INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA

2016/2017

TII

O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Manuel Artur Correia Alves da Costa

CAPITÃO, PILOTO AVIADOR

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

CAPITÃO, PILAV Manuel Artur Correia Alves da Costa

Trabalho de Investigação Individual do CPOS-FA

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS

CAPITÃO, PILAV Manuel Artur Correia Alves da Costa

Trabalho de Investigação Individual do CPOS-FA

Orientador: MAJOR, ENGENHEIRO ELETROTÉCNICO
João Manuel Moreira Simões

Pedrouços 2017

Declaração de compromisso Anti Plágio

Eu, Manuel Artur Correia Alves da Costa, declaro por minha honra que o documento intitulado "O Ciberespaço Como Nova Dimensão Nos Conflitos", corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do Curso de Promoção a Oficial Superior da Força Aérea 2016/2017, no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência de que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 26 de junho de 2017

Manuel Artur Correia Alves da Costa
CAPITÃO PILOTO AVIADOR

Agradecimentos

Gostaria de agradecer ao orientador deste trabalho, o MAJ/ENGEL João Manuel Moreira Simões, pela disponibilidade, ideias e revisões providenciadas. Agradeço também ao TCOR/TINF Mendes, ao MAJ/TINF Valente e ao MAJ/ENGEL Farinha, por se terem disponibilizado a responder às entrevistas estruturadas e dessa forma partilharem comigo os seus conhecimentos e experiências nesta temática. Agradeço ainda ao MAJ/PILAV Monteiro da Silva pela importante orientação na fase exploratória deste trabalho. Agradeço ainda aos meus camaradas de curso pela partilha de conhecimentos e pela camaradagem ao longo destes últimos meses.

Um agradecimento especial ao diretor de curso COR/PILAV António Pinto pela preocupação e atitude franca para com os auditores, assim como a todos os docentes pela sua dedicação ao ensino.

E finalmente, mas não menos importante, à família com que a vida me presenteou, muito especialmente à Indalécia, pela sua amizade, amor e apoio incondicional.

A todos sem exceção:

Obrigado!

Índice

Índice de Figuras

Índice de Equações

Resumo

Este trabalho tem como objeto de estudo o posicionamento dos recursos humanos (RH) da Força Aérea Portuguesa (FAP) face ao ciberespaço. Para tal, definimos como objetivo principal do estudo avaliar o nível de preparação desses RH para lidar com os desafios associados ao ciberespaço, a fim de criar mecanismos para manter ou melhorar a cibersegurança na FAP.

O processo metodológico baseou-se na perspetiva ontológica construtivista face à compreensão da realidade, partindo-se de um posicionamento epistemológico positivista/empirista. Utilizando um método de raciocínio hipotético dedutivo, através de uma estratégia de investigação quantitativa e de um desenho de pesquisa do tipo estudo de caso, com horizonte temporal transversal. O processo de investigação teve por base o método Quivy e Campenhoudt, complementado pela NEP/ACA 010.

O trabalho está organizado numa introdução, três capítulos e uma conclusão.

Os principais resultados foram a determinação estatística dos parâmetros populacionais relativos ao nível de conhecimento, nível de literacia, nível de interesse e nível de importância.

As conclusões recolhidas indicam que os RH têm baixo nível de conhecimento em matérias relativas ao ciberespaço, baixa literacia em procedimentos de cibersegurança, baixo interesse em receber formação neste âmbito e atribuem pouca importância à manutenção de um ciberespaço aberto e seguro.

Palavras-chave

Ciberespaço, Cibersegurança, Força Aérea, Recursos Humanos

Abstract

This work has as object of study the positioning of human resources (HR) of the Portuguese Air Force (PrtAF) in relation to cyberspace. Being so, our main goal is to assess the level of preparation of these HR to deal with the challenges associated with cyberspace, in order to create mechanisms to maintain or improve cyber security in the PrtAF.

The methodological process was based on the constructivist ontological perspective in the face of the understanding of reality, starting from a positivist/empiricist epistemological position. Using a deductive hypothetical reasoning method, through a quantitative research strategy and a research design of case study type, with transverse time horizons. The research process was based on the Quivy and Campenhoudt method, complemented by NEP/ACA 010.

This work is organized in an introduction, three chapters and a conclusion.

The main results obtained were the statistical determination of the following population parameters: level of knowledge, level of literacy, level of interest and level of importance.

The findings show that HR has a low level of knowledge on cyberspace, low literacy in cybersecurity procedures, low interest in receiving training in this field, and assign little importance to the maintenance of open and secure cyberspace.

Keywords

Cyberspace, Cybersecurity, Air Force, Human Resources

Lista de abreviaturas, siglas e acrónimos

AFA	Academia da Força Aérea
CEMFA	Chefe do Estado Maior da Força Aérea
CFMTFA	Centro de Formação Militar e Técnica da Força Aérea
CPOS	Curso de Promoção a Oficial Superior
DCSI	Direção de Comunicações e Sistemas de Informação
EMGFA	Estado Maior General das Forças Armadas
EUA	Estados Unidos da América
FAP	Força Aérea Portuguesa
FFAA	Forças Armadas
H	Hipótese
NEP/ACA-"X"	Nota de Execução Permanente/Académica n.º "X"
OE	Objetivo Específico
OP	Objetivo Principal
OTAN	Organização do Tratado do Atlântico Norte
PP	Pergunta de Partida
PD	Pergunta Derivada
RH	Recursos Humanos
TII	Trabalho de Investigação Individual
UE	União Europeia
USB	*Universal Serial Bus*
Vn	Variável "n"

Introdução

A flexibilidade e a facilidade no acesso à informação através da Internet e outras redes semelhantes proporcionam enormes vantagens económicas. Por este motivo recorre-se cada vez mais ao ciberespaço para satisfazer necessidades quotidianas da mais variada índole, colocando todos os que o usam numa posição de vulnerabilidade face às ciberameaças (Department of Defense, 2015). A conetividade global exige uma rede aberta, livre e segura a todos os níveis (Conselho da UE, 2009). Esta não é compatível com um ciberespaço sem lei e sem ordem, sendo por isso fundamental legislar para prevenir a cibercriminalidade (Assembleia da República, 2009) e garantir níveis aceitáveis de cibersegurança (Departement of the Prime Minister and Cabinet, 2016). As consequências que podem advir de determinadas ações desencadeadas nas redes informáticas implica um olhar atento a nível da segurança no ciberespaço (Janczewski & Colarik, 2012).

O tema do ciberespaço é excessivamente abrangente, por esse motivo iremos apenas abordar a cibersegurança, uma área importante na medida em que é a partir das falhas neste domínio que as ciberameaças se materializam. A justificação para o estudo desta temática neste trabalho resulta do facto de esta se inserir no corpo de conhecimento das Ciências Militares, mais concretamente, na área do conhecimento do comportamento humano em contexto militar. O desenvolvimento do tema permitirá a caracterização de possíveis fragilidades a nível da cibersegurança, decorrentes dos conhecimentos e comportamentos dos Recursos Humanos da Força Aérea Portuguesa neste domínio. Partindo dessa análise poderá ser possível criar mecanismos para manter ou melhorar a cibersegurança na FAP.

O objeto de estudo deste trabalho é, de uma forma global, o posicionamento dos RH da FAP face à temática do ciberespaço. Isto é, se os seus comportamentos constituem uma ameaça à cibersegurança da FAP; se percecionam o ciberespaço como uma nova realidade do conflito; qual a importância que lhe atribuem e se estes estão predispostos, ou julgam ser necessário, aumentar a sua formação nesta área.

Dado que o trabalho padece de alguns constrangimentos, nomeadamente o dimensional, iremos delimitar algumas dimensões do objeto de estudo. Assim, para um melhor enquadramento da investigação, procedemos às seguintes delimitações: em termos temporais, o objeto de estudo é contemporâneo à nossa investigação, versando analisar o presente, ou seja, a interação quotidiana dos RH da FAP com o ciberespaço; em termos espaciais, o objeto de estudo está delimitado às unidades, aos órgãos e aos serviços da FAP; a nível conceptual, a delimitação é mais difícil de estabelecer dada a grandeza do tema sobre

qual versa o objeto de estudo, no entanto, desenvolvemos um mapa conceptual (**Apêndice A**) onde se estabelecem os principais conceitos da nossa investigação.

A realização desta investigação tem como objetivo principal (**OP**) avaliar o nível de preparação dos RH da FAP para lidar com os desafios associados ao ciberespaço, a fim de criar mecanismos para manter ou melhorar a cibersegurança na FAP. Com base neste, definimos quatro objetivos específicos: (**OE1**) identificar o nível de conhecimento dos RH da FAP em relação ao ciberespaço como dimensão no conflito, a fim de avaliar o grau de perceção situacional da instituição nesta área; (**OE2**) caracterizar as ações e os comportamentos no ciberespaço dos RH da FAP, a fim de avaliá-los ao nível da cibersegurança; (**OE3**) identificar o nível de conhecimentos dos RH da FAP acerca do tema ciberespaço/cibersegurança, a fim de avaliar a necessidade da implementação de programas de formação; (**OE4**) identificar a importância que os RH da FAP dão ao ciberespaço, quando comparado com as restantes dimensões do conflito, a fim de avaliar a importância que estes dão em mantê-lo aberto e seguro.

Com base nestes objetivos procedemos à problematização da temática, elaborando a seguinte pergunta de partida (**PP**): Qual o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança?

De seguida procedemos à operacionalização deste problema, decompondo-o em quatro perguntas derivadas (**PD**):

1ª) Qual o nível de conhecimento dos RH da FAP relativamente ao ciberespaço como nova dimensão do conflito?

2ª) Qual o nível de literacia em cibersegurança dos RH da FAP?

3ª) Qual o nível de interesse no tema ciberespaço e de predisposição dos RH da FAP para receberem formação na área?

4ª) Qual o nível de importância que os RH da FAP dão à existência de um ciberespaço aberto e seguro?

Em termos metodológicos, o nosso estudo adota uma perspetiva ontológica construtivista face à compreensão da realidade, partindo de um posicionamento epistemológico positivista/empirista. Utilizando um método de raciocínio hipotético-dedutivo, através de uma estratégia de investigação quantitativa, tem um desenho de pesquisa do tipo estudo de caso e um horizonte temporal transversal (Bryman, 2012). O processo de investigação que vamos adotar tem por base o método Quivy e Campenhoudt (2005), complementado sempre que necessário ou pertinente pelo método preconizado na

NEP/ACA-010 (IESM, 2015).

O trabalho obedece ao preconizado nas NEP ACA-010 (IESM, 2015) e ACA-018 (IESM, 2015a). Está organizado na seguinte forma e conteúdo: introdução, com o enquadramento, a justificação, o objeto, a delimitação, os objetivos, a problematização e uma síntese metodológica; capítulo um, com os aspetos essenciais à investigação; capítulo dois, com a explicação do processo de recolha, de tratamento e de análise de dados; capítulo três, com a interpretação de dados recolhidos; e conclusão, com um sumário da metodologia, uma avaliação dos resultados, uma explicação dos contributos da investigação, as recomendações, as limitações da investigação e possíveis temas a serem tratados no futuro.

1. Aspetos essenciais da investigação

1.1. Revisão da literatura

O mundo está em transformação e essa mudança é percecionada através da constatação de que as ameaças já não têm fronteiras físicas, fragilizando o tradicional conceito de segurança. Atualmente as ameaças adquiriram uma nova dimensão, ou se preferirmos, uma ciberdimensão. Segundo o General Leandro (Leandro, 2007, p. 12), "…a segurança já não é um dado adquirido em nenhuma parte do globo e deve ser trabalhada e garantida por todos, todos os dias… ", ou seja, como nos diz o Chefe de Estado Maior da Força Aérea, "Os desafios atuais, ao nível da Segurança e da Defesa, são caracterizados pela sua globalidade, imprevisibilidade e assimetria…" (EMFA, 2016).

O ciberdomínio é algo de complexo, veja-se a título de exemplo a aplicação do Direito Internacional à ciberguerra (Schmitt, 2013), o desenvolvimento de operações ultra-táticas no ciberespaço (Caton, 2013), o desacordo conceptual referente às matérias do ciberespaço (Brookson, *et al*., 2015) e as consequências da aplicação de medidas de cibersegurança nos direitos dos cidadãos (Klimburg, 2012).

Das problemáticas referidas no parágrafo anterior percebe-se a necessidade que tivemos em seguir uma linha de investigação mais concreta. Nesse sentido, começamos por aceitar como verdadeira a premissa de que o ciberespaço é uma dimensão do conflito (Dunn, 2001; Klimburg, 2012; Conselho da UE, 2014; United States Department of Defense, 2011; White House, 2011; UE, 2006) e, partindo desse pressuposto, desenvolvemos todo o processo metodológico de recolha, tratamento e análise de dados, com o intuito de compreender como os RH da FAP encaram esse novo paradigma.

Segundo o estudo desenvolvido por Miguel Maria (2015), os eventos perniciosos na rede da FAP passíveis de colocar em risco a segurança da informação, são diários e em número considerável. Parte dessa atividade tem origem externa, no entanto, pelo que se depreende dos dados recolhidos pelo estudo, uma outra parte decorre de comportamentos de risco dos RH da FAP no domínio da cibersegurança.

A Força Aérea, enquanto instituição militar, está sujeita ao escrutínio e orientação do poder político, que define por via legislativa as competências e capacidades que deve possuir, nomeadamente no âmbito do ciberespaço (Lei Nº 67/98, 1998; Lei Nº 109/2009, 2009; Decreto-Lei Nº 62/2011, 2011; Decreto-Lei Nº 3/2012, 2012; Decreto-Lei Nº 69/2014, 2014; RCM Nº 42/2012, 2012; RCM Nº 19/2013, 2013; RCM Nº26/2013, 2013; Despacho Nº 13692/2013 MDN , 2013; Despacho Nº 11400/2014 MDN, 2014). Caberá posteriormente

à FAP a incorporação nos seus regulamentos os diplomas legais relativos às matérias que lhe digam respeito, nomeadamente no que se refere à ciberdefesa e à cibersegurança (RCM Nº 36/2015, 2015; FAP, 2008; FAP, 2009; FAP, 2011; FAP, 2011a). Neste âmbito destaca-se a Diretiva 09/2016 do CEMFA (Chefe do Estado Maior da Força Aérea), relativa ao desenvolvimento da cibersegurança na FAP.

1.2. **Modelo de análise**

1.2.1. Hipóteses

Para cada pergunta derivada sugerimos a seguinte hipótese de resposta: (**H1**) sendo, o ciberespaço como dimensão no conflito, um tema recente e complexo, então, é expectável que os RH da FAP tenham um nível de conhecimento baixo relativamente a esta temática; (**H2**) sendo que, os aspetos a que é dada maior relevância a nível de segurança na interação com a rede são as palavras-chave e os "vírus informáticos", então, é expectável que os RH da FAP possuam um baixo nível de literacia no que se refere às regras e procedimentos fundamentais de cibersegurança; (**H3**) sendo o ciberespaço uma temática tão presente na vida atual, então, é expectável que os RH da FAP tenham interesse na obtenção de mais conhecimentos nesta área; (**H4**) sendo a ligação à rede uma realidade vincada nas sociedades ocidentais atuais, então, é expectável que os RH da FAP tenham a perceção da importância em manter o ciberespaço aberto e seguro.

1.2.2. Conceitos

O quadro conceptual que permite materializar o modelo de análise encontra-se, pormenorizadamente elaborado, no **Apêndice A**. Nele são identificados os conceitos que descrevem as hipóteses, como por exemplo o ciberespaço, a doutrina, a complexidade, a cibersegurança, as ciberarmas, entre outros. Nesse quadro é ainda possível identificar as dimensões que caracterizam esses conceitos.

O **Apêndice B** apresenta uma descrição mais aprofundada dos conceitos que jugamos mais relevantes.

Alguns dos conceitos não são unanimemente aceites, por isso, adotamos uma conceptualização próxima da realidade portuguesa, ou seja, baseada da doutrina dos Estados Unidos da América (EUA), da Organização do Tratado do Atlântico Norte (OTAN) e da União Europeia (UE).

1.2.3. Variáveis

Decorrente da problematização e dos objetivos da investigação, assim como das hipóteses levantadas, foram identificados os principais fatores que permitem a avaliação do objeto de estudo, ou seja, as quatro variáveis independentes representativas das qualidades dos RH da FAP a serem estudadas. São elas: (**V1**) nível de conhecimento; (**V2**) nível de literacia; (**V3**) nível de interesse; e (**V4**) nível de importância.

Para as operacionalizar (compreender os seus comportamentos, como se relacionam e as implicações dos valores que assumem) é necessário classificá-las. Assim, e seguindo a metodologia de Alan Bryman (2012), estas classificam-se como variáveis ordinais, ou seja, variáveis que podem ser categorizadas através de uma classificação ordenada, em que a distância entre as categorias não é rigorosamente idêntica, como teremos oportunidade de ver no capítulo subsequente.

1.2.4. Indicadores

Para tratar o objeto de estudo quantitativamente foi necessário operacionalizar os conceitos e as variáveis (para além da sua classificação). A forma como o fizemos consistiu na decomposição dos conceitos nas suas diferentes dimensões e estas, por sua vez, nos indicadores que permitissem quantificar as dimensões. Para tal recorremos a técnicas de recolha e tratamento de dados, como as entrevistas estruturadas e os questionários de autopreenchimento.

No **Apêndice A** poderá ser consultada a lista completa e a relação que se estabelece entre os conceitos, as suas dimensões, os seus indicadores e as variáveis.

1.3. **Metodologia seguida**

1.3.1. Estratégia de investigação

A metodologia adotada usa uma estratégia de investigação quantitativa para dar resposta às perguntas derivadas, sendo os dados recolhidos de forma estruturada e quantificável, a partir de eventos objetivos, num processo não influenciável pela observação do investigador ou pela investigação. O tratamento dos dados visa conhecer e controlar as variáveis de maneira a eliminar as incertezas da investigação e, se possível, generalizar os resultados obtidos, caso as hipóteses formuladas se verifiquem válidas.

1.3.2. Desenho de pesquisa

O desenho de pesquisa adotado foi o estudo de caso, sendo a unidade de estudo sobre a qual é feita a recolha de informação a comunidade da FAP. O estudo assume um carácter analítico, em que é feito o questionamento de quatro características dessa comunidade, confrontando o resultado com as hipóteses sugeridas de modo a verificar a validade destas.

O desenho de pesquisa tem também um horizonte temporal transversal, na medida em que só se procede à recolha de dados (avaliação da amostra) num único momento temporal. Neste domínio, o estudo é simultaneamente transversal descritivo (explica a frequência de determinados resultados na amostra) e transversal analítico (avalia a prevalência na população de vários aspetos em simultâneo).

1.3.3. Fases do percurso metodológico

Após a análise dos processos metodológicos propostos por Quivy e Campenhoudt (2005) e pela NEP/ACA-010 (IESM, 2015), verificamos que ambos são complementares. As diferenças correspondem, essencialmente, ao número de etapas do processo e não à natureza do método. Em ambos os casos, o processo de investigação está dividido em três fases, cada uma composta por várias etapas. Porém, a NEP supra mencionada, preconiza um conjunto de etapas que, pela natureza do TII do CPOS-FA, têm que obrigatoriamente ser cumpridas.

