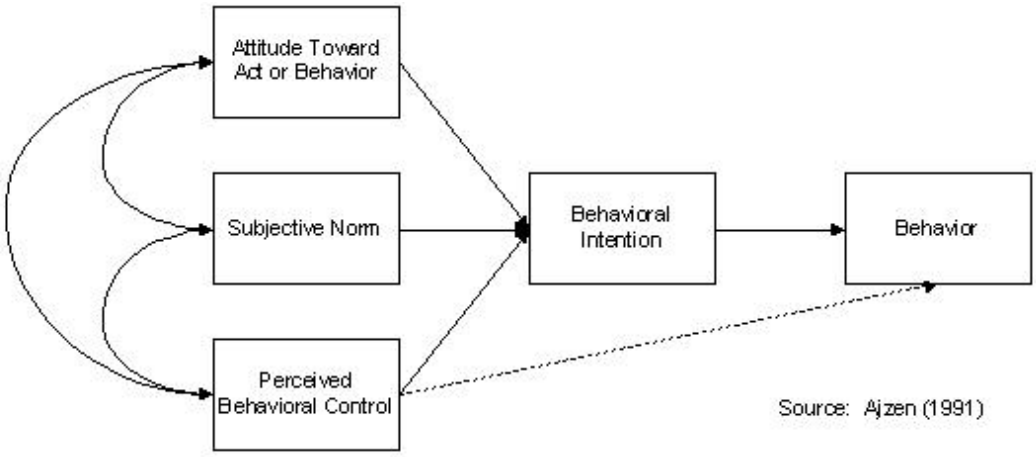
3. Modelo Conceptual de Análise

A revisão de literatura teve como base conteúdos científicos, os quais foram sustentados por diversas bases teóricas relacionadas com várias áreas científicas, como a área da Ciência da Informação e dos Sistemas de Informação, os quais sustentam o modelo teórico que será proposto no capítulo seguinte

3.1. Base Teórica

Este estudo tem como base teórica a *Theory of planned behavior* (TPB), ou Teoria do comportamento planeado, visto que o objetivo é determinar fatores que influenciam ou implicam o comportamento ciberseguro das pessoas. Esta teoria foi desenvolvida por Ajzen, em 1991, não só na área dos sistemas de informação como na área da psicologia social, com o fim de compreender como o comportamento individual é conduzido por intenções, isto é, atitudes individuais, normas subjetivas em torno da performance do indivíduo, e a perceção individual sobre o comportamento que pode ser aplicado (Ajzen, 1991). O modelo desenvolvido por este autor é ilustrado da seguinte forma:

Figura 5: Theory of Planned Behavior



3.2. Dimensões de Análise e Modelo

3.2.1. Dimensões de Análise

Tendo em conta a ideia teórica do modelo supramencionado, decidiu-se utilizar outras bases teóricas e, também, determinados construtos escolhidos de forma particular, com a ideia de analisar esses mesmos construtos à variável dependente deste

estudo, o *comportamento ciberseguro* (CC). Os construtos de seguida mencionados, foram escolhidos de forma específica em vários modelos teóricos, uns já idealizados e outros hipotetizados:

- ***Literacia Digital*** (LD) (Dodel & Mesch, 2018);
- ***Locus of Control*** (LC) (Howard, 2018);
- ***Technology Awareness*** (TA) (Dinev et al., 2009);
- ***Cyber-attack Experiences*** (CAE) (Kianpour et al., 2019);
- ***Self-efficacy*** (SE) (Hwang & Kuo, 2015);
- ***Impulsivity*** (I) (Whitty et al., 2015);
- ***Knowledge of Cybersecurity*** (KC) (Whitty et al., 2015).

A escolha destes construtos foi pensada de forma a dar uma complementação ao conceito de comportamento ciberseguro, tendo sido escolhidos não só pela força explicativa apresentada nos contextos científicos onde foram utilizados como, também, por serem construtos com uma forte relação com os modelos do comportamento informacional de Wilson (1997) e do comportamento planeado (TPB).

3.2.1.1. Literacia Digital

A *Literacia Digital* (LD) refere-se à capacidade que um indivíduo tem em usar o meio digital, seja para realizar tarefas pessoais, laborais ou académicas, ler e interpretar conteúdos *media*, ou gerir e aplicar novos conhecimentos no contexto digital (Dodel & Mesch, 2018).

Hipótese 1: A Literacia Digital está positivamente relacionada com o comportamento ciberseguro.

3.2.1.2. Locus of Control

O termo *Locus of Control* (LC) é uma variável de personalidade dos indivíduos, a qual está intimamente ligado ao controlo que é dado sobre o indivíduo em determinadas circunstâncias (Howard, 2018). O mesmo está relacionado com as atitudes que os indivíduos têm num ambiente cibernético, podendo haver indivíduos

com níveis elevados de *LC* e os indivíduos com baixos níveis de *LC* (Howard, 2018). Neste sentido o LC poderá estar relacionado com o comportamento ciberseguro.

Hipótese 2: O Locus of control está positivamente relacionado com o comportamento ciberseguro.

3.2.1.3. Self-efficacy

O conceito de *Self-efficacy* (SE), ou *autoeficácia*, está relacionado com a capacidade que as pessoas têm de usar a Internet para coletar e organizar informações e produzir resultados por si só (Hwang e Kuo, 2015). Por exemplo, um indivíduo com um nível de SE elevado, tende a obter melhores informações em contextos *online* do que um indivíduo que tenha um nível de SE mais baixo (Hwang e Kuo, 2015). A SE, segundo Hwang e Kuo (2015) , tem um efeito positivo, nos indivíduo, na intenção de aprenderem a desvendar soluções quanto à sua utilização da Internet. Contudo, pressupõe-se que a SE está relacionada com um comportamento ciberseguro.

Hipótese 3: A autoeficácia está positivamente relacionada com o comportamento ciberseguro.

3.2.1.4. Impulsivity

O termo *Impulsivity* (I), ou *impulsividade*, é uma variável de personalidade, cuja pode ser caraterizada por um tipo de comportamento aplicado pelo indivíduo de pouca premeditação ou reflexão sobre os resultados das suas ações (Whitty et al., 2015). Esta variável foi medida por Whitty et al. (2015) numa escala chamada *UPPS-R Impulsivity Scale* durante o seu trabalho empírico. Ora, como o nível de *impulsividade* dos indivíduos estavam relacionados com a partilha de *keywords* (palavras-chave), pressupõe-se, portanto, que a *impulsividade* esteja relacionada com um comportamento ciberseguro.

Hipótese 4: A Impulsividade está negativamente relacionada com o comportamento ciberseguro.

3.2.1.5. Technology Awareness

O termo *Technology Awareness* (TA), refere-se à motivação que os indivíduos têm em adquirir conhecimento sobre tecnologias de informação e respetivas estratégias para a sua utilização (Dinev et al., 2009). Por exemplo, quando um indivíduo nota que existe um problema como um ataque malicioso no seu dispositivo, o mesmo tem a intenção de agir (Dinev et al., 2009), isto é, o indivíduo tem um comportamento de intenção para resolver o problema em questão (Dinev et al., 2007). Portanto, neste caso, presume-se que a TA estará relacionada com um comportamento ciberseguro.

Hipótese 5: A Technology Awareness está positivamente relacionada com o comportamento ciberseguro.

3.2.1.6. Cyber-attack Experiences

O termo *Cyber-attack Experiences* (CAE), ou *experiência de ciberataques,* é basicamente uma experiência de uma tentativa maliciosa e propositada, por parte de um ou vários indivíduos, em violar o sistema de informações digitais do padecente (Kianpour et al., 2019). Portanto, pressupõe-se que quando se é vítima de um ciberataque, implica a que se aplique um comportamento ciberseguro.

Hipótese 6: A experiência de ciberataques está positivamente à aplicação de um comportamento ciberseguro.

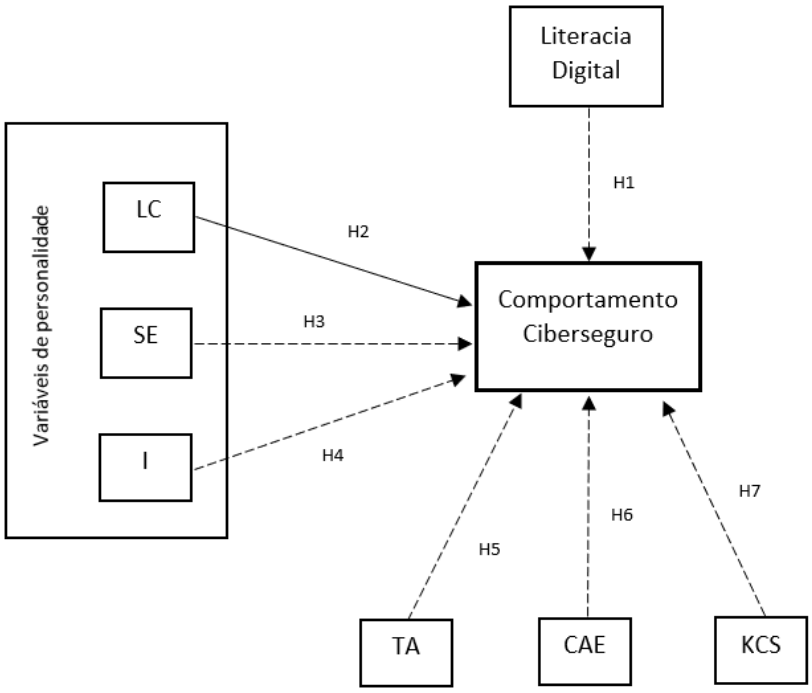
3.2.1.7. Knowledge of Cyber Security

O Knowledge of Cyber Security (KCS), ou o *conhecimento de cibersegurança*, implica que um indivíduo esteja ciente da sua segurança online, havendo de facto diferenças entre indivíduos sobre esta matéria, isto é, os especialistas e os não especialistas quanto a comportamentos básicos de segurança, como por exemplo instalar e/ou atualizar um *software* (Whitty et al., 2015). Neste sentido, pressupõe-se que um indivíduo que tenha *conhecimento de cibersegurança*, aplique um comportamento ciberseguro.

Hipótese 7: O conhecimento de cibersegurança está positivamente relacionado com o comportamento ciberseguro.

3.2.2. Modelo Conceptual de Hipóteses

Figura 6: Proposta de Modelo Conceptual.
Fonte: Elaboração própria



O modelo desenvolvido acima tem como intuito em apresentar uma nova base teórica que possa explicar a relação do comportamento humano e a sua ação na *Word Wide Web*. Acrescenta-se ainda que as hipóteses H1, H3, H4, H5, H6 e H7, são hipóteses que não tem comprovação teórica, porém vão ao encontro de conceitos semelhantes ao que se pretende estudar. Neste sentido, apela-se a que, futuramente, se possa testar as mesmas e, desta forma, contribuir para um novo modelo teórico no estudo dos comportamentos ciberseguros.

Todos os construtos que estão apresentados neste modelo foram conceptualizados na seguinte forma: Nome original do construto; Definição dada pelo autor desenvolvedor do construto; Definição crítica; Os operacionalizadores usados para sustentar o construto; A hipótese gerada do construto perante a variável dependente (CC). Ver tabela abaixo.

Tabela 2: Conceptualização dos construtos. Fonte: Elaboração própria.

Construct	Definição (autor)	Definição (crítica)	Itens/Operacionalizadores	Hipóteses	Referência
Digital Literacy	"(…) as Internet skills, e-skills and certain types of digital literacy, (…) are a broad concept describing different sets or types of abilities related to the knowledge of the digital world. (…) the basic abilities required to operate digital systems and also the skills needed to understand and use the Internet's online content."	Digital literacy refers to an individual's ability to use the digital medium, to perform necessary tasks, such as reading and interpreting media content to manage and apply new knowledge in digital context.	"Respondents were asked to rate their abilities such as knowing how to install antivirus software, update it, set up mobile security, use an anonymous browser, delete browsing the history and cookies and identify executable files." / "Respondents rated their ability to perform such tasks on a 5-point Likert scale ranging from 'unable to perform the task/operation at all' to 'very capable of performing the task'."	"Users who report having security skills are more likely to engage in antivirus behaviors." Security skills -> antivirus behaviors	Dodel e Mesch (2018)
Locus of control	"Locus of control is a personality variable that explains why some people attribute control of events to themselves or to outside forces"	Locus of control is a variable of individuals personality in which those assigned to give control over themselves in certain circumstances.	"Those who attribute control of events to themselves are higher on internal locus of control, and those who attribute control of events to others or the environment are high on external locus of control."	"Locus of control will be positively related to cybersecurity behaviors."	Howard (2018)
Technology Awareness	"(…) defined technology awareness as the user's following, being interest in, and knowledgeable about technological issues, problems, and techniques to solve them."	The technology awareness refers to the motivation that individuals have in acquiring knowledge about information technologies and the respective strategies in their use.	"A person who is aware of a problem and who comes from an individualist society will more readily form an attitude towards the issue. On contrary, a person from a collectivist society would be more careful in forming his or her personal attitudes".	"(…) awareness of the spyware problem alone could motivate a computer user to form the intention to act."	Dinev et al. (2009) Dinev et al. (2007)
Cyber Attack Experiences	"A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another	Experience of a malicious and purposeful attempt by and	"(…) 59% of respondents confirm that their organizations experienced a data breach caused by one of their third parties. 42% of respondents say they had such a data breach in	"Cyber-attack experience increases the perceived cybersecurity value".	Kianpour et al. (2019)

	individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network.	individual (s) to breach the personal information system.	the past 12 months. Additionally, 22% of respondents do not know if they had a third-party data breach in the past 12 months."		
Self-Efficacy ***PMT (Protection Motivation Theory)***	"(…) refers to individuals' belief in their capability to use the Internet to organize information to produce given results; (…) personal judgement of one's ability to use the Internet.".	Capacity of individuals to use the Internet to collect and organize information and, ultimately, produce results. For example, an individual with a high level of self-efficacy tends to obtain better information in online contexts.	"(…) high self-efficacy students apply more high-level learning strategies, such as elaborative strategies and critical thinking. The students in their study who provided elaborated feedback also had higher self-efficacy than those who did not."	"Internet self-efficacy has a positive effect on the usage intention of adopting the web-based problem-solving learning approach."	Hwang e Kuo (2015)
Impulsivity	"Individuals who score high on impulsivity questionnaires are individuals who tend to act on a whim, displaying behaviors characterized by little forethought or consideration of the consequences of their actions."	Impulsivity is a behavior that is characterized by little premeditation or reflection of the results of actions.	"Impulsivity was measured using the UPPS-R Impulsivity Scale." "(…) a direct scale to measure impulsivity (e.g., Barratt Impulsivity Scale (BIS) – see Patton et al (1995) for discussion of scale), or, a scale that is closely related to impulsivity" (Aivazpour, 2019).	"Individuals who score high on measures of impulsivity are more likely to share passwords compared with those who score low on impulsivity"	Whitty et al. (2015)
Knowledge of Cyber Security	"(…) general population are typically aware of online security, there are still clear distinctions between experts and nonexperts regarding basic security behaviors, such as patching and updating software."	Knowledge of basic cybersecurity behaviors.	Knowledge of cyber security was measured using a single question. Participants were asked to rate their knowledge about cyber security issues on a 5-point Likert scale.	"Individuals who believe they are more knowledgeable about cybersecurity issues are more likely to share passwords compared with those who believe they are less knowledgeable."	Whitty et al. (2015)

4. Metodologia

Para se produzir ciência é preciso que se determine uma metodologia, ou seja, é necessário instituir certos e determinados procedimentos que deem seguimento à investigação, sendo eles através de um ou vários métodos (Fernandes, 2020). Segundo Maria Fernandes (2020), é através do método pré-estabelecido que é possível alcançar-se o objetivo delineado para a investigação, e que é através desse método que são definidas regras, critérios, técnicas e instrumentos a aplicar no estudo, organizando, desta forma, todo o conhecimento criado.

Para este estudo foi delineada uma metodologia que pudesse dar sustentação à abordagem teórica apresentada nos capítulos anteriores e desenvolver um método que definisse o objetivo deste estudo, organizando e aplicando toda a matéria idealizada para produzir conhecimento sobre a temática da presente investigação. Neste caso, será importante utilizar uma abordagem metodológica mista como forma a poder serem produzidos resultados complementados e robustos.

Esta abordagem metodológica é baseada em métodos quantitativos e métodos qualitativos, sendo que o método qualitativo ou investigação qualitativa pode ser descrita como sendo uma ciência interpretativa, não só com o objetivo natural do comportamento humano, mas também por disposições subjetivas, isto é, atitudes, motivações e situações recolhidas através de material empírico, através de entrevistas, grupos focais, etc. (Aspers & Corte, 2019), e, por outro lado, o método quantitativo é compreendido como sendo um método com resultados de dados observacionais, organizando fatores do comportamento humano ou não-humano através das perceções e experiências dos indivíduos, tendo como base o levantamento de dados de campo, laboratório ou levantamentos naturais (Gilad, 2021).

4.1. Metodologia quantitativa

Neste quadro metodológico foi criado um inquérito em que se pudesse explorar as dinâmicas “literacia digital” e “cibersegurança” dos inquiridos, sendo quase como uma autoavaliação da proficiência digital de cada inquirido. (Apêndice A)

Este inquérito teve como base o Quadro Europeu de Referência para a Competência Digital (DigComp), um documento de trabalho em desenvolvimento no Laboratório de Conteúdos Digitais (LCD) do CIDTFF, Departamento de Educação e Psicologia da Universidade de Aveiro, sendo este uma junção da *DIGICOMP: A Framework for Developing and Understanding Digitial Competence in Europe* e do *DigComp 2.0: The Digital Competence Framework for Citizens*, como forma de se poder fazer um estudo empírico teoricamente estruturado e holístico. Ao longo do inquérito são abordadas cinco áreas, sendo elas: Informação; Comunicação; Criação de Conteúdo; Segurança; e Resolução de problemas.

A área Informação está relacionada com a literacia de informação e dados, ou seja, com a articulação, localização, recuperação, ajuizamento, armazenamento, e gestão da informação por parte do utilizador (LCD, 2017). São abordados nesta área, três temas relacionados entre si, sendo eles: a Navegação, Procura e Filtragem da Informação; Avaliação da Informação; e o Armazenamento e Recuperação da Informação. Na área da Comunicação aborda-se a questão da comunicação em ambientes digitais, bem como a partilha, interação e participação no meio digital (LCD, 2017). A Criação de conteúdo refere-se à criação e edição de conteúdo digital, bem como a aplicação de direitos de autor e licenças de conteúdo (LCD, 2017). Na área da Segurança, aborda-se questões relacionadas com a proteção dos dispositivos, conteúdo e dados pessoais, bem como a própria saúde física e psicológica do utilizador e bem-estar cibersocial (LCD, 2017). Por fim, na área da Resolução de problemas trata-se particularmente na identificação e resolução de problemas em ambientes digitais, seja a resolução de problemas técnicos com o dispositivo ou na identificação de respostas tecnológicas no meio digital (LCD, 2017).

Em cada área são então apresentadas questões às quais o inquirido auto aliava-se através de uma escala de concordância avaliada de 1 a 5, sendo 1 “Discordo totalmente”, 2 “Tendo a discordar”, 3 “Indiferente”, 4 “Tendo a concordar” e 5 “Concordo totalmente”, qual corresponderia melhor à sua situação. Todas as questões utilizadas foram retiradas do quadro supramencionado, sendo mais concretamente os exemplos sugeridos no mesmo. Foram escolhidos os exemplos que melhor correspondessem ao interesse deste estudo e que, posteriormente, foram colocados na

primeira pessoa do singular, passando a ser uma espécie de autoavaliação para o inquirido.

À parte das áreas centrais, no início do inquérito, foram colocadas algumas questões introdutórias, nomeadamente se o inquirido possui computador pessoal, telemóvel pessoal, fácil acesso à internet, e para que motivos utiliza a internet. No final do inquérito são, então, apresentadas questões que possam conhecer as características pessoais do indivíduo que, mantendo sempre a garantia de anonimato, se de questões como o género, idade, habilitações literárias e, por fim, a ilha de residência do mesmo. Importa referir que estes dois últimos serão fatores de interesse, bem como a habilitações literárias, pois serão fatores com alguma importância na interpretação de resultados.

4.2. Análise de resultados quantitativos

Este inquérito tinha como objetivo atingir, pelo menos, 200 respostas, sendo uma amostra "bola de neve", à qual foi feita uma análise por conveniência. Numa duração de dois meses, tendo sido entre o mês de maio de 2021 e o mês de julho do mesmo ano, obteve-se um resultado total de 202 respostas, havendo respostas de todas as ilhas, participando várias entidades desde o público em geral, da função pública e, especialmente, da Secretaria Regional da Cultura, Ciência e Transição Digital dos Açores. Apesar da questão final do inquérito, relativa à ilha de residência dos participantes, ter sido colocada de forma opcional, obteve-se 200 respostas, tendo havido duas pessoas que não indicaram qual a sua ilha de residência. Neste sentido e num modo descritivo, houve apenas uma resposta da ilha do Corvo, três da ilha das Flores, dez da ilha do Faial, quatro da ilha Graciosa, oito da ilha do Pico, duas da ilha Santa Maria, cento e trinta e duas da ilha de São Jorge, dezanove da ilha de São Miguel e, por fim, vinte e uma da ilha Terceira. Neste modo, houve uma maior quantidade de respostas por parte de residentes da ilha de São Jorge e menor por parte da ilha do Corvo.

Tabela 3: Nº de respostas por cada ilha dos Açores.

Ilha de Residência	Nº de respostas	%
Corvo	1	0,50
Flores	3	1,50
Faial	10	5
Graciosa	4	2
Pico	8	4
Santa Maria	2	1
São Jorge	132	66
São Miguel	19	9,50
Terceira	21	10,50
TOTAL	**200**	**100**

Das 202 respostas, importa referir duas variáveis, sendo elas o Género e as Habilitações Literárias dos respondentes. Quanto ao género, responderam 111 pessoas do género feminino e 91 pessoas do género masculino, não tendo respondido qualquer pessoa de outro género. Houve, portanto, uma maior representatividade do público feminino ao estudo.

No que toca às habilitações literárias dos participantes, importa referir que, para questionar a mesma, foi utlizado a tabela de habilitações literárias feita pela Direção-Geral da Administração e do Emprego Público, fazendo-se uma pequena alteração, ao invés de "Habilitação Ignorada" utilizou-se "Sem Habilitações". Descrevendo os resultados obtidos desta questão houve 1 pessoa que detém 4 anos de escolaridade (1º ciclo do ensino básico), 4 com 6 anos de escolaridade (2º ciclo do ensino básico), 18 com o 9º ano (3º ciclo do ensino básico), 13 com o 11º ano de escolaridade, 58 com o 12º ano (ensino secundário), 16 com Curso Tecnológico/Profissional/Outro (Nível III - Nível de qualificação da formação (c/equivalência ao ensino secundário), 5 com Bacharelato,

56 com Licenciatura, 9 com Pós-Graduação, 17 com Mestrado, 2 com Doutoramento, e 3 com Curso de Especialização Tecnológica. Não respondeu qualquer pessoa que tivesse menos de 4 anos de escolaridade ou que não tivessem habilitações. Deste modo, cerca de 56,4% dos respondentes possuem o 12º ano de escolaridade (28,70) e/ou licenciatura (27,70).

Tabela 4: Nº de respostas e Habilitações literárias.

