INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2018/2019, 2.ª Edição

TII

NÍVEL DE *AWARENESS* EM CIBERDEFESA NA FORÇA AÉREA PORTUGUESA

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.

Pedro Duarte Faia Morgado

CAP/TINF

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

NÍVEL DE *AWARENESS* EM CIBERDEFESA NA FORÇA AÉREA PORTUGUESA

CAP/TINF Pedro Duarte Faia Morgado

Trabalho de Investigação Individual do CPOS FA 2018/2019, 2.ª Edição

Pedrouços 2019

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

NÍVEL DE *AWARENESS* EM CIBERDEFESA NA FORÇA AÉREA PORTUGUESA

CAP/TINF Pedro Duarte Faia Morgado

Trabalho de Investigação Individual do CPOS FA 2018/2019, 2ª. Edição

Orientador: TCOR/TINF José António Sacramento Marques
Coorientador: TCOR/ENGEL Pedro Miguel da Silva Costa

Pedrouços 2019

Declaração de compromisso Antiplágio

Eu, **Pedro Duarte Faia Morgado**, declaro por minha honra que o documento intitulado **Nível de *Awareness* em Ciberdefesa na Força Aérea Portuguesa** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial Superior – Força Aérea 2018/19, 2.ª Edição** 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 que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 28** de **julho** de **2019**

Pedro Duarte Faia Morgado

Agradecimentos

"Mesmo as pessoas que dizem que tudo está predeterminado e que não podemos fazer nada para mudá-lo, olham para os dois lados antes de atravessar a rua."

Stephen Hawking

A realização deste trabalho de investigação não se extingue na minha conceção individual; é resultado do contributo de todos aqueles que neste momento especifico e ao longo de todo o meu percurso profisssional contribuiram para que eu sentisse o prazer e o querer em produzir algo novo e reflexo dos ensinamentos de muitos; a todos estou eternamente grato.

À "melhor Repartição da NATO" pela extraordinária dedicação, profissionalismo e qualidade de trabalho, cujos feitos ecoam por esta Força Aérea, tendo sido para mim uma fonte extra de motivação.

Ao meu orientador, Tenente-Coronel José Marques, pela sua inestimável ajuda, disponibilidade, paciência e amizade.

Ao meu coorientador, Tenente-Coronel Pedro Costa, pela preocupação e precioso apoio às exigências formais deste Trabalho de Investigação.

Ao diretor de curso, docentes e camaradas auditores do CPOS18-19 2.ª edição pela orientação e preocupação constantes, assim como por todos os conselhos que me deram.

À minha familia nuclear cujas palavras aqui escritas nunca conseguiriam representar o quanto vos amo.

Índice

Índice de Apêndices

Índice de Figuras e Gráficos

Resumo

O ciberespaço constitui hoje domínio privilegiado para realização de atividades maliciosas com impacto em sistemas empresariais, infraestruturas críticas e até num Estado. Tem-se assistido à maturação de um novo conceito de guerra que desafia a segurança e bem-estar das populações e coloca a nu as vulnerabilidades existentes.

Este estudo investiga o Nível de *Awareness* em Ciberdefesa da Força Aérea Portuguesa (FA) posicionando a Instituição num nível de maturidade resultante daquilo que é a perceção e consciencialização dos seus membros para a Ciberdefesa, ao mesmo tempo que analisa a dimensão organizacional, reflete as suas vulnerabilidades e ameaças e procura mecanismos incrementadores do seu Nível de *Awareness*.

Por intermédio de uma metodologia de raciocínio indutivo, assente numa investigação mista (qualitativa com reforço quantitativo) e no desenho de pesquisa de estudo de caso, recorreu-se à pesquisa da literatura existente, condução de entrevistas a entidades com responsabilidades neste domínio da Ciberdefesa e análise do questionário dirigido aos militares e civis da FA, concluindo-se que o Nível de *Awareness* em Ciberdefesa da FA está no nível 2 – Em Desenvolvimento –, porque não existe definição, governação ou Otimização de processos, as pessoas apenas possuem noções mínimas de Ciberdefesa e a tecnologia mantem-se por consolidar.