Por este motivo, o processo metodológico que iremos adotar inclui estas duas vertentes: será baseado no método proposto por Quivy e Campenhoudt (2005), complementado quando necessário ou pertinente pelo método preconizado na NEP/ACA-010 (IESM, 2015).

1.3.3.1. Percurso metodológico segundo Quivy e Campenhoudt

Este processo é composto pelas seguintes fases e correspondentes etapas: rutura, já efetuada (pergunta de partida, exploração – leituras e entrevistas exploratórias, problematização); construção (do modelo de análise) definida neste capítulo; e verificação (observação, análise das informações e conclusões), descrita nos capítulos seguintes.

1.3.3.2. Percurso metodológico segundo a NEP/ACA-010

Este processo é composto pelas seguintes fases e correspondentes etapas: exploratória (escolha do tema, estado da arte, objeto de estudo, objetivo geral e problematização,

delimitação e conceptualização, identificação de variáveis, objetivos específicos, questões secundárias e hipóteses, revisão da literatura, modelo de análise, procedimentos de investigação, projeto de investigação); analítica (recolha, análise e apresentação dos dados); e conclusiva (avaliação e discussão dos resultados, conclusões e implicações, contributos e recomendações, ética da investigação, redação do trabalho, apresentação e defesa do trabalho).

1.3.4. Técnicas de recolha, de tratamento e de análise de dados

Durante a etapa de observação (recolha) devemos responder a três perguntas: o quê; a quem e como. Relativamente ao "o quê", neste estudo corresponde às quatro variáveis que pretendemos estudar. No que diz respeito ao "a quem", são os RH da FAP. E no que se refere ao "como", usamos a entrevista estruturada e o inquérito por questionário como técnicas de recolha de dados.

Quanto ao tratamento de dados, a estatística descritiva consistiu na construção de tabelas e no cálculo das características amostrais (estatísticas); a estatística indutiva foi feita com recurso ao *software* IBM® SPSS® Versão 23 (*Statistical Package for the Social Sciences*); e as entrevistas com recuso à análise de conteúdo.

Na análise testamos as variáveis e estudamos a relação entre elas. Para tal, recorremos à estatística descritiva (resumo da informação contida na amostra) e à estatística indutiva (estimativa das variáveis desconhecidas da população e teste das hipóteses sobre as variáveis).

2. Processo de recolha, de tratamento e de análise de dados

2.1. Processo de recolha de dados

2.1.1. Recolha de dados por questionário

A principal técnica utilizada na recolha de dados foi do tipo não documental, através da observação não participante. Para tal, recorremos ao inquérito por questionário autoadministrado, aplicado por correio eletrónico, tal como documentado por Couper e Miller (2008).

O processo metodológico subjacente à formulação do questionário teve as seguintes fases: problematização do objeto de estudo, formulação de hipóteses apoiadas em conceitos, operacionalização dos conceitos através das suas dimensões e indicadores, resultando daí as questões.

A inexistência de um questionário estandardizado para esta problemática obrigou à sua construção de raiz, designado "O ciberespaço como nova dimensão nos conflitos", para aplicação a todos os RH da FAP. A sua construção encontra-se detalhada nos **Apêndices C**.

A tipologia das perguntas são, quanto ao conteúdo, de três tipos, objetivas (questionam factos), subjetivas (pedem a opinião) e de intenção (perguntam o que faria em determinada situação); quanto à forma, de dois tipos, abertas (resposta livre) e fechadas (opção de resposta limitada). Quanto às respostas fechadas foram usadas três tipologias: as dicotómicas, as de escolha múltipla em leque fechado e as de escolha múltipla de estimação. Procuramos ainda, que as questões gozassem das qualidades de redação (clareza, coerência e neutralidade), de ordem e de número.

Uma vez concluída a primeira versão do questionário foi pedido a dez militares da FAP, com atributos próximo da amostra teórica, que o respondessem e reportassem as suas dificuldades e sugestões. Com base nessas reações foram retiradas ou reestruturadas perguntas, por serem complexas ou confusas, modificada a escala de estimação, identificado o tempo médio de resposta e corrigidas algumas gralhas.

O pré-teste permitiu ensaiar a aplicação do questionário por correio eletrónico, através do envio de uma hiperligação de acesso à aplicação Formulário da plataforma *Google Drive* (https://drive.google.com), onde o questionário foi construído.

2.1.2. Recolha de dados por entrevista

A segunda técnica de recolha de dados foi também não documental e por observação não participante, recorrendo a entrevistas estruturalmente diretivas. Estas visaram recolher

a opinião de três oficiais da FAP com funções ligadas à cibersegurança.

As entrevistas foram efetuadas de modo semelhante, quer na formulação das perguntas, quer na sequência das mesmas. Recorreu-se a questões do tipo abertas, ordenadas e apresentadas num guião de entrevista. A opção por este tipo de entrevista resulta das vantagens subjacentes à sua aplicação e análise de conteúdos.

O processo metodológico para a criação do guião é em tudo semelhante ao realizado para o questionário, podendo ser consultado em pormenor no **Apêndice C**.

A entrevista foi estruturada em duas partes, a primeira de cariz introdutório (apresentação e introdução da entrevista, a sua natureza, os seus objetivos e o contexto em que se insere) e a segunda de exposição das questões.

No **Apêndice D** encontram-se as perguntas e as respostas dadas pelos entrevistados.

2.2. **Processo de tratamento de dados**

2.2.1. Tratamento de dados dos questionários

2.2.1.1. População

A população alvo corresponde ao universo dos RH da FAP, na efetividade de serviço, a 31 de dezembro de 2016.

Contudo, é expectável não termos chegado a toda a população, em resultado de: o correio eletrónico não ter sido consultado; não ter correio eletrónico atribuído; férias; missão no estrangeiro; indisponibilidade para responder; não querer responder. Estas limitações reduzem a população alvo (**Figura 1**) à população acessível (amostra).

Classe	Género	Formação					Totais
		1.º, 2.º ou 3.º Ciclo do Ensino Básico	Ensino Secundário	Ensino Técnico-Profissional	Licenciatura/ Pós-Graduação/ Bacharelato	Doutoramento /Mestrado	
Oficias	M	0	228	0	939	340	1507
	F	0	21	0	226	94	341
Total		**0**	**249**	**0**	**1165**	**434**	**1848**
Sargentos	M	328	1572	126	152	12	2190
	F	0	227	14	70	7	318
Total		**328**	**1799**	**140**	**222**	**19**	**2508**
Praças	M	97	643	657	11	1	1409
	F	11	127	91	25	3	257
Total		**108**	**770**	**748**	**36**	**4**	**1666**
Civis	M	299	42	3	15	1	360
	F	219	99	4	22	4	348
Total		**518**	**141**	**7**	**37**	**5**	**708**
TOTAL		***954***	***2959***	***895***	***1460***	***462***	***6730***

Classe	Género	Grupo Etário				Totais
		20 anos ou menos	21-35 anos	36-50 anos	Mais de 50 anos	
Oficias	M	44	716	460	287	1507
	F	7	183	148	3	341
Total		**51**	**899**	**608**	**290**	**1848**
Sargentos	M	26	723	849	592	2190
	F	3	152	163	0	318
Total		**29**	**875**	**1012**	**592**	**2508**
Praças	M	221	1188	0	0	1409
	F	32	225	0	0	257
Total		**253**	**1413**	**0**	**0**	**1666**
Civis	M	0	5	88	267	360
	F	0	4	80	264	348
Total		**0**	**9**	**168**	**531**	**708**
TOTAL		***333***	***3196***	***1788***	***1413***	***6730***

Figura 1 – Distribuição por categorias dos RH da FAP no ativo a 31 de dezembro de 2016

Fonte: (Direção de Pessoal da FAP, 2017)

2.2.1.2. Amostra

Aquando da construção da amostra procuramos controlar dois aspetos: o enviesamento e os erros da amostra. Na prática, é extremamente difícil eliminar totalmente estas anomalias, contudo, procuramos reduzir o seu efeito através da representatividade da amostra.

Uma forma de o fazer é através da técnica de amostragem probabilística que, embora não eliminem totalmente os problemas amostrais, redu-los. Adicionalmente, este tipo de amostragem permite o recurso à inferência estatística. Como veremos adiante, o processo de

recolha de dados utilizado, para além dos ganhos evidentes em tempo e em custos, possuí características que o qualificam de probabilístico.

2.2.1.2.1. Caracterização da amostra

Um aspeto importante no processo de caracterização da amostra corresponde à necessidade de a dotar de características próximas da população alvo. Mas como nos diz Bryman (2012, p. 200), relativamente a populações homogéneas como as militares, estas não precisam de amostras grandes para caracterizar a população. Adicionalmente, as amostras não precisam espelhar a totalidade das características da população, mas apenas as que podem influenciar as variáveis.

Posto isto, os elementos a que recorremos para caracterizar a amostra foram: a classe a que os RH pertencem; o seu género; o seu grupo etário e a sua formação académica.

2.2.1.2.2. Seleção da técnica de amostragem

A técnica de amostragem utilizada foi probabilística, por amostragem aleatória simples.

A componente probabilística resulta da aleatoriedade relativamente a quem respondeu ao inquérito. Como diz Ronald Fricker (2008, p. 202), a forma como estes questionários são aplicados transformam a seleção dos elementos da amostra num processo aleatório.

Adicionalmente, a população foi dividida em quatro categorias pertinentes para a investigação: a classe; o género; o grupo etário e a formação académica.

2.2.1.2.3. Dimensão da amostra

A dimensão da amostra teve por base considerações como: técnicas de amostragem utilizadas; homogeneidade da população e categorias consideradas.

Tendo por base a homogeneidade da população, podemos dizer que a dimensão da amostra não necessita ser grande. Esta ilação resulta do facto da população possuir várias características de homogeneidade, nomeadamente, indivíduos com comportamentos, hábitos e valores partilhados e tendencialmente aproximados, faixa etária maioritária entre os 21 e 35 anos, nível de vida aproximado e nível de instrução maioritariamente entre ensino secundário e licenciatura.

No entanto, para um resultado mais rigoroso, socorremo-nos da **Equação 1** para determinar matematicamente a dimensão da amostra:

$$n = \frac{N.Z^2.p.(1-p)}{Z^2.p.(1-p) + e^2.(N-1)}$$

Equação 1 - Fórmula de cálculo da dimensão da amostra para uma população finita

Fonte: (Santos, s.d.)

Este cálculo foi efetuado em linha, na página de Glauber Santos (s.d.), estando-lhe subjacente os seguintes pressupostos: erro de amostragem admitido (*e*) de 5%; nível de confiança utilizado (*Z*) de 95 %; dimensão da população (*N*) de 6730 indivíduos; percentual máximo utilizado (1-*p*) de 50%.

Resolvendo a equação, o valor da mostra (*n*) obtido foi de 364 indivíduos (5,41%), distribuídos de acordo com a **Figura 2**.

Por outro lado, se recorrermos ao método sugerido por Huot (2002, cit. por Santos, *et al*., 2015, p. 68), para uma população com 6730 indivíduos, a amostra deve conter 363, mantendo-se a consistência do resultado.

2.2.1.3. Parametrização de dados

As perguntas do questionário, à exceção de uma, são do tipo fechadas, exigindo ao respondente a opção por uma das respostas sugeridas. Esta metodologia permite parametrizar as respostas com recurso a diferentes tipos de escalas.

As escalas usadas foram: a nominal, a ordinal e a intervalar. Os dois primeiros tipos produzem variáveis estatísticas qualitativas, permitindo o recurso a modelos estatísticos não paramétricos. A intervalar produz variáveis estatísticas quantitativas, permitindo recorrer a modelos estatísticos paramétrios. A escala de *Likert* foi utilizada para produzir variáveis quantitativas intervalares, com base nos pressupostos de Bryman e Cramer (2011, pp. 71-73).

2.2.1.4. Métodos estatísticos empregues

Os dados obtidos através do inquérito foram organizados e tratados de diferentes formas. Construíram-se tabelas de frequências e tabelas com dados estatísticos para facilitar a interpretação dos resultados obtidos. O estudo estatístico efetuado aos dados do inquérito foram de dois tipos: os estudos de estatística descritiva e os estudos de inferência estatística.

2.2.2. Tratamento de dados das entrevistas

2.2.2.1. Análise de conteúdo

A utilização da entrevista estruturada permitiu recolher dados de forma sistematizada, com recurso ao método de análise de conteúdo. Este processo teve por base o mapa conceptual do **Apêndice A**, que deu origem às perguntas da entrevista.

As respostas dos entrevistados, oficiais superiores da FAP com funções ligadas à cibersegurança, encontram-se transcritas no **Apêndice D**.

A análise de conteúdo foi a que Guerra (2006, pp. 69-86) sugeriu, englobando cinco etapas: transcrição das entrevistas; leitura e primeiras impressões; resumo das entrevistas em forma de grelha; análise da informação com recurso ao método categorial, com a redução do texto a categorias; e interpretação dos dados recolhidos.

2.3. **Processo de análise de dados**

2.3.1. Análise de dados dos questionários

2.3.1.1. Caracterização da amostra

A distribuição dos elementos da amostra pelas diversas categorias é a que consta na **Figura 2**, onde verificamos que 61,8% são oficiais *[27,5% **(na população)**]*, 29,7% são sargentos *[37,3%]*, 4,1% são praças *[24,8%]* e 4,4% são civis *[10,4%]*.

Destes, 16,2% são do sexo feminino *[18,8%]* e 83,8% são do sexo masculino *[81,2%]*.

Quanto à formação, 2,7% têm o ensino básico *[14,2%]*, 23,6% têm o ensino secundário *[44%]*, 8,5% têm formação técnico-profissional *[13,2%]*, 46,8% têm licen./pós-grad./bacharel. *[21,7%]* e 18,4% têm mestrado/doutoramento *[6,9%]*.

Em termos etários, 0% têm 20 anos ou menos *[4,9%]*, 29,7% têm entre 21 e 35 anos *[47,5%]*, 50,4% têm entre 36 e 50 anos *[26,6%]* e 19,9% têm mais de 50 anos *[21%]*.

Classe	Género	Formação					Totais
		1.º, 2.º ou 3.º Ciclo do Ensino Básico	Ensino Secundário	Ensino Técnico-Profissional	Licenciatura / Pós-Graduação/ Bacharelato	Doutoramento /Mestrado	
Oficias	M	0	6	4	125	50	185
	F	0	0	0	29	11	40
Total		**0**	**6**	**4**	**154**	**61**	**225**
Sargentos	M	0	62	23	11	4	100
	F	0	5	0	2	1	8
Total		**0**	**67**	**23**	**13**	**5**	**108**
Praças	M	0	7	2	0	0	9
	F	0	3	1	1	0	6
Total		**0**	**10**	**3**	**1**	**1**	**15**
Civis	M	8	2	1	0	0	11
	F	2	1	0	2	0	5
Total		**10**	**3**	**1**	**2**	**0**	**16**
TOTAL		***10***	***86***	***31***	***170***	***67***	***364***

Classe	Género	Grupo Etário				Totais
		20 anos ou menos	21-35 anos	36-50 anos	Mais de 50 anos	
Oficias	M	0	61	93	31	185
	F	0	10	30	0	40
Total		**0**	**71**	**123**	**31**	**225**
Sargentos	M	0	17	51	32	100
	F	0	5	3	0	8
Total		**0**	**22**	**54**	**32**	**108**
Praças	M	0	9	0	0	9
	F	0	6	0	0	6
Total		**0**	**15**	**0**	**0**	**15**
Civis	M	0	0	4	7	11
	F	0	0	3	2	5
Total		**0**	**0**	**7**	**9**	**16**
TOTAL		***0***	***108***	***184***	***72***	***364***

Figura 2 – Distribuição por categorias dos elementos da amostra populacional

Fonte: (Autor, 2017)

2.3.1.2. Análise dos dados obtidos

Um aspeto importante para a investigação é mensurar quantitativa e qualitativamente as variáveis **V1** (nível de conhecimento), **V2** (nível de literacia), **V3** (nível de interesse) e **V4** (nível de importância). Para tal, recorremos à medida estatística da média, dando-lhes assim uma dimensão quantitativa. A conversão para a dimensão qualitativa, especialmente útil para a interpretação e conclusão, foi efetuada por convenção: quando o valor "média da

variável" é igual ou superior a quatro, corresponde ao nível qualitativo "nível alto/têm interesse/têm a perceção"; quando é inferior, corresponde qualitativamente ao inverso.

A racional que suporta esta convenção, prende-se com o intervalo de valores que a média das variáveis pode assumir, entre "um" e "cinco", correspondente aos limites das opções de respostas no questionário. Assim, uma média de valor "um" corresponde a um resultado completamente desfavorável; uma média de valor "cinco" corresponde a um resultado completamente favorável; as respostas intermédias correspondem ao valor "três", um nível mediano. Desta forma, por motivos de coerência e lógica matemática, adotámos que, quando o valor da média das variáveis é quatro ou superior, corresponde a um nível qualitativo "bom".

Passamos a explicar seguidamente como se calcula os valores de **V1**, **V2**, **V3** e **V4**. Para cada uma das perguntas do questionário foi calculada a média das respostas, uma vez aferido esse valor, foi calculada a média desses resultados, separadamente para cada secção do questionário. O valor da média de cada secção corresponde assim ao valor de cada uma das variáveis.

Passemos à análise dos resultados estatísticos obtidos, onde se inclui os dados relativos às frequências de respostas dadas aos questionários e os resultados das estatísticas descritivas efetuadas sobre esses dados, nomeadamente: a média, a mediana e a moda para as medidas de tendência central; a variância, o desvio de padrão e o coeficiente de variação para as medidas de dispersão; a assimetria e o achatamento para as medidas de forma; e o erro padrão da média para a medida de associação.

Das tabelas retira-se a média das variáveis: 3,72 para **V1**; 3,55 para **V2**; 3,74 para **V3** e 3,92 para **V4**. Em termos de medidas de dispersão, a mais significativa para esta análise é o desvio de padrão, indicando-nos que as respostas aos questionários não estão muito afastadas da média obtida. Os valores da assimetria comprova-nos que a distribuição é assimétrica e com um descaimento para a direita, corroborando os dados das médias. As medidas de associação indicam-nos que se existissem duas amostras da mesma população, a variabilidade das respostas não seria muito diferente da obtida.

A pergunta $P_{3.1}$ (se já recebeu formação específica em cibersegurança) teve 81,9% de respostas "Não".

A pergunta $P_{4.8}$ (forma preferencial para receber formação sobre matérias do ciberdomínio) teve 35,4% de respostas "*B-Learning*" e 29,1% de respostas "Formação presencial".

A pergunta $P_{5.2}$ (meio mais usado para aceder à Internet) teve 83% de respostas "*Smartphones*".