Habilitações Literárias	**Nº de respostas**	**%**
Menos de 4 anos de escolaridade	0	0
4 anos de escolaridade (1º ciclo do ensino básico)	1	0,50
6 anos de escolaridade (2º ciclo do ensino básico)	4	2
9º ano (3º ciclo do ensino básico)	18	8,90
11º ano	13	6,40
12º ano (ensino secundário)	58	28,70
Curso Tecnológico/Profissional/Outro (Nível III)	16	7,90
Bacharelato	5	2,50
Licenciatura	56	27,70
Pós-Graduação	9	4,50
Mestrado	17	8,40
Doutoramento	2	1
Curso de Especialização Tecnológica	3	1,50
Sem Habilitações	0	0
TOTAL	**202**	**100**

Passando para a análise às questões introdutórias do inquérito, houve alguns dados interessantes. Relativamente à questão "Tem computador pessoal?", 185 pessoas responderam que "Sim" e 17 pessoas responderam que "Não". Ora, neste sentido, as 17 pessoas que responderam que não tinham um computador pessoal, participaram ao inquérito ou com um computador de um familiar/amigo, ou um computador de algum estabelecimento, seja laboral ou académico. No que toca à questão "Tem telemóvel pessoal?", das 202 respostas, 200 pessoas responderam que "Sim", tinham um telemóvel pessoal enquanto as restantes 2 pessoas responderam que "Não", não possuíam um telemóvel pessoal. Quanto à questão "Consegue aceder

facilmente à internet?", 201 pessoas responderam que "Sim", enquanto apenas 1 pessoa respondeu não conseguir aceder facilmente à internet.

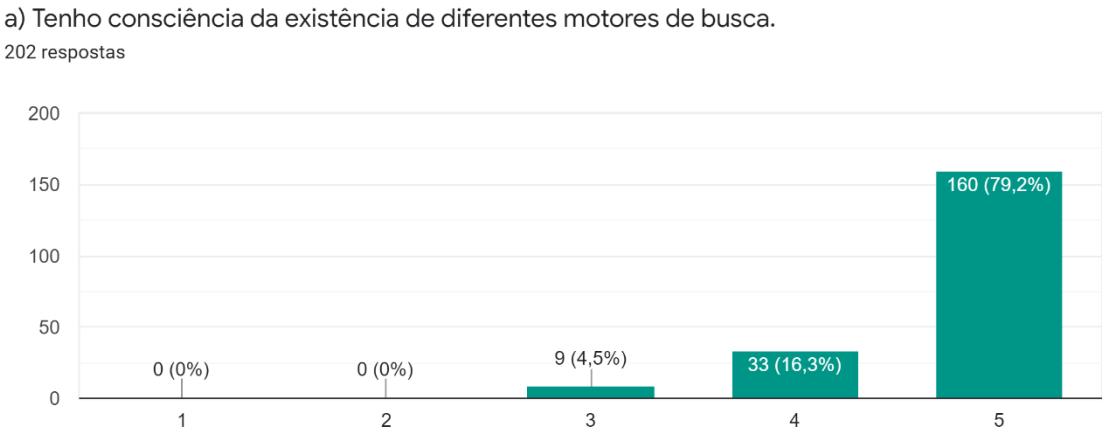
Sobre o acesso à internet foi questionado quais os motivos da utilização e acesso à internet, dando quatro opções de escolha sendo possível a escolha de mais do que uma. As opções foram: "Profissionais"; "Lazer"; "Académicos" e "Outros". Na última opção dava a liberdade do inquirido de dizer outros motivos de utilização da internet. Relativamente aos dados quantitativos a opção "Profissionais" foi selecionada por 163 pessoas, a opção "Lazer" foi selecionada por 184 pessoas, a opção "Académicos" por 58 pessoas e, por fim a opção "Outros" foi selecionada por 7 pessoas. Nota-se, portanto, que grande parte das pessoas utiliza a internet para motivos de lazer, podendo este motivo estar relacionado com a utilização de redes sociais, busca de informação, ou simplesmente ver filmes.

Dentro da opção "Outros", houve respostas interessantes levando a entender outros motivos específicos que levam as pessoas à utilização da internet, sendo eles: "Homebanking"; "Compras online"; "Cumprimento de obrigações (Finanças, Segurança Social)"; "Acesso a serviços (Fatura eletrónica)"; "Plataformas diversas (Gestão de seguros, contratos)"; "Formações não relacionadas com a profissão"; "Investigação de temas sobre áreas específicas"; "Jogar jogos e ver vídeos".

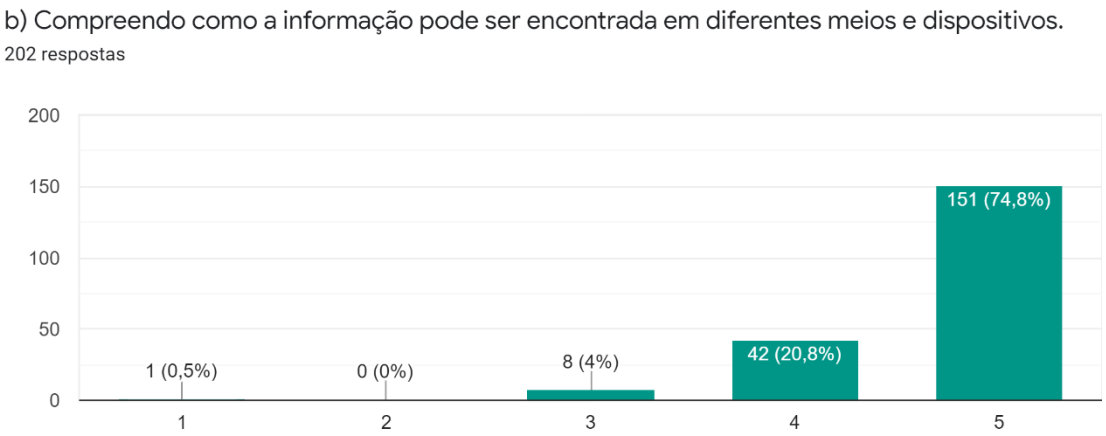
4.2.1. Informação

Dentro deste subcapítulo do inquérito, constatou-se vários resultados relativamente à capacidade de navegação, procura e filtragem da informação, avaliação da informação, e armazenamento e recuperação da informação dos açorianos. Primeiramente constata-se que 79.2% (160) dos inquiridos dizem ter consciência da existência de diferentes motores de busca na internet, e que 74.8% (151) compreendem como é que a informação pode ser encontrada em diferentes meios e dispositivos eletrónicos.

1 - Consciência da existência de diferentes motores de busca.

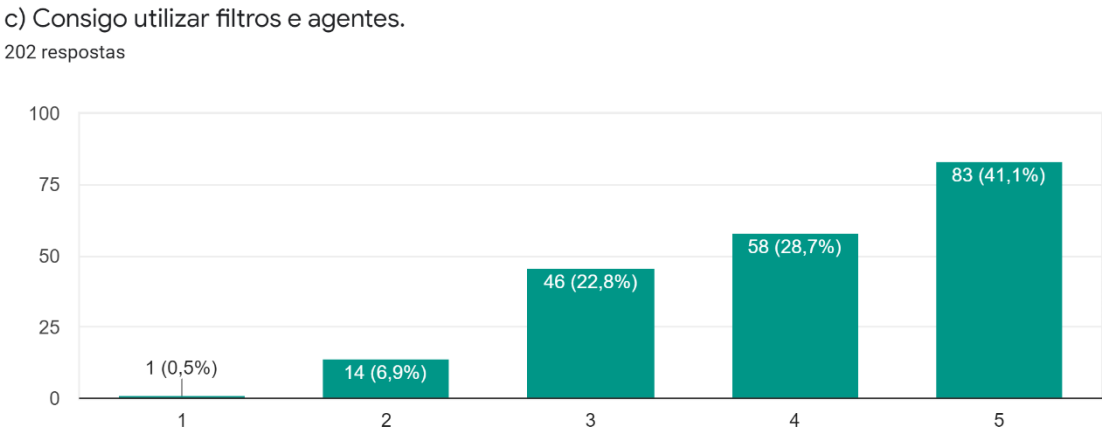


2 - Compreensão sobre como a informação pode ser encontrada.

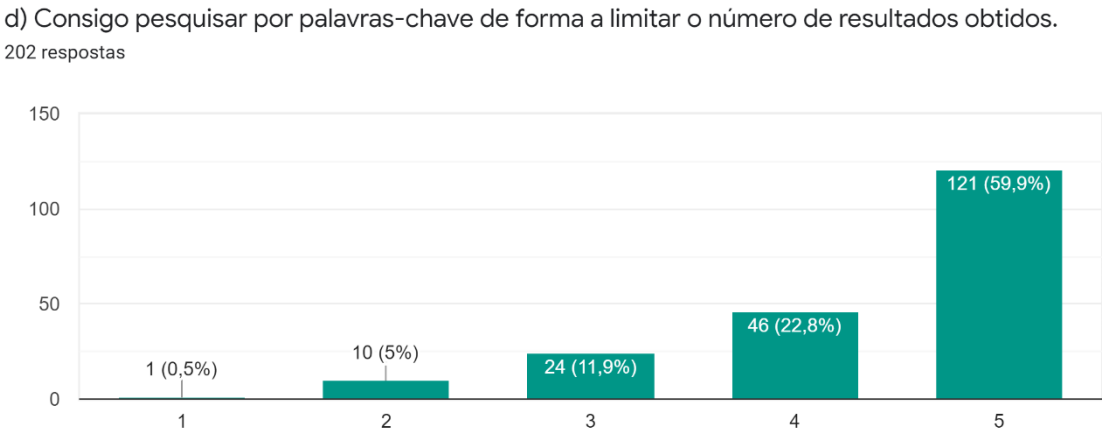


Todavia, os resultados relativos à filtração de informação são mais díspares, isto é, 41.1% (83) dos inquiridos diz conseguir utilizar filtros e agentes, 28.7% (58) tende a conseguir, 22.8% (46) diz não concordar nem discordar, 6.9% (14) tende a não conseguir e apenas 0.5% (1) não consegue de todo utilizar filtros e agentes. Por outro lado, 59.9% (121) dos inquiridos diz conseguir pesquisar informação por palavras-chave com o intuito de limitar o número de resultados a obter, 22.8% (46) tende a conseguir, 5% (10) não concorda nem discorda, e apenas 0.5% (1) não consegue pesquisar desta forma.

3 - Utilização de filtros e agentes de pesquisa.



4 - Precisão por palavras-chave.

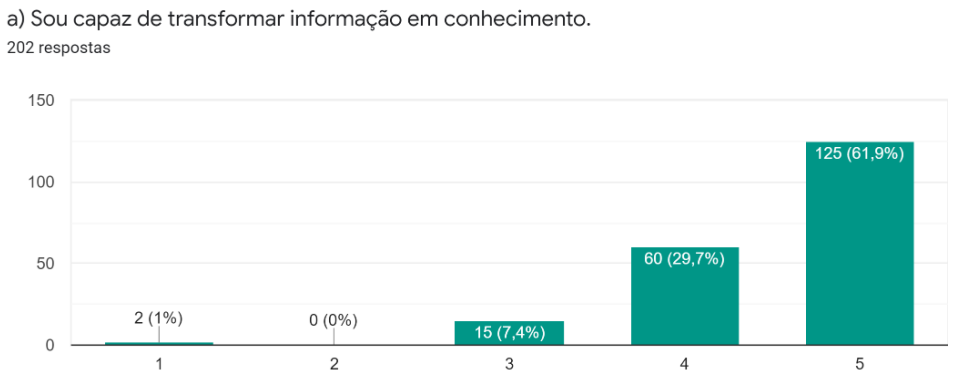


No que toca à capacidade dos açorianos em avaliar a informação que obtêm da internet geralmente, segundo os dados obtidos, tendem a serem bastante capazes de fazerem uma boa avaliação da mesma. Ora, 61.9% (125) dos inquiridos são capazes de transformar informação em conhecimento, sendo que apenas 1% (2) dos inquiridos não é capaz de fazer esse processo. Dentro dessa informação, 55.4% (112) é capaz de compreender a fiabilidade de diferentes fontes de informação, 54% (109) dos inquiridos consegue ajuizar a validade do conteúdo encontrado na internet e nos média, 53% (107) diz conseguir comparar, contrastar e integrar informação de diferentes fontes, e 60.4% (122) consegue reconhecer que nem toda a informação pode ser encontrada na internet. Contudo, houveram resultados que ficaram abaixo dos 50% apresentando uma

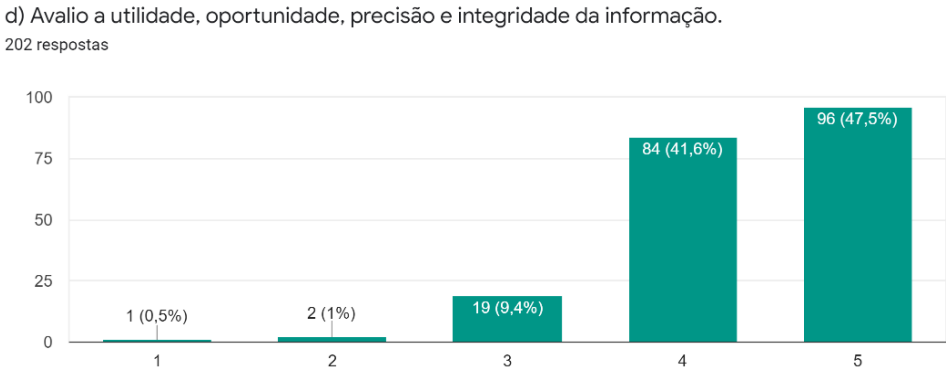
disparidade de respostas a duas questões, sendo elas a capacidade de avaliar a utilidade, oportunidade, precisão e integridade da informação encontrada (cerca de 47.5% (96) dos inquiridos concordam totalmente que o fazem, 41.6% (84) tendem a concordar, 9.4% (19) não concordam nem discordam, 1% (2) tende a discordar, e 0.5% (1) discorda totalmente que avalia a informação dessa forma), e a capacidade crítica sobre a informação encontrada (cerca de 45.5% (92) dos inquiridos concordem totalmente que são críticas sobre a informação que encontram, 36.6% (74) tendem a concordar, 15.3% (31) não concordam nem discordam, 1.5% (3) tendem a discordar, e 1% (2) discorda totalmente ser crítico(a) sobre a informação que encontram).

Perante estes dados conclui-se que, a maioria dos inquiridos, são capazes de avaliar a informação transformando-a em conhecimento e, também, que a informação pode ser obtida para além da internet, porém grande parte dos inquiridos não concorda totalmente quanto à avaliação feita sobre a utilidade, oportunidade, precisão e integridade da informação, e criticidade da informação encontrada, acabando por dar a entender que a informação obtida por grande parte dos inquiridos é utilizada conforme é obtida.

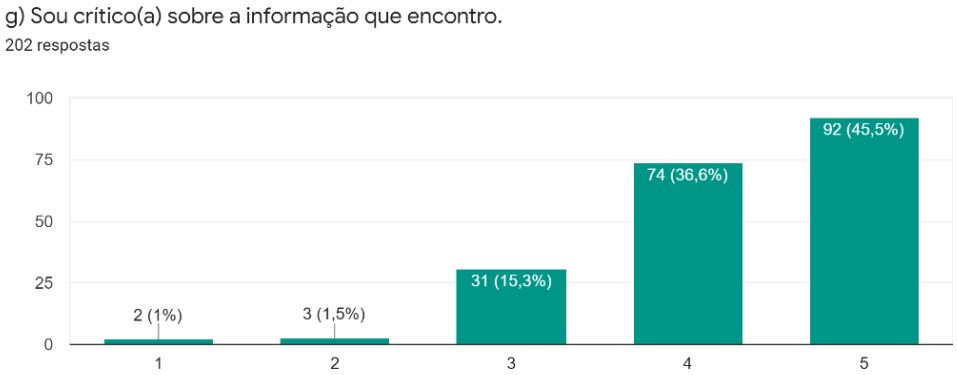
5 - Capacidade de transformação da informação em conhecimento.



6 - Utilidade, oportunidade, precisão e integridade da informação.

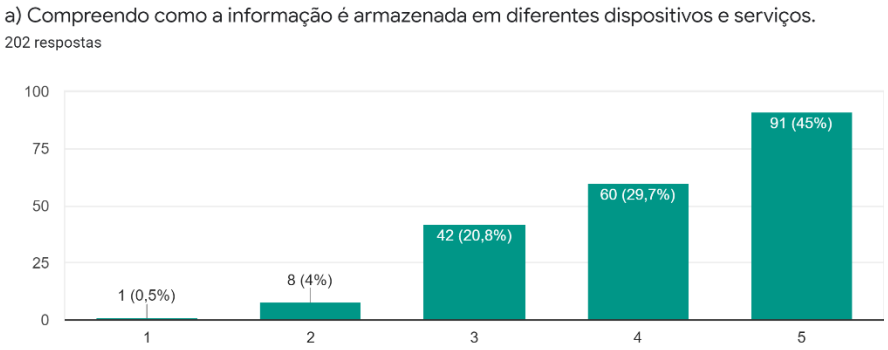


7 - Criticidade sobre a informação.

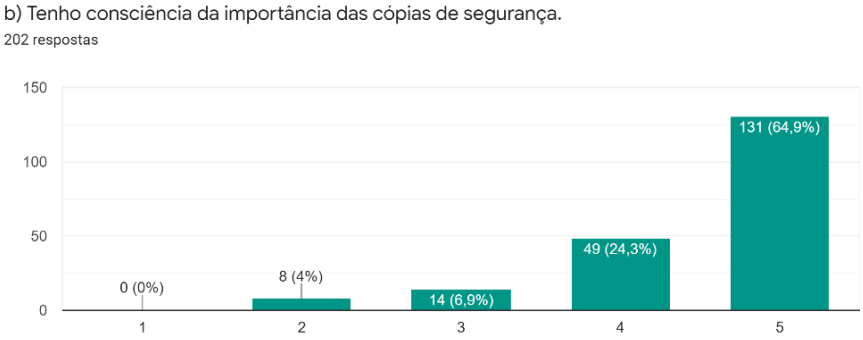


Falando concretamente sobre o tema do armazenamento e recuperação da informação, 55% dos inquiridos não compreende totalmente como é que a informação é armazenada em diferentes dispositivos e serviços (sendo 29.7% (60) dos inquiridos tendem a concordar que compreendem o processo, 20.8% (42) não concordam nem discordam, 4% (8) tendem a discordar e 0.5% (1) discorda totalmente), contudo têm a maior parte tem consciência da importância das cópias de segurança de dados dos seus dispositivos (64.9%) e das consequências que resultam do armazenamento de conteúdo de forma pública ou privada (55.9%).

8 - Compreensão de como a informação é armazenada em diferentes meios.



9 - Importância das cópias de segurança.



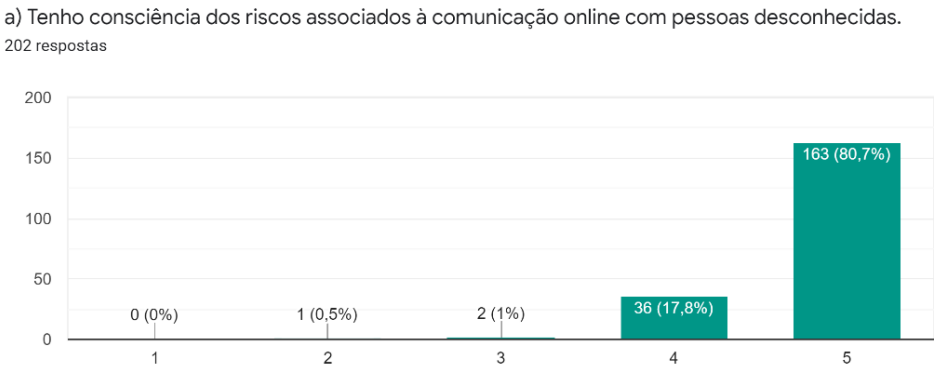
4.2.2. Comunicação

Neste tema, registaram-se alguns resultados interessantes no sentido em que os inquiridos demonstraram que não tomam atitudes nem habilidades totalmente seguras e sensatas na comunicação digital. Quanto à consciência dos riscos associados à comunicação online com pessoas desconhecidas, 80.7% (163) dos inquiridos responderam ter total consciência desses riscos e ainda 66.3% (134) responderam ter total consciência dos riscos e benefícios que estejam relacionados com a exposição da identidade online. Porém, quanto à atitude e capacidade de proteção online, houve respostas mais diversificadas sendo que, quanto à atitude seguras e sensata em atividades digitais, 59.4% (120) responderam não ter uma total concordância sobre esse assunto (45.5% (92) responderam que tendem a concordar, 10.9% (22) não concordam nem discordam, e 3% (6) tendem a discordar). Quanto à capacidade de se protegerem de ameaças online, também houve resultados mais diversificados, havendo 64.4% (134) dos inquiridos a responderem não concordar na totalidade quanto ao assunto (38.1%

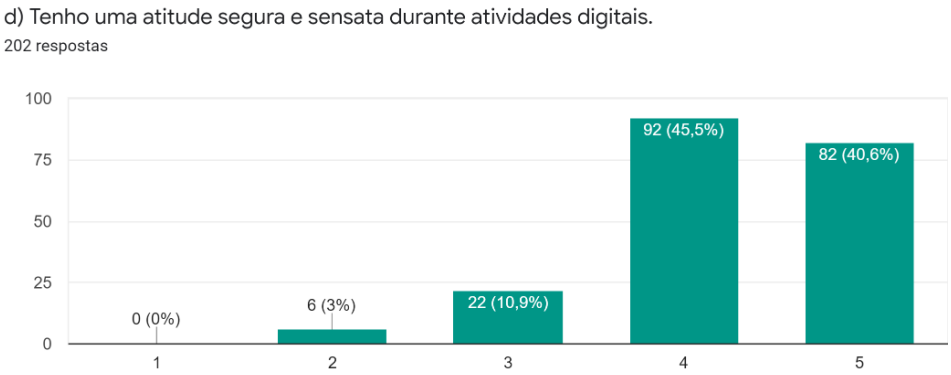
(77) responderam que tendem a concordar, 22.8% (46) não concordam nem discordam, 4.5% (9) tendem a discordar, e 1% (2) discordam totalmente quanto a possuírem capacidade de se protegerem a si e aos outros de ameaças online). De acrescentar que, também, grande parte dos inquiridos (54.5%) diz não conseguir totalmente banir ou denunciar abusar e ameaças na internet (33.2% (67) tendem a concordar que conseguem, 17.8% (36) não concordam nem discordam, 2.5% (5) tendem a discordar, e 1% (2) discordam totalmente dessa capacidade).

Portanto, perante os resultados obtidos, os inquiridos têm consciência que existem riscos que estão associados à comunicação online com pessoas desconhecidas e exposição das suas identidades online, porém não têm a total capacidade ou habilidade necessária para reverter ameaças ou abusos online e capacidade total de se protegerem a si e aos outros online.

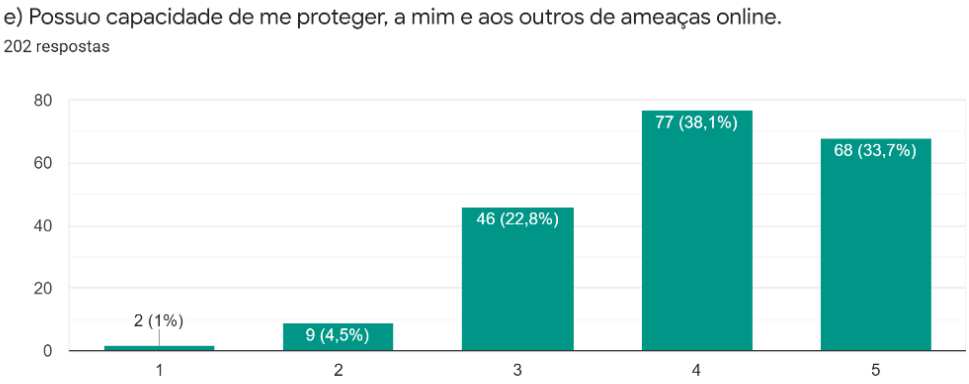
10 - Riscos associados à comunicação online com pessoas desconhecidas.