Palavras-chave

Ciberdefesa, Ciberespaço, Cibersegurança, Força Aérea Portuguesa, Nível de *Awareness*, Maturidade.

Abstract

The Cyberspace is nowadays a privileged domain for malicious activities with an impact on business systems, critical infrastructures and even in a state. There has been a maturation of the new concept of war that defies the security and well-being of populations and exposes the existing vulnerabilities in this area.

This study investigates the Level of Awareness in Cyberdefense in the Portuguese Air Force (FA), positioning the Institution in a level of maturity resulting from what is the Cyberdefense Awareness of its members, while analyzing the organizational dimension, reflects about its vulnerabilities and threats and seeks mechanisms that increase their Level of Awareness.

Based on a methodology of inductive reasoning, based on a mixed (qualitative with quantitative reinforcement) investigation and on the case study research design, we resorted to the research of the existing literature, conducting interviews with entities with responsibilities in this Cyberdefense area and analysis of the questionnaire addressed to the FA's military and civilians, it was concluded that the Level of Awareness in FA's Cyberdefence is at Level 2 - In Development - because there is no definition, governance or process optimization, people only have basic Cyberdefense knowledge and technology keeps distant of nurturing.

Keywords

Awareness Level, Cyberdefense, Cyberespace, CyberSecurity, Maturity, Portuguese Air Force

1. Introdução

O Ciberespaço é atualmente um dos principais domínios de aposta das nações para obterem superioridade nas operações militares e, ano após ano, tem sido dada prioridade a nível nacional no sentido de promover e incrementar a capacidade de Ciberdefesa (Estado-Maior-General das Forças Armadas [EMGFA], 2018; Governo de Portugal [Governo], 2018) no Estado, sendo reconhecida por todos como fundamental para operar neste novo domínio da guerra[1].

Alicerçadas nas prioridades acima indicadas e na Estratégia Nacional de Segurança do Ciberespaço (ENSC), em vigor desde 2015, as Forças Armadas Portuguesas (FFAA) assumem-se como ator principal da garantia da "segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais"; contribuindo para a afirmação do "[…] ciberespaço como um domínio de desenvolvimento económico e de inovação" (Governo, 2015, p. 3739).

Contudo, num ambiente totalmente assimétrico e livre de barreiras físicas tangíveis, parece difícil distinguir um utilizador interno, com falta de cultura de Cibersegurança, de um membro de uma qualquer associação criminosa (independentemente do propósito das suas ações: económico; religioso; político), pois ambos contribuem para o aumento do risco nas instituições, no que respeita à preservação da sua informação e segurança dos seus ativos (Instituto da Defesa Nacional [IDN], 2013).

É, portanto, fundamental ir ao encontro do proposto no Eixo 4 da ENSC, promulgada na Resolução do Conselho de Ministros n.º 36/2015, e "informar, sensibilizar e consciencializar" os militares e civis da FA, dotando a Instituição de mecanismos que permitam "lidar com os complexos desafios da segurança do ciberespaço" (Governo, 2015, p. 3741).

No decorrer deste processo normativo e rearranjo organizacional, assim como do crescente interesse dos *media* nesta área – fruto em especial dos recentes casos que envolvem fugas de informação e combate político – a Ciberdefesa tornou-se um termo quotidiano na FA e também nos restantes Ramos das FFAA. No entanto, parece existir uma deficiente perceção, por parte dos militares e civis da Instituição Militar, sobre as capacidades, alcance e competências deste domínio, e de como a desvalorização das ações individuais poderá ter impacto na sua capacidade militar. Ao mesmo tempo, a ausência formal da doutrina e

[1] A Organização do Tratado do Atlântico Norte reconheceu formalmente o ciberespaço como um novo domínio operacional na Cimeira de Varsóvia (7-8 julho 2016).

processos dentro da Instituição e a falta de prioridade dada à Ciberdefesa, parece condicionar a geração de *Awareness* dentro do seio militar.