A pergunta $P_{5.7}$ (maior controlo no acesso à Internet por parte das autoridades estatais para garantir a segurança na mesma) teve 76,1% de respostas "Sim".

Outros três tipos de medidas estatísticas calculadas foram as medidas descritivas de associação (covariância e coeficientes de correlação de *Spearman* e de *Pearson*), e a regressão linear simples e múltipla. Para melhor esclarecimento sobre o cálculo e significado destas medidas, deve recorrer-se à leitura das notas explicativas existentes no **Apêndice E**.

Deste apêndice é importante reter que existe **correlação positiva** e **estatisticamente significativa** (valor-p < 0,05) entre os seguintes pares de variáveis: com **correlação moderada** as variáveis **V1/V2**, **V1/V3**, **V1/V4**, **V2/V3**, **V2/V4**, **V3/V4**, **$P_{4.1}$/V3**, **$P_{4.9}$/V3**, **$P_{4.7}$/$P_{4.2}$**, **$P_{2.1}$/$P_{4.3}$**, **$P_{4.7}$/$P_{4.9}$**; com **correlação forte** as variáveis **$P_{4.2}$/V3**, **$P_{4.7}$/V3**, **$P_{4.1}$/$P_{4.2}$**.

Quanto à regressão linear simples, podemos afirmar que somente **V1** é passível de ser explicada por outra variável, **V2**, em 47,3%. A equação matemática que estabelece essa relação é **$V1 = 1{,}23 + 0{,}7*V2$ ($R^2 = 0{,}473$)**.

Quando realizamos a regressão linear múltipla é possível determinar que as variáveis **V2**, **V3** e **V4** explicam a variável **V1** em 59,8%. A equação matemática que estabelece a relação é **$V1 = 0{,}03 + 0{,}428*V2 + 0{,}246*V3 + 0{,}318*V4$ ($R^2 = 0{,}598$)**.

Já as **V2**, **V3** e **V4** não são explicáveis em percentagem significativa através do método de regressão linear, ou seja, a previsão não produz resultados estatisticamente significativos.

Com base nos dados dos questionários, foram efetuados cálculos de inferência estatística, quer através da teoria de estimação (pontual e por intervalo de confiança), quer através da Teoria da Decisão. Por motivo de espaço e de precisão estatística, analisaremos apenas os resultados obtidos através da Teoria da Decisão, com recurso à técnica de Teste de Hipóteses. Esta consiste num processo de inferência estatística, através do qual é possível prever parâmetros da população.

O parâmetro populacional inferido foi a média das variáveis, tendo-se obtido os seguintes resultados: **V1**, **V2**, **V3**, **V4**, **$P_{2.1}$**, **$P_{4.3}$**, **$P_{4.5}$**, **$P_{4.6}$**, **$P_{4.7}$**, **$P_{4.9}$** e **$P_{5.9}$** com média populacional inferior a quatro; e **$P_{4.4}$** com média populacional superior a quatro.

Foram ainda construídas tabelas que permitissem fazer o cruzamento das variáveis **V1**, **V2**, **V3** e **V4**, com os elementos caracterizadores da amostra, tendo por referência o valor da média das variáveis.

Assim, analisando o comportamento das variáveis face à idade dos respondentes,

verificamos que não existe diferença significativa nas suas médias para os diferentes grupos etários.

Se fizermos a análise por género, verificamos que o valor médio de **V1** e **V4** é geralmente superior no género masculino do que no feminino, enquanto que **V2** e **V3** têm um valor médio aproximadamente igual em ambos os grupos.

Comparando as variáveis tendo por base a formação dos respondentes, verificamos que as médias são próximas da amostra em todos os níveis de formação, exceto nos respondentes com ensino básico onde a média é inferior.

Analisando por classes, verificamos que os valores médios das variáveis são próximas da amostra em todas as classes, exceto nos respondentes civis onde a média é inferior.

2.3.1.3. Contributos dos respondentes para a cibersegurança

A última pergunta do questionário visava recolher sugestões para melhorar a cibersegurança na FAP. A panóplia de sugestões recebidas foi analisada e elencada no **Apêndice F**. De forma resumida foram três as ideias chave para melhorar o nível de cibersegurança: **formação, sensibilização e controlo de acesso**.

2.3.2. Análise de dados das entrevistas

Foram efetuados os resumos das entrevistas, de acordo com a terceira etapa da análise de conteúdo (Guerra, 2006, p. 74), seguindo-se a análise categorial, segundo o modelo proposto por Guerra (2006, p. 79).

3. Interpretação de dados recolhidos

3.1. Interpretação de dados dos questionários

A interpretação dos resultados estatísticos incidirá sobre dois tipos de variáveis: as centrais ao estudo (**V1**, **V2**, **V3** e **V4**) e um conjunto de variáveis secundárias que permitem melhor enquadrar a problemática (a serem tratadas no ponto 3.1.5.).

3.1.1. Interpretação de **V1**: nível de conhecimento

O valor da média de **V1** foi 3,72, significando que na amostra, de acordo com o convencionado, o **nível de conhecimento em matéria de ciberespaço é baixo**.

Como vimos, existe uma correlação estatisticamente significativa de **V1** com **V2**, **V3** e **V4**, ou seja, o nível de conhecimento dos RH sobre o ciberespaço correlaciona-se e é

proporcional à literacia em cibersegurança, ao interesse em obter conhecimentos na área e à importância que dão à liberdade e segurança no ciberespaço.

Esta correlação pode ser expressa por equações resultantes do processo de regressão linear, verificando-se, para a regressão simples, que a percentagem de **V1** é explicável por **V2** em 47,3%.

Inferindo esta variável para a população, apuramos com um intervalo de confiança de 95%, que a média **V1** na população é inferior a quatro, ou seja, existe um **baixo nível de conhecimento em matéria de ciberespaço na população**.

Quanto ao comportamento de **V1** face ao género, verificamos que é superior no género masculino, provavelmente porque, de uma forma geral, os elementos masculinos na FAP desempenham funções mais relacionadas com tecnologias informáticas.

Outro aspeto apurado foi o baixo valor da variável em indivíduos com escolaridade baixa, donde se deduz uma causa-efeito direta.

3.1.2. Interpretação de **V2**: nível de literacia

O valor da média de **V2** obtido foi 3,55, indicando que na amostra o **nível de literacia relativamente às regras e procedimentos de cibersegurança é baixo**.

Verificamos que existe uma correlação estatisticamente significativa de **V2** com **V1**, **V3** e **V4**, indicando-nos que o nível de literacia em cibersegurança dos RH correlaciona-se e é diretamente proporcional ao conhecimento em matérias relativas ao ciberdomínio, ao interesse em obter conhecimentos nesta área e à importância dada à liberdade e segurança no ciberespaço.

Reproduzir essa correlação numa equação obtida pelo processo de regressão linear, simples ou múltipla, não produz resultados significativos, isto é, o maior ou menor nível de literacia em cibersegurança não é explicado pelas restantes variáveis numa percentagem relevante.

Inferindo **V2** para a população verificamos que, com um intervalo de confiança de 95%, esta possui um valor inferior a quatro, ou seja, existe um **baixo nível de literacia relativamente às regras e procedimentos de cibersegurança na população**.

O valor de **V2** nas diferentes categorias que caracterizam a amostra não apresenta grandes variações, exceto na categoria formação e classe, em que os respondentes com baixo nível de formação e da classe civis obtêm uma média mais baixa. O baixo nível de formação académica poderá ser o fator explicativo desse resultado, associado ao facto dos civis serem

os RH com menor formação.

3.1.3. Interpretação de **V3**: nível de interesse

O valor da média de **V3** obtido foi 3,74, indicando na amostra um **baixo nível de interesse na obtenção de conhecimentos nesta área**.

Verificamos existir uma correlação moderada, estatisticamente significativa, entre **V3** e as variáveis **V1**, **V2** e **V4**, o que significa que o nível de interesse em receber formação correlaciona-se, e é diretamente proporcional, ao nível de conhecimento, ao nível de literacia e ao nível de importância.

Contudo, não são relevantes os contributos de **V1**, **V2** e **V4** para a previsão de **V3** através da regressão linear, uma vez a percentagem em que o fazem é baixa.

Quanto à inferência de **V3** para a população verificamos, com um intervalo de confiança de 95%, que o seu valor é inferior a quatro, ou seja, que a população tem um **baixo nível de interesse na obtenção de conhecimento nesta área**.

Atentemos também à proximidade dos resultados de **V3** e $\mathbf{P_{4.7}}$, em que na segunda variável é questionado o interesse do respondente em receber formação nesta área. A média destas variáveis é 3,74 e 3,97 respetivamente, validando o resultado de **V3**. Apesar disso, o valor de $\mathbf{P_{4.7}}$ é próximo de quatro, convencionado como limite mínimo para considerar o nível de uma variável alto. Esta diferença poderá resultar de em $\mathbf{P_{4.7}}$ a pergunta ser colocada diretamente, enquanto em **V3** o mesmo resultado é obtido de forma indireta.

Já o comportamento de **V3** face às categorias caracterizadoras da amostra não apresenta grandes variações, exceto na categoria formação e classe, onde se verifica que os respondentes civis com baixo nível de formação apresentam uma média mais baixa. Este resultado estará associado à baixa escolaridade dos respondentes, assim como será decorrente das funções tecnologicamente menos exigentes que estes desempenham na FAP.

3.1.4. Interpretação de **V4**: nível de importância

O valor da média de **V4** obtida foi de 3,74, indicando na amostra a **atribuição de um baixo nível de importância à manutenção de um ciberespaço aberto e seguro**.

Verificamos existir uma correlação moderada, estatisticamente significativa, entre **V4** e as variáveis **V1**, **V2** e **V3**, o que significa que o nível de importância em receber formação correlaciona-se, e é diretamente proporcional, ao nível de conhecimento, de literacia e de interesse.

Contudo, não são relevantes os contributos de **V1**, **V2** e **V3** para a previsão de **V4** através da regressão linear, uma vez a percentagem em que o fazem é baixa.

Quanto à inferência de **V4** para a população verificamos, com um intervalo de confiança de 95%, que o seu valor é inferior a quatro, ou seja, que a população **atribui um baixo nível de importância à manutenção de um ciberespaço aberto e seguro**.

Quanto ao comportamento de **V4** face às categorias caracterizadoras da amostra não apresenta grandes variações, exceto na categoria sexo, formação e classe. Relativamente ao género, a média de **V4** é superior no género masculino, provavelmente porque, como no caso de **V1**, de uma forma geral, os elementos masculinos na FAP desempenham funções mais relacionadas com tecnologias informáticas, estando mais sensibilizados para estas matérias.

Verifica-se ainda, que os respondentes civis com baixo nível de formação, como nos casos anteriores, apresentam uma média mais baixa, possivelmente devido à baixa escolaridade e desempenho de funções tecnologicamente menos exigentes.

3.1.5. Outras interpretações

Considerações interpretativas do resultado inferencial de algumas variáveis (perguntas) do questionário:

$P_{2.1}$ – A população autoavalia-se com baixo nível de conhecimento em matérias do ciberespaço (converge com o resultado de **V1**).

$P_{4.3}$ – A população autoavalia-se com baixo nível de conhecimento sobre cibersegurança (converge com o resultado de **V2**).

$P_{4.4}$ – A população considera importante a existência de colaboradores com conhecimentos em cibersegurança (este resultado é contrário a **V3**, ou seja, consideram importante os colaboradores terem conhecimentos em cibersegurança, mas não manifestam interesse, na qualidade de colaboradores, receber essa formação – esta aparente contradição poderá dever-se à falta de motivação dos respondentes para receberem formação).

$P_{4.5}$ – A população classifica o nível de cibersegurança na FAP de baixo (esta perceção poderá resultar de situações e experiências quotidianas, ou da falta de ações/medidas desenvolvidas pela organização neste âmbito).

$P_{4.6}$ – A população estabelece fraca correspondência entre comportamentos de risco e falha nas regras de cibersegurança (é interessante o facto de a população classificar como baixo o nível de cibersegurança na FAP, contudo, isentam os elementos da organização de qualquer cota-parte de responsabilidade nessa situação, quando se sabe que parte das

fragilidades nesta área resulta de colaboradores incautos, ou seja, existe falta de segurança cibernética, mas essa é responsabilidade da própria "organização").

$P_{4.7}$ – A população tem interesse em receber formação sobre ciberespaço e cibersegurança (este resultado converge com o de **$P_{4.4}$**, mas é contrário a **V3**, por motivos que serão semelhantes aos apresentados para **$P_{4.4}$**).

$P_{4.9}$ – A população concorda em promover a adoção de uma cultura organizacional ativa de cibersegurança (este resultado reforça os dados obtidos anteriormente, indicativo da existência de uma predisposição positiva dos elementos da população para o desenvolvimento de um ambiente seguro e estável a nível cibernético).

$P_{5.9}$ – A população concorda que haja um maior controlo no acesso e conteúdos da Internet de forma a promover a cibersegurança (é um resultado contrário ao obtido em **$P_{5.7}$**, a diferença é que neste caso o controlo é efetuado pelo Estado, ou seja, tudo indica que não há oposição ao conceito, mas ao agente que o impõe).

3.2. Interpretação de dados das entrevistas

A última etapa da análise de conteúdo corresponde à interpretação, que tem por base a análise categorial.

3.2.1. Interpretação das respostas à primeira pergunta

A primeira pergunta procura recolher a opinião dos entrevistados quanto ao nível de conhecimento dos RH da FAP em relação às matérias do ciberespaço.

Com base na análise categorial, verificamos que as opiniões dos entrevistados não são unânimes nesta matéria. Para uns, admitem que o ciberespaço acarreta um conjunto de desafios aos quais a FAP não pode ficar indiferente e para os quais os seus RH estão cientes. Para outros, essa perceção não existe, especialmente no escalão superior, sendo prova disso a falta de investimento em recursos materiais e humanos neste domínio.

Assim, e apesar de se verificar uma certa influência das experiências pessoais nas respostas, a ideia geral transmitida é no sentido de que existe a perceção de uma nova realidade emergente e da reduzida preparação para lidar com ela.

3.2.2. Interpretação das respostas à segunda pergunta

A segunda pergunta procura recolher as opiniões quanto ao nível de literacia em cibersegurança dos RH da FAP.

Da análise efetuada, verificamos que as opiniões dos entrevistados não é, mais uma vez, unânime. A argumentação predominante admite que, os RH da FAP, não são conhecedores dos riscos reais resultantes de determinados comportamentos em rede. As respostas mais fundamentadas referem que são frequentes os comportamentos de risco dos utilizadores. Quanto aos motivos destes comportamentos, apontam a falta de formação e sensibilização em matéria de cibersegurança, assim como o excesso de permissões dadas aos utilizadores no acesso à Internet, através dos recursos tecnológicos da FAP.

3.2.3. Interpretação das respostas à terceira pergunta

A terceira pergunta procura recolher as opiniões quanto ao nível de interesse no tema ciberespaço e da predisposição dos RH da FAP para receber formação nesta área.

Da análise efetuada, verificamos que existe unanimidade nas respostas, ou seja, teria todo o interesse generalizar-se a formação em matéria de cibersegurança a todos os RH da FAP.

Quanto ao momento para o fazer, a opinião geral é que deverá ser durante a frequência da AFA (Academia da Força Aérea) e do CFMTFA (Centro de Formação Militar e Técnica da Força Aérea). Adicionalmente, deveria ser dada ao longo da carreira dos militares, através da formação contínua, extensível a todo o universo da FAP.

3.2.4. Interpretação das respostas à quarta pergunta

A quarta pergunta procura recolher as opiniões quanto ao nível de importância que os RH da FAP dão ao ciberespaço.

Da análise efetuada, verificamos que as opiniões são unânimes no reconhecimento da importância do ciberespaço na vida das pessoas e das organizações na atualidade, sendo necessário que este se mantenha aberto e seguro.

Nesse sentido, os entrevistados defendem maior restrição no acesso à rede através da rede da FAP, isto porque, o risco associado ao ciberespaço, o comportamento negligente dos utilizadores e a elevada dependência das tecnologias de informação, podem colocar em risco de funcionamento alguns sistemas da instituição. Uma vulnerabilidade que, só através do investimento na área, poderá ser colmatada ou controlada.

Assim, de forma a manter o ciberespaço um domínio seguro, especialmente para a FAP, seria inevitável aumentar o controlo e as restrições de acesso à Internet através das tecnologias de informação da FAP.

3.2.5. Síntese conclusiva

Os dados recolhidos das entrevistas carecem de alguma ponderação, isto porque, embora os entrevistados lidem diariamente com a problemática da cibersegurança e da ciberdefesa, os seus trabalhos não visam compreender a realidade comportamental dos RH da FAP. O contributo das suas opiniões para o nosso trabalho visa essencialmente a obtenção de uma perspetiva enquadradora da problemática.

Nesse sentido, a principal ideia a reter é que, apesar de se reconhecer no ciberespaço um desafio à segurança da organização, isso não se traduz em investimento direto na área.

Conclusões

O estudo que agora se conclui insere-se no corpo de conhecimentos das Ciências Militares. O seu desenvolvimento foi balizado em termos temporais, espaciais e conceptuais, de forma a atingir o objetivo principal e os objetivos secundários a que nos prepusemos. Começamos pela problematização do problema, traduzida na elaboração de uma pergunta de partida e respetivas perguntas derivadas, cujo modelo de análise passou pela elaboração de hipóteses.

Em termos metodológicos, este estudo tem uma perspetiva ontológica construtivista face à edificação da realidade, partindo de um posicionamento epistemológico positivista/empirista. Com recurso ao raciocínio hipotético-dedutivo e através do método de investigação quantitativo, efetuou-se um desenho de pesquisa tipo estudo de caso, com um horizonte temporal transversal. O método de investigação desenvolvido teve por base a proposta metodológica de Quivy e Campenhoudt, complementada, quando necessário, pela metodologia proposta pela NEP/ACA-010.

Da avaliação dos resultados obtidos na investigação, que teve por base o inquérito e a entrevista, foi-nos possível estimar o nível de preparação dos RH da FAP para lidar com os desafios associados ao ciberespaço, o que, consequentemente, permitiu-nos propor mecanismos para melhorar a cibersegurança na FAP.

Da interpretação dos resultados obtido foi-nos possível retirar ilações relativas a possíveis modalidades de ação que, se adotadas, são passíveis de melhorar a preparação desses RH. Para tal contribuíram as sugestões dadas nos questionários e que, por provirem dos utilizadores, poderão ter maior aceitação e utilidade.

O estudo permitiu-nos de igual forma ir ao encontro dos objetivos específicos propostos, tendo sido possível quantificar as seguintes variáveis: o nível de conhecimento em matérias relativas ao ciberespaço, através da determinação do parâmetro **V1**; caracterizar o comportamento dos RH da FAP quanto à sua adequabilidade aos procedimentos de cibersegurança, através da determinação do parâmetro **V2**; o nível de interesse em receber formação em matérias de ciberespaço, através da determinação do parâmetro **V3**; e, finalmente, o nível de importância atribuído à necessidade do ciberespaço ser um domínio livre e seguro, através da determinação do parâmetro **V4**.