11 - Atitude segura e sensata em atividades digitais.



12 - Capacidade de proteção de ameaças online.

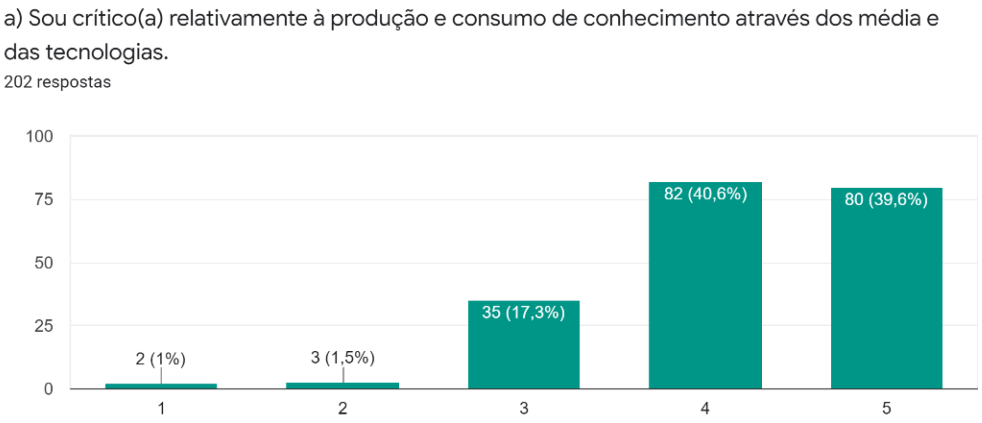


4.2.3. Criação de conteúdos

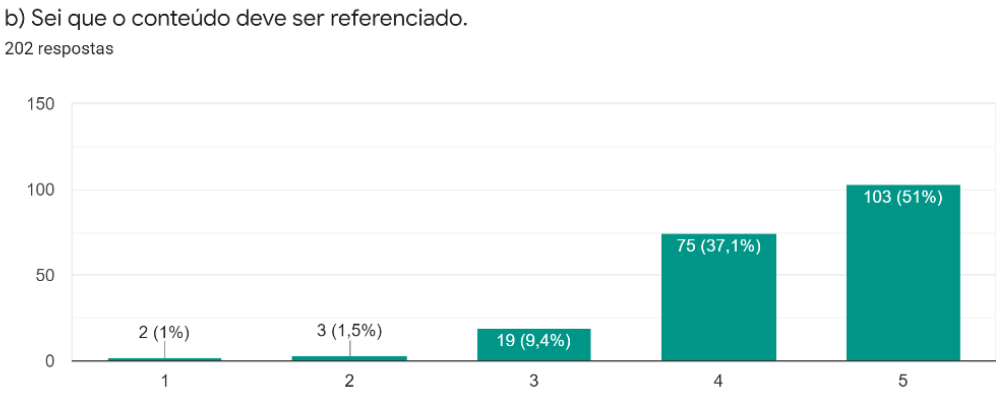
A criação de conteúdos tem por base a produção de conhecimento através das tecnologias e redes sociais, pondo desta forma à prova as competências, habilidades e atitudes dos utilizadores nesta temática. Dada a dificuldade anteriormente referida sobre a transformação da informação em conhecimento por parte dos inquiridos, constatou-se que, quanto à criticidade sobre a produção e consumo através dos média e das tecnologias, grande parte dos inquiridos são concorda totalmente sobre esta atitude (60%), sendo 40.6% (82) tendem a concordar, 17.3% (35) não concordam nem discordam, 1.5% (3) tendem a discordar, e 1% (2) discordam totalmente. Porém, mais de 50% dos inquiridos sabe que o conteúdo que é produzido deve ser referenciado (51%) e que compreendem as regras dos direitos de autor e licenças (52.5%).

Resumidamente, ao produzirem conteúdo nas redes sociais e tecnologias, os inquiridos não são totalmente críticos sobre o mesmo conteúdo, limitando-se geralmente a produzir o que já foi produzido, contudo têm consciência que esse mesmo conteúdo deve ser referenciado, respeitando as regras dos direitos de autor e licença.

13 - Criticidade sobre a produção e consumo de conhecimento online.



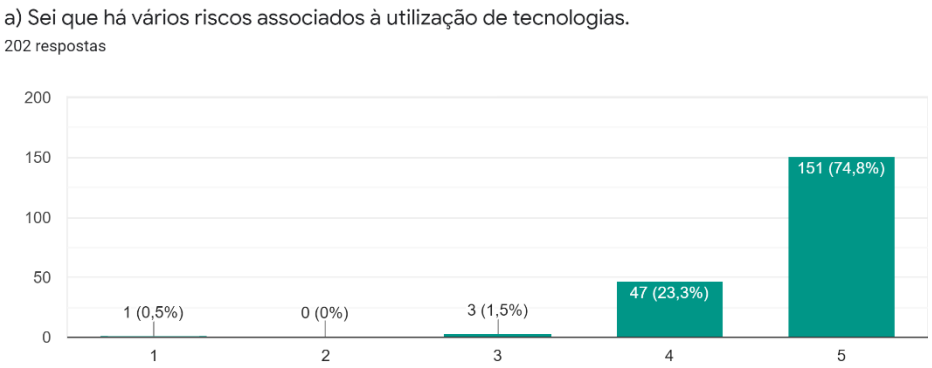
14 - Consciência sobre a referenciação de conteúdo.



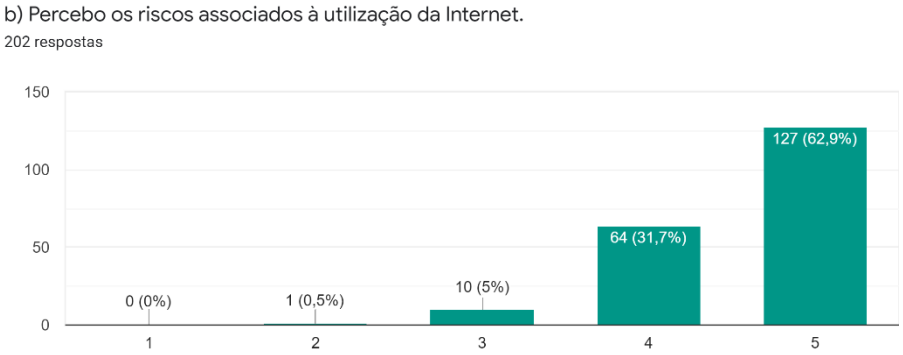
4.2.4. Segurança

Pondo à prova uma reflexão sobre como os inquiridos pensam ser as suas competências, habilidades e atitudes acerca de temas como a proteção pessoal, proteção de dados, identidade digital, medidas de segurança digital e a utilização sustentável e segura das tecnologias e ambiente digital, constatou-se alguns aferimentos interessantes sobre a forma como é percecionada a segurança digital pelos mesmos. Segundo os dados obtidos e falando concretamente sobre os riscos associados ao uso das tecnologias e da internet, maior parte dos inquiridos (74.8%) respondeu que sabem da existência de vários riscos associados à utilização de tecnologias, tal como também maior parte dos mesmos (62.9%) responderam que sabem dos riscos associados à utilização da internet.

15 - Consciência sobre os riscos associados à utilização de tecnologias.

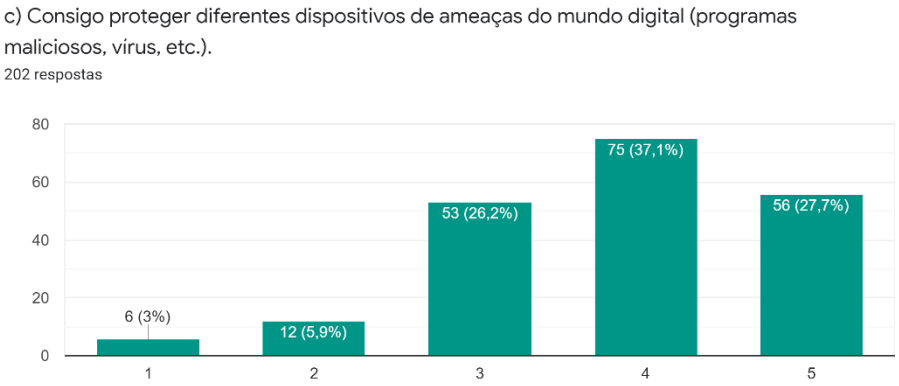


16 - Consciência sobre os riscos associados à utilização da internet.



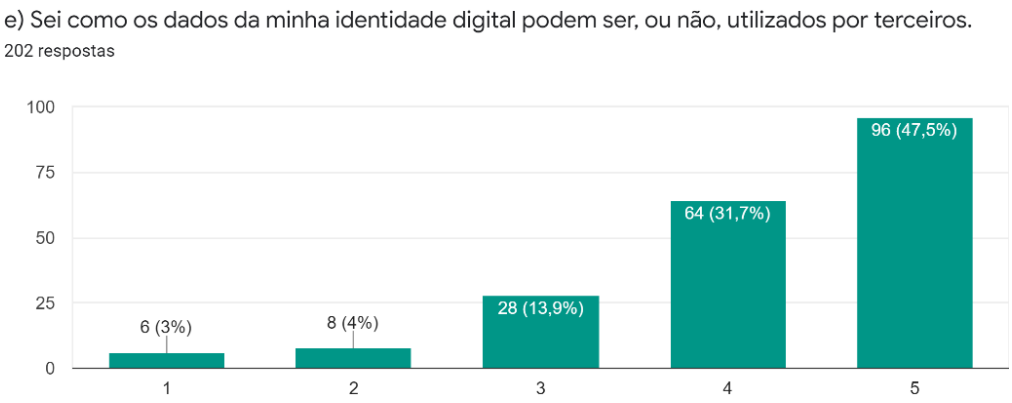
Tendo em conta que maior parte dos inquiridos têm a consciência sobre os riscos associados à utilização das tecnologias e da internet, é percetível que, perante os dados obtidos, a capacidade dos mesmos se protegerem de diferentes dispositivos de ameaças digitais, tais como por exemplo, programas maliciosos, vírus ou tentativas de fraude, não é consideravelmente a melhor, sendo que apenas 27.7% (56) dos inquiridos respondeu que concordavam totalmente em conseguirem proteger-se e 72.2% (146) não responderam que concordaram totalmente, isto é, 37.1% (75) tendem a concordar, 26.2% (53) não concordam nem discordam, 5.9% (12) tendem a discordar e 3% (6) discordam totalmente que conseguem proteger-se de tais ameaças.

17 - Capacidade de proteger diferentes dispositivos de ameaças do mundo digital.

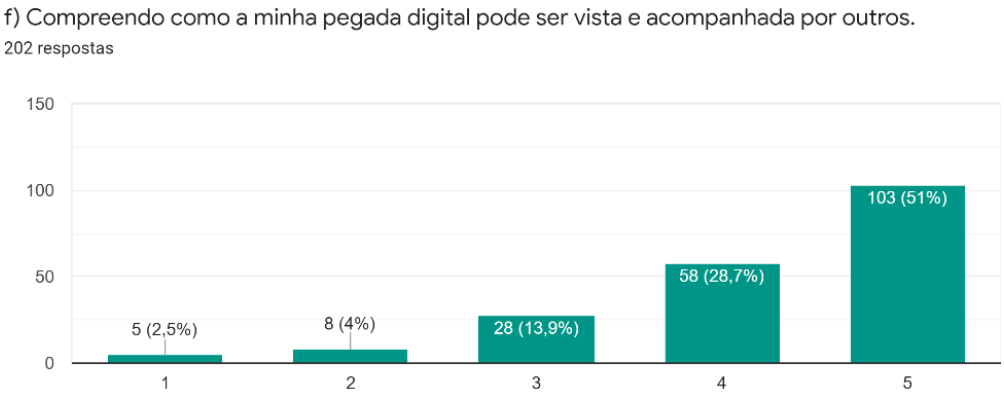


Sobre a exposição dos dados pessoais no meio digital, 52.6% dos inquiridos não sabe totalmente como é que os dados das suas identidades digitais podem, ou não ser, utilizados por terceiros. Porém, 51% dos inquiridos respondeu que compreendiam totalmente como as suas pegadas digitais podem ser vistas e acompanhadas por outros. Neste caso, havendo alguma complexidade linguística, pode ter havido alguma confusão de conceitos como o de "identidade digital" e o de "pegada digital", sendo que houveram resultados um pouco contraditórios nestas duas questões, contemplando a mesma finalidade, contudo com perceções diferentes entre os inquiridos.

18 - Consciência sobre como a identidade digital pode, ou não, ser utilizada por terceiros.

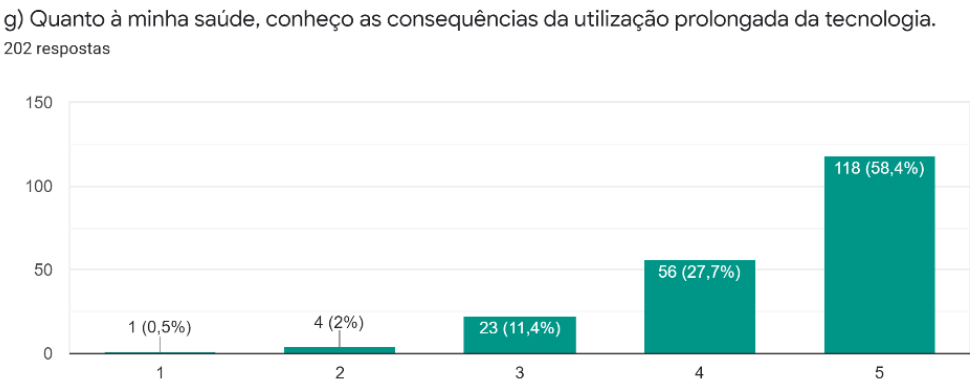


19 - Compreensão sobre como a pegada digital pode ser vista e acompanhada por outros.

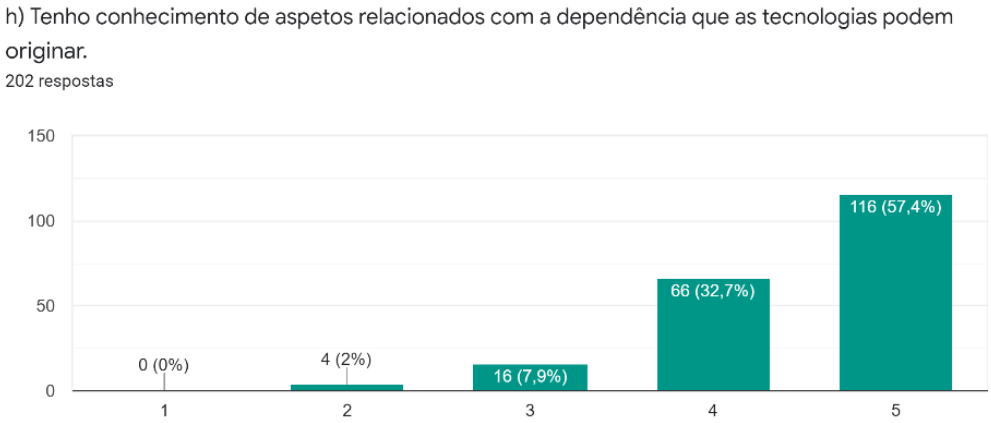


Quanto à saúde dos utilizadores aquando do uso das tecnologias e consequente usufruto da internet, a maior parte dos inquiridos (58.4%) respondeu que concordavam totalmente conhecer as consequências da utilização prolongadas das tecnologias. Neste sentido, também, maior parte dos inquiridos (57.4%) respondeu que concordavam totalmente terem conhecimento dos vários aspetos que estão relacionados com a dependência que as tecnologias podem causar.

20 - Conhecimento sobre as consequências da utilização da tecnologia.



21 - Conhecimento sobre a dependência que as tecnologias originam.

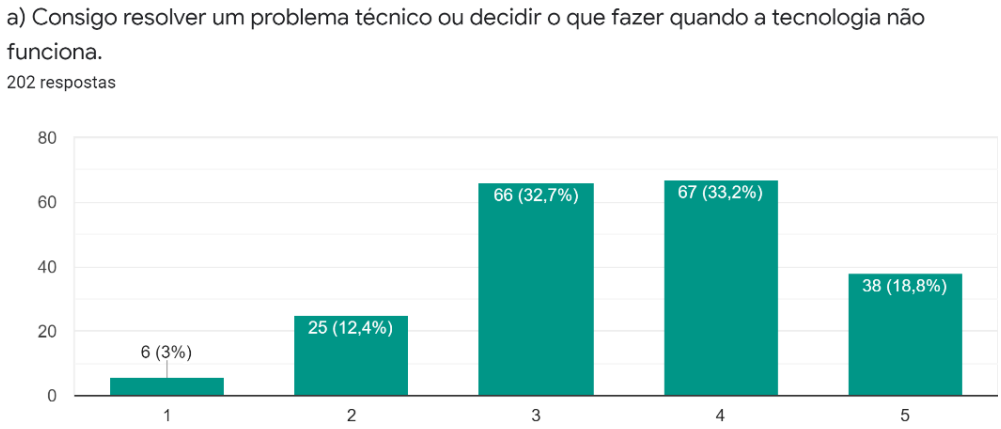


4.2.5. Resolução de problemas

Este tema tinha como intuito tentar entender as competências, habilidades e atitudes dos inquiridos na resolução de problemas técnicos, aprendizagem e adaptação a novas tecnologias digitais emergentes.

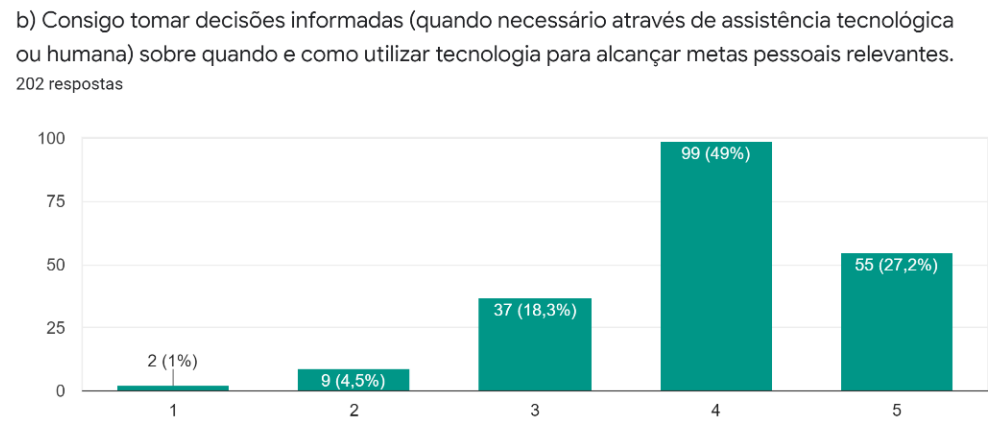
Sobre a capacidade dos inquiridos em resolverem um problema técnico ou, pelo menos, saber o que fazer quando a tecnologia utilizada deixa de funcionar, 81.3% dos inquiridos responderam não concordar na totalidade, sendo que 32.2% (67) responderam que tendem a concordar que conseguem (não conseguindo na totalidade), 32.7% (66) não concordam nem discordam, 12.4% (25) tendem a discordar, e 3% (6) discordam totalmente. Por outro lado, apenas 18.8% (38) responderam que concordavam totalmente sobre conseguirem resolver um problema técnico ou decidir o que fazer.

22 - Resolução de um problema técnico.



Quanto à tomada de decisões informadas sobre quando e como utilizar uma tecnologia para alcançar metas pessoais relevantes, maior parte dos inquiridos (72.8%) não concordam na totalidade em conseguirem dar seguimento a esse processo, sendo que 49% (99) tendem a concordar (não concordando na totalidade), 18.3% (37) não concordam nem discordam, 4.5% (9) tendem a discordar, e 1% (2) discordam totalmente. Todavia, apenas 27.2% (55) inquiridos concordam totalmente em conseguirem tomar tais decisões.

23 - Tomada de decisões informadas sobre a utilização de tecnologia para diversos fins



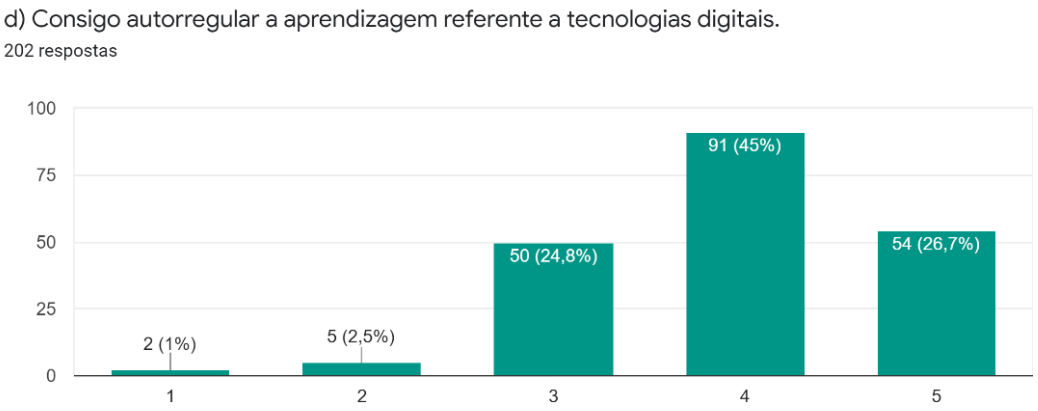
Passando para a vertente da pedagogia técnico-digital, constatou-se que maior parte dos inquiridos (73.3%) não consegue, na totalidade, autorregular a aprendizagem

referente a tecnologias digitais, sendo que 45% (91) dos inquiridos tende a concordar (não concordando na totalidade), 24.8% (50) não concorda nem discorda, 2.5% (5) tende a discordar, e 1% (2) discorda totalmente. Contudo, apenas 26.7% (54) dos inquiridos diz concordar totalmente sobre esta questão.

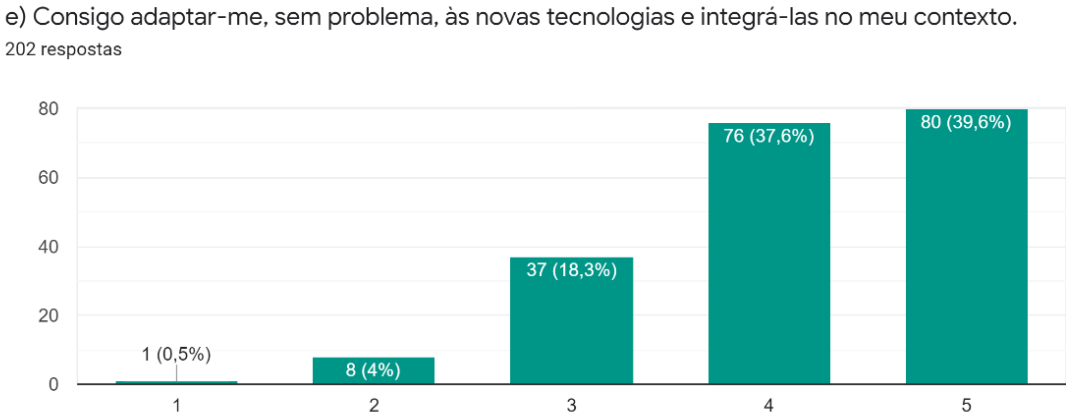
Quanto à adaptação a novas tecnologias e integração das mesmas em variados contextos do quotidiano, novamente, maior parte dos inquiridos (60.4%) não concordar totalmente sobre este processo, sendo que 37.6% (76) dos inquiridos tende a concordar, 18.3% (37) não concorda nem discorda, 4% (8) tende a discordar, e 0.5% (1) discorda totalmente. Por outro lado, somente 39.6% (80) dos inquiridos diz concordar totalmente sobre conseguirem adaptar e integrar as novas tecnologias.