A investigação visou determinar o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança. Nesse sentido, chegamos à conclusão de que estes, ao possuírem baixo nível de conhecimento em matéria de ciberespaço e baixo nível de literacia

em cibersegurança, não estão preparados para a conjuntura digital atual, nem para a progressiva "conectividade do todo".

Da problemática tratada no parágrafo anterior decorriam quatro questões secundárias, às quais também foi possível responder: determinamos o nível de conhecimento dos RH em matérias do ciberespaço (verificamos ser baixo); identificamos o nível de literacia em cibersegurança dos RH (verificamos ser baixo); vimos o nível de interesse dos elementos da FAP em receber formação nesta área (verificamos ser baixo); e finalmente, a investigação permitiu-nos aferir o nível de importância que os militares e civis da FAP dão a um ciberespaço aberto e seguro (os dados obtidos apontam para a atribuição de um baixo nível de importância).

No que se refere à validação das hipóteses sugeridas inicialmente, concluímos que:

Quanto à hipótese primeira, isto é, de que os RH da FAP têm um nível de conhecimento baixo em relação à temática do ciberespaço, verificamos que, com base no cálculo do parâmetro **V1**, estes possuem de facto um baixo nível de conhecimento nestas matérias. Este resultado permite-nos aferir que a nossa primeira hipótese foi desta forma confirmada.

Já a hipótese segunda, de que é expectável que os RH da FAP possuam um baixo nível de literacia no que se refere às regras de cibersegurança, verificamos que, com base no cálculo do parâmetro **V2**, estes possuem de facto um baixo nível de literacia em procedimentos e atividades de cibersegurança. Este resultado permite-nos aferir que a nossa segunda hipótese foi desta forma confirmada.

No que se refere à hipótese terceira, ou seja, a expectativa de que os RH da FAP tenham interesse na obtenção de conhecimentos adicionais nestas matérias, verificamos que, com base no cálculo do parâmetro **V3**, estes possuem um baixo nível de interesse em receber esta formação. Este resultado permite-nos aferir que a nossa terceira hipótese não foi confirmada, ou seja, a nossa terceira hipótese de investigação (**H3**) está errada.

Relativamente à hipótese quarta, ou seja, a expectativa de que os RH da FAP tenham a perceção da importância que assume a existência de um ciberespaço aberto e seguro, verificamos que, com base no cálculo do parâmetro **V4**, estes atribuem um baixo nível de importância a um ciberespaço com essas qualidades. Este resultado permite-nos aferir que a nossa quarta hipótese não foi confirmada, ou seja, a nossa quarta hipótese de investigação (**H4**) está errada.

Da investigação efetuada foi possível tecer as seguintes considerações relativamente

aos contributos que esta trouxe ao conhecimento.

De uma forma geral, contribuiu para definir o posicionamento dos RH da FAP em matérias relacionadas com o ciberespaço, assim como determinar o valor, importância e cuidado que estes indivíduos atribuem ao ciberespaço nas suas vidas quotidianas.

Este estudo veio permitir clarificar vários aspetos de importante relevo para a organização, nomeadamente a nível da sua segurança, isto é, cibersegurança. Para o cumprimento eficaz, eficiente e seguro das missões é inevitável, na presente atualidade, o recurso às tecnologias de informação. Este domínio está permanentemente presente e progressivamente mais difundido nas atividades diárias. Porém, é um ambiente cada vez mais complexo e perigoso, no qual o fator humano ainda é parte integrante e, na generalidade das vezes, e o elo mais fraco. Por este motivo, criar um retrato do posicionamento dos RH da FAP face a esta temática é importante, essencialmente para possibilitar, a partir daqui, desenvolver e construir um conjunto de ações e programas que permitam tornar a organização mais "cibercapaz".

Efetuadas as avaliações dos resultados obtidos à luz dos objetivos, da problemática e das hipóteses, vamos seguidamente tecer algumas recomendações e considerações de ordem prática, decorrentes da investigação realizada.

Assim, recomendamos que, dado que a FAP parece não possuir recursos humanos suficientemente preparados para lidar com os desafios da era digital, sejam desenvolvidos esforços na prevenção, traduzidos em três grandes áreas: na formação, no treino e na sensibilização.

Ainda relativamente à formação, de referir que, com base nos resultados do inquérito, aqueles que precisam de especial atenção neste domínio são os elementos do sexo feminino, os civis de uma forma geral e os elementos que possuem uma baixa formação académica.

Seria também importante que se desenvolvessem medidas de fiscalização da atividade individual na rede, ou seja, dos militares e civis quando estes utilizam os recursos tecnológicos da instituição. Paralelamente, sugere-se que se procedesse à alteração de algumas regras e procedimentos de acesso e utilização das tecnologias de informação, nos locais de trabalho.

Como complemento a estas recomendações, sugerimos que seja averiguada a viabilidade de implementação de algumas das sugestões feitas pelos respondentes dos questionários. Estas encontram-se explanadas no **Apêndice F**.

Posto isto, e com base nos estudos realizados, será ainda possível elaborar algumas considerações de ordem prática, com relevância para a compreensão da situação dos RH face a esta problemática.

Em primeiro lugar, constatamos através do estudo que, a esmagadora maioria da população da FAP nunca recebeu qualquer formação no âmbito da cibersegurança. Estes resultados são pouco animadores numa organização tecnológica como a FAP e num mundo digital como o atual, reforçando a ideia de que é perentório à organização investir nesta área.

A segunda consideração que gostaríamos de fazer, prende-se com a forma como os militares e civis da FAP gostariam de receber formação, se isso tivesse de acontecer. O resultado obtido pelo inquérito aponta para duas soluções, sendo aquela que obteve maior aprovação o ensino por "*B-Learning*" (35,4%), logo seguido da "Formação presencial" (29,1%). Assim, com base nestes resultados, se se optar por implementar programas de formação, será aconselhável ter em linha de conta estes resultados.

A terceira consideração prende-se com a constatação de que, a grande maioria dos elementos da FAP (83%), recorrem aos dispositivos móveis, especialmente o "*Smartphone*", para aceder à internet. Esta poderia ser uma via a explorar, caso se optasse pelos programas de formação através de "*B-Learning*", facilitando o estudo autónomo.

Por último, gostaríamos de referir que, uma maioria considerável dos RH da FAP concorda com o aumento das restrições no acesso à Internet e seus conteúdos, no sentido de aumentar o controlo da rede. Este aspeto pode ser um indicador a ter em consideração pelos decisores da organização, no caso de quererem mudar as políticas de acesso às tecnologias de informação na organização.

É importante ainda referir, que o desenvolvimento do estudo não ficou isento de limitações de ordem prática, donde se destacam dois aspetos fundamentais: por um lado, uma limitação de espaço, em termos do número de palavras disponíveis para desenvolver o trabalho; e por outro, uma limitação de ordem temporal, dado que o estudo teve de ser desenvolvido em seis meses, em simultâneo com as unidades curriculares do restante CPOS.

Por fim, terminaremos esta conclusão, apontando duas linhas de investigação passíveis de serem seguidas em estudos futuros, de forma a dar desenvolvimento ao trabalho que agora terminamos. Assim, e uma vez identificadas algumas limitações nesta área, seria útil investigar como outras Forças Aéreas aliadas estão a lidar com esta problemática e estabelecer pontes com a situação portuguesa, de forma a poder melhorar a situação na FAP; outro caminho que terá de ser trilhado nesta área, corresponde ao desenvolvimento de um

programa de formação em cibersegurança, ajustado aos diferentes grupos de RH da FAP e às funções que desempenham.

Bibliografia

Assembleia da República, 2009. *Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro* (Lei Nº 109/2009 de 15 deSetembro), Lisboa: Diário da Republica.

Assembleia da República, 2011. *Estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, de 8 de dezembro* (Decreto-Lei Nº 62/2011), Lisboa: Diário da Republica.

Assembleia da República, 2012. *Aprova a orgânica e o quadro de pessoal dirigente do GNS, estabelecendo as suas atribuições e competências* (Decreto-Lei Nº 3/2012), Lisboa: Diário da Republica.

Assembleia da República, 2014. *Aprova a orgânica do GNS, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança* (Decreto-Lei Nº 69/2014), Lisboa: Diário da Republica.

Assembleia da República, 2009. *Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro* (Lei Nº 109/2009), Lisboa: Diário da Republica, 15 Setembro.

Assembleia da República, 1998. *Lei da Proteção de Dados Pessoais. Transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995* (Lei Nº 67/98), Lisboa: Diário da República.

Brookson, C., Cadzow, S. *et al*, 2015. *Definition of Cybersecurity - Definition of Cybersecurity* [livro eletrónico] Atenas: European Union Agency for Network and Information Security. Disponível em: https://www.enisa.europa.eu/publications/definition-of-cybersecurity, [Acedido em 9 dez. 2016].

Bryman, A., 2012. *Social Research Methods.* 4 ed. Nova Iorque: Oxford University Press Inc..

Bryman, A. & Cramer, D., 2011. *Quantitative Data Analysis with IBM SPSS 17, 18 and 19: A Guide for Social Scientists.* Londres: Routledge.

Callegaro, M., Manfreda, K. & Vehovar, V., 2015. *Web Survey Method.* London: SAGE Publications Ltd..

Caton, J. L., 2013. Complexity and Emergence in Ultra-Tactical Cyberspace Operations. In: K. Podins, J. Stinissen & M. Maybaum, eds. *5th International Conference on Cyber Conflict (CyCon).* Tallinn: NATO CCD COE Publications, pp. 299-312.

Chew, K., Fontes, A. & Lavrakas, P., 2015. *Boosting Probability-Based Web Survey Response Rates via Nonresponse Follow-Up.* s.l., s.n.

Conselho de Ministros, 2013. *Conceito Estratégico de Defesa Nacional* (RCM Nº 19/2013), Lisboa: Diário da República.

Conselho de Ministros, 2015. *Estratégia Nacional de Segurança do Ciberespaço* (RCM Nº 36/2015), Lisboa: Diário da República.

Conselho Ministros, 2012. *Cria a Comissão da Republica Instaladora do Centro Nacional de Cibersegurança* (RCM Nº 42/2012), Lisboa: Diário da República.

Conselho de Ministros, 2013. *Aprova as linhas de orientação para a execução da reforma estrutural da defesa nacional e das Forças Armadas, designada por Reforma «Defesa 2020»* (RCM Nº26/2013), Lisboa: Diário da Republica.

Conselho da UE, 2009. *Programa de Estocolmo: Uma Europa aberta e segura que sirva e proteja os cidadãos,* Bruxelas: Conselho da Europa.

Conselho da UE, 2014. *EU Cyber Defence Policy Framework,* Bruxelas: Council of the European Union.

Couper, M. & Miller, P., 2008. Web Survey Methods. *Public Opinion Quarterly,* 72(5), pp. 831-835.

Departement of the Prime Minister and Cabinet, 2016. *Australia's Cyber Security Strategy.* [Em linha] Diponível em: https://cybersecuritystrategy.dpmc.gov.au [Acedido em 26 novembro 2016].

Department of Defense, 2015. *The Department of Defense Cyber Strategy,* Washington, DC: Department of Defense.

DICIO, 2016. *Dicionário Online de Português.* [Em linha] Disponível em: https://www.dicio.com.br/ [Acedido em 26 novembro 2016].

Dunn, M. A., 2001. The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method. *Information & Security,* Volume 7, pp. 145-158.

Dvorsak, A., 2013. *Development of cyber defense strategy in the framework of Slovenian strategic culture.* Brugge: s.n.

EMFA, 2016. *Relatório Anual de Atividades 2015,* Lisboa: EMFA.

FAP, 2008. *RFA 390-3 Política de Segurança da Informação e dos Sistemas de Informação e Comunicações na Força Aérea.* Alfragide: FAP.

FAP, 2009. *RFA 390-4 Organização e Estruturas de Segurança dos Sistemas de Informação e Comunicações da Força Aérea.* Alfragide: FAP.

FAP, 2011a. *RFA 391 Política de Gestão da Informação da Força Aérea.* Alfragide: FAP.

FAP, 2011. *RFA 390-6 Política de Ciberdefesa da Força Aérea.* Alfragide: FAP.

Godwin, J. B., Kulpin, A., Rauscher, K. F. & Yaschenko, V., 2013. *Critical Terminology Foundations 2 - The Russia-U.S. Bilateral on Cybersecurity.* Nova Iorque: EastWest Institute.

Guerra, I., 2006. *Pesquisa Qualitativa e Análise de Conteúdo. Sentidos e formas de uso.*. Lisboa: Principia.

IESM, 2015a. *NEP/ACA-018 Regras de Apresentação e Referenciação para os Trabalhos Escritos a Realizar no IESM.* Pedrouços: Instituto Universitário Militar.

IESM, 2015. *NEP ACA-010 Trabalhos de Investigação.* Pedrouços: Instituto Universitário Militar.

Janczewski, L. & Colarik, A. M., 2012. Establishing Cyber Warfare. *Jornal of Strategic security*, Primavera, 5(1), pp. 31-48.

Kissel, R., 2013. *Glossary of Key Information Security terms,* Gaithersburg: National Institute of Standards and Technology.

Klimburg, A., 2012. *National Cyber Securit y Framework Manual.* Tallinn: NATO CCD COE Publ icat ion.

Leandro, J. E. G., 2007. O Estado, o Cidadão e a Segurança. Novas soluções para um novo paradigma. *Segurança e Defesa,* fevereiro, pp. 12-19.

Marconi, M. & Lakatos, E., 1990. *Técnicas de Pesquisa.* 2ª ed. revista e apliada ed. São Paulo: Editora Atlas S.A..

Maria, M. F., 2015. *A Cultura de Segurança na Força Aérea.* Lisboa: Instituto Militar Universitário.

Maroco, J., 2003. *Análise Estatística.* 2ª Edição ed. Lisboa: Edições Sílabo.

Moser, C. & Kalton, G., 1971. *Survey Methods in Social Investigation.* Londres: Heinemann.

Ministério da defesa Nacional, 2014. *Diretiva Ministerial de Planeamento de Defesa Militar* (Despacho Nº 11400/2014 MDN), Lisboa: Diário da Republica, 2ª Série, 11 Setembro, p. 2014.

Ministério da defesa Nacional, 2013. *Determina a publicação da diretiva iniciadora com a orientação política para a ciberdefesa* (Despacho Nº 13692/2013 MDN), Lisboa: Diário da Republica.

Oxford Living Dictionaries, 2016. *https://www.oxforddictionaries.com/.* [Em linha] Disponível em: https://en.oxforddictionaries.com/definition/doctrine [Acedido em 26 Novembro 2016].

Parlamento Europeu, 2013. *Estratégia da UE para a cibersegurança: um ciberespaço aberto, seguro e protegido.* Beuxelas: União Europeia.

Priberam Dicionário, 2016. *Priberam Dicionário.* [Em linha] Disponível em: http://www.priberam.pt [Acedido em 26 Novembro 2016].

Quivy, R. & Campenhoudt, L. V., 2005. *Manual de Investigação em Ciências Sociais.* 4 ed. Lisboa: Gradiva.

Ronald, F. D., 2008. Sampling Methods for Web and E-mail Surveys. *The SAGE Handbook of Online Research Methods,* pp. 195-217.

Santos, G., s.d. *Cálculo amostral: calculadora on-line.* [Em linha] Disponível em: http://www.calculoamostral.vai.la [Acedido em 10 janeiro 2017].

Santos, L. *et al*., 2015. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação.* Lisboa: Instituto de Estudos Superiores Militares.

Schmitt, M. N., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridg University Press.

Strategy Department, 2014. *Cyber Security Strategy for Defence,* Brussel: Belgian Joint Staff, Strategy & International Relations Department.

UE, 2006. *Programa Europeu de Proteção das Infraestruturas Críticas,* Bruxelas: União Europeia.

United States Department of Defense, 2011. *Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act Fiscal Year 2011, Secção 934.* United States Department of Defense ed. Washington: United States Department of Defense.

White House, 2011. *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World.* White House ed. Washington: White House.

Apêndice A — Mapa conceptual

SECÇÃO A: Conhecimento do ciberespaço como dimensão do conflito

Tabela Apd A-1 – SECÇÃO A: Conhecimento do ciberespaço como dimensão do conflito

Pergunta de partida	Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Indicadores	Variáveis	Instrumentos
PP: Qual o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança?	**PD1**: Qual o nível de conhecimento dos RH da FAP relativamente ao ciberespaço como nova dimensão do conflito?	**H1**: Sendo, o ciberespaço como dimensão no conflito, um tema recente e complexo, então, é expectável que os RH da FAP tenham um nível de conhecimento baixo relativamente a esta temática.	Ciberespaço	Ciberguerra	Estado que penetra a rede de outro Estado para causar danos ou impedir o acesso a esta	**V1**: Nível de conhecimento	Questionário e Entrevistas Estruturadas
				Ciberataque	Ações realizadas no ciberespaço cujo principal objetivos é causar danos ou a denegação de serviços *on-line* do visado no ataque		
				Ciberameaça	Funcionários insatisfeitos, *hackers*, *crackers*, espiões, cibercriminosos, *hacktivistas*, terroristas, Estados		
				Cibercrime	Uso de computadores e de redes para violar a lei		
				Ciberdefesa	Conjunto de ações desenvolvidas, ou mecanismos implementados, que visam prevenir, detetar, neutralizar e recuperar de ciberataques realizados através da Internet ou outras redes		
				Infraestrutura Crítica Nacional	Infraestruturas essenciais para o funcionamento regular da economia e da sociedade		
			Doutrina	Constituição da República Portuguesa	Artigo Nº 272 – Polícia Título X – Defesa Nacional (Arts. Nº 273 a 276)		
				Lei Nº 109/2009 de 15 de setembro	Lei do Cibercrime		
				Resolução da Assembleia da República Nº 88/2009 de 15 de setembro	Aprova a Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001		
				Lei n.º 59/2015 de 24 de junho	Primeira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna		
				Decreto-Lei Nº 03/2012 de 16 de janeiro	Governo reestabelece o Gabinete Nacional de Segurança		
				Decreto-Lei Nº 69/2014 de 09 de maio	Segunda alteração à lei orgânica do Gabinete Nacional de Segurança e à criação, instalação e operacionalização de um Centro Nacional de Cibersegurança		
				RCM Nº 05/90	Aprova as Instruções Sobre a Segurança Informática		
				RCM Nº 7-A/2015	Aprova a Estratégia Nacional de Combate ao Terrorismo		
				RCM Nº 36/2015	Aprova a Estratégia Nacional de Segurança do Ciberespaço		
				Conceptualização	Conceito Estratégico de Defesa Nacional		
				PEMGFA/CSI/004 de 14 fev 2005	EMGFA - Organização e Normas de Segurança nos Sistemas de Informação e Comunicações Conjuntos		
				PEMGFA/CSI/301 de 23 set 2008	EMGFA - Estabelecer a estrutura orgânica, normas e procedimentos para garantir a capacidade de resposta a incidentes de segurança informática das Forças Armadas		
				União Europeia	Decisão-Quadro 2005/222/JAI – Relativa a Ataques Contra os Sistemas de Informação		
				União Europeia	*EU Cyber Defence Policy Framework*, adotado pelo Conselho da Europa em 18 novembro de 2014		
				União Europeia	*EU cybersecurity initiatives: working towards a more secure online environment*		
				OTAN	Declaração da Cimeira de Gales sobre Ciberdefesa		
			Indefinição	Fronteiras no ciberespaço	Não são definíveis		
				Motivações de um ciberataque	Estratégicas; Criminosas; Políticas; Ideológicas; Económicas; Intelectuais		
				Quantificação dos Danos Causados por um ciberataque	A nível do bem-estar social, das infraestruturas críticas, do sistema económico		
				Atacante	Estados; Organizações Terroristas; Grupo de *hackers* organizados; Grupos de *hackers* não organizados; Indivíduos; Crime Organizado		