Ainda sobre as novas tecnologias e mais concretamente sobre uma atitude positiva de aprendizagem das tecnologias digitais emergentes, cerca de 45% (91) dos inquiridos respondeu que concordava totalmente em ter este tipo de atitude, pelo que 55% (111) não concorda totalmente em possuírem este tipo de atitude, sendo que 41.6% (84) dos inquiridos responderam que tendiam a concordar (não concordando na totalidade), 10.9% (22) não concordam nem discordam, 2% (4) tendem a discordar, e 0.5% (1) discorda totalmente que possui ou mantém este tipo de atitude.

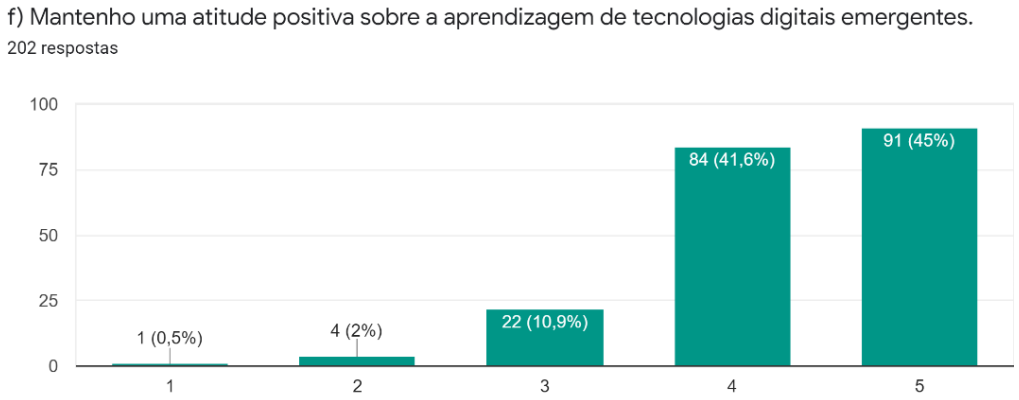
24 - Aprendizagem referente a tecnologias digitais



25 - Adaptação às novas tecnologias e integração das mesmas no quotidiano



26 - Atitude positiva sobre a aprendizagem de tecnologias emergentes



4.2.6. Nível de proficiência digital

Esta questão teve dois intuitos dentro do inquérito, sendo que o primeiro foi como uma parte estratégica introduzida no meio do inquérito de modo que o mesmo não se tornasse tão monótono e para aferir a atenção e veracidade dos inquiridos, e o segundo tinha como intenção fazer com que os inquiridos refletissem sobre as suas competências digitais e que se autoavaliassem através de três níveis de proficiência digital: Básico, Intermédio, Avançado.

Neste sentido, maior parte dos inquiridos autoavaliou-se como sendo utilizadores de proficiência digital "Intermédio", respondendo a esta opção 63.9% (129) dos inquiridos. Contudo, constatou-se que para além do esperado, que era haver uma

maior parte de respostas que apontassem o nível “Intermédio”, houve mais pessoas que se autoavaliaram como sendo utilizadores de proficiência digital de nível “Avançado” do que de nível “Básico”, sendo que 21.3% (43) responderam “Avançado” e 14.9% (30) responderam possuir o nível “Básico”.

27 - Nível de proficiência digital

Portanto, pode-se constatar que perante a amostra de 202 respostas, existe uma minoria de utilizadores de nível de proficiência digital básica e, por outro lado existe uma parte bastante considerável de utilizadores se autoavaliam de grau intermédio.

4.2.7. Observações

Durante a publicação do inquérito e após o fecho do mesmo, foram constatadas algumas observações por parte de alguns inquiridos e por parecer próprio. Estas observações foram retidas de forma crítica, sendo que não pôs em causa a validade do inquérito.

Abaixo encontra-se uma tabela onde são indicadas as observações e as possíveis correções caso o inquérito fosse realizado novamente.

Tabela 5: Observações sobre o inquérito metodológico

Observações	Possíveis correções
Algumas questões com um grau gramatical complexo, acabando por limitar o nível de compreensão por uma parte dos inquiridos.	Simplificação das questões para que todos os inquiridos possam entender o conteúdo da questão.
A última questão "Ilha de residência" foi colocada como questão opcional, tendo havido dois inquiridos que não responderam a essa questão.	Colocação da questão como obrigatória, de forma a obter o número de resultados exato para todas as questões.
A questão "Idade (apenas algarismos)" teve dois problemas: • O primeiro foi relativamente à palavra "algarismos" podendo ter havido alguma confusão com o significado da mesma, isto é, houve algumas respostas por extenso e não em algarismos. • O segundo é relativamente à própria colocação da questão, sendo que houve um excesso de algarismos que acabaram por dificultar a análise.	Colocar a questão em formato de intervalos de idades, facilitando a resposta ao inquirido e, também, na posterior análise da questão.
Falta de uma maior variedade de escolhas na questão "Para que motivos utiliza a internet?"	Colocar outras opções de escolha, de modo a obter resultados mais variados e concretos.

4.3. Metodologia Qualitativa (*Focus Group*)

Neste quadro metodológico foi pensada a execução de um *focus group* (FG) ou grupo focal, para que se pudesse obter informação mais detalhada sobre as temáticas abordadas neste estudo. Este método começou a ser desenvolvido por Robert King Merton, na década de 1940, como uma nova forma de recolha de dados para a produção de saber científico. Mais tarde, na década de 80, este método começou a desenvolver-se de forma intensa, tornando-se numa importante forma de pesquisa, sendo utilizada geralmente por cientistas sociais (Galego e Gomes, 2005).

O termo *focus group* é compreendido como uma discussão organizada em grupo, onde são exploradas uma série de problemáticas debatendo, refletindo e expondo perceções e experiências dos intervenientes (Kitzinger, 2005). É através desta metodologia que, através das perceções dos participantes, compreende-se o porquê e como as pessoas respondem às problemáticas de determinadas formas (O. Nyumba et al., 2018), proporcionando uma panóplia de visões e reações de cada participante do grupo (Galego e Gomes, 2005). Neste sentido, os resultados do método *focus group* são uma espécie de matéria-prima para a produção de conhecimento científico, procurando estabelecer um sentido e compreensão de fenómenos sociais complexos complementando, também, a recolha e análise de dados em determinados tipos de estudos (Galego e Gomes, 2005). Contudo e podendo haver uma preponderância mais sociológica, psicológica ou educativa, este tipo de estudo tem, também, como objetivo obter atitudes e objeções dos participantes do grupo relativamente a opiniões e sentimentos que possam contribuir para um novo conhecimento para os próprios participantes (havendo um processo de autoformação) e, também, para o investigador (Vieira e Vieira, 2007).

No que toca ao confronto de ideias, as questões que são colocadas pelo moderador (que neste caso foi o autor deste trabalho de investigação) e devem ter como objetivo a promoção de um debate entre os participantes (Vieira e Vieira, 2007). Durante o debate, o moderador não deve forçar a que os participantes deem respostas de concordância ou discordância, ou seja, essas dinâmicas de consensos ou concordância surgem mesmo sem que o moderador as denuncie, portanto evita-se formar o debate desta forma porque pode acontecer de forma natural entre os

participantes, mas sempre de forma controlada com o intuito de continuar com a ideia de debate e não de entrevista (Vieira e Vieira, 2007).

Segundo Ana Maria Vieira e Ricardo Vieira (2007), para que o grupo focal se torne viável é necessário selecionar participantes que assegurem uma espécie de "equilíbrio entre identidade e a diversidade de grupo" (Vieira & Vieira, 2007), seja por características comuns ou por algum projeto/situação de vida similares. Neste sentido, selecionou-se para este FG cinco pessoas, cujas características eram parecidas, porém houve a preocupação de terem algumas dissemelhanças de modo a haver uma pequena diversidade grupal para que houvesse algum confronto de ideias, fugindo à supramencionada dinâmica de consensos ou concordâncias.

Foi pedido a cada participante, particularmente, que assinassem uma declaração de aceitação do uso de imagem e voz para fins académicos, ao qual todos aceitaram e consentiram (Apêndice D). Entretanto, também, foi pedido a cada participante que preenchesse um pequeno questionário sociodemográfico no qual eram pedidos alguns dados respetivos aos respondentes, de modo a poder complementar e descrever as características de cada um para o debate e discussão do tema relativo a este estudo. Reforça-se que, para o preenchimento dos dois documentos supramencionados bem como na gravação do FG, foi garantido aos participantes o total anonimato dos mesmo aquando da transcrição dos dados.

Na descrição de dados, foi atribuída uma abreviatura a cada participante (por exemplo, Participante 1 = P.1, Participante 2 = P.2, Participante 3 = P.3, etc.), e na transcrição da videoconferência foram dados nomes fictícios a cada participante, de modo a respeitar o total anonimato dos mesmos e mesmas. Deste modo, foram selecionados cinco participantes que tivessem idades similares, porém com algumas características diferentes, respetivamente às habilitações literárias e profissão dos mesmos e mesmas. Foi também preocupação em conseguir ter um equilíbrio de géneros neste debate.

Tabela 6: Quadro Sociodemográfico (Focus Group)

Participantes	*Idade*	*Género*	*Hab. Literárias*	*Profissão*
P.1	24	Masculino	Curso Profissional	Operador fabril
P.2	24	Feminino	Mestrado	Geografa
P.3	27	Feminino	Ensino Secundário	Estudante
P.4	24	Masculino	Ensino Secundário	Desempregado
P.5	24	Feminino	Mestrado	Desempregada

Segundo a tabela acima apresentada é possível descrever que quatro dos participantes têm 24 anos de idade e uma tem 27 anos, ou seja, estão incluídos dentro da mesma faixa etária e de geração respetivamente evolução digital. Três participantes são do género feminino e dois são do género masculino.

Quanto às características dissemelhantes, podemos ver que, quanto às habilitações literárias, todos detém no mínimo o ensino secundário, havendo um participante que detém um curso profissional e dois participantes com o grau de Mestrado. No que toca à profissão, é possível constatar que dois dos cinco participantes estão empregados, sendo um operador fabril e outra exercendo funções de geógrafa, uma participante é estudante e os restantes dois participantes estão desempregados. Importa referir que a escolha dos participantes, também, foi tendo em conta a diversidade de conhecimentos adquiridos, ou seja, procurou-se pelo menos uma pessoa que tivesse conhecimentos na área da criminologia, que neste caso detém mestrado em Criminologia Forense, e outras de áreas distintas como: o participante (P.1) que é operador fabril que, segundo o questionário sociodemográfico, detém um curso profissional em Técnico de Produção Agrária; a participante (P.2) que exerce funções

como geógrafa, detém mestrado em Sistemas de Informação Geográficos e Ordenamento do Território; a participante (P.3) que é estudante na área nutricional; e por fim, o participante (P.4) que para além de estar desempregado, detém o curso de aviação (Pilotagem em aeronaves comerciais do tipo A320) mas que exerce funções como bombeiro voluntário. Esta diversidade de conhecimentos foi tida em conta para que houvesse um confronto de ideias que tentasse responder às questões lançadas em debate de forma diversificada e complementar.

Para a preparação do FG foi feito um Guião de Preparação para o *Focus Group* (Apêndice B) para que se pudesse organizar de forma estruturada todo o procedimento relativo ao mesmo. Neste Guião de Preparação constava todas as dinâmicas de preparação, desde a hora, número de participantes, guião (onde consta a apresentação, objetivos e questões) e um quadro sociodemográfico. Quanto ao procedimento do FG, foi pensado ser, primeiramente, presencialmente, porém e dadas as circunstâncias de pandemia como também a dificuldade em organizar um dia para que todos os participantes pudessem deslocar-se ao local definido. Desta forma, a alternativa foi ser concebido via videoconferência e assim conseguir fazer com que os participantes, estando no seu lar, pudessem comparecer e participar no FG. Foi feita uma pequena pesquisa sobre qual seria a melhor plataforma a utilizar, tendo sido pensada em primeira instância a plataforma Zoom, porém, como a mesma com mais de 3 participantes apenas disponibilizava de forma gratuita 45 minutos de videoconferência, então pensou-se numa alternativa, caso o debate prolongasse para além de 45 minutos. Neste sentido, utilizou-se a plataforma Webex, indo ao encontro das expetativas idealizadas para o debate, em que cada participante não precisaria instalar a plataforma nos seus dispositivos, clicando apenas no *link* enviado por e-mail.

O debate decorreu no dia 29 de setembro de 2021, pelas 21h, e teve uma duração de cerca 40 minutos em que todos os participantes tiveram a mesma oportunidade e tempo para discutirem, conforme foi informado aos mesmos de início.

4.4. Análise dos dados qualitativos

Ao dar início à videoconferência, foi feita uma breve apresentação tanto pessoal e do se iria suceder, dando a conhecer o conteúdo e os objetivos deste estudo, bem como o que se entende por grupo focal. No final desta fase introdutória os participantes foram questionados se se sentiam sensibilizados com o tema que iria ser-se discutido, tendo sido confirmado por todos/as. De seguida, numa forma de "quebra-gelo", foi pedido aos participantes que se apresentassem, dizendo apenas o primeiro nome, idade e outras informações por livre-arbítrio.

Uma observação notória durante as apresentações foi a vontade que alguns participantes tiveram em fazer relações com o tema geral do estudo com as suas áreas de conhecimento, bem como o interesse por aprender um pouco mais com este estudo, tanto pelo debate que iria decorrer como pela finalidade deste estudo.

Dadas as apresentações, foi colocada a primeira questão, sendo ela: "Quando é que receberam o vosso primeiro computador e como é que aprenderam o usar básico da máquina?". Esta questão tinha como intuito perceber quando é que os participantes tinham recebido o seu primeiro computador pessoal e, também, de que forma ou em que contexto é que começaram a utilizar o mesmo seja de que forma fosse. Na generalidade os participantes receberam o seu primeiro computador entre os 7 e os 14 anos de idade, sendo que usavam maior parte das vezes um computador escolar em contexto de escola para a aprendizagem de alguns conteúdos escolares, como por exemplo trabalhos para algumas disciplinas, ou aprendizagem de conteúdos correntes da disciplina TIC (Tecnologia da Informação e Comunicação). Para além do contexto escolar, a Participante 2 (P.2) referiu que usufruiu de pequenas formações durante o período de férias da escola, lecionadas por um Clube de Informática da localidade, onde se aprendia a redigir textos nos softwares Microsoft Word e Microsoft PowerPoint. Referiu ainda que aprendeu a criar um e-mail e outras formas de comunicação online.

"Eu recebi o meu primeiro computador tinha 7 anos, se não me engano, (…) era novinho, mas fazia muito pouco nele porque só vim ter acesso à internet lá para os 12/13. Portanto, jogava uns joguinhos e tal… Quando a internet chegou ao meu computador, eu já tinha TIC na escola e que ajudou nas coisas básicas e, também, fazia muitas pequenas formações nas férias que havia nos clubes de informática que havia ali no quartel dos bombeiros, ou na Ribeira Seca nos baixos da Sociedade Filarmónica. Eles faziam pequenas formações no verão, coisas simples de uma semana que aprendiam

(HESITAÇÃO) que aprendiam não, que ensinavam a digitar textos no Word, a usar o PowerPoint, a criar um e-mail, coisas desse género." (P.2)

"Eu acho que foi por volta dos 10 ou dos 12, não tenho a certeza. Acho que foi por aí que recebi o meu primeiro computador. Mas eu lembro-me de estar na escola, quando eu tinha 7 ou 8 anos, e eles começaram a introduzir aulas de informática e a ensinar-nos a escrever no computador, a redigir alguns textos e assim, portanto essas foram as primeiras coisas que aprendi a fazer num computador. (…)" (P.5)

Alguns dos participantes, afirmaram que utilizavam o computador para contextos de lazer, como por exemplo videojogos, nos quais jogavam tanto online (em contato com outros jogadores online) como offline (não estando em contato com outros jogadores na internet). Um dado curioso foi o facto do Participante 1 (P.1) que quando recebeu o seu primeiro computador, tinha à volta de 9 ou 10 anos e teve logo contato com a internet, utilizando-a principalmente para jogar, o que o motivou a saber escrever no computador e outras dinâmicas computacionais (como instalar e desinstalar aplicações, etc.), afirmando que se sentia à frente dos seus colegas de escola em termos de conhecimentos digitais aquando das aulas de TIC.

"Eu recebi o meu computador havia de ter 9 ou uns 10 anos e tive logo internet e comecei a usar mais o computador foi mesmo mais para jogar, tanto que hoje ensinou-me a escrever e a fazer tudo, tanto que quando cheguei às aulas de TIC na escola já ia um pouco mais avançado que os outros miúdos que ainda não sabiam ligar um computador e abrir uma aplicação." (P.1)

"Eu só tive o meu computador próprio praí no 8º ano ou 7º ano da escola. Sempre tivemos um computador fixo lá em casa. Era da minha irmã. Praí no 1º ciclo comecei a jogar aqueles jogos didáticos com ela, da história, do corpo humano… (…)" (P.3)

Outro dado curioso é que dois participantes referiram que, na altura dos 12 ou 13 anos começaram a usufruir das redes sociais, como por exemplo o MSN Messenger e o Hi5, onde comunicavam com os seus amigos digitalmente.

"Bem, eu pessoalmente lembro-me também de ter uns 8 ou 9 anos e nós tínhamos lá em casa um computador fixo, também sem internet. Foi a primeira vez que comecei a usar um computador. Acho que na altura eram aqueles jogos que costumava ter lá, brincar com cassetes e assim, e depois o meu (HESITAÇÃO) quando comecei a ter um computador mesmo para mim penso que foi à volta dos 13… 12/13 anos, que foi um que antes era da minha irmã, como era mais velha, usava para a escola e depois fiquei com ele, para aí um ano depois, e o que fazia nele, principalmente, que eu me lembre, era jogar e lembro-me muito do MSN, principalmente daqueles GIFS animados (ACENO COM A MÃO) (RISOS) que é o que me lembro desse computador. E era isso que a gente fazia (HESITAÇÃO) que eu fazia, pelo menos." (P.4)

"(…) Mas lembro-me, (…) do MSN e do Hi5, também falava muito com os meus amigos por aí, e depois sim, nas aulas, quando tínhamos talvez aos 10 anos ou assim, lembro-me de nos ensinarem a criar um e-mail e pronto, a partir daí comecei a ter aulas do tipo mais avançadas e aí já tinha um computador." (P.5)

Fechando a discussão sobre a primeira questão e sem intenção por parte de acrescentar algo mais ao debate sobre a mesma, passou-se para a seguinte questão: "Quais os riscos que os jovens, hoje em dia, podem enfrentar com a utilização da internet de forma descuidada e de que forma pode afetar o seu crescimento?".

Esta questão gerou uma partilha de opiniões bastante similares, desde compras feitas online a partilha de conteúdo privado nas redes sociais. Contudo, houve um dos participantes que referiu haver uma diferença de gerações quanto ao uso da internet de forma segura, ou seja, segundo o Participante 2, quando recebeu o seu primeiro computador, havia uma preocupação constante da parte das pessoas mais velhas que a rodeavam em avisar-lhe sobre os perigos da internet, como não partilhar certos e determinados conteúdos e ter a preocupação em possuir palavras-chave com algum grau de complexidade de forma a ser uma palavra-chave 'forte'.

"Eu acho que já se nota, claramente, uma diferença grande entre a nossa geração e a geração do hoje. E digo isto porquê? Nós recebemos o nosso computador 7, 8, 10, 12 anos… E foi numa altura em que eu acho, pelo menos na minha opinião, em que eu acho que havia muito… (HESITAÇÃO) muitos cuidados. As pessoas diziam sempre para ter cuidado, para não partilhar isto, não partilhar aquilo, é preciso ter boas passwords, é preciso… Nunca se dá o nome verdadeiro, etc. Até nos jogos online, nunca ponhamos o nosso nome verdadeiro." (P.2)

Ainda sobre o assunto dos riscos que os jovens podem enfrentar com a utilização da internet de forma descuidada, foi discutido em grande parte a partilha de conteúdo, principalmente, em redes sociais. Este conteúdo, como grande parte dos participantes referiu, é basicamente fotografias e vídeos pessoais que, por sua vez, não temem que alguém possa usufruir desse tipo de conteúdo de forma perversa, ou seja, utilizar esse conteúdo como uma entrada em contato com o mundo da pedofilia, através de perfis falsos nas redes sociais, ou até mesmo ações de fraude através de informação adicional sobre esse conteúdo, como por exemplo, o nome ou morada do jovem em questão. Isto tudo porque, segundo dizem alguns dos participantes, os jovens atualmente têm acesso

a imensos recursos e informação da internet e acabam por não ter capacidade de gerir os impulsos em partilhar alguma coisa na internet. Quanto a este assunto, a Participante 3 apontou um dado interessante que serve de solução a este tipo de problema, ou seja, refere-se basicamente a programas ou aplicações computacionais que tem uma componente de bloquear a entrada em websites que possam dar um impacto negativo aos jovens que, neste caso, é utilizado por pais que têm a preocupação da fraca gestão de impulsos dos seus filhos aquando do contato com a internet e, desta forma, conseguem supervisionar minimamente as suas ações. Porém é algo ainda bastante complexo e, segundo a mesma participante, não conseguem chegar a tudo o que os filhos utilizam devido à quantidade de recursos digitais que estes têm possibilidade de usufruir.

Todavia, houve uma opinião contrária por parte do Participante 4 quanto à capacidade dos jovens de saberem proteger-se em ambiente digital, argumentando que como os jovens têm um contato cada vez mais precoce com os recursos digitais, estes tendem a reconhecer quais as ações que podem aplicar para uma utilização mais correta da internet, bem como riscos e problemas que podem ter com a partilha de certos conteúdos. Mas a sua argumentação acabou por levar à mesma conclusão supramencionada sobre a vulnerabilidade de impulsos que os jovens podem enfrentar com a utilização da internet.