				Tratados Internacionais sobre conflitos no ciberespaço	Não há nenhum tratado internacional que contemple concretamente esta matéria		
				Lei Internacional	Tribunal Internacional de Justiça: lei sobre conflitos armados aplica-se a todo o uso da força, independentemente das armas usadas. Tribunal Internacional Permanente de Justiça: atos não proibidos pela lei internacional são na sua generalidade permitidos		
				Aplicação da Lei Internacional	Apesar de não existirem tratados ou acordo sobre as operações militares no ciberespaço, isso não desresponsabiliza os Estados de cumprirem com as normas e princípios aplicáveis às ciberoperações, nomeadamente no que se refere ao *jus ad bellum* e ao *jus in bello*		
				Leis Nacionais	Compete a cada Estado criar legislação relativa ao cibercrime		
				Ciberguerra	EUA: conflito armado conduzido por ciberarmas RÚSSIA: não tem uma definição de ciberguerra CHINA: operações de guerra em rede e ataques cibernéticos		
			Complexidade	Ciberarmas	Código informático complexo e de difícil compreensão e deteção		
				Criação de Ciberarmas	Custos muito reduzidos na sua produção e passíveis de serem criadas, testadas e lançadas em segredo		
				Atacante	Muito difícil de identificar a origem do atacante, se é entidade estatal ou não-estatal		
				Dimensão	Fácil acesso à rede, número de indivíduos a interagir com a rede, número de interligações entre redes		

Fonte**: (Autor, 2017)**

SECÇÃO B: Conhecimento no domínio da cibersegurança

Tabela Apd A-2 – SECÇÃO B: Conhecimento no domínio da cibersegurança

Pergunta de partida	Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Indicadores	Variáveis	Instrumentos
PP: Qual o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança?	**PD2**: Qual o nível de literacia em cibersegurança dos RH da FAP?	**H2**: Sendo que, os aspetos a que é dada maior relevância a nível de segurança na interação com a rede são as palavras-chave e os "vírus informáticos", então, é expectável que os RH da FAP possuam um baixo nível de literacia no que se refere às regras e procedimentos fundamentais de cibersegurança.	Redes de computadores	Internet	*World Wide Web*	**V2**: Nível de literacia	Questionário e Entrevistas Estruturadas
				Intranet	Força Aérea Portuguesa		
			Interação com a Rede	Computadores	Em casa para fins pessoais e/ou profissionais; na FAP para fins profissionais		
				Tablet	A qualquer momento para fins pessoais e/ou profissionais		
				S*martphone*	A qualquer momento e essencialmente para fins pessoais		
			Cibersegurança	Tecnológica	A capacidade de proteger ou defender o uso do ciberespaço de ciberataques		
				Processos			
				Práticas			
			Ciberarmas	Espionagem Cibernética	*Malware Flamer*		
				Roubo de certificados digitais e atacar sistemas de controlo industrial	*Malware Duqu*		
				Ataque ao sistema operacional SCADA da Siemens	*Malware Stuxnet*		
				Capturar senhas e números de cartão de crédito	*Malware Key logger*		
				Apaga os dados do	*Malware Wiper*		

				disco rígido ou similares de computador com o *Microsoft Windows*			

Fonte**: (Autor, 2017)**

SECÇÃO C: Interesse dos militares e civis da FAP sobre o ciberespaço e a sua predisposição para receberem formação nesta área

Tabela Apd A-3 – SECÇÃO C: Interesse dos militares e civis da FAP sobre o ciberespaço e a sua predisposição para receberem formação nesta área

Pergunta de partida	Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Indicadores	Variáveis	Instrumentos
PP: Qual o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança?	**PD3**: Qual o nível de interesse no tema ciberespaço e de predisposição dos RH da FAP para receberem formação na área?	**H3**: Sendo o ciberespaço uma temática tão presente na vida atual, então, é expectável que os RH da FAP tenham interesse na obtenção de mais conhecimentos nesta área.	Ciberespaço na vida quotidiana	Pessoal	Redes sociais, *Cloud* (*Dropbox*, *Spotify*), Notícias, Correspondência eletrónica, *Home Banking* (…)	**V3**: Nível de interesse	Questionário e Entrevistas Estruturadas
				Institucional	Correspondência eletrónica, Acesso a base de dados e Serviços Institucionais		
			Ensino	Atualidade	Cibersegurança e ciberdefesa são áreas das FFAA que só agora começam a ser desenvolvidas em Portugal		
				Utilidade a nível pessoal	Proteção de dados e informação pessoal, assim como dos seus dispositivos eletrónicos no acesso privado à rede		
				Utilidade a nível profissional	Proteção de dados e informação institucional, assim como da rede, servidores e os dispositivos eletrónicos da FAP		
				Perspetiva futura	É expectável que as questões de cibersegurança e ciberdefesa venham a adquirir cada vez maior importância com a proliferação das ciberameaças e ciberataques		

Fonte**: (Autor, 2017)**

SECÇÃO D: Importância do ciberespaço para os militares e civis da FAP

Tabela Apd A-4 – SECÇÃO D: Importância do ciberespaço para os militares e civis da FAP

Pergunta de partida	Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Indicadores	Variáveis	Instrumento
PP: Qual o grau de preparação dos RH da FAP para atuarem no ciberespaço em segurança?	**PD4**: Qual o nível de importância que os RH da FAP dão ao ciberespaço comparativamente com outras dimensões do conflito?	**H4**: Sendo a ligação à rede uma realidade vincada nas sociedades ocidentais atuais, então, é expectável que os RH da FAP tenham a perceção da importância em manter o ciberespaço aberto e seguro, à semelhança das dimensões terrestre, aérea e marítima.	Conectividade	Carro	Ligação à *World Wide Web*	**V4:** Nível de importância	Questionário e Entrevistas Estruturadas
				Tablets			
				S*martphones*			
				Computadores			
				Relógios			
				Comboios			
				Aeronaves			
				Barcos			
				Edifícios			
			Ciberespaço aberto e seguro	Segurança	*Home Banking*		
				Confidencialidade	Troca de mensagens		
				Privacidade	Fotografias e Vídeos		
				Acesso	Consulta livre a *sites* e bases de dados		

Fonte: (Autor, 2017)

Apêndice B — Glossário de termos

Ciberespaço:
É um meio eletrónico através do qual a informação é criada, transmitida, recebida, processada e apagada (Godwin, *et al*., 2013, p. 17).
Ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e do espectro eletromagnético, para armazenar, modificar, e trocar informação usando redes de computadores (Schmitt, 2013, p. 58).
O ambiente global criado pela interligação de computadores e sistemas de informação. O ciberespaço incluí redes de computadores reais e virtuais, sistemas computacionais e dados digitais (Strategy Department, 2014, p. 18).

Doutrina:
É a codificação, de uma ou de um conjunto, de crenças e princípios, ensinados ou transmitidos, sobre um determinado ramo do conhecimento ou sistema de crenças (Oxford Living Dictionaries, 2016).

Indefinição:
Estado ou qualidade de algo que não é exato ou claro (Priberam Dicionário, 2016). Podem ser palavras, signos ou significados (Oxford Living Dictionaries, 2016).

Complexidade:
É uma qualidade do que é complexo, ou seja, de algo que é de difícil compreensão, abrangendo um vasto conjunto de elementos ou aspetos distintos, cujas múltiplas formas, materiais e/ou imateriais, assumem relações de interdependência num nexo comum (Priberam Dicionário, 2016; Oxford Living Dictionaries, 2016; DICIO, 2016).

Redes de computadores:
Uma estrutura de informação criada para permitir aos computadores trocarem dados. A infraestrutura pode ser ligada por fios, sem fios ou uma mistura de ambos (Schmitt, 2013, p. 211).

Interação com a rede:
Agregado de indivíduos, organizações e/ou sistemas, que recolhem, processam ou disseminam informação, onde também se inclui a própria informação (Kissel, 2013, p. 93).

Cibersegurança:
A capacidade de proteger ou defender o uso do ciberespaço de ciberataques (Kissel, 2013, p. 58).
É uma propriedade do ciberespaço e uma habilidade para resistir a ameaças intencionais e/ou não intencionais, de responder e de recuperar (Brookson, *et al*., 2015, p. 33).

Ciberarmas:
Software, *firmware* ou *hardware* desenhado ou aplicado para causar danos através do ciberdomínio (Godwin, *et al*., 2013, p. 56).

Ciberespaço na vida quotidiana:
Conectividade das pessoas à rede, permitindo-lhes a utilização de ferramentas das tecnologias da informação e da comunicação, preferencialmente num ambiente digital seguro e fiável que seja concebido para garantir a proteção e a preservação das liberdades e o respeito dos direitos fundamentais em linha e que neles se baseie, em particular no que se refere ao direito à vida privada e à proteção dos dados (Parlamento Europeu, 2013, p. 3).

Ensino:
Programas de formação que visam sensibilizar, promover e melhorar as competências e a educação, em particular no que diz respeito à integração da segurança pessoal nos programas curriculares em matéria de literacia digital desde muito cedo, a fim de fomentar a sensibilização para os desafios relativos à proteção das redes e dos sistemas de informação. A educação para a cibersegurança contribui para a consciencialização das ameaças informáticas, incentivando assim uma utilização responsável do ciberespaço, e para o aumento da oferta de competências no domínio da cibersegurança (Parlamento Europeu, 2013, p. 4).

Conectividade:
Os sistemas de redes e de informação estão profundamente interligados e têm um caráter global, transcendendo as fronteiras nacionais. Os serviços em linha são uma força vital da Internet, beneficiando tanto os cidadãos como o setor público e o setor privado (Parlamento Europeu, 2013, p. 6).

Ciberespaço aberto e seguro:
Os ciberdesafios não cessam de aumentar e constituem uma grande ameaça à segurança, à estabilidade e à prosperidade económica, do setor público, do setor privado e da comunidade em geral. O ciberespaço e a cibersegurança devem ser um dos pilares estratégicos das políticas de segurança e de defesa, sendo essencial garantir que o ciberespaço permaneça aberto à livre circulação das ideias e da informação e à liberdade de expressão (Parlamento Europeu, 2013, p. 1).

Apêndice C — Processo metodológico subjacente à construção das perguntas dos questionários/entrevista

SECÇÃO 1: Perfil do Inquirido

Tabela Apd C-1 – SECÇÃO 1: Perfil do inquirido

Identificador	Questão
$P_{1.1}$	Classe a que pertence: A) Oficiais; B) Sargentos; C) Praças; D) Civis.
$P_{1.2}$	Sexo: A) Masculino; B) Feminino.
$P_{1.3}$	Grupo etário: A) 20 anos ou menos; B) 21-35 anos; C) 36-50 anos; D) Mais de 50 anos.
$P_{1.4}$	Formação académica: A) Doutoramento/Mestrado; B) Licenciatura/Pós-Graduação/Bacharelato; C) Ensino Técnico-Profissional; D) Ensino Secundário; E) 1º, 2º ou 3º Ciclo do Ensino Básico.

Fonte: (Autor, 2017)

SECÇÃO 2 (SECÇÃO A): Conhecimento do ciberespaço como uma dimensão do conflito

Tabela Apd C-2 – SECÇÃO 2: Conhecimento do ciberespaço como uma dimensão do conflito

Pergunta Derivada	Hipótese	Conceito	Dimensão	Id.	Questão
PD1: Qual o nível de conhecimento dos RH da FAP relativamente ao ciberespaço como nova dimensão dos conflitos?	**H1**: Sendo o ciberespaço como dimensão do conflito, uma realidade ainda incipiente no seu desenvolvimento conceptual e doutrinário, muito à conta da complexidade técnica e desacordo relativo aos conceitos que o caracterizam, então, é expectável que uma parte importante dos RH da FAP tenham um nível de conhecimento doutrinário e conceptual relativamente baixo.	Ciberespaço	-	$P_{2.1}$	De 1 (Desconhecimento total) a 5 (Conhecimento especializado), classifique o seu nível de conhecimento em matérias relacionadas com o ciberespaço.
			Ciberguerra	$P_{2.2}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre a palavra ciberguerra e a frase "Escalada do ciberconflito entre Estados, no qual são desencadeados ciberataques por atores estatais contra ciberinfraestruturas, como parte da campanha militar"[1].
			Ciberataque	$P_{2.3}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito ciberataque e a seguinte frase "Ciberoperação, ofensiva ou defensiva, da qual é razoavelmente expectável resultar o ferimento ou a morte de pessoas e estragos ou destruição de objetos"[2].
			Ciberameaça	$P_{2.4}$	De 1 (Nenhuma gravidade) a 4 (Extremamente grave) que nível de gravidade atribui à disseminação de *software* malicioso (*malware*) nas redes informáticas portuguesas[3].
			Cibercrime	$P_{2.5}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito cibercrime e as seguintes ações: A) Intercetar dados informáticos; B) Aceder a sistemas informáticos sem autorização; C) *Phishing*; D) Sabotagem informática; E) Provocar danos em programas ou dados informáticos; F) Assédio *online*; G) Invasão de privacidade; H) Perseguição virtual.
			Ciberdefesa	$P_{2.6}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito ciberdefesa e a seguinte frase "capacidades organizadas para proteger, mitigar e rapidamente recuperar dos efeitos de um ataque"[4].
			Infraestrutura Crítica Nacional	$P_{2.7}$	De 1 (Nenhuma ameaça) a 5 (Ameaça extrema), que nível de ameaça a Internet representa para as Infraestruturas Críticas Nacionais. (Sistemas e recursos físicos ou virtuais sob a jurisdição de um Estado que são tão vitais que a sua inutilização ou destruição pode debilitar a segurança, economia, saúde publica, proteção e o meio ambiente de um Estado[5], ex: Rede Elétrica Nacional).
		Doutrina	Constituição da Republica Portuguesa	$P_{2.8}$	De 1 (Discordo totalmente) a 5 (Concordo totalmente), qual o seu nível de correspondência com a seguinte frase: "Quando no artigo nº 275, alínea 1) da Constituição da República Portuguesa diz que 'Às Forças Armadas incumbe a defesa militar da República', está implícita a defesa militar no ciberespaço, que se assume assim como uma dimensão no conflito".
		Indefinição	Atacante	$P_{2.9}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito de "atacante" num ciberconflito e os seguintes atores: Estados, Funcionários Insatisfeitos e Hactivistas.
		Complexidade	Ciberarmas	$P_{2.10}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito ciberarma e os seguintes termos: *Stuxnet* e *Flame*.

Fonte: (Autor, 2017)

[1] (Godwin, *et al*., 2013, p. 32)
[2] (Schmitt, 2013, p. 92)
[3] (Department of Defense, 2015, p. 9)
[4] (Godwin, *et al*., 2013, p. 47)
[5] (Schmitt, 2013, p. 211)

SECÇÃO 3 (SECÇÃO B): Conhecimento no domínio da cibersegurança

Tabela Apd C-3 – SECÇÃO 3: Conhecimento no domínio da cibersegurança

Pergunta Derivada	Hipótese	Conceito	Dimensão	Id.	Questão
PD2: Qual o nível de literacia em cibersegurança dos RH da FAP?	**H2**: Sendo que, nas interações quotidianas com a rede e com os dipositivos de acesso à rede, os principais fatores críticos com que os utilizadores são confrontados a nível de cibersegurança são as palavras-chave e vírus informáticos, então, é possível que os RH da FAP desconheçam um conjunto elementar de regras e procedimentos, considerados fundamentais, para garantirem a segurança no ciberespaço, não só a nível pessoal como institucional.	Cibersegurança	Tecn/Pro/Pra	$P_{3.1}$	Já recebeu formação específica, dentro ou fora da FAP, sobre segurança no ciberespaço (cibersegurança)? A) Sim; B) Não.
		Redes de computadores	Internet	$P_{3.2}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre os "grandes dados" (quantidades colossais de dados resultantes da utilização massiva das tecnologias de informação) e uma redução na cibersegurança.
			Intranet	$P_{3.3}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre "engenharia social"[6] e uma redução na cibersegurança. (Engenharia Social: Tipo de fraude social que explora as fragilidades psicológicas do ser humano, para recolher informações e cometer fraudes.)
		Interação com a Rede	*Tablet*	$P_{3.4}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o acesso a uma rede *Wi-Fi* aberta e a necessidade de o fazer através de uma RPV (Rede Privada Virtual) para proteger a comunicação.
			S*martphone*	$P_{3.5}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre as autorizações dadas durante a instalação de aplicações num *smartphone* e a segurança dos dados e do dispositivo.
		Cibersegurança	Tecnológica	$P_{3.6}$	De 1 (Nunca acontece) a 5 (Acontece sempre), com que frequência um ciberataque contra uma organização tem origem nos seus próprios colaboradores[7].
			Processos	$P_{3.7}$	De 1 (Nunca acontece) a 5 (Acontece sempre), com que frequência um ciberataque contra uma organização, com origem nos seus próprios colaboradores, resultou de uma ação inconsciente[8].
			Práticas	$P_{3.8}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre a existência de *botnets* (redes de computadores infetados), ciberataques do tipo DDoS (*Distributed Denial-of-Service*) e a sua cibersegurança como utilizador da Internet.
		Ciberarmas	Espionagem Cibernética	$P_{3.9}$	Um recente método de Ciberataque a privados e organizações tem por base o *ransomware* (*malware* que restringe o acesso aos sistemas informáticos ou aos dados). De 1 (Nada grave) a 5 (Extremamente grave) qual o grau de gravidade que atribui à dispersão deste *malware* nos computadores da FAP.
			Capturar senhas e números de cartão de crédito	$P_{3.10}$	De 1 (Nenhuma correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre o conceito de *phishing* e a sua cibersegurança como utilizador de tecnologias da comunicação. [9]

Fonte: (Autor, 2017)

SECÇÃO 4 (SECÇÃO C): Interesse dos militares e civis da FAP sobre o ciberespaço e a sua predisposição para receberem formação nesta área

Tabela Apd C-4 – SECÇÃO 4: Interesse dos militares e civis da FAP sobre o ciberespaço e a sua predisposição para receberem formação nesta área

Pergunta Derivada	Hipótese	Conceito	Dimensão	Id.	Questão
PD3: Qual é o nível de interesse no tema Ciberespaço e de predisposição dos RH da FAP para receberem formação nesta área?	**H3**: Sendo o ciberespaço uma temática tão presente na vida quotidiana de hoje em dia, quer a nível pessoal, quer a nível institucional, então, é expectável que os RH da FAP tenham interesse na obtenção de conhecimentos nesta área.	Ciberespaço na vida quotidiana	Pessoal	$P_{4.1}$	De 1 (Nenhum interesse) a 5 (Extremo interesse) qual o seu nível de interesse na evolução tecnológica, numa perspetiva de utilização do *hardware* (ex: *smartphones*, *tablets*, carros, relógios).
			Institucional	$P_{4.2}$	De 1 (Nenhum interesse) a 5 (Extremo interesse) qual o seu nível de interesse na evolução tecnológica, numa perspetiva do estudo e aprendizagem de conhecimentos nesta área.
				$P_{4.3}$	De 1 (Desconhecimento total) a 5 (Conhecimento especializado), classifique o seu nível de conhecimento em matérias relacionadas com procedimentos de cibersegurança.
				$P_{4.4}$	De 1 (Nenhum interesse) a 5 (Extremo interesse) como avalia o interesse para a FAP em possuir colaboradores com bons conhecimentos em matéria de cibersegurança.
				$P_{4.5}$	De 1 (Totalmente inseguro) a 5 (Totalmente seguro), como qualifica o nível de cibersegurança na FAP.
		Ensino	Atualidade	$P_{4.6}$	Considere as seguintes ações: A) Utilização de *pen drive* pessoal em computadores da FAP; B) Abrir um *link* suspeito numa mensagem de correio eletrónico pessoal, num computador da FAP; C) Utilizar um computador da FAP para aceder a redes sociais como o *youtube*; D) Instalar *software* num computador da FAP sem prévia autorização das entidades competentes. De 1 (Nenhuma

[6] (Godwin, *et al*., 2013, p. 31)
[7] (Godwin, *et al*., 2013, p. 31)
[8] (Godwin, *et al*., 2013, p. 32)
[9] (Godwin, *et al*., 2013, p. 33)

					correspondência) a 5 (Total correspondência), que nível de correspondência estabelece entre estas ações e a violação das regras básicas de cibersegurança.
			Utilidade a nível pessoal	$P_{4.7}$	De 1 (Nenhum interesse) a 5 (Extremo interesse) qual o seu nível de interesse em receber formação específica sobre o tema ciberespaço e cibersegurança.
			Utilidade a nível profissional	$P_{4.8}$	Se tivesse de receber formação em matérias relacionadas com o ciberespaço (ex: ciberdefesa e cibersegurança), qual das seguintes formas de organização da formação preferia: A) *E-Learning* (ensino não presencial); B) Formação presencial; C) *B-learning* (parte em *E-Learning* e parte em sala de aula); D) Formação em contexto de trabalho.
			Perspetiva futura	$P_{4.9}$	De 1 (Discordo totalmente) a 4 (Concordo totalmente), quanto concorda com esta frase: Devemos "promover a adoção de uma cultura organizacional ativa de cibersegurança, criando mecanismos de melhoria contínua dos níveis de segurança pessoal e organizacional no ciberespaço"[10].

Fonte: (Autor, 2017)

SECÇÃO 5 (SECÇÃO D): Importância do ciberespaço para os militares e civis da FAP

Tabela Apd C-5 – SECÇÃO 5: Importância do ciberespaço para os militares e civis da FAP

Pergunta Derivada	Hipótese	Conceito	Dimensão	Id.	Questão
PD4: Qual o nível de importância que os RH da FAP dão ao ciberespaço comparativamente com outras dimensões do conflito?	**H4**: Sendo a vida em rede e a conectividade das coisas uma realidade cada vez mais vincada nas sociedades ocidentais, então, é natural que os RH da FAP tenham a perceção de quanto a manutenção de um ciberespaço aberto e seguro, seja importante para o normal funcionamento de uma sociedade moderna.	Conectividade	Carro, *Tablets*, *Smartphones*, Computadores, Relógios, etc…	$P_{5.1}$	De 1 (Nenhuma importância) a 5 (Extrema importância), qual o nível de importância do ciberespaço na sua vida quotidiana (no acesso a bens e serviços na Internet).
				$P_{5.2}$	Das opções seguintes, indique APENAS TRÊS daquelas que utiliza com mais frequência para aceder à Internet: A) *Smartphones*; B) Computador; C) *Tablet*; D) Carro; E) Relógio; F) Comboio; G) Avião; H) Barco.
				$P_{5.3}$	De 1 (Discordo totalmente) a 5 (Concordo totalmente), quanto concorda com esta frase: "A Internet começou por ser uma rede de computadores, depois, passou a ser considerada uma rede de pessoas e, num futuro próximo, será uma rede das coisas (qualquer objeto)".
		Ciberespaço aberto e seguro	Segurança	$P_{5.4}$	De 1 (Nenhum impacto) a 5 (Extremo impacto), qual o nível de impacto nas sociedades ocidentais se, por algum motivo, amanhã deixasse de ser possível aceder à Internet.
				$P_{5.5}$	De 1 (Nenhuma importância) a 5 (Extrema importância), que nível de importância atribui à manutenção da segurança no ciberespaço (ex: privacidade das suas mensagens).
			Confidencialidade	$P_{5.6}$	Na FAP, o acesso à Intranet (Internet) é um dado incontornável. De 1 (Nenhum impacto) a 5 (Extremo impacto), qual o nível de impacto dessa dependência na organização militar.
			Privacidade	$P_{5.7}$	Concorda com um acesso mais restrito e regulamentado, de forma a garantir maior segurança na Internet? A) Sim; B) Não.
			Acesso	$P_{5.8}$	De 1 (Nenhuma importância) a 5 (Extrema importância), que nível de importância atribui à Internet como forma de garantir os direitos de acesso à informação e de livre expressão.
				$P_{5.9}$	De 1 (Discordo totalmente) a 5 (Concordo totalmente), quanto concorda com esta frase: "Os governos europeus, com o objetivo de salvaguardar a privacidade e garantir a segurança das redes e dados dos Estados membros, vão bloquear o acesso a páginas da *Web* com domínio fora da União Europeia".

Fonte: (Autor, 2017)

SECÇÃO 6: A cibersegurança é uma responsabilidade partilhada...

Tabela Apd C-6 – SECÇÃO 6: A cibersegurança é uma responsabilidade partilhada...

Pergunta Aberta	$P_{6.1}$	Deixe-nos uma sugestão sobre como melhorar a cibersegurança na FAP (Ex: Utilização de um cartão de identificação para permitir usar o PC). A) ----------

Fonte: (Autor, 2017)

[10] (Brookson, *et al*., 2015)

Apêndice D — Respostas às entrevistas

Entrevistado: TCor/TINF Mendes

(Divisão de Comunicações e Sistemas de Informação)

(telf. 500 835)

No âmbito do Curso de Promoção a Oficial Superior da Força Aérea pretendemos desenvolver um Trabalho de Investigação Individual (TII) sobre "O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS". Dentro desta temática, o objetivo principal é determinar o nível de preparação dos recursos humanos da FAP para lidar com os desafios do ciberespaço.

É neste contexto que solicitamos a participação de alguns militares da FAP ligados às questões da ciberdefesa e da cibersegurança, a responderem a quatro questões acerca desta temática, de forma a recolher as suas opiniões.

1. Atualmente é consensual considerar o ciberespaço como uma nova dimensão no conflito. Na sua opinião, acha que a comunidade da FAP está consciente desta realidade, encarando-a da mesma forma que encara a dimensão terrestre, naval, aérea e espacial do conflito?

Resposta: Sem dúvida que o ciberespaço é uma dimensão de conflito. Desde o *bug* do ano 2000 que o salto cibernético foi enorme. O Século XXI acordou para uma nova realidade, com um novo vetor estratégico para o desenvolvimento cultural, social, económico, industrial e para a defesa, de fácil manuseamento e privilegiado, mas requerendo por essa razão uma clara perceção dos perigos e ameaças e das vulnerabilidades que estão associadas na utilização do ciberespaço.

Deste modo, estando a comunidade da FA envolvida na estratégia militar e económica quer da NATO, quer da UE, respetivamente, a utilização do ciberespaço está presente como uma arma de conflito na mesma dimensão que as clássicas.

2. Com base na sua experiência, como qualificaria o comportamento dos militares e civis da FAP, numa perspetiva de cibersegurança? Por exemplo, a nível de atitudes negligentes no uso dos computadores da FAP.

Resposta: Os militares e civis da FA estão cientes dos perigos que podem surgir na utilização abusiva da Internet. Não tem havido comportamentos negligentes no uso dos computadores, os utilizadores recebem, através dos oficiais de segurança da informação de cada Unidade ou Direção, informação e formação quanto aos perigos que podem advir da utilização de ferramentas no ciberespaço. Têm sido efetuados exercícios em diversos serviços da FA, conduzidos pela Secção de Ciberdefesa da DCSI, no sentido de avaliar a consciencialização dos utilizadores para os perigos do ciberespaço do qual tem resultado de uma forma positiva a sua colaboração.

3. Na sua opinião, e tendo por base os perigos subjacentes ao ciberespaço, acha que seria proveitoso investir na formação em cibersegurança na FAP? Se sim, que tipo de formação julga ser a melhor opção: formação específica e dedicada (ex: os cursos de CRM, Fisiologia de Voo e Guerra Eletrónica); integrada em outras formações (ex: ICCS) ou *ab initio* (ex: Academia da Força Aérea ou Centro de Formação Militar e Técnica da Força Aérea).

Resposta: Sem dúvida que se deve investir na formação em cibersegurança. Todos os militares, aquando da sua formação académica (Academia ou CFMTFA), devem ter uma disciplina cujo conteúdo deveria ser a cibersegurança e ciberdefesa, como parte integrante do curso de formação.

4. Nas sociedades ocidentais atuais observa-se uma crescente conetividade das pessoas e das coisas, onde bens, serviços, ideias e experiências são "transacionados" a todo o momento. Estes são alguns dos motivos pelos quais o ciberespaço deve ser mantido aberto e seguro. Partindo desta premissa, na sua opinião, seria legítimo ou adequado, em nome da segurança, aumentar o controlo e limite sobre o que podem ou não fazer os utilizadores da Internet? E os utilizadores da Intranet na FAP?

Resposta: Deve-se investir em ferramentas de segurança e em pessoas qualificadas. O decréscimo investimento nos computadores pessoais, em *software* e antivírus adequados, para os novos desafios do ciberespaço, estão a ser postos, como não sendo uma prioridade na FA. Estamos a caminhar no sentido errado quanto à segurança da informação que a FA manuseia diariamente. O número de técnicos ou engenheiros informáticos que se formam anualmente na FA, não é suficiente para a segurança da informação administrativa quanto mais para a segurança da informação operacional.

Sabemos que no mundo empresarial e mesmo na indústria da defesa a procura de informáticos é enorme. De igual modo a questão põe-se ao nível das Forças Armadas, no qual a procura de melhores vencimentos leva a militares a abandonarem a carreira da informática.

O controlo faz-se ao nível de ferramentas de segurança adequados, de servidores e *firewalls* de última geração, e com software atualizado. Não é limitando a utilização de ferramentas de trabalho que se formam bons militares ou profissionais nas suas áreas de formação, mas sim adequar os meios para que possam cumprir a missão para a qual foi determinado.

"Por mares nunca antes navegados", Canto I, Luís de Camões, é o modo como procedemos para a exploração do espaço cibernético e os seus desafios e conflitos que vão ser encontrados neste novo domínio, tal com Camões o encontrou na exploração do mar.

Entrevistado: Maj/ENGEL Farinha

(EMGFA - Direção de Comunicações e Sistemas de Informação - Centro de Ciberdefesa)

(telf. 225 679)

No âmbito do Curso de Promoção a Oficial Superior da Força Aérea pretendemos desenvolver um Trabalho de Investigação Individual (TII) sobre "O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS". Dentro desta temática, o objetivo principal é determinar o nível de preparação dos recursos humanos da FAP para lidar com os desafios do ciberespaço.

É neste contexto que solicitamos a participação de alguns militares da FAP ligados às questões da ciberdefesa e da cibersegurança, a responderem a quatro questões acerca desta temática, de forma a recolher as suas opiniões.

1. Atualmente é consensual considerar o ciberespaço como uma nova dimensão no conflito. Na sua opinião, acha que a comunidade da FAP está consciente desta realidade, encarando-a da mesma forma que encara a dimensão terrestre, naval, aérea e espacial do conflito?

Resposta: No geral, a comunidade de planeadores militares das Forças Armadas não consegue ainda materializar de que forma é que o ciberespaço poderá ser potenciado no contexto das operações militares. A falta de doutrina de emprego operacional (quer a nível nacional, como NATO), os escassos recursos humanos qualificados nas Forças Armadas para a exploração do ciberespaço ou a fase inicial em que se encontra o desenvolvimento da Capacidade de Ciberdefesa nas Forças Armadas são fatores que levam a esse distanciamento. Tal como a aviação nos seus primórdios, só com o surgimento dos principais teorizadores do emprego do poder aéreo é que começaram a ser dados passos concretos para a sua utilização como capacidade militar. O mesmo tem vindo a ser verificado com o vetor das aeronaves não tripuladas. As principais potências militares mundiais utilizam de forma massiva esse tipo de aeronaves, no entanto as nações com maiores limitações de recursos (orçamentais e de pessoal) ainda dão passos tímidos nesse campo, continuando a focar os recursos existentes na manutenção das capacidades operacionais que já possuem.

2. Com base na sua experiência, como qualificaria o comportamento dos militares e civis da FAP, numa perspetiva de cibersegurança? Por exemplo, a nível de atitudes negligentes no uso dos computadores da FAP.

Resposta: Os militares e civis da FAP têm, no geral, um comportamento de risco na utilização dos sistemas e das tecnologias de informação da organização. Este comportamento é motivado pela pouca sensibilização que a maioria da população portuguesa tem para os riscos da utilização dos sistemas de informação, em especial aqueles que estão ligados à Internet, e é potenciado pelas poucas restrições que são colocadas na utilização dessas tecnologias na Força Aérea, permitindo a ligação de dispositivos de armazenamento externos aos postos de trabalho da organização, o acesso a contas de correio eletrónica pessoais, entre outros vetores de ataque que são hoje em dia explorados pelos atacantes.

3. Na sua opinião, e tendo por base os perigos subjacentes ao ciberespaço, acha que seria proveitoso investir na formação em cibersegurança na FAP? Se sim, que tipo de formação julga ser a melhor opção: formação específica e dedicada (ex: os cursos de CRM, Fisiologia de Voo e Guerra Eletrónica); integrada em outras formações (ex: ICCS) ou *ab initio* (ex: Academia da Força Aérea ou Centro de Formação Militar e Técnica da Força Aérea).

Resposta: A formação em cibersegurança é um dos pilares essenciais para o aumento do nível de segurança coletivo das Forças Armadas. Essa formação de base deve abranger:

- a sensibilização de todos os utilizadores para os riscos genéricos e os comportamentos defensivos que devem ser adotados no dia a dia. Este tipo de formação deve ser acautelado durante os cursos *ab initio* e reforçada periodicamente ao longo da carreira dos militares (ações de sensibilização anuais, por exemplo, à semelhança do que é feito para os testes de aptidão médica e de avalização da condição física).

- a sensibilização específica de comunidades de risco especialmente elevado, quer pelos lugares funcionais que ocupam (por lidarem com informação sensível, ou pela visibilidade pública desses lugares), como pelas missões em que estão envolvidos. Este tipo de sensibilização deve ser dado antes do início da missão ou de assumir o cargo de risco elevado.

- a formação específica técnica para todos os elementos envolvidos em projetos que envolvem a implementação de sistemas e tecnologias de informação. Esta formação deveria abranger elementos das diversas direções técnicas do CLAFA (uma vez que hoje em dia, a maioria dos projetos, sejam de sistemas de armas, de infraestruturas físicas ou de sistemas funcionais, incluem uma componente relacionada com os sistemas e tecnologias de informação). Este tipo de formação deverá ser específica e dedicada, com conteúdos desenvolvidos especificamente para o universo das Forças Armadas.

- a formação específica técnica para os administradores dos sistemas e tecnologias de informação, para os cuidados a ter na área da cibersegurança, durante a implementação e manutenção dos sistemas pelos quais são responsáveis. Este tipo de formação é desenvolvida à medida, caso a caso.

4. Nas sociedades ocidentais atuais observa-se uma crescente conetividade das pessoas e das coisas, onde bens, serviços, ideias e experiências são "transacionados" a todo o momento. Estes são alguns dos motivos pelos quais o ciberespaço deve ser mantido aberto e seguro. Partindo desta premissa, na sua opinião, seria legítimo ou adequado, em nome da segurança, aumentar o controlo e limite sobre o que podem ou não fazer os utilizadores da Internet? E os utilizadores da Intranet na FAP?

Resposta: Na minha opinião, o controlo e o limite de utilização dos utilizadores da Intranet da FAP tem de aumentar. O nível de risco é cada vez maior, assim como a dependência da organização nos seus sistemas de informação, pelo que ao colocar em causa a segurança desses sistemas, um utilizador pode estar a colocar em causa o funcionamento da Força Aérea, com impacto na produtividade de diversos militares e, no limite, da missão. A diminuição do risco passa pela formação, como focado no ponto anterior, aliada ao aumento dos mecanismos de controlo de segurança implementados. Infelizmente, o aumento desses mecanismos de controlo leva à menor liberdade de utilização dos meios da organização (por colocar restrições adicionais), pelo que a implementação destas restrições deve ser obrigatoriamente acompanhada por uma campanha de comunicação que explique claramente aos utilizadores a racional por trás dessas restrições.

No que diz respeito à Internet em geral, é natural que tenham de vir a ser impostos mecanismos de regulação que permitam aumentar a segurança global de quem utiliza essa rede. Por ser um domínio comum (*global common*) com um impacto económico sem antecedentes na história da humanidade, qualquer medida de restrição que venha a ser implementada sobre a Internet é abordada de forma cautelosa, estando atualmente o debate colocado sobre a forma de regulação da Internet, nomeadamente se deverá ser uma função do setor económico (através dos fabricantes e operadores) ou do setor governamental (através de regulamentação legal). Na minha opinião, deverão ser colocadas obrigatoriedades de cumprimento de um conjunto de medidas básicas de segurança a qualquer operador económico que disponibilize serviços ou ligue sistemas à Internet (da mesma forma que existem obrigações de segurança alimentar a todos os operadores económicos na área da restauração, com fiscalização por parte da ASAE), uma vez que a maioria das grandes quebras de segurança que se têm verificado nos últimos 24 meses estão associadas a esse tipo de operadores (quebras de confidencialidade de bases de dados, comprometimento de sistemas ligados à Internet, entre outros. Este tipo de medidas está agora a dar os primeiros passos na Europa, nomeadamente através da Diretiva NIS e do Regulamento de Proteção de Dados (GDPR), que entrarão em vigor em 2018.