"A nível pessoal e profissional pode afetar muito a vida deles. (HESITAÇÃO) Fazer compras em sites e não utilizar cartões virtuais, ou fazer numa plataforma de pagamento como o Paypal ou assim, podem perder dados do seu banco e serem vítimas de fraude, ou introduzirem os seus nomes, as suas coisas, as suas fotos, podem ser vítimas de roubo de identidade… é comum (HESITAÇÃO) É bastante comum e, atualmente, vê-se bastante segundo as contas de… (HESITAÇÃO) jovens que criam contas para gozarem com os amigos, a fingirem que são outras pessoas…" (P.1)

"Eu acho que já se nota, claramente, uma diferença grande entre a nossa geração e a geração do hoje. E digo isto porquê? Nós recebemos o nosso computador 7, 8, 10, 12 anos… E foi numa altura em que eu acho, pelo menos na minha opinião, em que eu acho que havia muito… (HESITAÇÃO) muitos cuidados. As pessoas diziam sempre para ter cuidado, para não partilhar isto, não partilhar aquilo, é preciso ter boas passwords, é preciso… Nunca se dá o nome verdadeiro, etc. Até nos jogos online, nunca ponhamos o nosso nome verdadeiro." (P.2)

"Acho que atualmente tens acesso a muita informação, não tens uma base de dados propriamente fidedigna e uma segurança adequada. Portanto, os jovens atualmente, não tem um filtro, recebem tudo. Não sabem se está certo ou errado, se aquilo é correto (HESITAÇÃO) e acho que devia de haver mais segurança nesse aspeto. Sei que alguns… (HESITAÇÃO) alguns… (HESITAÇÃO) como eu hei de dizer… alguns programas que bloqueiam alguns sites e os pais têm alguma supervisão, mas não conseguem chegar a tudo." (P.3)

"É assim… Eu… Eu acho que hoje em dia… Como a Ana disse, os jovens têm acesso a todo esse material e toda essa informação muito mais cedo, o que faz com que eles sejam mais competentes, talvez, com a máquina em si mas continuam a ser jovens, ou seja, não têm ainda o conhecimento de todos os riscos e de todos o problemas que podem vir a ter com o que partilham e das pessoas, e enquanto… (HESITAÇÃO) enquanto que… (HESITAÇÃO) estão mais lá, ou seja, continuam, talvez mais do que nós nesse ambiente virtual… (…) Acho que esse risco está sempre cá e ainda é mais perigoso digamos… Acho que hoje em dia, para eles, como há mais recursos é mais fácil cair nesse risco para esses jovens. (P.4)

Um outro dado interessante foi o facto da Participante 5 referir a tentação dos mais jovens serem influenciados com facilidade ao que assistem na internet, mais concretamente em redes sociais, como o Facebook e o Youtube, ou seja, o facto de serem jovens, tendem a ceder à tentação de repetirem algo que outras pessoas partilham nesses meios, não tendo a capacidade de perceber o que é certo ou errado de se fazer.

A questão dos videojogos também foi discutida, tendo em conta a partilha de identidade quando são utilizados em modo online, havendo por um lado a opinião de que estes possam ser um fator de risco para os jovens levando a cabo certos problemas como a pedofilia e a pornografia e, por outro lado, a opinião de que os mesmo têm tido em conta essa segurança em não partilhar demasiada informação pessoal, tornando os jovens num jogador "anónimo" para com outros jogadores. Porém, foi discutida a importância que os videojogos têm para com o contato com amigos, como uma forma de rede social e, também, uma forma de criar amizades, tornando este tema dos videojogos uma possível fonte de debate futura como sendo uma plataforma de socialização entre jovens ou até mesmo adultos.

"Pronto, eu lembrei-me logo de algo que vai ao encontro da área que eu estudei, que é o crime, (…) falando das redes sociais, também me lembrei… (HESITAÇÃO) por exemplo, atualmente vê-se tudo no Facebook, no Youtube e, como falaste no que é que isso pode ter impacto no desenvolvimento das crianças/jovens… Como se vê tudo, atualmente, em vídeos e publicações, se calhar as crianças podem… como não sabem (…) o que é certo ou errado, pois vêm uma criança a fazer uma coisa, querem fazer… Ou vêm uma criança a terem uma coisa, também querem ter. Portanto, aquilo depois é muito complicado para os pais e para a criança." (P.5)

"(…) que é verdade que nós temos o hábito, pelo menos todos aqueles que eu conheço que joga tem o hábito e esse cuidado de não partilhar a sua informação pessoal… (HESITAÇÃO) Não me lembro de momento algum em que tenha alguma perda de dados ou que me tenha descuidado ao ponto de… (HESITAÇÃO) de ter o risco de fraudes fiscais, como o Alexandre falou. Não… (…) Isto de experiência pessoal, pronto, falo do meu irmão que está sempre no computador e ele tem sempre o cuidado, pelo menos nos jogos e assim, nunca põe o seu nome… agora falando isto, como eu disse, continuam a ser jovens, fazem os seus amigos e partilham tudo e mais alguma coisa." (P.4)

Fechando a discussão sobre esta questão, passou-se para a seguinte: "O que pensam das redes sociais como fonte de informação? De que forma essas redes podem beneficiar ou comprometer a segurança dos utilizadores, seja pela informação em si ou por algum vírus/fraude?".

Nesta questão discutiram-se vários benefícios e riscos que as redes sociais podem ter como fontes de informação.

Tabela 7: Benefícios e Riscos das Redes Socais como fontes de informação.

Benefícios	**Riscos**
Fonte de informação para motivos profissionais	Informação extra (morada, fotos pessoais e materiais, e-mail)
Comunicação e partilha de conteúdos com familiares	Partilha de conteúdo pessoal (dia-a-dia)
Conhecimento sobre tendências	Partilha de *links* fraudulentos ou virulentos
Consulta de conteúdos relevantes	Fraca capacidade de utilização das redes sociais

Neste sentido, foi referido pela maior parte dos participantes sobre o benefício que as redes sociais têm como uma fonte de informação para motivos profissionais, isto é, na preocupação de organizar o perfil de forma apelativa para que organizações possam ter o interesse em contatar para eventuais vaga de emprego e nisto, foram referidas as redes Facebook e LinkdIn. Outro benefício do mesmo ponto é a partilha de conteúdo profissional, isto é, a partilha de conquistas ao nível profissional e ou académico de forma que, também, possa ser um fator aliciante de possíveis contatos de empresas.

Outro benefício discutido, foi o da partilha de conteúdos a familiares que se encontram longe, ou seja, as redes sociais facilitam uma aproximação para com familiares através de conteúdos como fotografias ou vídeos que podem ser pessoais ou não. Para além do contexto familiar, as redes sociais, segundo alguns participantes também têm o benefício de serem fonte de informação em relação ao acompanhamento de tendências, sejam elas sobre cinema, moda, etc. Não só através da partilha de conteúdo relacionado com tendências entre utilizadores como, também, através de publicidades que assistem nestas redes, tendo desta forma o setor do marketing digital um papel relevante no que toca a esta temática. Por fim, também foi discutido o benefício das redes sociais como fonte de informação através da escolha de conteúdos relevantes, isto é, conteúdos que os utilizadores procuram consumir, podendo ser através de perfis ou de páginas que entendem ser relevantes em termos de informação que se deseja consumir.

"Eu acho que… (HESITAÇÃO) Que só se torna perigoso… As redes sociais só se tornam perigosas dependendo da informação que tu dizes querer colocar nas redes sociais. Que é uma fonte de dados que pode ser importante, acredito que sim… A nível de tendências, por exemplo, se tu tens muitas pessoas que partilham… (HESITAÇÃO) Vês uma série e há muitas partilhas acerca daquela série, se calhar para as pessoas que realizam séries, não é? Se calhar vai ser importante saber… As pessoas gostam mais desta ou gostam menos daquela, aí acredito que seja importante. Agora, a nível de segurança de dados, nós vemos muitas vezes avisos a dizer "Ah, X pessoa está a tentar entrar na tua página, na tua conta" … Isso pode ser muito grave, se tu tiveres informação muito pessoal na página, mas caso contrário… claro que vais ter informação pessoal, porque a tua página tem fotografias tuas, tem… pronto, mas eu acho que depende muito daquilo que tu decides partilhar nas redes sociais." (P.2)

"Epá, eu acho que é uma boa fonte de informação mais em termo de… (HESITAÇÃO) Como é que eu vou explicar? Conhecer pessoas… Que é muito mais fácil conhecer pessoas, se calhar, que vão ter mais impacto na tua vida profissional ou teres… Se falares com pessoas da tua família mais longínqua, acho que é uma boa maneira de passar dados de uns para os outros, como procura de emprego… Hoje em dia, muita gente utiliza Facebook, LinkdIn, para a procura de emprego, isso é um bom impacto, mas depois tudo depende da quantidade de informação que tu deixas que as outras pessoas acedam sobre ti (…)." (P.1)

"Eu acho que é uma plataforma muito interessante para mostrares o teu trabalho, para as pessoas te encontrarem, para encontrares… olha, para uma empresa te contactar, para criares uma rede de clientes, para receberes patrocínio de determinado produto… a coisa pode correr muito bem como pode correr muito, não é? Uma empresa pode encontrar o teu perfil e pode não achar interessante. Podem olhar para ti e, se calhar, era a pessoa ideal para promover o nosso produto…" (P.3)

Por outro lado, foram discutidos alguns riscos sendo um dos mais falados a partilha de informação adicional, isto é, por exemplo, a partilha da localização do dispositivo em uso ou do conteúdo partilhado (foto, vídeo) ou a partilha de informação pessoal nas redes. No que toca a conteúdo pessoal, também, foi discutida a partilha de conteúdo do dia-a-dia, ou seja, de momentos do quotidiano do utilizador e desta forma ser possível rastrear o que o próprio faz ou está a fazer de momento e, desta forma, ser possível de ser seguido por alguém indesejado. Quanto à partilha de conteúdo, foi discutido por alguns participantes o facto de nessa partilha serem expostos *links* que possam ser fraudulentos ou até mesmo conterem vírus que comprometam a boa utilização da rede. Por fim, também, foi discutida por parte do Participante 1 sobre a ótica do utilizador, isto é, a capacidade que este tem em utilizar as funcionalidades da aplicação de forma segura, como entrar e sair de forma correta da rede social ou utilizar uma palavra-passe 'forte'. Neste sentido, falou-se também da existência de funcionalidades dessas redes sociais que podem fortalecer a privacidade do utilizador, como restringir o acesso a fotografias pessoais ou até mesmo ao conteúdo que é publicado. Acrescentou-se uma nota dada por um participante sobre a importância em se falar e aprofundar mais sobre riscos que as redes sociais têm como fontes de informação

"Acho que é muito bom para partilhar informação, por exemplo oportunidades de trabalho, ou por exemplo a Netflix, fazer patrocínios para publicidade e tudo mais… Mas é sempre preciso ter em atenção e saber que, por exemplo, há pessoas que se fazem passar por outras… pronto, é preciso também saber naquilo que vamos acreditar ou não… Obviamente que há páginas que nós temos um bocadinho de bom senso, como a Madalena disse, nós conseguimos ver se aquelas página não é fidedigna e, pronto, se calhar aí já pode ter vírus, ou a pessoa pode ter más intenções. Pronto, acho que é sempre preciso ter uma consciência dos riscos que estão por detrás disso, mas pronto… há pessoas que não têm muito essa consciência, por isso acho que também é muito importante, hoje em dia, cada vez mais falar sobre estes riscos." (P.5)

"(…) os sistemas de informação geográfica estão intimamente ligados aos sistemas de GPS e de localização e nós, praticamente, temos a localização dos nossos telemóveis, dos nossos smartphones acionada, quer pela segurança de perda do telemóvel ou de roubo, etc. etc. e aí pode ser totalmente útil, mas depois, não há bela sem senão, também pode ser utilizado por pessoas mal intencionadas que consigam adquirir a localização, a tua localização, a localização do teu smartphone e usar essa informação, esses dados… porque esses dados são públicos, aliás há aplicações…" (P.2)

"Conheço pessoas que partilham a sua vida toda, até o que lancharam ontem à tarde e pessoas quem nem uma fotografia da sua cara têm, e usam aquilo como uma forma de manterem uma forma de

contato com a família, ou só para se lembrarem dos aniversários, neste caso estou a falar mais do Facebook. Mas mesmo assim, a verdade, por ser uma rede, porque és amigo de uma pessoa ou assim, há sempre o risco da transmissão de links ou vírus, mesmo que tenhas muito cuidado… (HESITAÇÃO) através dessas redes, consegues ver quem são os amigos dos teus amigos e claro… estás a perceber?... claro que essa definição de privacidade dá para muda, mas cada um pode escolher o que partilha e não é só o que a pessoa escolhe para partilhar que define o quão exposta está virtualmente, digo eu." (P.4)

"Epa, depende de pessoas para pessoa, por exemplo, eu sei entrar e sei utilizar o que quero fazer das redes socais, e sei sair e correr bem. Mas é como a gente já falou aqui há pouco, existem ainda muitas pessoas que ainda não têm muito a ótica de utilizador quando entram nas redes sociais. Não sabem mudar a sua palavra-passe, não sabem o seu e-mail, precisam de ajuda, memorizam tudo, não memorizam as memórias chaves no browser e fazem tudo é assim… não sabem mandar uma mensagem privada, ou escrevem mensagens nos comentários nas fotos dos amigos. Para essas pessoas consegue ser mais perigoso. Elas estão sujeitas a que muitas mais pessoas se envolvam na vida delas nas redes sociais." (P.1)

Encerrada mais uma temática, seguiu-se a seguinte questão final: "Já tiveram ou assistiram alguma experiência com fraudes, vírus ou outro tipo de ameaças que pudessem comprometer a normal utilização do computador/internet? Se sim, por favor, partilhem.".

Nesta questão foram partilhados alguns momentos que comprometeram de algum modo os participantes ou seus familiares, desde um pagamento para utilização de uma plataforma de videojogos, a burlas por chamada telefónica, e problemas com compra de viagens online. No final desta pequena partilha de experiências, foi dado como terminado o FG, agradecendo a colaboração de todos os participantes.

4.5. Contribuições do *Focus Group*

A elaboração deste FG foi certamente um elemento metodológico que complementou o estudo no sentido em que se pôde perceber opiniões e realidades de utilizadores da internet, da utilização de um computador, contato com a internet e, por fim os juízos sobre gerações futuras quanto aos comportamentos ciberseguros aplicados. Foi mostrado um interesse particular em aprender e perceber novos conceitos e ideias sobre a literacia digital dos açorianos, bem como a segurança que estes abdicam aquando da utilização de redes sociais como fonte de informação. Neste sentido, foi possível constatar que os participantes tiveram contato com um computador bastante cedo e que as aprendizagens de ações básicas do mesmo tiveram fruto através da escola e de formações que, eventualmente, surgiram nessa altura. Mais

se acrescenta que os videojogos, também, têm um papel importante para a aprendizagem a curto prazo de ações simples, melhorando a ótica do utilizador de computador. Esta informação é relevante para o estudo na medida em que o que se pretende estudar é a literacia digital dos açorianos bem como perceber de que forma esta literacia chega aos mesmos.

Pôde-se constatar que existe uma conformidade quanto aos riscos e benefícios que a internet, mais concretamente as redes sociais, podem ter na população mais jovens e, também, houve uma discussão de argumentos e contra-argumentos que geraram conclusões e soluções quanto aos comportamentos a aplicar na utilização destes meios. Neste sentido, pôde-se recolher toda esta informação como conteúdo complementar e de suporte para este estudo, na medida em que podem ser formuladas ou repensadas novas políticas pedagógicas no sentido de melhorar os comportamentos ciberseguros dos açorianos. De igual modo, discutiu-se diferenças entre a geração dos participantes e as gerações futuras quanto à ótica de utilizador da internet e os riscos e benefícios dessa diferença geracional. Quanto à utilização das redes sociais como fonte de informação, do que foi discutido, constatou-se uma série de fatores relevantes para o estudo de forma que se possa incentivar a exploração destes meios como fonte de informação para os utilizadores, bem como possíveis novas funcionalidades de segurança da informação.

Por fim, perceber as experiências tidas de ameaças digitais por parte dos participantes foi relevante, na medida em que se pôde perceber que outras formas podem surgir comprometimentos na utilização da internet, como foi o exemplo de compras online de viagens ou, fora do contexto da utilização de internet, através de telefonemas fraudulentos. Conclui-se ter sido um processo metodológico importante para a sustentação deste trabalho de investigação.

5. A Literacia Digital e Cibersegurança na Região Autónoma dos Açores

Constatando os resultados da metodologia mista elaborada neste estudo é possível aferir vários aspetos interpretativos bem como algumas recomendações que podem ser utilizadas em projetos futuros tendo como base este estudo.

Descrevendo o princípio da metodologia quantitativa, realça-se a presença de observações de todas as ilhas tendo desta forma uma amostra e visão sobre o que se pretendia com o uso do método por inquérito, isto é, foi possível confrontar perceções dos açorianos no seu conceito mais integral, podendo extrapolar resultados acerca da Região em si ao invés de se fazer representar por algumas ilhas mais populosas. Afunilando a análise, pode-se observar uma particularidade quanto aos motivos pelos quais os açorianos utilizam a internet, mesmo que o leque de opções na questão relacionada com este assunto fosse diminuto, houve a intenção de acrescentar um pouco mais de informação acerca do mesmo. Com isto, confere-se que o maior motivo pelo qual a população açoriana utiliza a internet é para lazer, isto é, pode-se englobar neste termo a utilização de redes sociais, como por exemplo o Facebook, o jogar videojogos ou atém mesmo o visionamento de filmes, vídeos e outras ações relacionadas com o lazer digital. Fora do contexto de lazer, são vários os motivos igualmente importantes a realçar, como o caso dos motivos profissionais e académicos. Outras ações, também, são apontadas como as compras online ou o acesso a serviços digitais, tais como o portal das finanças, serviços bancários, ou pagamentos de faturas. Maior parte dos participantes do método qualitativo deste estudo, quando começaram a usufruir de um computador, afirmaram usá-lo maioritariamente para lazer. Posteriormente, afirmaram que utilizam ou utilizaram a internet para fins académicos e de lazer.

No que toca ao assunto da informação no meio digital, os açorianos tendem a ter uma boa capacidade em aceder à informação em diferentes meios e dispositivos, estando eles ligados à internet. Porém, consta-se que tendem a apresentar alguma dificuldade no que toca a uma pesquisa avançada por informação, como por exemplo a pesquisa por palavras-chave ou a utilização de filtros como forma de reduzir a

quantidade de informação que pesquisa de forma que encontrem a mais desejada. Contudo demonstram que têm a capacidade de transformar a informação que encontram em conhecimento, todavia desconhece-se se esse conhecimento será com base em informação fidedigna ou não. Esta questão da capacidade de transformação de informação em conhecimento pode dever-se ao facto de um grande número de respondentes ao inquérito terem o ensino superior. Por contrário à ideia de transformação de conhecimento, maior parte dos açorianos demonstrou que o serem críticos quanto à informação que encontram e avaliação da sua integridade é posta um pouco de lado, dando a entender que há um descuido em querer saber se a informação que se encontrou é fidedigna ou válida para a sua partilha ou para criação de conhecimento, ou seja, desta forma entende-se que existe uma intenção da utilização da informação tal como ela é encontrada.

Falando de informação, o setor da comunicação na população açoriana é algo que também merece um pouco de atenção, isto é, existe uma consciência sobre os riscos associados à comunicação, seja com utilizadores desconhecidos como no uso de informação que não seja fidedigna. Deste modo, constata-se que maior parte dos açorianos não toma uma atitude totalmente segura e sensata quanto às atividades digitais, podendo deste modo pôr em causa o seu bem-estar como o dos utilizadores que o rodeiam, como por exemplo a partilha de um *link* malicioso com familiares e amigos através de algum meio de comunicação digital. Como foi apontado no grupo focal, existe uma constante despreocupação na forma como se pode comunicar no meio digital, podendo afetar o dispositivo digital do utilizador como, também, da saúde do próprio. Ao haver esse descuido, grande parte dos açorianos diz não ter uma total capacidade de conseguirem proteger-se de ameaças online, resultantes de atos indevidos em meios de comunicação digitais, podendo resultar em vários problemas técnicos e psicossociais, como por exemplo o roubo de uma conta de rede social, o "*cyber bullying*", pedofilia ou fraude. Este tipo de acontecimentos foi bastante discutido no grupo focal, havendo uma preocupação por grande parte dos participantes na necessidade de haver uma maior atenção para a monitorização dos jovens recém-utilizadores da internet, bem como as pessoas em geral que desconheçam a possibilidade de serem vítimas desses acontecimentos.

Como há a partilha o conteúdo pelos meios e dispositivos digitais, é preciso que alguém o crie. Neste caso, a criticidade na produção e consumo de conhecimento através das redes sociais por parte dos açorianos é diminuta, isto é, grande parte dos mesmos tende a produzir ou consumir conhecimento da mesma forma como encontraram a informação. Resultado deste processo é a partilha de notícias falsas e de conteúdo malicioso, pensando-se que é algo fidedigno ou válido. Contudo, nota-se que grande parte dos açorianos tem a consciência que o conteúdo partilhado na internet deve ser referenciado respetivamente pelo criador do mesmo. Numa outra perspetiva é de salientar o valor dado à criação de conteúdo nas redes sociais para fins profissionais ou até mesmo académicos, pois nestes meios digitais, tal como alguns participantes do grupo focal apontaram, é bastante útil para a partilha de conquistas ao nível profissional, de conhecimento desenvolvido no meio académico, ou até mesmo na criação de conteúdo para recrutamento profissional.

Sendo a informação, a comunicação e a criação de conteúdo fatores ligados à segurança que se deve ter, grande parte dos açorianos têm consciência dos riscos associados à utilização da internet e respetivas tecnologias, porém grande parte demonstra não ter a completa capacidade em protegerem os seus dispositivos de ameaças vindas do mundo digital. Estas ameaças, como a proteção da sua identidade digital, por parte de terceiros é também um fator que grande parte dos açorianos não tem capacidade de se assegurarem. Tal como foi falado no grupo focal, apontou-se, principalmente nas camadas jovens e idosas, a despreocupação quanto à proteção da identidade digital, sendo que por vezes, ao deixar uma conta de uma rede social aberta ou até mesmo não fazer o “Log Out” das mesmas pode acabar por serem roubadas ou monitorizadas por utilizadores não autorizados, ou, noutra perspetiva, não terem consciência de como são monitorizados pelas próprias aplicações ou navegador de internet. Outro aspeto que vai ao encontro do tema da segurança é o da pegada digital e saúde dos utilizadores, sendo que se pode constatar que grande parte dos inquiridos têm a consciência da sua pegada digital, isto é, o tempo que despendem a utilizar as tecnologias e internet. Neste sentido, também, grande parte dos inquiridos tem a completa consciência das consequências para a saúde com a utilização prolongada e

frequente das tecnologias, tal como os aspetos que estão relacionados com a dependência que estas podem originar.

Quanto à utilização das tecnologias, grande parte dos açorianos não tem uma completa capacidade de resolver um problema técnico caso haja algum problema ou não funciona. Deste modo, também, não há uma completa capacidade de tomar decisões informadas, sejam elas através de assistência humana ou tecnológica, sobre quando e como utilizar as tecnologias para alcançar metas pessoais que sejam relevantes. Tal como foi discutido no FG, há pessoas que não têm a capacidade de instalar um programa num computador ou até mesmo utilizá-lo para fins necessários como aceder à internet para tratamento de assuntos pessoais. Para além do contexto de resolução de problemas, a emergência de novas tecnologias são, também, um fator de grande parte dos açorianos tende a não ter capacidade de acompanhar, isto é, não têm a completa capacidade de se autorregularem na aprendizagem referente a tecnologias digitais. Grande parte da população açoriana refere, também, não ter a completa capacidade de se adaptarem às novas tecnologias, nem a sua integração nos respetivos contextos de vida. Neste sentido, há uma carência na aplicação de uma atitude positiva quanto à aprendizagem de tecnologias emergentes. Porém, foi discutido no FG que existe uma pequena diferença geracional que pode ser um fator de mudança quanto a este assunto, ou seja, todos os participantes apontaram ter recebido um computador numa altura bastante precoce da sua vida, sendo a escola o maior agente de aprendizagem ao nível tecnológico e que, por outro lado, houve uma intenção na procura de um melhor conhecimento face às tecnologias e internet, sendo ela através do frequentar clubes de informática e cursos relacionados com a obtenção de conhecimentos informáticos, ou simplesmente jogar videojogos que tenham objetivos como comunicar e interagir com a tecnologia de forma mais complexa.