Entrevistado: Maj/TINF Valente

(Direção de Comunicações e Sistemas de Informação – Repartição de Tecnologias de Informação - Secção de Ciberdefesa)

(telf. 500 689)

No âmbito do Curso de Promoção a Oficial Superior da Força Aérea pretendemos desenvolver um Trabalho de Investigação Individual (TII) sobre "O CIBERESPAÇO COMO NOVA DIMENSÃO NOS CONFLITOS". Dentro desta temática, o objetivo principal é determinar o nível de preparação dos recursos humanos da FAP para lidar com os desafios do ciberespaço.

É neste contexto que solicitamos a participação de alguns militares da FAP ligados às questões da ciberdefesa e da cibersegurança, a responderem a quatro questões acerca desta temática, de forma a recolher as suas opiniões.

1. Atualmente é consensual considerar o ciberespaço como uma nova dimensão no conflito. Na sua opinião, acha que a comunidade da FAP está consciente desta realidade, encarando-a da mesma forma que encara a dimensão terrestre, naval, aérea e espacial do conflito?

Resposta: Existem diversas comunidades na FAP com graus de preocupação e conhecimento acerca do aparecimento de uma nova dimensão em que podem ser efetuadas operações militares. Na minha opinião, julgo que a comunidade de decisão da FAP (Comandantes, Diretores e Chefes), está consciente deste novo domínio operacional.

2. Com base na sua experiência, como qualificaria o comportamento dos militares e civis da FAP, numa perspetiva de cibersegurança? Por exemplo, a nível de atitudes negligentes no uso dos computadores da FAP.

Resposta: No que respeita à cibersegurança o comportamento dos militares e civis da Força Aérea é semelhante ao comportamento da restante sociedade nos seus locais de trabalho.

Existem alguns casos de desrespeito pelas normas e pelas boas práticas que dizem respeito à cibersegurança, mas de um modo geral a reação a um incidente de cibersegurança é satisfatória. Em exercícios de cibersegurança efetuados dentro da Força Aérea foi possível avaliar estes comportamentos.

3. Na sua opinião, e tendo por base os perigos subjacentes ao ciberespaço, acha que seria proveitoso investir na formação em cibersegurança na FAP? Se sim, que tipo de formação julga ser a melhor opção: formação específica e dedicada (ex: os cursos de CRM, Fisiologia de Voo e Guerra Eletrónica); integrada em outras formações (ex: ICCS) ou *ab initio* (ex: Academia da Força Aérea ou Centro de Formação Militar e Técnica da Força Aérea).

Resposta: É, sem dúvida proveitoso investir em formação na área da cibersegurança. Na minha opinião deve ser aproveitados os momentos de formação já existentes durante a carreira militar. Ex: Academia e CFMTFA; CBC; CPOS.

Adicionalmente podem ser efetuadas outras ações de formação principalmente na área da sensibilização sob a forma de palestras ou pequenos cursos.

4. Nas sociedades ocidentais atuais observa-se uma crescente conetividade das pessoas e das coisas, onde bens, serviços, ideias e experiências são "transacionados" a todo o momento. Estes são alguns dos motivos pelos quais o ciberespaço deve ser mantido aberto e seguro. Partindo desta premissa, na sua opinião, seria legítimo ou adequado, em nome da segurança, aumentar o controlo e limite sobre o que podem ou não fazer os utilizadores da Internet? E os utilizadores da Intranet na FAP?

Resposta: Tal como no mundo físico, existem comportamentos e indícios de práticas criminais que devem ser controlados e limitados, mesmo que isso implique uma perda de privacidade. Em nada este controlo e imposição de limites deve reduzir a liberdade de movimentos e de ações de cada cidadão. O grande dilema prende-se não com a liberdade de ação mas com a privacidade. Esta é que normalmente é condicionada com o aumento de controlo e de segurança. Nos dias que correm nenhum cidadão estranha a recolha de imagens de vídeo vigilância em espaços públicos e confia que esta perda de privacidade confere uma maior segurança nestes espaços. Resposta à primeira pergunta: Sim, não vejo porque razão deve ser permitido o acesso a locais no ciberespaço onde existem indícios de crime quando podem existir mecanismos que impeçam o acesso a estes locais.

Em relação à Intranet da Força Aérea, o âmbito é diferente. Trata-se de uma rede organizacional que está ligada à Internet para existir comunicação institucional ou privada com outras entidades. A Força Aérea tem o direito de limitar e controlar da forma que entender o acesso à internet que é providenciado na rede interna. No limite pode decidir separar as duas redes. Este direito de controlos e limitações nunca pode ir contra as leis em vigor em Portugal no âmbito da proteção de dados pessoais.

Apêndice E — Estatística de associação, regressão linear e teste de hipóteses

Tabela Apd E-1 – Medidas de associação e regressão entre varáveis, calculadas com base no IBM® SPSS® Versão 23

Número de respondentes: N = 364					
Variáveis relacionadas	**Medida de associação**			**Regressão Linear Simples**	**Regressão Linear Múltipla[11]**
	Covariância	**Coeficiente de correlação de *Spearman* (*rho* de *Spearman*)**	**Coeficiente de correlação de *Pearson* (*ρ* de *Pearson*)**		
V1/V2	0,243	0,610 (valor-*p* < 0,05)	0,688 (valor-*p* < 0,05)	V1 = 1,23 + 0,7*V2 (R^2 = 0,473)	V1 = 0,03 + 0,428*V2 + 0,246*V3 + 0,318*V4 (R^2 = 0,598)
V1/V3	0,198	0,524 (valor-*p* < 0,05)	0,604 (valor-*p* < 0,05)	V1 = 1,24 + 0,66*V3 (R^2 = 0,364)	V2 = 0,496 + 0,512*V1 + 0,166*V3 + 0,136*V4 (R^2 = 0,504) [BETA de V3 e V4 é muito baixo (0,154 e 0,120 respetivamente), ou seja, praticamente não influenciam a variável dependente]
V1/V4	0,195	0,495 (valor-*p* < 0,05)	0,624 (valor-*p* < 0,05)	V1 = 0,9 + 0,72*V4 (R^2 = 0,390)	V3 = 0,992 + 0,290*V1 + 0,163*V2 + 0,278*V4 (R^2 = 0,433) [BETA de V2 e V4 é baixo (0,176 e 0,265 respetivamente), ou seja, influenciam pouco a variável dependente. Adicionalmente, apenas 43,3% (R^2) de V3 é explicável por V1, V2 e V4]
V2/V3	0,172	0,454 (valor-*p* < 0,05)	0,534 (valor-*p* < 0,05)	V2 = 1,4 + 0,58*V3 (R^2 = 0,286)	V4 = 1,368 + 0,328*V1 + 0,118*V2 + 0,244*V3 (R^2 = 0,449) [BETA de V2 e V3 é baixo (0,133 e 0,257 respetivamente), ou seja, influenciam pouco a variável dependente. Adicionalmente, apenas 44,9% (R^2) de V4 é explicável por V1, V2 e V3]

Fonte: (Autor, 2017)

Considere as seguintes notas explicativas para melhor compreender o processo estatístico da Teoria da Estimação (estimativa pontual e estimativa por intervalos de confiança):
Este tipo de inferência estatística visa estimar o valor de parâmetros da população, tendo por base estimativas estatísticas da amostra.
Estimação Pontual (Maroco, 2003, pp. 52-53)
Nota 1: Na estimação pontual recorre-se à estatística da amostra para determinar uma aproximação (é expectável a existência de pequenos erros) ao parâmetro populacional. Assim, no caso de se pretender estimar a média populacional, a média da amostra será assim o melhor estimador pontual para esse efeito; já se se quiser estimar o parâmetro variância populacional, a variância da amostra será o melhor estimador pontual para o efeito.
Nota 2: Como é expectável, a verdadeira média e desvio de padrão populacional muito dificilmente será igual ao da amostra. De igual forma, se se construísse amostras diferentes, muito dificilmente o valor das médias e dos desvios de padrão obtidos seriam exatamente iguais.
Nota 3: O estimador pontual é um valor fixo, não permitindo nenhuma medida de certeza, ou incerteza, que esteja associada à estimativa que se determina, isto é, não permite estabelecer um intervalo de confiança probabilística, tornando-o menos preciso.
Estimação por Intervalos de Confiança (Maroco, 2003, pp. 53-56)
Nota 4: O processo de estimação por intervalos de confiança visa determinar a confiabilidade da estimativa de um parâmetro, obtida através da atribuição de um certo grau de confiança ao estimador pontual, e após determinar o tipo de distribuição amostral que o estimador tem. Para tal, estabelece-se um intervalo de valores, com uma certa significância estatística, que irá conter o verdadeiro valor do parâmetro populacional em estudo. Um intervalo assim estabelecido tem a designação de intervalo de confiança. Este intervalo é definido pelo pesquisador e não pelos dados da amostra.
Nota 5: O intervalo de confiança definido pelo investigador é complementar ao nível de significância, ou seja, se o investigador definir um intervalo de confiança de 95%, tal significa que a significância estatística para esse intervalo de valores é de 5%.
Nota 6: É possível calcular o intervalo de confiança para qualquer tipo de associação de variáveis, desde que a distribuição amostral destas seja conhecida.
Nota 7: Quando se trabalha com intervalos de confiança é necessário ter em atenção à forma como se interpreta o significado do que é um intervalo de confiança. Quando se diz que o intervalo de confiança do parâmetro média da população é de 95%, tal não significa que a verdadeira média da população tem 95% de probabilidade de se encontrar no intervalo. A interpretação correta é que, se forem calculados, por exemplo, 100 intervalos de confiança, para 100 amostras aleatórias diferentes de uma população, 95 desses intervalos de confiança irão conter efetivamente o verdadeiro valor da média populacional.
Nota 8: O processo de estimação por intervalos de confiança, utilizado neste trabalho, teve por base o teste de hipóteses estatístico e foi calculado com recurso ao IBM® SPSS® Versão 23:
1) O parâmetro estimado foi a média populacional, para a situação em que a variância populacional é desconhecida;
2) Para a estimação por intervalo de confiança recorreu-se ao teste estatístico, paramétrico, *Teste t* para uma só amostra;
3) Este teste permite comparar a estatística amostral média com o valor do parâmetro média que se pretende testar;
4) Assume-se a seguinte hipótese nula: H0 = média da população é 0 (se valor p > 0,05);
5) Assume-se a seguinte hipótese alternativa: H1 = média da população é diferente de 0 (se valor p < 0,05);
6) Estabeleceu-se um grau de confiança de 95%, ou seja, um nível de significância estatística de 5% (este valor é definido no início da investigação pelo investigador);
7) Realiza-se o *Teste t* de uma amostra com recurso ao IBM® SPSS® Versão 23;
8) Analisa-se e interpreta-se o valor da significância estatística (*valor-p*): se *valor-p* for menor que 0,05, então rejeita-se com uma probabilidade de erro de 5% a hipótese nula (H0), a média da população não é 0, ou seja, a média da população é

[11] Com base na análise de regressão linear múltipla, verificou-se que de entre as variáveis V2, V3 e V4, é a V2 aquela que mais influencia a variável V1 (é a V2 que possui um maior Coeficiente Padronizado BETA), ou seja, **a variável nível de literacia (V2) é a que mais influencia a variável nível de conhecimento (V1)**.

diferente de 0; se o *valor-p* for superior a 0,05, então a hipótese nula (H0) é aceite, ou seja, assume-se que a média da população é 0;

9) Define-se a margem de erro, dividindo a diferença do intervalo de confiança por dois;

10) PARA UMA MAIS COMPLETA DESCRIÇÃO E ANÁLISE DO PROCESSO DE TESTE DE DECISÃO, VER AS NOTAS SEGUINTES.

Considere as seguintes notas explicativas para melhor compreender o processo estatístico da Teoria da Decisão (Maroco, 2003, pp. 56-77,120-121):

Tem como objetivo fundamentar uma decisão, tendo por base testes de hipóteses relativos a parâmetros da população.

Nota 9: Intervalo de confiança para a média da população: se se assumir que a amostra é selecionada de forma aleatória, a partir de uma população que segue uma distribuição do tipo normal, então, com 95% de confiança a média da população estará incluída no intervalo de confiança. Com base neste intervalo de confiança é possível criar outros intervalos de confiança associados a qualquer parâmetro estatístico.

Nota 10: Não sendo possível, nem viável, na generalidade das vezes, analisar os parâmetros da população, recorre-se ao processo de teste de hipóteses estatísticas. Este teste é um método de inferência estatística, que tem por base a análise de uma amostra obtida de forma probabilística. A aleatoriedade na seleção da amostra e o processo estatístico associado ao teste de hipóteses permite inferir alguns parâmetros desconhecidos da população, tendo por base os dados dessa amostra. Por norma, os parâmetros da população inferidos são a média e/ou o desvio de padrão, tendo por base estatísticas semelhantes da amostra.

O processo consiste, no essencial, em testar duas hipóteses diferentes: a hipótese nula (H0) e a hipótese alternativa (H1).

A hipótese nula (H0) (pode consistir numa afirmação relativa a um determinado parâmetro ou propriedade estatística da população) corresponde à hipótese que o investigador assume inicialmente como sendo a verdadeira. Seguidamente, essa hipótese é confrontada com os dados obtidos na amostra, de forma a verificar o grau de plausibilidade estatística de ser de facto verdadeira. Se for plausível a hipótese nula (H0) ser verdadeira, ela é aceite; se se verificar que não é plausível a hipótese nula (H0) ser verdadeira, ela será rejeitada.

No caso da hipótese nula (H0) ser rejeitada, será adotada a hipótese (H1) como sendo a hipótese verdadeira, ou seja, a hipótese alternativa (H1) é validada em resultado da rejeição estatística da hipótese nula (H0).

Contudo, o processo de inferência com base em dados da amostra pode gerar erros de dois tipos: Erro do tipo I e Erro do tipo II.

Obs.: O teste de hipóteses estatísticas é um processo lógico para a resolução do problema de validação/rejeição de uma hipótese em teste. Na base do teste de hipóteses está um teste estatístico que pode ser paramétrico (ex. *Testes t*; Testes ANOVA I/II) ou não paramétrico (ex. Teste de ajustamento do *Qui Quadrado*; Teste de *Mann Whitney*; Teste *Q de Cochran*).

Nota 11: O Erro tipo I (α) corresponde à probabilidade da hipótese nula (H0) ser rejeitada quando, na realidade, ela é efetivamente verdadeira.

Esta probabilidade é designada de nível de significância (α) e é definida na fase inicial do estudo pelo investigador.

A probabilidade da significância estatística ("*valor-p*") corresponde ao valor da probabilidade (obtido através do tratamento dos dados da amostra), que permitirá rejeitar ou validar a hipótese nula (H0). Se o *valor-p* for inferior à significância estatística definida no início da investigação, então a hipótese nula (H0) deve ser rejeitada.

Em termos práticos, ao definir-se no início da investigação uma significância de 0,05 (5%), significa que está-se a admitir a existência de 5% de probabilidade da hipótese nula ser rejeitada, sendo ela, na realidade, verdadeira (Erro tipo I). Porém, se se reduzir o valor da significância, ou seja, a probabilidade de ocorrer o Erro tipo I, está-se a aumentar a probabilidade de ocorrer o Erro tipo II.

Adicionalmente, é importante ter em consideração que *valor-p* é diferente de significância estatística. O primeiro é sempre obtido a partir dos dados da amostra, enquanto o segundo é fixado pelo investigador no início da investigação.

Nota 12: O Erro tipo II corresponde à probabilidade da hipótese nula (H0) não ser rejeitada quando, na realidade, ela é efetivamente falsa.

Tabela Apd E-2 – Relação da aceitação/rejeição da H0 com os Erro Tipo I/II

	H_0 verdadeira	**H_0 falsa**
Aceitar H_0	Decisão correta	Erro Tipo II
Rejeitar H_0	Erro Tipo I (α)	Decisão correta

Fonte: (Autor, 2017)

Nota 13: Se o resultado do teste de hipóteses for no sentido de rejeitar a hipótese nula (H0) (*valor-p* < α), isso significa dizer que essa hipótese é falsa. No entanto, no caso contrário, da não rejeição (aceitação) da hipótese nula (H0) (*valor-p* > α), não é possível daí concluir que a hipótese é verdadeira, apenas pode concluir-se que não existe uma plausibilidade estatística suficientemente forte para rejeitar a hipótese nula (H0): considera-se que existe uma plausibilidade estatística suficientemente forte quando a significância estatística (*valor-p*) é menos que 0,05 (probabilidade de erro de 5%).

Nota 14: Ao teste de hipóteses estatísticas está subjacente, como se poderá depreender, um teste estatístico que procura verificar o grau de plausibilidade estatística de uma hipótese nula (H0) poder ser rejeitada.

Estes testes estatísticos podem ser de dois tipos: bilaterais ou unilaterais. No primeiro caso, testes bilaterais, à hipótese nula (H0) está sempre subjacente o sinal de igual (=);ao passo que a hipótese alternativa (H1) inclui sempre o sinal de desigualdade (< ou >). No segunda caso, testes unilaterais, à hipótese nula (H0) está subjacente o sinal de maior ou igual (> ou =); ao passo que a hipótese alternativa (H1) inclui o sinal oposto (< ou ≠).

Obs.: Os testes estatísticos unilaterais são mais apropriados para os casos em que é possível afirmar com certeza (mesmo antes da recolha dos dados), que as médias não serão diferentes ou serão no sentido do indicado nas hipóteses. Desta forma, se assim não for, deve-se usar sempre os testes estatísticos bilaterais.

Nota 15: No que se refere aos testes estatísticos, existem de dois tipos: os testes paramétricos e os testes não paramétricos.

Os testes paramétricos, ou *testes t* (ex.), implicam uma amostra cuja distribuição é do tipo normal, especialmente se a dimensão dessa amostra for inferior a 30 observações. Nos casos em que a dimensão da amostra é superior a 30 observações, a distribuição da amostra aproxima-se do tipo normal e, como tal, os testes paramétricos (*testes t*) também se aplicam. Nos testes paramétricos os tipos de variáveis utilizadas são normalmente intervalares ou de rácio; por outro lado, a medida de localização central é normalmente a média.

Os testes não paramétricos são usados para amostras inferiores a 30 observações e/ou quando a amostra não tem uma distribuição do tipo normal. Estes testes têm porém a desvantagem de não permitirem encontrar tantas diferenças entre os dados da amostra, o que significa que são teste menos "fortes" que os testes paramétricos.

Obs.: NO CASO DO NOSSO ESTUDO, APESAR DA DISTRIBUIÇÃO DAS VARIÁVEIS TESTADAS NÃO POSSUÍREM UMA DISTRIBUIÇÃO NORMAL, UMA VEZ QUE A AMOSTRA É COMPOSTA POR 364 OBSERVAÇÕES, CONSIDERA-SE QUE A DISTRIBUIÇÃO DA AMOSTRA É NORMAL E, COMO TAL, APLICAM-SE OS TESTES ESTATÍSTICOS PARAMÉTRICOS.