Posto isto, são necessárias ações perante a população açoriana para que a literacia digital e a cibersegurança não sejam um "tendão de Aquiles" face ao restante país. Neste sentido, podem ser formuladas algumas recomendações que, segundo este estudo, podem ser aplicadas tanto ao nível macro como ao nível micro da Região.

A primeira recomendação formulada é a criação de estratégias regionais através do Plano Nacional de Leitura 2027[1] e o Centro Nacional de Cibersegurança[2] com o intuito de serem motivadas, a partir do meio escolar, um maior conhecimento e autorregulação na aprendizagem das tecnologias, sendo elas emergentes ou não, e da própria internet. A par disto, reforça-se a ideia da participação de instituições como a Polícia de Segurança Pública e Polícia Judiciária colaborarem com as escolas de modo a alertarem os perigos existentes com o uso da internet de forma indevida, bem como de situações como o "*cyber bullying*" e utilização de perfis falsos em redes sociais, podendo estes serem fatores de comprometimento do crescimento saudável dos jovens utilizadores.

A segunda recomendação é a valorização dos clubes de informática públicos, sendo estes bons meios de transmissão de conhecimentos relacionados com a tecnologia, nomeadamente os computadores, fortalecendo a capacidade de resolver problemas técnicos ou saber decidir o que fazer quando a tecnologia não funciona, adaptação das tecnologias no quotidiano, e valorizando a ideia de estes serem um bom ponto de utilização de tecnologias para contextos académicos e de lazer, principalmente, para pessoas que não têm acesso às tecnologias. Estes clubes de informática também podem ser um ponto importante para projetos com juntas de freguesia ou municípios em oferecer cursos de informática básicos, podendo estes serem divididos por faixas etárias de modo a adaptar as necessidades de todos os participantes, bem como expandir o conhecimento básico do uso de tecnologias digitais.

A terceira recomendação é a aplicação dos videojogos em contextos escolares ou em outros contextos pedagógicos, isto é, a valorização do videojogo como um meio de aprendizagem e adaptação às tecnologias, bem como um meio de comunicação à distância. Esta recomendação adveio do grupo focal aquando de um dos participantes referir que o que aprendeu a nível técnico do computador foi através dos videojogos,

[1] O PNL2027 tem como uma das missões o aprofundamento do potencial da literacia digital, na promoção das competências de escrita e leitura dos jovens, bem como na formação docente no meio digital, promovendo um curso de formação acreditado em E-learning com o tema "Metodologias e Recursos para Promover as Literacias Digitais" (www.pnl2027.gov.pt).

[2] No âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, o CNCS tem como missão a sensibilização e formação, produção e disseminação de alertas, e produção de conhecimento, atuando como forma de coordenador operacional e autoridade nacional no que toca à cibersegurança, não só para entidades do Estado, como para a sociedade em geral (www.cncs.gov.pt).

sentindo-se, no contexto escolar, mais avançado que os outros colegas. Neste sentido, prende-se a ideia de que os videojogos que tenham a capacidade de estimular a criatividade, a comunicação e, principalmente, a adaptação e aprendizagem do uso das tecnologias digitais, possam ser aplicados ao nível escolar na Região.

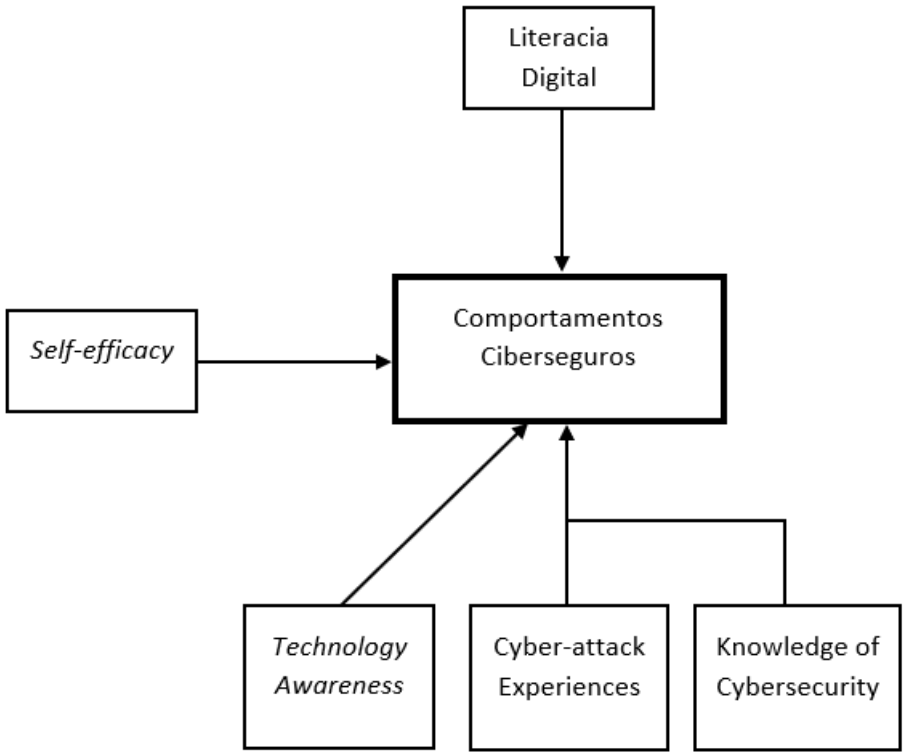
Face ao modelo conceptual apresentado, verificamos que as hipóteses H1, H3, H5, H6 e H7 podem ser comprovadas pelos resultados deste estudo, particularmente, nas seguintes dimensões:

- A *Literacia Digital* (H1), para além de estar relacionada teoricamente com a variável dependente *Comportamentos Ciberseguros*, pôde-se constatar que, tanto no estudo quantitativo e no qualitativo, a literacia digital é essencial para que se possa garantir um comportamento ciberseguro, tanto ao nível da utilização do computador como ao nível de utilização da internet;
- O *Self-efficacy* (H3), ao nível quantitativo, constatou-se que existe alguma carência na capacidade de obter e organizar a informação que é encontrada para que esta seja válida para a produção de resultados. Com isto, pode-se dar como válida ser uma hipótese fortemente relacionada com os comportamentos ciberseguros de cada um. Todavia, ao nível qualitativo, pôde-se complementar o argumento, na medida em que, de facto, na opinião dos participantes, as pessoas tendem a ter dificuldade em conseguirem obter informação viável na internet, acabando por serem vítimas de algum constrangimento no ambiente digital;
- A *Technology-Awareness* (H5), constata-se que, ao nível quantitativo, existe uma fraca motivação para adquirir conhecimentos sobre a tecnologias de informação e respetivas estratégias para a sua utilização que, por sua vez, é uma dimensão que afeta um comportamento ciberseguro, na medida em que, não acompanhando a evolução tecnológica, tende-se a não ter a capacidade necessária para um correto comportamento ciberseguro.
- Quanto ao *Cyber-attack experiences* (H6) e *Knowledge of Cyber Security* (H7), pode-se constatar que se podem relacionar uma com a outra, afetando positivamente o comportamento ciberseguro, ou seja, com a complementação do estudo qualitativo, pôde-se entender que as experiências de ciberataques por parte dos participantes, puderam alterar o seu comportamento ciberseguro de

forma que as próximas utilizações da internet pudessem ser mais seguras. Neste sentido, tendo experiência e conhecimento sobre cibersegurança estão fortemente relacionadas com os comportamentos ciberseguros.

As hipóteses H2 (*Locus of Control*) e H4 (Impulsividade), não foram verificadas no sentido em que teriam de ser estudas através de ferramentas do nível psicológico, de modo que se pudesse dar uma melhor compreensão destas dimensões para com os comportamentos ciberseguros da população açoriana.

Figura 7: Modelo dos Comportamentos Ciberseguros na R.A.A.



6. Conclusões

Esta dissertação tinha como objetivo contribuir para o estudo dos comportamentos ciberseguros na Região Autónoma dos Açores, compreendendo o impacto que a literacia digital e a cibersegurança tem na Região. Para isso foi traçado um estado de arte, onde se explorou conceitos como o comportamento informacional e a cibersegurança, um modelo conceptual de análise, em que se conceptualizou várias dimensões de análise que pudessem ter uma relação com os comportamentos ciberseguros, como a literacia digital, o *locus of control*, a impulsividade, o *self efficacy*, o *cyber attack experiences*, ou o *knowledge of cyber security*, que por sua vez serviram de ferramenta para a compreensão de dimensões relevantes para o processo de estudo seguinte. Foram, também, traçados procedimentos metodológicos para que se pudesse ser realizada uma análise, não só de conteúdo, como de métodos quantitativos e qualitativos. Nesta análise procedeu-se ao estudo empírico por inquérito de modo a compreender de forma quantitativa as experiências e perceções dos participantes, para que, num formato de amostra por conveniência, se pudesse retirar alguns resultados sobre a problemática em estudo. Neste método foram categorizadas várias dimensões relacionadas com a literacia digital e cibersegurança: a informação; a comunicação; a segurança; a resolução de problemas, com o intuito de simplificar a análise que por este método se idealizava estudar. No método qualitativo, também se procedeu à categorização de temas: primeiro computador e aprendizagem do básico do mesmo; riscos e consequências para os jovens; redes sociais como fonte de informação; experiências de ameaças online, com o intuito de moderar e compreender aspetos e perceções mais explicitas sobre a problemática em estudo.

Na discussão de resultados concluiu-se que de facto existe uma falta de capacidade crítica sobre a informação que é retirada da internet, expondo assim um grande risco de transmissão de falsa informação, vírus ou fraudes e criação de conhecimento inválido, tornando os comportamentos ciberseguros por parte dos açorianos algo que merece alguma atenção e valorização para o bem-estar digital dos mesmos. Concluiu-se, também, que a capacidade de proteção da identidade digital dos açorianos não é a melhor, sendo uma valência preocupante para os residentes na Região na medida em que pode ser posta em causa o bem-estar pessoal e ou financeiro de

muitos açorianos e até pode vir a ser um problema ao nível laboral ou académico dos mesmos. Segundo o relatório de perceções "Future Series: Cybersecurity, emerging technology and systemics risk", de 2020 (World Economic Forum & University of Oxford, 2020), afirma-se que é importante evitar circunstâncias nas quais falsas suposições sobre a segurança de sistemas usados para apoiar gestão de identidade podem levar a cabo uma segurança abaixo dos ideais de serviços, ou seja, por exemplo, o uso de SMS para apoiar a autenticação dos utilizadores em transações financeiras.

Revela-se, também, como aspeto conclusivo a dificuldade que os açorianos têm na resolução de problemas relacionados ao mau funcionamento tecnológico, não tendo a capacidade necessária para decidir o que fazer em relação ao problema. Deste modo, e para além da resolução de problemas técnicos, conclui-se que existe uma falta de capacidade de se usar a tecnologia para alcançar metas pessoais relevantes, tomando partido apenas do uso básico da tecnologia bem como o do uso da internet. Tal como foi discutido no "2º Congresso Literacia, Media e Cidadania de 2014" (Silva e Pereira, 2014), as competências das gerações mais novas tendem a desenvolver-se e a consolidar-se com a idade, porém nem sempre conseguem tirar um melhor partido das potencialidades que a internet pode oferecer, confrontando-se futuramente com dificuldades num uso mais complexo e sério que seja solicitado.

Um outro aspeto conclusivo é o da dificuldade em acompanhar a emergência das novas tecnologias. Neste sentido fala-se da fraca capacidade no acompanhamento da evolução da tecnologia bem como da sua integração em determinados contextos do quotidiano, podendo este ser um grande fator de acessibilidade e contato com setores essenciais na sociedade, como a saúde, economia e escolarização. Ações como pesquisar informação por motivos educacionais, avaliar de forma crítica a informação, ou avaliar com rigor e veracidade de conteúdos podem ser um dilema para os que não têm a capacidade necessária para acompanhar a evolução da tecnologia, nem mesmo os jovens que se assumem peritos das redes sociais e dos videojogos (Silva e Pereira, 2014).

Após a constatação dos aspetos conclusivos referidos anteriormente, nota-se que a fomentação da literacia digital é algo de difícil exercício, porém a educação das gerações mais novas pode-se ser um fator determinante para o combate tanto à

carência de literacia digital como a cibersegurança. Assim o afirmam Ana Isabel Santos e Sandro Serpa, ambos docentes da Faculdade de Ciências Sociais e Humanas da Universidade dos Açores, num artigo no Jornal da Faculdade de Ciências Sociais e Humanas da Universidade dos Açores "Ágora", em 2018, que se trata de prover às crianças e jovens ferramentas para que possam desenvolver a visão crítica no mundo digital, promovendo capacidades, habilidade e atitudes de forma a que se tornem cidadãos mais prudentes na recolha de informação mais privilegiada, traduzindo-se, posteriormente, num melhor apresto para o sucesso ao nível social, profissional, académico e, também, ao nível da literacia digital (Santos & Serpa, 2018).

Posto isto, são apontadas algumas implicações práticas e teóricas, bem como de contributos para outras áreas de estudo, particularmente:

- Foi traçada apenas uma análise de uma amostra por conveniência da população da Região Autónoma dos Açores. Recomenda-se aplicar um estudo de gerações ou de jovens estudantes dos Açores;
- Seria necessária a utilização de ferramentas de estudo que pudessem validar as hipóteses H2 (*Locus of Control*) e H4 (Impulsividade), sendo dimensões de cariz psicológico, em que os métodos utilizados neste estudo não puderam validar;
- A análise metodológica quantitativa foi feita a partir da descrição de dados gerados pela plataforma Google Forms. Recomenda-se a aplicação de softwares estatísticos de modo a atingir resultados mais robustos;
- A análise quantitativa deste estudo foi feita a partir de uma amostra de 202 respostas, sendo uma amostras "bola de neve" e por conveniência, em relação a uma população de 236 440 residentes (INE, 2021). Recomenda-se a aplicação de uma evolução da amostra;
- Sugere-se a aplicação de ferramentas que possam compreender a relação entre variáveis, como por exemplo entre o nível de habilitações literárias e o nível de literacia digital dos açorianos;
- Este estudo baseou-se em produção científica nacional e internacional, não tendo sido possível encontrar produção científica sobre estas temáticas na Região.

Contudo, apesar das limitações supramencionadas, este estudo pode contribuir de forma significativa não só pela produção científica a nível regional, como para uma melhor compreensão sobre o impacto que a literacia digital e cibersegurança tem na Região Autónoma dos Açores. A par desta contribuição, também se valoriza o facto que este estudo possa contribuir para a produção científica em relação à Gestão e Curadoria da Informação e, também, de como esta área pode ser relevante para o conhecimento da literacia digital e cibersegurança.

Por fim, em relação ao objeto de estudo desta dissertação, sugere-se possíveis investigações futuras, nomeadamente em áreas da Psicologia, da Sociologia, do Comportamento Informacional Regional e da Pedagogia Digital através de áreas do entretenimento, como a dos videojogos, prevalecendo um maior incentivo quanto à produção científica sobre a literacia digital e a cibersegurança, especialmente, na Região Autónoma dos Açores.

Bibliografia

Addae, J. H., Sun, X., & Radenkovic, M. (2019). *Exploring User Behavioural Data For Adaptive Cybersecurity*. *29*, 701–750.

Aivazpour, Z. (2019). *Impulsivity and Risky Cybersecurity Behaviors: A Replication*.

Ajzen, I. (1991). The Theory of Planned Behavior. Em *Organizational Behavior and Human Decision Processes* (Vol. 50, pp. 179–211).

Alshboul, Y. (2017). Information Security Awareness: Antecedents and User Satisfaction Perspective. *Masters Theses & Doctoral Dissertations*, 307.

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

Behrens, S. J. (1994). A Conceptual Analysis and Historical Overview of Information Literacy. *College & Research Libraries*, *55*(4), 309–322. https://doi.org/10.5860/crl_55_04_309

Bellinger, G., Castro, D., & Mills, A. (2004). *Data, Information, Knowledge, and Wisdom*. 5.

Borko, H. (1968). *Information science: What is it?* 3–5. Wiley Online Library.

Carreiras, H., Barrinha, A., Marques, A. G., Santos, L., Santos, D., de Jesus, H. F., Barbas, J., Confraria, J., Gouveia, L. B., Nunes, P. F. V., Santos, S. J., & Geraldes, S. M. (2020). *Cibersegurança e Ciberdefesa em tempos de pandemia*. National Defense Institute of Portugal; JSTOR. https://www.jstor.org/stable/resrep25591

Case, D. O. (2006). Information behavior. *Annual Review of Information Science and Technology*, *40*(1), 293–327. https://doi.org/10.1002/aris.1440400114

Centro Nacional de Cibersegurança. (2020). *Alerta COVID-19 e as ciberameaças*. https://www.cncs.gov.pt/recursos/noticias/alerta-covid-19-e-as-ciberameacas

Correia, P. M. R. A., Santos, S. I. da S., & Bilhim, J. A. de F. (2016). Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio. *Revista da FAE*, *19*(2), 22–37.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 9.

da Silva, S. G., & Pereira, S. (2014). *Livro de Atas do 2º Congresso Literacia, Media e Cidadania* (Gabinete para os Meios de Comunicação Social-Grupo de Trabalho Informal sobre Literacia para os Media).

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). *A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults*. *3*, 15.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x

Dinev, T., Hu, Q., & Florida Atlantic University. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/10.17705/1jais.00133

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712–728. https://doi.org/10.1080/1369118X.2018.1428652

Fernandes, M. J. O. (2020). Comportamentos e modelos informacionais da geração Google: Contributos para o perfil das gestoras e curadoras de informação em Portugal. *Faculdade de Ciências Sociais e Humanas (FCSH-UNL)*, 149.

Galego, C., & Gomes, A. A. (2005). Emancipação, rutura e inovação: O «focus group» como instrumento de investigação. *Revista Lusófona de Educação*, 173–184.

Gilad, S. (2021). *Mixing Qualitative and Quantitative Methods in Pursuit of Richer Answers to...: Sistema de descoberta para FCCN*. 26.

Head, A. J., Fister, B., & MacMillan, M. (2020). *Information Literacy in the Age of Algorithms*. 55.

Howard, D. J. (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents. *University of South Florida*, 86.

Hwang, G.-J., & Kuo, F.-R. (2015). A structural equation model to analyse the antecedents to students' web-based problem-solving performance. *Australasian Journal of Educational Technology*, *31*, 400–420. https://doi.org/10.14742/ajet.284

INE. (2019). *Proporção de indivíduos com idade entre 16 e 74 anos com competências digitais ao nível básico ou acima de básico (%) por Local de residência (NUTS - 2013); Anual*. Instituto Nacional de Estatística. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0010710&contexto=bd&selTab=tab2

INE. (2021). *População residente (N.º) por Local de residência, Sexo e Grupo etário; Decenal—INE, Recenseamento da população e habitação—Censos 2021*. Instituto Nacional de Estatística.

https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&contecto=pi&indOcorrCod=0011166&selTab=tab0

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't. *American Behavioral Scientist*, *65*(2), 371–388. https://doi.org/10.1177/0002764219869406

Kianpour, M., Øverby, H., Kowalski, S., & Frantz, C. (2019). *Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties* (pp. 149–163). https://doi.org/10.1007/978-3-030-22351-9_10

Kitzinger, J. (2005). Focus group research: Using dynamics to explore perceptions, experiences and understandings. Em *Qualitive Research in Health Care* (p. 320). Immy Holloway.

Kyriakidou, V., Michalakelis, C., & Sphicopoulos, T. (2011). Digital divide gap convergence in Europe. *Technology in Society*, *33*(3), 265–270. https://doi.org/10.1016/j.techsoc.2011.09.001

Laboratório de Conteúdos Digitais. (2017). *DigComp—Quadro Europeu de Referência para a Competência Digital [DIGICOMP: A Framework for Developing and Understanding Digital Competence in Europe] + [DigiComp 2.0: The Digital Competence Framework for Citizens]*.

Landøy, A., Popa, D., & Repanovici, A. (2020). Basic Concepts in Information Literacy. Em A. Landøy, D. Popa, & A. Repanovici (Eds.), *Collaboration in Designing a Pedagogical Approach in Information Literacy* (pp. 23–38). Springer International Publishing. https://doi.org/10.1007/978-3-030-34258-6_3

Loureiro, A., & Rocha, D. (2012). *Literacia Digital e Literacia da Informação—Competências de uma Era digital*. 12.

Marcum, J. (2002). Rethinking Information Literacy. *Library Quarterly - LIBR QUART*, *72*, 1–26. https://doi.org/10.1086/603335

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and Evolution*, *9*(1), 20–32. https://doi.org/10.1111/2041-210X.12860

PORDATA. (2020a). *PORDATA - Indivíduos com 16 e mais anos que utilizam computador e Internet em % do total de indivíduos: Por grupo etário*. https://www.pordata.pt/Portugal/Indiv%c3%adduos+com+16+e+mais+anos+que+utilizam+computador+e+Internet+em+percentagem+do+total+de+indiv%c3%adduos+por+grupo+et%c3%a1rio-1139

PORDATA. (2020b). *PORDATA - Indivíduos com 16 e mais anos que utilizam computador e Internet em % do total de indivíduos: Por nível de escolaridade mais elevado completo*. https://www.pordata.pt/Portugal/Indiv%c3%adduos+com+16+e+mais+anos+que+utilizam+computador+e+Internet+em+percentagem+do+total+de+indiv%c3%adduos+por+n%c3%advel+de+escolaridade+mais+elevado+completo-1141

Quesinberry, M. (2016). An Analysis of Faculty and Staff's Identification of Malware Threats. *Eletronic Theses and Dissertations*, 57.

Ramos, A., & Faria, P. (2012). LITERACIA DIGITAL E LITERACIA INFORMACIONAL: Breve análise dos conceitos a partir de uma revisão sistemática de literatura. *Revista Linhas*, *13*(02), 29–50. https://doi.org/10.5965/1984723813022012029

Rosa, H., Pereira, N., Ribeiro, R., Ferreira, P. C., Carvalho, J. P., Oliveira, S., Coheur, L., Paulino, P., Veiga Simão, A. M., & Trancoso, I. (2019). Automatic cyberbullying detection_ A systematic review. *Elsevier Enhanced Reader*, 13. https://doi.org/10.1016/j.chb.2018.12.021

Santos, A. I., & Serpa, S. (2018). *A literacia digital*. 4.

SCONUL. (2011). *The SCONUL Seven Pillars of Information Literacy: Core Model for Higher Education*.

Shaw, R. R. (1948). Royal Society Scientific Information Conference. *American Association for the Advancement of Science*, *108*(2798), 148–151.

Vieira, A. M., & Vieira, R. (2007). A entrevista em grupo: Formas de desocultar representações e práticas de trabalho social nas escolas. *Etnografia (Actas do III Congresso Internacional)*, 1–22.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Wilson, T. (2000). Human Information Behavior. *Informing Science*, *3*, 49–55. https://doi.org/10.28945/576

Wilson, T. D. (1997). *Information Behavior: An interdisciplinary perspective*. *33*(4), 551–572.

World Economic Forum, & University of Oxford. (2020). *Future Series: Cybersecurity, emerging technology and systemic risk* (p. 59).

Zins, C. (2007). Conceptions of information science. *Journal of the American Society for Information Science and Technology*, 17. https://doi.org/10.1002/asi.20507

APÊNDICES

APÊNDICE A - Inquérito em Google Forms.

Literacia Digital e Cibersegurança: contributo para o estudo dos comportamentos ciberseguros.