Nota 16: Para verificar o tipo de distribuição da variável, deve realizar-se um teste de normalidade. Assim, para verificar se a distribuição da variável adere à normalidade, ou seja, verificar se podemos pressupor uma distribuição normal, pode-se recorrer a dois tipos de testes: Teste de *Kolmogorov-Smirnov* e o Teste de *Shapiro-wilkes*. O processo de produção e interpretação dos resultados obtidos através destes testes, com recurso ao IBM® SPSS® Versão 23, é o seguinte:

1) Assume-se a hipótese nula: H0 = a distribuição é normal (se valor-p > 0,05);

2) Realiza-se os dois testes de normalidade: Teste de *Kolmogorov-Smirnov* e o Teste de Shapiro-wilkes;

3) Analisa-se e interpreta-se o valor da significância estatística (*valor-p*): se *valor-p* for menor que 0,05, então rejeita-se com uma probabilidade de erro de 5% a hipótese nula (H0), ou seja, a distribuição não é normal; se o *valor-p* for superior a

0,05, então a hipótese nula (H0) é aceite, ou seja, assume-se que a distribuição é normal.

Nota 17: Processo de produção e interpretação do teste estatístico paramétrico *Teste t* para uma só amostra, com recurso ao IBM® SPSS® Versão 23:

1) Com base nos valores determinados estatisticamente de uma amostra aleatória, pretende-se com este teste, comparar os valores observados na amostra com um valor que se pretende testar (ex. testar que a média é 10);

2) Assume-se a hipótese nula: H0 = média da população é 10 (se *valor-p* > 0,05);

3) Realiza-se o *Teste t* de uma amostra com recurso ao IBM® SPSS® Versão 23;

4) Analisa-se e interpreta-se o valor da significância estatística (*valor-p*): se *valor-p* for menor que 0,05, então rejeita-se com uma probabilidade de erro de 5% a hipótese nula (H0), a média da população não é 10, ou seja, a média da população é diferente de 10; se o *valor-p* for superior a 0,05, então a hipótese nula (H0) é aceite, ou seja, assume-se que a média da população é 10.

Tabela Apd E-3 – Inferência estatística calculada com base no IBM® SPSS® Versão 23

Número de respondentes: N = 364			
Variáveis	**Teoria da Estimação**		**Teoria da Decisão**
	Estimativa pontual	**Estimativa por intervalos de confiança** *1) Situação em que a variância da população é desconhecida;* *2) O parâmetro estimado é a média populacional da variável, tendo por estimador a média amostral;* *3) O intervalo de confiança é de 95%, ou seja, o nível de significância é de 5%.*	**Teste de hipótese estatística** *1) As variáveis V1, V2, V3, V4, $P_{2.1}$, $P_{4.3}$, $P_{4.4}$, $P_{4.5}$, $P_{4.6}$, $P_{4.7}$, $P_{4.9}$, $P_{5.9}$ não têm distribuição normal, porém, como a dimensão da amostra é significativamente superior a 30, a distribuição aproxima-se da distribuição normal e por esse motivo poderá fazer-se o teste t-student.*
V1	Estimador pontual: **média** Média populacional = 3,72	Estimador: **média** Média = 3,72 Intervalo de confiança: [3,65;3,78] Margem de erro: 0,065	**H_0**: Os RH da FAP têm alto nível de conhecimento; V1 ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP têm baixo nível de conhecimento; V1 < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de alto nível de conhecimento (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de alto nível de conhecimento (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -9,056; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 0,284 **95% intervalo de confiança da diferença =** [-0, 35 ; -0,22] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados se infere que o parâmetro "média de V1" da população composta pelos RH da FAP é, com um intervalo de confiança de 95%, inferior a quatro, o que corresponde a um baixo nível de conhecimento **(PROVA A H1 DA NOSSA INVESTIGAÇÃO)**
V2	Estimador pontual: **média** Média populacional = 3,55	Estimador: **média** Média = 3,55 Intervalo de confiança: [3,49;3,61] Margem de erro: 0,06	**H_0**: Os RH da FAP têm alto nível de literacia; V2 ≥ 4; Média ≥ 4. **(H_1**: Os RH da FAP têm baixo nível de literacia; V2 < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de alto nível de literacia (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de alto nível de literacia (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -14,595; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 0,451 **95% intervalo de confiança da diferença =** [-0, 51 ; -0,39] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias (amostral e populacional) estão significativamente afastados. Destes dois dados se infere que o parâmetro "média de V2" da população, composta pelos RH da FAP é, com um intervalo de confiança de 95%, inferior a quatro, o que corresponde a um baixo nível de literacia face às regras e procedimento de cibersegurança **(PROVA A H2 DA NOSSA INVESTIGAÇÃO)**.
V3	Estimador pontual: **média** Média populacional = 3,74	Estimador: **média** Média = 3,74 Intervalo de confiança: [3,68;3,80] Margem de erro: 0,06	**H_0**: Os RH da FAP têm alto nível de interesse; V3 ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP têm baixo nível de interesse; V3 < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de alto nível de interesse (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de alto nível de interesse (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -9,088; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 0,261 **95% intervalo de confiança da diferença =** [-0, 32 ; -0,20] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados se infere que o parâmetro "média de V3" da população composta pelos RH da FAP é, com um intervalo de confiança de 95%, inferior a quatro, o que corresponde a um baixo nível de interesse na obtenção de conhecimento na área do ciberdomínio **(REPROVA A H3 DA NOSSA INVESTIGAÇÃO)**.

V4	Estimador pontual: **média** Média populacional = 3,92	Estimador: **média** Média = 3,92 Intervalo de confiança: [3,86;3,97] Margem de erro: 0,055	**H_0**: Os RH da FAP atribuem um alto nível de importância; V4 ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP atribuem um baixo nível de importância; V4 < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de atribuição de um alto nível de importância (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de atribuição de um alto nível de importância (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -2,993; **Significância estatística (valor-*p*) =** 0,003; **Diferença da média real e testada** = - 0,082 **95% intervalo de confiança da diferença =** [-0, 14 ; -0,03] **Interpretação**: Dado que a significância estatística é 0,003 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados se infere que o parâmetro "média de V4" da população composta pelos RH da FAP é, com um intervalo de confiança de 95%, inferior a quatro, o que corresponde à atribuição de um baixo nível de importância à segurança no ciberespaço **(REPROVA A H4 DA NOSSA INVESTIGAÇÃO)**.
$P_{2.1}$	Estimador pontual: **média** Média populacional = 2,99	Estimador: **média** Média = 2,99 Intervalo de confiança: [2,91;3,07] Margem de erro: 0,08	**H_0**: Os RH da FAP autoavaliam-se com um alto nível de conhecimento sobre o ciberespaço; $P_{2.1}$ ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP autoavaliam-se com um baixo nível de conhecimento sobre o ciberespaço; $P_{2.1}$<4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de uma autoavaliação de alto nível de conhecimento sobre o ciberespaço (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de uma autoavaliação de alto nível de conhecimento sobre o ciberespaço (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -24,026; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 1,011 **95% intervalo de confiança da diferença =** [-1, 09 ; -0,93] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP autoavaliam-se como possuidores de um baixo nível de conhecimento sobre as matérias do ciberespaço **(ESTE RESULTADO VAI AO ENCONTRO DAQUILO QUE SE INFERE DO RESULTADO DE V1 NA POPULAÇÃO)**.
$P_{4.3}$	Estimador pontual: **média** Média populacional = 2,87	Estimador: **média** Média = 2,87 Intervalo de confiança: [2,78;2,96] Margem de erro: 0,09	**H_0**: Os RH da FAP autoavaliam-se com um alto nível de conhecimento sobre cibersegurança; $P_{4.3}$ ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP autoavaliam-se com um baixo nível de conhecimento sobre cibersegurança; V1 < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese autoavaliam-se com um alto nível de conhecimento sobre cibersegurança (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese autoavaliam-se com um alto nível de conhecimento sobre cibersegurança (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -24,515; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 1,132 **95% intervalo de confiança da diferença =** [-1,22 ; -1,04] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP autoavaliam-se como possuidores de um baixo nível de conhecimento sobre as matérias de cibersegurança **(ESTE RESULTADO VAI AO ENCONTRO DAQUILO QUE SE INFERE DO RESULTADO DE V2 NA POPULAÇÃO)**.
$P_{4.4}$	Estimador pontual: **média** Média populacional = 4,02	Estimador: **média** Média = 4,02 Intervalo de confiança: [3,91;4,14] Margem de erro: 0,115	**H_0**: Os RH da FAP atribuem grande interesse à existência de colaboradores com conhecimentos em cibersegurança na FAP; $P_{4.4}$ ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP atribuem pouco interesse à existência de colaboradores com conhecimentos em cibersegurança na FAP; $P_{4.4}$ < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de atribuição de grande interesse à existência de colaboradores com conhecimentos em cibersegurança na FAP (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de atribuição de grande interesse à existência de colaboradores com conhecimentos em cibersegurança na FAP (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = 0,419; **Significância estatística (valor-*p*) =** 0,676; **Diferença da média real e testada** = 0,025 **95% intervalo de confiança da diferença =** [-0, 09 ; 0,14] **Interpretação**: Dado que a significância estatística é 0,676 (superior a 0,05) podemos aceitar a hipótese nula. Isto significa que não existe uma plausibilidade estatística suficientemente forte para rejeitar a hipótese nula (*H_0*), levando-nos a aceita-la como verdadeira. Contudo, por outro lado, o intervalo de confiança da diferença contém o valor zero, significando que os valores das médias estão significativamente próximos. Destes dois dados infere-se que, os RH da FAP atribuem grande interesse à existência de colaboradores com conhecimentos em cibersegurança na FAP **(ESTE RESULTADO VAI CONTRA ÀQUILO QUE SE INFERE DO RESULTADO DE V3 NA POPULAÇÃO).**
$P_{4.5}$	Estimador pontual: **média** Média populacional = 2,97	Estimador: **média** Média = 2,97 Intervalo de confiança: [2,89;3,05] Margem de erro: 0,08	**H_0**: Os RH da FAP classificam o nível de cibersegurança na FAP de alto; $P_{4.5}$ ≥ 4; Média ≥ 4. **H_1**: Os RH da FAP qualificam o nível de cibersegurança na FAP de baixo; $P_{4.5}$ < 4; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de qualificação do nível de cibersegurança na FAP ser alto (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de qualificação do nível de cibersegurança na FAP ser alto (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -24,750; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = - 1,027 **95% intervalo de confiança da diferença =** [-1,11 ; -0,95]

			Interpretação: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados se infere que, com um intervalo de confiança de 95%, os RH da FAP classificam o nível de cibersegurança na FAP de baixo.
$P_{4.6}$	Estimador pontual: **média** Média populacional = 3,90	Estimador: **média** Média = 3,90 Intervalo de confiança: [3,80;4,00] Margem de erro: 0,1	**H_0**: Os RH da FAP estabelecem uma boa correspondência entre comportamentos de risco e falta de cibersegurança; $P_{4.6} \geq 4$; Média ≥ 4. **H_1**: Os RH da FAP estabelecem uma fraca correspondência entre comportamentos de risco e falha nas regras de cibersegurança; $P_{4.6} < 4$; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de estabelecer uma boa correspondência entre comportamentos de risco e falta de cibersegurança (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de estabelecer uma boa correspondência entre comportamentos de risco e falta de cibersegurança (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -2,008; **Significância estatística (valor-*p*) =** 0,045; **Diferença da média real e testada** = - 0,099 **95% intervalo de confiança da diferença =** [-0,20 ; 0,00] **Interpretação**: Dado que a significância estatística é 0,045 muito próximo do valor fronteira 0,05, mas que nos permite rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Por outro lado, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias não estão significativamente afastados. Destes dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP estabelecem uma fraca correspondência entre comportamentos de risco e falha nas regras de cibersegurança.
$P_{4.7}$	Estimador pontual: **média** Média populacional = 3,97	Estimador: **média** Média = 3,97 Intervalo de confiança: [3,87;4,06] Margem de erro: 0,095	**H_0**: Os RH da FAP têm alto interesse em receber formação sobre ciberespaço e cibersegurança; $P_{4.7} \geq 4$; Média ≥ 4. **H_1**: Os RH da FAP têm baixo interesse em receber formação sobre ciberespaço e cibersegurança; $P_{4.7} < 4$; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de alto interesse em receber formação sobre ciberespaço e cibersegurança (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de alto interesse em receber formação sobre ciberespaço e cibersegurança (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -0,666; **Significância estatística (valor-*p*) =** 0,506; **Diferença da média real e testada** = - 0,033 **95% intervalo de confiança da diferença =** [-0,13 ; 0,06] **Interpretação**: Dado que a significância estatística é 0,506 (superior a 0,05) podemos aceitar a hipótese nula. Isto significa que não existe uma plausibilidade estatística suficientemente forte para rejeitar a hipótese nula (H_0), levando-nos a aceita-la como verdadeira. Por outro lado, o intervalo de confiança da diferença contém o valor zero, significando isto que os valores das médias estão significativamente próximos. Destes dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP têm alto interesse em receber formação sobre ciberespaço e cibersegurança **(ESTE RESULTADO APOIA O RESULTADO OBTIDO NO PARÂMETRO P4.4 MAS VAI CONTRA O RESULTADO OBTIDO NO PARÂMETRO V3).**
$P_{4.9}$	Estimador pontual: **média** Média populacional = 4,38	Estimador: **média** Média = 4,38 Intervalo de confiança: [4,30;4,47] Margem de erro: 0,085	**H_0**: Os RH da FAP concordam em promover a adoção de uma cultura organizacional ativa de cibersegurança; $P_{4.9} \geq 4$; Média ≥ 4. **H_1**: Os RH da FAP não concordam em promover a adoção de uma cultura organizacional ativa de cibersegurança; $P_{4.9} < 4$; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese de concordam muito em promover a adoção de uma cultura organizacional ativa de cibersegurança (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese de concordam muito em promover a adoção de uma cultura organizacional ativa de cibersegurança (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = 9,059; **Significância estatística (valor-*p*) =** 0,000; **Diferença da média real e testada** = 0,385 **95% intervalo de confiança da diferença =** [0,30 ; 0,47] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP concordam pouco em promover a adoção de uma cultura organizacional ativa de cibersegurança **(ESTA INFERÊNCIA ESTATÍSTICA CONTRARIA OUTROS RESULTADOS NA POPULAÇÃO)**.
$P_{5.9}$	Estimador pontual: **média** Média populacional = 2,28	Estimador: **média** Média = 2,28 Intervalo de confiança: [2,15;2,40] Margem de erro: 0,125	**H_0**: Os RH da FAP concordam que haja um maior controlo no acesso à Internet e aos seus conteúdos, de forma a promover a cibersegurança; $P_{5.9} \geq 4$; Média ≥ 4. **H_1**: Os RH da FAP não concordam que haja um maior controlo no acesso à Internet e aos seus conteúdos de forma a promover a cibersegurança; $P_{5.9} < 4$; Média < 4. **Erro Tipo I**: Rejeitamos a hipótese concordam em que haja um maior controlo no acesso à Internet e nos seus conteúdos de forma a promover a cibersegurança (H_0), quando esta hipótese é a verdadeira. **Erro Tipo II**: Aceitamos a hipótese concordam em que haja um maior controlo no acesso à Internet e nos seus conteúdos de forma a promover a cibersegurança (H_0), quando esta hipótese é falsa. **Valor testado** = 4; **t** = -27,173; **Significância estatística (valor-*p*) =** 0,000 ; **Diferença da média real e testada** = - 1,723 **95% intervalo de confiança da diferença =** [-1,85 ; -1,60] **Interpretação**: Dado que a significância estatística é 0,000 (inferior a 0,05) podemos rejeitar a hipótese nula com uma probabilidade de erro de 5%, aceitando a hipótese alternativa. Adicionalmente, o intervalo de confiança da diferença não contém o valor zero, significando que os valores das médias estão significativamente afastados. Destes dois dados infere-se que, com um intervalo de confiança de 95%, os RH da FAP não concordam que haja um maior controlo no acesso à Internet e aos seus conteúdos de forma a promover a cibersegurança.

Fonte: (Autor, 2017)

Apêndice F — Sugestões de medidas a adotar para melhorar a cibersegurança na FAP, fornecidas pelos respondentes do inquérito

Seguidamente encontra-se explanado um resumo das sugestões dadas pelos respondentes do questionário quanto às medidas a adotar para melhorar o nível de cibersegurança na FAP:

a) Limitar acesso a determinados sítios;

b) Retirar entradas *Universal Serial Bus* (USB) dos computadores;

c) Identificação biométrica;

d) Reduzir significativamente o uso de dispositivos pessoais no local de trabalho, eliminá-los totalmente em todas as áreas Classe 1 e 2;

e) A validação pessoal, através de um cartão de identificação;

f) Controlar o acesso aos postos de trabalho informáticos e criar níveis de acesso e de conteúdos entre os colaboradores;

g) Instruir os colaboradores;

h) Bloquear a possibilidade de guardar documentos de serviço em USB ou *cloud providers*;

i) Utilização de um *login* (Número de Identificação Pessoal + password) para aceder a um motor de busca nos computadores da FAP e respetiva monitorização do histórico de navegação associado a esse login;

j) Impossibilitar o acesso às redes externas;

k) Criação de um gabinete especializado em segurança da rede;

l) Vigilância da atividade na rede;

m) Punir quem utilizar indevidamente a rede, anunciando aos demais que está a ser punido e porquê, para que se saiba que há consequências;

n) Incluir esta matéria na formação base dos militares e promover ações de sensibilização/exercícios periódicos;

o) Palavra passe individual para acesso à Internet;

p) Criação de um quantificador que permita aferir em tempo real se a matéria que está a ser consultada põe em risco a segurança da organização;

q) Jornadas de sensibilização;

r) Não deve haver limitação à utilização dos computadores. A instituição, deve sim limitar o acesso a determinadas redes e adotar medidas e sistemas de segurança da rede FAP;

s) Atualização e melhoramento do parque informático da FAP;

t) Utilização de assinatura digital;

u) Todos os ficheiros executáveis só o poderão ser com autorização superior, especialmente em computadores em rede segura. O acesso às redes sociais e aos jogos em linha deverão ser bloqueados a todos os utilizadores, assim como, o acesso a sítios provenientes de Estados potencialmente perigosos onde possam existir células terroristas, e ou inimigos da NATO;

v) Formação dos militares sobre os perigos da engenharia social, especialmente os militares que vão para o estrangeiro em missões;

w) Contratar pessoal especializado e criar um departamento ou ramo responsável pela cibersegurança;

x) Divulgação de informação sobre cibersegurança, com dicas e avisos contra erros mais comuns;

y) Diminuir a dependência da Internet;

z) A cibersegurança passa pela informação dos utilizadores sobre quais as atitudes e comportamentos a tomar em rede e desligado da rede, assim como a criação de equipas que possam controlar e defender os sistemas da FAP, mas que também tenham capacidade de atacar outros sistemas;

aa) Promover informação sobre o tema, seguindo o exemplo das informações que são preparadas pelos Gabinetes de Prevenção de Acidentes quando ocorre algum acidente/incidente, através da divulgação das situações em que a cibersegurança na FAP foi colocada em causa, de modo a sensibilizar os militares e civis para esta temática.