O meu nome é Ivo Teixeira e sou estudante do curso de Mestrado em Gestão e Curadoria da Informação, parceria entre a Faculdade de Ciências Sociais e Humanas e a Information Management School, ambas da Universidade NOVA de Lisboa.

Este inquérito faz parte da metodologia da minha dissertação, intitulada "Literacia Digital e Cibersegurança: contributo para o estudo dos comportamentos ciberseguros", e tem uma duração cerca de 5 minutos. O principal objetivo deste estudo é dar um contributo ao estudo dos comportamentos ciberseguros, tentando perceber as competências, atitudes e habilidades, ao nível digital, nos Açores.

Ao longo do inquérito serão abordados 5 temas centrais, sendo eles: Informação; Comunicação; Criação de Conteúdo; Segurança; Resolução de problemas.

As respostas dadas neste inquérito serão anónimas, respeitando a política de proteção de dados presentes no RGPD (Regulamento Geral sobre a Proteção de Dados).

Caso tenha alguma dúvida, pode contatar-me através do seguinte correio eletrónico: a52089@campus.fcsh.unl.pt

Obrigado pela colaboração!

*Obrigatório

Questões introdutórias

1. Tem computador pessoal? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

2. Tem telemóvel pessoal? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

3. Consegue aceder facilmente à internet? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

4. Para que motivos utiliza a internet? *

Marcar tudo o que for aplicável.

- ☐ Profissionais.
- ☐ Lazer.
- ☐ Académicos.
- Outra: ☐ _____

Área 1: Informação

Nesta área serão abordados três temas relacionados com o acesso de informação online, sendo eles a Navegação, Procura e Filtragem da Informação; Avaliação da Informação; e o Armazenamento e Recuperação da Informação.

Numa escala de 1 a 5, sendo 1 "Discordo totalmente", 2 "Tendo a Discordar", 3 "Indiferente", 4 "Tendo a Concordar" e 5 "Concordo totalmente", indique a opção que melhor corresponde à sua situação.

1.1. Navegação, Procura e Filtragem da Informação.

5. a) Tenho consciência da existência de diferentes motores de busca. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

6. b) Compreendo como a informação pode ser encontrada em diferentes meios e dispositivos. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

7. c) Consigo utilizar filtros e agentes. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

8. d) Consigo pesquisar por palavras-chave de forma a limitar o número de resultados obtidos. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

9. e) Assumo uma atitude proativa relativamente à pesquisa de informação. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

1.2. Avaliação da Informação

10. a) Sou capaz de transformar informação em conhecimento. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

11. b) Compreendo a fiabilidade de diferentes fontes de informação. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

12. c) Ajuizo a validade do conteúdo encontrado na Internet e nos média, avalio e interpreto a informação. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

13. d) Avalio a utilidade, oportunidade, precisão e integridade da informação. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

14. e) Consigo comparar, contrastar e integrar informação de diferentes fontes. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

15. f) Reconheço que nem toda a informação pode ser encontrada na Internet. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

16. g) Sou crítico(a) sobre a informação que encontro. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

1.3. Armazenamento e recuperação da Informação.

17. a) Compreendo como a informação é armazenada em diferentes dispositivos e serviços. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

18. b) Tenho consciência da importância das cópias de segurança. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

19. c) Tenho consciência das consequências que resultam do armazenamento de conteúdo de forma pública ou privada. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Área 2: Comunicação

Esta área corresponde à comunicação em ambientes digitais, bem como a partilha de recursos, interação e participação em comunidades online e a consciência intercultural.

Numa escala de 1 a 5, sendo 1 "Discordo totalmente", 2 "Tendo a Discordar", 3 "Indiferente", 4 "Tendo a Concordar" e 5 "Concordo totalmente", indique a opção que melhor corresponde à sua situação.

20. a) Tenho consciência dos riscos associados à comunicação online com pessoas desconhecidas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

21. b) Tenho uma opinião própria e informada sobre práticas de partilha, benefícios, riscos e limites. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

22. c) Possuo compreensão crítica dos media sociais, de redes e de comunidades online. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

23. d) Tenho uma atitude segura e sensata durante atividades digitais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

24. e) Possuo capacidade de me proteger, a mim e aos outros de ameaças online. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

25. f) Consigo banir/denunciar abusos e ameaças. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

26. g) Estou consciente dos riscos e benefícios relacionados com a exposição da identidade online. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Área 3: Criação de conteúdos

Esta área vai pôr à prova as competências, habilidades e atitudes relativos à produção de novos conteúdos digitais, bem como a aplicação de direitos de propriedade intelectual e de licenças de utilização.

Numa escala de 1 a 5, sendo 1 "Discordo totalmente", 2 "Tendo a Discordar", 3 "Indiferente", 4 "Tendo a Concordar" e 5 "Concordo totalmente", indique a opção que melhor corresponde à sua situação.

27. a) Sou crítico(a) relativamente à produção e consumo de conhecimento através dos média e das tecnologias. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

28. b) Sei que o conteúdo deve ser referenciado. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

29. c) Compreendo as regras dos direitos de autor e licenças. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Autoavaliação

30. Até agora, qual pensa ser o seu nível de proficiência digital? *

Marcar apenas uma oval.

- ◯ a) Básico
- ◯ b) Intermédio
- ◯ c) Avançado

Área 4: Segurança

Esta área é a mais importante para este estudo, pondo à prova a reflexão sobre as competência, habilidades e atitudes quanto à proteção pessoal, proteção de dados, identidade digital, medidas de segurança e a utilização sustentável e segura.

Numa escala de 1 a 5, sendo 1 "Discordo totalmente", 2 "Tendo a Discordar", 3 "Indiferente", 4 "Tendo a Concordar" e 5 "Concordo totalmente", indique a opção que melhor corresponde à sua situação.

31. a) Sei que há vários riscos associados à utilização de tecnologias. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

32. b) Percebo os riscos associados à utilização da Internet. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

33. c) Consigo proteger diferentes dispositivos de ameaças do mundo digital (programas maliciosos, vírus, etc.). *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

34. d) Tenho uma atitude positiva, mas realista em relação aos benefícios e riscos associados às tecnologias online. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

35. e) Sei como os dados da minha identidade digital podem ser, ou não, utilizados por terceiros. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

36. f) Compreendo como a minha pegada digital pode ser vista e acompanhada por outros. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

37. g) Quanto à minha saúde, conheço as consequências da utilização prolongada da tecnologia. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

38. h) Tenho conhecimento de aspetos relacionados com a dependência que as tecnologias podem originar. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Área 6: Resolução de problemas

Esta é a última área a responder.

Aqui serão testadas as competências, habilidades e atitudes relativas à tomada de decisões informadas, resolução de problemas conceptuais e técnicos através dos meios digitais e atualização de competências digitais.

Numa escala de 1 a 5, sendo 1 "Discordo totalmente", 2 "Tendo a Discordar", 3 "Indiferente", 4 "Tendo a Concordar" e 5 "Concordo totalmente", indique a opção que melhor corresponde à sua situação.

39. a) Consigo resolver um problema técnico ou decidir o que fazer quando a tecnologia não funciona. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

40. b) Consigo tomar decisões informadas (quando necessário através de assistência tecnológica ou humana) sobre quando e como utilizar tecnologia para alcançar metas pessoais relevantes. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

41. c) Tenho uma atitude crítica sobre a produção e consumo de conhecimento através dos media e das tecnologias. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

42. d) Consigo autorregular a aprendizagem referente a tecnologias digitais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

43. e) Consigo adaptar-me, sem problema, às novas tecnologias e integrá-las no meu contexto. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

44. f) Mantenho uma atitude positiva sobre a aprendizagem de tecnologias digitais emergentes. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Final do questionário!

Mais uma vez, agradeço a sua colaboração!

45. Género *

Marcar apenas uma oval.

- ◯ Masculino
- ◯ Feminino
- ◯ Outra: _____

46. Idade (apenas algarismos) *

_____

47. Habilitações Literárias *

Marcar apenas uma oval.

- ◯ Menos de 4 anos de escolaridade
- ◯ 4 anos de escolaridade (1º ciclo do ensino básico)
- ◯ 6 anos de escolaridade (2º ciclo do ensino básico)
- ◯ 9º ano (3º ciclo do ensino básico)
- ◯ 11º ano
- ◯ 12º ano (ensino secundário)
- ◯ Curso Tecnológico/Profissional/Outros (Nível III)*
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Pós-graduação
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Curso de Especialização Tecnológica
- ◯ Sem Habilitações

*

Nível III : Nível de qualificação da formação (c/ equivalência ao ensino secundário)

48. Ilha de residência *

Marcar apenas uma oval.

- ◯ Corvo
- ◯ Flores
- ◯ Faial
- ◯ Graciosa
- ◯ Pico
- ◯ Santa Maria
- ◯ São Jorge
- ◯ São Miguel
- ◯ Terceira

APÊNDICE B - Guião de Preparação do *Focus Group*

Guia de Preparação para o *Focus Group*

Via: Webex

Data: 29/09/2021

Hora de início: 21h

Número de participantes: 5 participantes

Preparação (*Check-list*):

- Garantir participantes com algumas diversidades de perfil;
- Documento com objetivos do estudo e temas que serão abordados na discussão (a entregar aos participantes);
- Meios técnicos: garantir que todos os participantes consigam utilizar a plataforma Webex;
- Em caso de falha técnica, preparar uma solução.

1

Guião

Apresentação:

Olá! Chamo-me Ivo, tenho 24 anos e sou estudante de mestrado em Gestão e Curadoria da Informação, sendo um curso lecionado pela parceria entre a Faculdade de Ciências Sociais e Humanas e a Information Management School, ambas da Universidade NOVA de Lisboa. Estou neste momento a terminar a fase não letiva do curso, sendo ela uma dissertação de conclusão de mestrado.

Quero agradecer a todos a vossa disponibilidade em participar nesta que será a 2ª fase metodológica da minha dissertação, sendo uma forma complementar e de sustentação de todo o estudo que tenho vindo a fazer.

O que se irá passar será uma espécie de discussão/debate (o chamado grupo focal) em que eu serei ser o moderador e irei colocar-vos algumas questões para que se possa proceder à discussão/debate entre vós. Peço que respondam de forma sincera e que não se preocupem em dar respostas certas ou erradas. Peço, também, a que não haja conversas paralelas e privadas.

Como este grupo focal será gravado, foi pedido a todos vocês que consentissem a utilização da vossa imagem e voz, a qual foi assinada por todos uma declaração de confidencialidade e autorização de gravação audiovisual. Neste sentido, relembro que foi garantido a todos vocês que não serão identificados na transcrição de dados, mantendo a garantia de anonimato.

Resta-me dizer que esta sessão terá uma duração de, mais ou menos, 45 e minutos e que todos terão a mesma oportunidade de falar.

Sensibilização do tema de discussão:

Ora, esta dissertação tem como título "A Literacia Digital e a Cibersegurança: Contributo para o estudo dos comportamentos ciberseguros" e pretende-se estudar a competência dos açorianos com a tecnologia e a internet, bem como os comportamentos ciberseguros dos mesmos.

Os objetivos principais deste estudo são, basicamente, contribuir para o estudo dos comportamentos ciberseguros e contribuir para o desenvolvimento de novas políticas públicas e pedagógicas ao nível digital.

Depois desta breve descrição, pergunto-vos se se sentem sensibilizados com o tema.

Entrevista:

- Colocar as perguntas em formato de discussão/debate entre os participantes do *focus-group*.

Questões

1. *Quando é que receberam o vosso primeiro computador e como é que aprenderam o usar básico da máquina?*
2. *Quais os riscos que os jovens, hoje em dia, podem enfrentar com a utilização da internet de forma descuidada, e de que forma pode afetar o seu crescimento?*
3. *O que pensam das redes sociais como fonte de informação? De que forma essas redes podem beneficiar ou comprometer a segurança dos utilizadores, seja pela informação em si ou por algum vírus/fraude?*
4. *Já tiveram ou assistiram alguma experiência com fraudes, vírus ou outro tipo de ameaças que pudessem comprometer a normal utilização do computador/internet? Se sim, por favor, partilhem.*

Terminadas as questões, pergunto se alguém tem alguma coisa a acrescentar?

Conclusão e Agradecimentos

Portanto, damos por concluída a discussão/debate e agradeço mais uma vez a participação de todos vós, sendo muito importante para que este estudo possa ir a bom porto.

Um obrigado e um bem-haja a todos!

FIM.

Quadro Sociodemográfico

Participantes	*Idade*	*Género*	*Hab. Literárias*	*Profissão*
P.1	24	Masculino	Curso Profissional	Operador fabril
P.2	24	Feminino	Mestrado	Geografa
P.3	27	Feminino	Ensino Secundário	Estudante
P.4	24	Masculino	Ensino Secundário	Desempregado
P.5	24	Feminino	Mestrado	Desempregada

5

APÊNDICE C - Transcrição do *Focus Group*

Focus Group 2021-09-29-21-03-32.mp4

Transcrição do Grupo Focal

29/09/2021 – 21h – Plataforma WEBEX

MODERADOR - Olá! Chamo-me Ivo, tenho 24 anos e sou estudante de mestrado em Gestão e Curadoria da Informação, sendo um curso lecionado pela parceria entre a Faculdade de Ciências Sociais e Humanas e a Information Management School, ambas da Universidade NOVA de Lisboa. Estou neste momento a terminar a fase não letiva do curso, sendo ela uma dissertação de conclusão de mestrado.

Quero agradecer a todos a vossa disponibilidade em participar nesta que será a 2ª fase metodológica da minha dissertação, sendo uma forma complementar e de sustentação de todo o estudo que tenho vindo a fazer.

O que se irá passar será uma espécie de discussão/debate (o chamado grupo focal) em que eu serei ser o moderador e irei colocar-vos algumas questões para que se possa proceder à discussão/debate entre vós. Peço que respondam de forma sincera e que não se preocupem em dar respostas certas ou erradas. Peço, também, a que não haja conversas paralelas e privadas.

Como este grupo focal será gravado, foi pedido a todos vocês que consentissem a utilização da vossa imagem e voz, a qual foi assinada por todos uma declaração de confidencialidade e autorização de gravação audiovisual. Neste sentido, relembro que foi garantido a todos vocês que não serão identificados na transcrição de dados, mantendo a garantia de anonimato.

Resta-me dizer que esta sessão terá uma duração de, mais ou menos, 45 e minutos e que todos terão a mesma oportunidade de falar.

Ora, esta dissertação tem como título "A Literacia Digital e a Cibersegurança: Contributo para o estudo dos comportamentos ciberseguros" e pretende-se estudar a competência dos açorianos com a tecnologia e a internet, bem como os comportamentos ciberseguros dos mesmos.

Os objetivos principais deste estudo são, basicamente, contribuir para o estudo dos comportamentos ciberseguros e contribuir para o desenvolvimento de novas políticas públicas e pedagógicas ao nível digital.

Depois desta breve descrição, pergunto-vos se se sentem sensibilizados com o tema. Basta dizer que sim, ou que não.

PARTICIPANTES – Sim!

MODERADOR – Então vamos começa. Ora, a primeira pergunta que vos coloco é... (HESITAÇÃO) antes de mais... vamos a apresentações. Eu gostava que vocês se apresentassem, dizendo o primeiro nome, a idade, os vossos estudos e o que é que costumam fazer no dia a dia.

P.4 – Como é que queres organizar a ordem? (RISOS)

MODERADOR – Quem quiser, pode começar.

P.2 – Força, João!

P.4 – Pronto, está bem. Já que comecei a falar. (RISOS) O meu nome é João, tenho 24 anos, (HESITAÇÃO), tenho o ensino secundário. Depois do ensino secundário tirei um curso de piloto e depois do curso vim para São Jorge (HESITAÇÃO). Estou desempregado (FAZENDO SINAL DE ASPAS COM AS MÃOS), estou a trabalhar nos bombeiros, e no meu dia a dia estou aqui, bebo uns cafés com os amigos, faço umas caminhadas... é isto.

MODERADOR – Bem. Ok, João.

P.2 – Olha, sou a Ana (HESITAÇÃO). Tenho 24 anos e vivo em São Jorge. Sou licenciada em Geografia. Mestre em Sistemas de Informação Geográficos e Ordenamento do Território. Neste momento estou a fazer um estágio no quartel dos bombeiros aqui da Calheta, em São Jorge, (HESITAÇÃO) em que estamos a fazer pela primeira vez nos Açores, planos rápidos de intervenção de edifícios públicos com muita gente... escolas, lares de idosos e etc. E pronto, acho que (HESITAÇÃO) este tema também tem a ver um bocadinho com a minha área de estudo porque os Sistemas de Informação Geográficos passam-se todos através do computador e internet, e tem tudo a ver com dados... e dados que são importantes e que nem sempre são fáceis de arranjar e de partilhar, portanto.

MODERADOR – Muito bem, Ana. Obrigado por te apresentares. Agora, qual é o próximo? (RISOS)

P.5 – Pode ser eu. (RISOS)

MODERADOR – Ok.

P.5 – O meu nome é Bárbara, tenho 24 anos, sou da ilha do Faial (HESITAÇÃO). Tenho uma licenciatura em Psicologia, um mestrado em Investigação Criminal. De momento vou começar a trabalhar na loja da NOS, ao atendimento ao público e, durante o meu dia a dia, além do trabalho, faço... tento fazer exercício físico e passado algum tempo com os meus amigos. (RISOS)

MODERADOR – Muito bem. Obrigado.

P.3 – (HESITAÇÃO) Olá, sou a Madalena , tenho 27 anos, estou no último ano da licenciatura de Ciências da Nutrição (HESITAÇÃO). Gosto de passear, gosto de ir ao ginásio, de estar com os meus amigos... acho que este tema, também, se incorpora um bocadinho na minha área, uma que nós trabalhamos muito com a confidencialidade e dados dos pacientes que não podemos partilhar.

MODERADOR – Muito bem. Faltas tu, Alexandre. (RISOS)

P.1 – Olá, sou o Alexandre, tenho 24 anos, sou operário fabril na ilha de São Jorge, na fábrica Santa Catarina e este tema é interessante porque a gente trabalha com vários dados e com muitas pessoas e é bom saber mais sobre o tema em questão.

MODERADOR – Sim senhor. Muito obrigado. Ora, dadas as apresentações, iremos começar com as questões, sendo que a primeira é ***"Quando é que receberam o vosso computador e como é que aprenderam a usar o básico da máquina?"***. Quem quiser responder primeiro está à vontade.

(BREVE SILÊNCIO)

(ALGUNS RISOS)

P.2 – Posso começar, se ninguém se...

MODERADOR – Podes Ana.

P.2 – Eu recebi o meu primeiro computador tinha 7 anos, se não me engano, mas sou do tempo em que... (HESITAÇÃO) eu não tenho irmãos, então fui a primeira pessoa a

precisar de um computador lá em casa e ainda sou daquele tempo em que se pensava em arranjar um computador em segunda mão para se aprender a mexer no computador e depois, então, comprar um computador novo, bom, quando já se soubesse mexer sem estragar (MOVIMENTO DE ASPAS COM AS MÃOS). Mas pronto, isso não aconteceu, eu recebi o computador, era novinho, mas fazia muito pouco nele porque só vim ter acesso à internet lá para os 12/13. Portanto, jogava uns joguinhos e tal... Quando a internet chegou ao meu computador, eu já tinha TIC na escola e que ajudou nas coisas básicas e, também, fazia muitas pequenas formações nas férias que havia nos clubes de informática que havia ali no quartel dos bombeiros, ou na Ribeira Seca nos baixos da Sociedade Filarmónica. Eles faziam pequenas formações no verão, coisas simples de uma semana que aprendiam (HESITAÇÃO) que aprendiam não, que ensinavam a digitar textos no Word, a usar o PowerPoint, a criar um e-mail, coisas desse género.

MODERADOR – Hmhm.

P.2 – E foi assim, que eu comecei a mexer.

MODERADOR – Muito bem. Bastante cedo então.

P.2 – Sim. (RISOS)

MODERADOR – Muito bem. Agora, quem será o seguinte?

P.1 – Eu recebi o meu computador havia de ter 9 ou uns 10 anos e tive logo internet e comecei a usar mais o computador foi mesmo mais para jogar, tanto que hoje ensinou-me a escrever e a fazer tudo, tanto que quando cheguei às aulas de TIC na escola já ia um pouco mais avançado que os outros miúdos que ainda não sabiam ligar um computador e abrir uma aplicação.

MODERADOR – Isso, mais ou menos, com que idade?

P.1 – Uns 9 ou 10 anos.

MODERADOR – Hmhm. E usavas só para jogar, ou fazias outras coisas para além de jogar computador?

P.1 – Trabalhos para a escola e poucas coisas assim. Não tinha muito mais que fazer.

MODERADOR – E utilizavas a internet para fazer esses trabalhos, certo?

P.1 – Sim, sim.

MODERADOR – Muito bem.

P.4 – Bem, eu pessoalmente lembro-me também de ter uns 8 ou 9 anos e nós tínhamos lá em casa um computador fixo, também sem internet. Foi a primeira vez que comecei a usar um computador. Acho que na altura eram aqueles jogos que costumava ter lá, brincar com cassetes e assim, e depois o meu (HESITAÇÃO) quando comecei a ter um computador mesmo para mim penso que foi à volta dos 13... 12/13 anos, que foi um que antes era da minha irmã, como era mais velha, usava para a escola e depois fiquei com ele, para aí um ano depois, e o que fazia nele, principalmente, que eu me lembre, era jogar e lembro-me muito do MSN, principalmente daqueles GIFS animados (ACENO COM A MÃO) (RISOS) que é o que me lembro desse computador. E era isso que a gente fazia (HESITAÇÃO) que eu fazia, pelo menos.

MODERADOR – Portanto, tu com 12/13 anos já (HESITAÇÃO) portanto, para além de jogares já mexias em redes sociais, como por exemplo o MSN, certo?

P.4 – Sim, acho que foi nessa altura que comecei com o MSN, principalmente e depois, em breve, também, o Hi5. (RISOS)

MODERADOR – Hmhm.

P.4 – E, sim, sim, principalmente essas pequenas redes sociais para falar com o grupo dos amigos, principalmente nada tão grande ou abrangente como o Facebook... isso só veio mais tarde. Mas foi por aí que eu comecei, principalmente em jogos e essas coisas assim.

MODERADOR – E como o Alexandre disse, usavas a internet para fazer trabalhos para escola também e assim?

P.4 – Boa pergunta. (PENSATIVO) Eu não sei se nessa altura se usava muito o Google, mas provavelmente... provavelmente só mais para a frente comecei a usar mais isso. Acho que nessa idade não fazia muitos trabalhos que precisassem de internet. Se eu me lembro corretamente. Também já foi há algum tempo. (RISOS)

MODERADOR – Muito bem. Ok, ok. Bárbara, como é que responderias a esta pergunta? Quando é que recebeste o teu primeiro computador e como é que começaste a usá-lo como deve de ser... o básico?

P.5 – Eu acho que foi por volta dos 10 ou dos 12, não tenho a certeza. Acho que foi por aí que recebi o meu primeiro computador. Mas eu lembro-me de estar na escola, quando eu tinha 7 ou 8 anos, e eles começaram a introduzir aulas de informática e a ensinar-nos a escrever no computador, a redigir alguns textos e assim, portanto essas foram as primeiras coisas que aprendi a fazer num computador. Por acaso não me lembro de jogar em computadores, nessa idade. Mas lembro-me, como o João falou, do MSN e do Hi5, também falava muito com os meus amigos por aí, e depois sim, nas aulas, quando tínhamos talvez aos 10 anos ou assim, lembro-me de nos ensinarem a criar um e-mail e pronto, a partir daí comecei a ter aulas do tipo mais avançadas e aí já tinha um computador.

MODERADOR – Ok. Madalena.

P.3 – Eu só tive o meu computador próprio praí no 8º ano ou 7º ano da escola. Sempre tivemos um computador fixo lá em casa. Era da minha irmã. Praí no 1º ciclo comecei a jogar aqueles jogos didáticos com ela, da história, do corpo humano... Depois, mais tarde, também íamos fazer trabalhos para o museu... aqueles computadores, também, toda a gente tinha acesso... E sim, lá para o 7º ou 8º ano é que tive o meu portátil.

MODERADOR – Hmhm, muito bem. (HESITAÇÃO) Bom, então, passemos para a próxima pergunta que será ***"Quais os riscos que os jovens, hoje em dia, podem enfrentar com a utilização da internet de forma descuidada, e de que forma pode afetar o seu crescimento?"***.

MODERADOR – Se quiserem, posso repetir a pergunta.

P.4 – Repete a pergunta.

P.2 – Se fizeres o favor. (RISOS)

MODERADOR - *"Quais os riscos que os jovens, hoje em dia, podem enfrentar com a utilização da internet de forma descuidada, e de que forma pode afetar o seu crescimento?"*.

P.3 – Acho que hoje (HESITAÇÃO) força Ana.

P.2 – Não, não, força Madalena.

P.3 – Acho que hoje em dia tens acesso a muita informação, não tens uma base de dados propriamente fidedigna e uma segurança adequada. Portanto, os jovens hoje em dia, não tem um filtro, recebem tudo. Não sabem se está certo ou errado, se aquilo é correto (HESITAÇÃO) e acho que devia de haver mais segurança nesse aspeto. Sei que alguns... (HESITAÇÃO) alguns... (HESITAÇÃO) como eu hei de dizer... alguns programas que bloqueiam alguns sites e os pais têm alguma supervisão, mas não conseguem chegara a tudo.

P.2 – Eu, na minha opinião, e não sei se vou fugir um bocadinho à pergunta que fizeste Ivo...

MODERADOR – Força.

P.2 – Eu acho que já se nota, claramente, uma diferença grande entre a nossa geração e a geração do hoje. E digo isto porquê? Nós recebemos o nosso computador 7, 8, 10, 12 anos... E foi numa altura em que eu acho, pelo menos na minha opinião, em que eu acho que havia muito... (HESITAÇÃO) muitos cuidados. As pessoas diziam sempre para ter cuidado, para não partilhar isto, não partilhar aquilo, é preciso ter boas passwords, é preciso... Nunca se dá o nome verdadeiro, etc. Até nos jogos online, nunca ponhamos o nosso nome verdadeiro.

MODERADOR – Hmhm.

P.2 – E hoje em dia, esta geração partilha tudo. E nas redes sociais já não há aquele... (HESITAÇÃO), já não há aquele medo, eu acho, de partilhar as coisas com todos, que é mesmo assim... Eles partilham tudo, desde fotografia, vídeos pessoais, as suas casas, os seus quartos, viagens... e quem diz isto da vida pessoal, diz dados mais importantes como... sei lá... para ingressar num site qualquer estrangeiro para fazer a compra Y precisam de pôr os dados do cartão, ok... não há problema nós pomos. Eu acho que já não há tanto aquele receio... (HESITAÇÃO) eu acho que esta geração nasceu, cresceu com o computador, desde sempre, e não tem aquele medo de o que é que pode vir a acontecer.

MODERADOR – Ok. Alexandre o que é que tu achas que pode afetar os jovens? Com esta partilha de dados assim de forma descuidada, de fotos... (HESITAÇÃO) de que forma é que isso pode afetar esses jovens?

P.1 – (HESITAÇÃO) A nível pessoal e profissional pode afetar muito a vida deles. (HESITAÇÃO) Fazer compras em sites e não utilizar cartões virtuais, ou fazer numa plataforma de pagamento como o Paypal ou assim, podem perder dados do seu banco e serem vítimas de fraude, ou introduzirem os seus nomes, as suas coisas, as suas fotos, podem ser vítimas de roubo de identidade... é comum (HESITAÇÃO) É bastante comum e, hoje em dia, vê-se bastante segundo as contas de... (HESITAÇÃO) jovens que criam contas para gozarem com os amigos, a fingirem que são outras pessoas...

MODERADOR – Hmhm.

P.1 – E isso acontece bastante.

MODERADOR – Bárbara, qual é a tua opinião acerca de... (HESITAÇÃO) acerca dos riscos que podem ter os jovens de forma... (HESITAÇÃO) no uso da internet de forma descuidada?

P.5 – Pronto, eu lembrei-me logo de algo que vai ao encontro da área que eu estudei, que é o crime, não é?... Por exemplo, alguém se partilha... (HESITAÇÃO) estão numa festa com crianças, quem é que diz que aquilo não é nada seguro porque quem sabe se não há alguém... (HESITAÇÃO) alguém lhe apetece raptar uma criança? Isto é muito extremo, mas são perigos, portanto a pessoa se partilha a sua localização, então toda agente fica a saber, desde que tenha acesso ao Facebook daquela pessoa, ou ao Instagram, por exemplo, não é? E isso pode-se falar de raptos com se pode falar de outra coisa qualquer, não é? E pronto... (HESITAÇÃO) Depois... (HESITAÇÃO) Outros riscos como a pornografia infantil e depois... (HESITAÇÃO) pedofilia e tudo mais, mas pronto. Também me lembrei, falando das redes sociais, também me lembrei... (HESITAÇÃO) por exemplo, hoje em dia vê-se tudo no Facebook, no Youtube e, como falaste no que é que isso pode ter impacto no desenvolvimento das crianças/jovens... Como se vê tudo, hoje em dia, em vídeos e publicações, se calhar as crianças podem... como não sabem, como a Madalena disse, o que é certo ou errado, pois vêm uma criança a fazer uma coisa,

querem fazer... Ou vêm uma criança a terem uma coisa, também querem ter. Portanto, aquilo depois é muito complicado para os pais e para a criança.

MODERADOR – Hmhm. João, tu tinhas falado que jogavas jogos desde pequenino, achas que devido a esses jogos ou ao jogares esses jogos... (HESITAÇÃO) achas que nesta altura, achaste que, em algum momento, tiveste a tua... (HESITAÇÃO) portanto, os teus dados em risco, a tua identidade em risco, enquanto jogavas esses jogos online?

P.4 – Não, não... Não só pelo que a Ana disse, que é verdade que nós temos o hábito, pelo menos todos aqueles que eu conheço que joga tem o hábito e esse cuidado de não partilhar a sua informação pessoal... (HESITAÇÃO) Não me lembro de momento algum em que tenha alguma perda de dados ou que me tenha descuidado ao ponto de... (HESITAÇÃO) de ter o risco de fraudes fiscais, como o Alexandre falou. Não... (HESITAÇÃO).

MODERADOR – E achas que os jovens, hoje em dia, podem ter um risco bastante elevado em jogar jogos de... (HESITAÇÃO) Pronto, sofrerem essas consequências da internet, que é, portanto, fraudes e, se calhar, pedofilia infantil, ou encontrarem alguém...

P.4 – Desculpa, mas vais ter que repetir o início da pergunta, desculpa que a internet quebrou e não ouvi o início.

MODERADOR – Achas que os jovens que jogam jogos online têm um grande risco de sofrerem essas consequências da internet, como por exemplo o que a Bárbara disse, da pornografia infantil, ou seja, de alguém que se queira aproveitar de jovens que jogam jogos digitais... o que é que tu pensas acerca disso?

P.4 – É assim... Eu... Eu acho que hoje em dia... Como a Ana disse, os jovens têm acesso a todo esse material e toda essa informação muito mais cedo, o que faz com que eles sejam mais competentes, talvez, com a máquina em si mas continuam a ser jovens, ou seja, não têm ainda o conhecimento de todos os riscos e de todos o problemas que podem vir a ter com o que partilham e das pessoas, e enquanto... (HESITAÇÃO) enquanto que... (HESITAÇÃO) estão mais lá, ou seja, continuam, talvez mais do que nós nesse ambiente virtual... (HESITAÇÃO) Eu pessoalmente não acho que haja uma grande diferença em termos deles para nós na quantidade de informação pessoal que deixam

sair. Isto de experiência pessoal, pronto, falo do meu irmão que está sempre no computador e ele tem sempre o cuidado, pelo menos nos jogos e assim, nunca põe o seu nome... agora falando isto, como eu disse, continuam a ser jovens, fazem os seus amigos e partilham tudo e mais alguma coisa. Tal como a Ana disse. Por isso, continuam a ser muito vulneráveis também às questões de... (HESITAÇÃO) de pedofilia, de fraudes e coisas assim... acho que esse risco está sempre cá e ainda é mais perigoso digamos... Acho que hoje em dia, para eles, como há mais recursos é mais fácil cair nesse risco para esses jovens.

MODERADOR – Ok. Então havendo uma maior quantidade de recursos, como tu dizes, na internet há um maior risco para os jovens cometerem, portanto, sofrerem essas consequências da internet, certo?

P.4 – Certo, porque apesar de saberem mexer no computador muito melhor do que eu sabia na altura deles, continuam a ter esses riscos e hoje em dia até há mais, sim.

MODERADOR – Ok. Sim senhor. Bem, então passemos à próxima questão que é ***"O que pensam das redes sociais como fonte de informação? De que forma essas redes podem beneficiar ou comprometer a segurança dos utilizadores, seja pela informação em si ou por algum vírus/fraude?"***.

P.2 – É assim. Eu acho que... (HESITAÇÃO) Que só se torna perigoso... As redes sociais só se tornam perigosas dependendo da informação que tu dizes querer colocar nas redes sociais. Que é uma fonte de dados que pode ser importante, acredito que sim... A nível de tendências, por exemplo, se tu tens muitas pessoas que partilham... (HESITAÇÃO) Vês uma série e há muitas partilhas acerca daquela série, se calhar para as pessoas que realizam séries, não é? Se calhar vai ser importante saber... As pessoas gostam mais desta ou gostam menos daquela, aí acredito que seja importante. Agora, a nível de segurança de dados, nós vemos muitas vezes avisos a dizer "Ah, X pessoa está a tentar entrar na tua página, na tua conta" ... Isso pode ser muito grave, se tu tiveres informação muito pessoal na página, mas caso contrário... claro que vais ter informação pessoal, porque a tua páginas tem fotografias tuas, tem... pronto, mas eu acho que depende muito daquilo que tu decides partilhar nas redes sociais.

MODERADOR – Hmhm, sim.

P.2 – Não sei se respondi...

MODERADOR – Tudo bem, é a tua resposta, é a tua opinião. Não respostas nem erradas nem certas. Alexandre, o que é que tu achas das redes sociais como uma fonte de informação?

P.1 – Epá, eu acho que é uma boa fonte de informação mais em termo de... (HESITAÇÃO) Como é que eu vou explicar? Conhecer pessoas... Que é muito mais fácil conhecer pessoas, se calhar, que vão ter mais impacto na tua vida profissional ou teres... Se falares com pessoas da tua família mais longínqua, acho que é uma boa maneira de passar dados de uns para os outros, como procura de emprego... Hoje em dia, muita gente utiliza Facebook, LinkdIn, para a procura de emprego, isso é um bom impacto, mas depois tudo depende da quantidade de informação que tu deixas que as outras pessoas acedam sobre ti, por exemplo [SOM NÃO PERCEPTIVEL] por telemóvel, por e-mail, ou por morada, rua, fotos da casa, vai muito da consciência do que a pessoa acha para si que é seguro.

MODERADOR – Ok. Alguém concorda com o Alexandre? Se tem uma opinião...

P.4 – Eu concordo. Eu gostava de realçar, como ele disse, cada um escolhe o que partilha. Conheço pessoas que partilham a sua vida toda, até o que lancharam ontem à tarde e pessoas quem nem uma fotografia da sua cara têm, e usam aquilo como uma forma de manterem uma forma de contato com a família, ou só para se lembrarem dos aniversários, neste caso estou a falar mais do Facebook. Mas mesmo assim, a verdade, por ser uma rede, porque és amigo de uma pessoa ou assim, há sempre o risco da transmissão de links ou vírus, mesmo que tenhas muito cuidado... (HESITAÇÃO) através dessas redes, consegues ver quem são os amigos dos teus amigos e claro... estás a perceber?... claro que essa definição de privacidade dá para muda, mas cada um pode escolher o que partilha e não é só o que a pessoa escolhe para partilhar que define o quão exposta está virtualmente, digo eu.

MODERADOR – Hmhm. Madalena tinhas... como estás ligada ao ramo nutricional, o que tu achas das redes sociais como uma fonte de informação?

P.3 – Eu acho que é uma plataforma muito interessante para mostrares o teu trabalho, para as pessoas te encontrarem, para encontrares... olha, para uma empresa te

contactar, para criares uma rede de clientes, para receberes patrocínio de determinado produto... a coisa pode correr muito bem como pode correr muito, não é? Uma empresa pode encontrar o teu perfil e pode não achar interessante. Podem olhar para ti e, se calhar, era a pessoa ideal para promover o nosso produto...

MODERADOR – Então tu vês mais benefícios do que riscos?

P.3 – É assim, é uma questão um bocadinho do bom senso. Se calhar não vou estar aqui a partilhar a porta da minha casa, nem vou estar a partilhar as informações assim mais pessoais. Acho que consegues partilhar o suficiente para que seja interessante para ti e que consigas ganhar algo com isso.

MODERADOR – Ok. Bárbara.

P.5 – Pronto. Eu concordo com o que todos disseram até agora. Acho que é muito bom para partilhar informação, por exemplo oportunidades de trabalho, ou por exemplo a Netflix, fazer patrocínios para publicidade e tudo mais... mas é sempre preciso ter em atenção e saber que, por exemplo, há pessoas que se fazem passar por outras... pronto, é preciso também saber naquilo que vamos acreditar ou não... obviamente que há páginas que nós temos um bocadinho de bom senso, como a Madalena disse, nós conseguimos ver se aquelas página não é fidedigna e, pronto, se calhar aí já pode ter vírus, ou a pessoa pode ter más intenções. Pronto, acho que é sempre preciso ter uma consciência dos riscos que estão por detrás disso, mas pronto... há pessoas que não têm muito essa consciência, por isso acho que também é muito importante, hoje em dia, cada vez mais falar sobre estes riscos.

MODERADOR – Então pensas que as pessoas não têm, na generalidade, muita consciência daquilo que procuram nas redes sociais, o que leva, portanto, a entrarem em contato com vírus ou esquemas de fraude, certo?

P.5 – Eu acho que sim. Não diria todas as pessoas, mas acho que uma grande percentagem, hoje em dia, pode se calhar ir por acreditar em coisas que, se calhar, não deviam acreditar, e depois pode ser enganado, quer seja por dinheiro, ou seja por outras coisas e sim, depois pode apanhar vírus que depois levam a outros problemas.

MODERADOR – Hmhm. Ana, segundo os teus estudos de Sistemas de Informação Geográfica, de que forma é que isso, portanto, pode levar ou induzir ao erro de informação... ou seja, pessoas partilharem informação segundo Sistemas de Informação Geográfica em redes sociais, como por exemplo, Proteção Civil e afins, de que forma é que isso, portanto, pode comprometer as pessoas? Será que existe alguma forma das pessoas serem enganadas com isso, ou não?

P.2 – Claro que sim. Não falo muito no serem enganadas, mas os sistemas de informação geográfica estão intimamente ligados aos sistemas de GPS e de localização e nós, praticamente, temos a localização dos nossos telemóveis, dos nossos smartphones acionada, quer pela segurança de perda do telemóvel ou de roubo, etc. etc. e aí pode ser totalmente útil, mas depois, não há bela sem senão, também pode ser utilizado por pessoas mal intencionadas que consigam adquirir a localização, a tua localização, a localização do teu smartphone e usar essa informação, esses dados... porque esses dados são públicos, aliás há aplicações...

MODERADOR – Por exemplo, partilhares a tua localização nas redes sociais?

P.2 – Exatamente. Exatamente. Isso pode ser... E isso é público. (HESITAÇÃO) Há aplicações, estava eu a dizer, que há aplicações em que tu consegues localizar o telemóvel de N pessoas que estejam à tua volta. Isso pode dar muito jeito, mas também pode ser um problema. Pode ser um problema porque, se cair nas mãos erradas, por assim dizer, pode trazer muitos problemas. Podemos voltar à história do rapto, sequestro, violações, o que quer que seja, porque lá está, isto a nível dos sistemas de informação geográfica. A nível da Proteção Civil, eu acho que os Sistemas de Informação Geográfica e a partilha de dados, redes sociais, etc. também é ótimo no caso da Proteção Civil aqui nos Açores e acho que falo e todos sabem, todos os presentes sabem que a nossa Proteção Civil, os nossos corpos de bombeiros estão também responsáveis pelo (HESITAÇÃO) pela parte dos... Agora está a faltar-me a palavra (RISOS), dos tratamentos pré-hospitalares, por assim dizer...

MODERADOR – Ok, ok... O Alexandre o que acha das redes sociais, portanto, acha que as redes sociais têm mais benefícios ou têm mais (HESITAÇÃO), portanto, comprometem uma maior insegurança para a generalidade dos utilizadores?

P.1 – Epá, depende de pessoas para pessoa, por exemplo, eu sei entrar e sei utilizar o que quero fazer das redes socais, e sei sair e correr bem. Mas é como a gente já falou aqui há pouco, existem ainda muitas pessoas que ainda não têm muito a ótica de utilizador quando entram nas redes sociais. Não sabem mudar a sua palavra-passe, não sabem o seu e-mail, precisam de ajuda, memorizam tudo, não memorizam as memórias chaves no browser e fazem tudo é assim... não sabem mandar uma mensagem privada, ou escrevem mensagens nos comentários nas fotos dos amigos. Para essas pessoas consegue ser mais perigoso. Elas estão sujeitas a que muitas mais pessoas se envolvam na vida delas nas redes sociais.

MODERADOR – Ok. Então, vamos passar para a última questão... que é se ***"Já tiveram ou assistiram alguma experiência com fraudes, vírus ou outro tipo de ameaças que pudessem comprometer a normal utilização do computador/internet? Se sim, por favor, partilhem"***.

P.1 – A única que me lembre assim... que me vi mais atrapalhado foi, uma vez de estar a jogar jogos com o meu irmão, que para jogar comigo tinha que pagar uma mensalidade para a utilização da plataforma do jogo e eu mandei-lhe a informação do cartão de crédito e ele pagou esquecendo-se de remover a informação... e quando dei por mim, cheguei à conta bancária e saía-me 5 euros por mês, ou 10 euros por mês por uma coisa que eu não sabia... e eu "matei-me" a tentar encontrar para onde aquele dinheiro estava a ir. Afinal ele tinha deixado a plataforma e nunca mais foi lá, nunca mais viu que aquilo estava a ser descontado... e é só. É como a ótica do utilizador, também...

P.4 – (IMPERCEPTIVEL)

MODERADOR – A Bárbara como é entendida em criminologia, qual é... se já teve alguma experiência ou se já assistiu alguma experiência desse género?

P.5 – Hm. Eu já tive mais ou menos uma experiência, quase uma experiência, mas... não foi bem no computador, mas eu não sei se, por exemplo, porque eles... a pessoa conseguiu o meu numero de telemóvel... não sei se foi por minha culpa porque se calhar fiz alguma coisa que não devia numa rede social, não sei bem... mas a verdade é que eles conseguiram arranjar o meu numero de telemóvel e ligaram-me fazendo-se passar pelo meu banco, e eu na altura como era uma nova utilizadora daquele banco não sabia

que o meu banco não me liga, eles pedem para eu (HESITAÇÃO) para eu lhe ligar. Portanto, eu aprendi e havia um problema... disseram que eu estava a ser vítima de fraude e que precisavam de fazer uma conta nova e que eu precisava de lhes dar, pronto, os meus dados e transferir mais de mil libras, porque foi em Inglaterra... mais de mil libras para a nova conta. Só assim é que podiam salvaguardar a minha conta. Eu achei aquilo muito estranho... Mas pronto, como também não estava bem ciente do que é que estava a acontecer e na segurança, também, estava a acreditar neles. A minha sorte é que a chamada foi abaixo e depois o meu banco pediu-me para lhes ligar e explicaram-me o que estava a acontecer.

MODERADOR – João, tinhas começado a responder e interrompi-te sem querer...

P.4 – Não, não. Não há problema nenhum.

MODERADOR – Pedia era que se tivessem alguma experiência, que fossem o mais breve possível, porque o tempo está a esgotar da chamada...

P.4 – A experiência que eu conheço é muito parecida com a do Alexandre. Conheço uma pessoa que lhe foi retirado perto de 80 euros da conta, para uma estadia no Airbnb num sítio qualquer, quando essa pessoa nem sequer usa esse serviço e isto porque os dados do cartão foram adquiridos de outra forma, ou seja, tem tudo a haver com fraude fiscal também.

MODERADOR – Ok.

P.2 – Eu não tenho assim nenhuma... nenhuma... má experiência. Tenho talvez compras feitas no eBay, coisas que (RISOS) nunca chegam. Mas acho que isso é normal, não é? Quero dizer, não é normal, mas não é algo grave. Mas assim a nível de dados e partilha de dados que não devem ser... (HESITAÇÃO) não tenho assim nada.

P.3 – A mim propriamente, nunca me aconteceu nada. Já aconteceu à minha irmã.

MODERADOR – Ok.

P.3 – Ela comprou umas passagens... foram para Florença... já não sei, foram para Itália e depois passados uns tempos, foi à conta e não tinha dinheiro na conta. Ela e mais dois

amigos. E depois o banco acabou por rastrear... clonaram-lhe o cartão e estavam a fazer compras no México (RISOS). Pronto, ela tinha... (IMPERCEPTIVEL).

MODERADOR – Ok. Tudo más experiências... Bom, não tendo mais perguntas, damos por concluída a discussão/debate e agradeço mais uma vez a participação de todos vós, sendo muito importante para que este estudo possa ir a bom porto. Um obrigado e um bem-haja a todos!

(Participantes agradecem).

APÊNDICE D - Declaração de aceitação da gravação do *focus group*

Declaração de aceitação da gravação do *focus group*

Eu, _____, declaro que autorizo a gravação vídeo e áudio dos conteúdos por mim apresentados no âmbito deste *focus group* e cedo os direitos de inclusão desses conteúdos na dissertação de conclusão de mestrado intitulada "A Literacia Digital e a Cibersegurança: Contributos para o estudo dos comportamentos ciberseguros", pela Faculdade de Ciências Sociais e Humanas e *Information Management School* (IMS), da Universidade NOVA de Lisboa.

Declaro ainda que tomei conhecimento que não serei identificado na descrição dos dados obtidos.

Data: _____ / _____ / _____

_____

Assinatura

APÊNDICE E - Questionário Sociodemográfico

Questionário Sociodemográfico

Data: _____

A. Dados pessoais[1]

Idade: _____

Género: Masculino ☐ Feminino ☐ Outro ☐

Habilitações Literárias:

1º ciclo (4ª classe) ☐

2º ciclo (6º ano) ☐

3º ciclo (9º ano) ☐

Ensino Secundário ☐

Curso profissional ☐ Qual: _____

Licenciatura ☐ Qual: _____

Mestrado ☐ Qual: _____

Doutoramento ☐ Qual: _____

Pós-graduação ☐ Qual: _____

Sem Habilitações ☐

Profissão: _____

[1] É de relembrar que estes dados terão em conta o respeito pela proteção de dados, segundo o Regulamento Geral de Proteção de Dados, e que a descrição de dados será de total anonimato, identificando cada participante com um número apenas.