Com este trabalho, pretende-se criar conhecimento que beneficie a FA, avaliando o atual estado da perceção e consciencialização (*Awareness*) em Ciberdefesa na FA, analisando possíveis fragilidades, correlacionando-as com riscos e consubstanciando esse Nível de *Awareness* no impacto que ele gera na Capacidade de Ciberdefesa da Instituição. Com base nesta avaliação, é ainda objetivo deste trabalho propor um conjunto de instrumentos cuja aplicação contribua para o aumento do *Awareness* em Ciberdefesa na FA.

A presente investigação tem como objeto de estudo o Nível de *Awareness* em Ciberdefesa e encontra-se delimitada (Santos & Lima, 2016, p. 44), nos domínios:

- Temporal, o presente, com avaliação do atual Nível de *Awareness* em Ciberdefesa na FA; fazendo referência a perspetivas futuras, fruto da aplicação dos instrumentos necessários para a maturação do mesmo;
- Espacial, na FA, reforçado com análises pontuais das perspetivas e metodologias utilizadas pelo órgão máximo em Ciberdefesa nas FFAA – Centro de Ciberdefesa (CCD) – e por entidades civis Nacionais com responsabilidades na Cibersegurança Nacional;
- De conteúdo, nos conceitos de *Awareness*, Capacidade de Ciberdefesa e Cibersegurança.

Neste enquadramento, este estudo tem como objetivo geral (OG) *Avaliar o impacto que o Nível de Awareness em Ciberdefesa na FA tem na Capacidade de Ciberdefesa da FA*, alicerçado em três objetivos específicos (OE):

OE1: Avaliar o Nível de *Awareness* em Ciberdefesa na FA.

OE2: Analisar as vulnerabilidades e ameaças da FA de acordo com o Nível de *Awareness* em Ciberdefesa.

OE3: Propor instrumentos cuja utilização poderá elevar o Nível de *Awareness* em Ciberdefesa na FA.

Um conjunto de objetivos operacionalizados na seguinte Pergunta de Partida (PP): *Será que o Nível de Awareness da FA em Ciberdefesa compromete a Capacidade de Ciberdefesa da FA?*

Estruturalmente, este Trabalho de Investigação Individual (TII) encontra-se organizado em cinco capítulos, sendo o primeiro é a presente introdução. O segundo, tem por objetivo proceder ao enquadramento teórico e concetual da investigação. O terceiro, é destinado à apresentação da metodologia e do método utilizados na elaboração deste

trabalho. O quarto, é dedicado à apresentação dos dados, discussão dos resultados e resposta às questões da investigação. O quinto, e último capítulo, apresenta um sumário da investigação e dos resultados obtidos, identifica os contributos para o conhecimento e possíveis novas linhas de ação em estudos futuros, indica limitações do estudo e enumera algumas recomendações de ordem prática.

2. Enquadramento teórico e conceptual

Neste capítulo apresentam-se o estado da arte, os conceitos base e a metodologia seguida neste estudo.

2.1. Revisão da literatura e conceitos estruturantes

O ciberespaço é hoje um apetecível território para a execução de ações maliciosas que, dada a sua abrangência e complexidade, têm como consequência o rápido escalar para uma dimensão internacional. São inúmeros os exemplos recentes de eventos com impacto mundial[2], tendo por isso as organizações com responsabilidades na área da defesa e segurança sentido necessidade de darem passos firmes para responder à ameaça através do reforço das suas capacidades.

A Ciberdefesa tornou-se assim numa área prioritária para a *North Atlantic Treaty Organization* (NATO), tendo sido reconhecido o seu domínio de atuação – o ciberespaço – como o 4º domínio das operações militares, para o qual devem ser desenvolvidas capacidades para o defender, à semelhança dos restantes domínios do mar, terra e ar (NATO, 2016). Decorrente deste desiderato, as nações assinaram um compromisso de intenções, designado de *Cyber Defense Pledge,* com vista ao acompanhamento do cenário de ameaças cibernéticas e melhoria das infraestruturas e redes nacionais numa perspetiva indivisível da segurança e defesa coletiva (NATO, 2016).

Alinhado com as diretivas e recomendações da NATO e da União Europeia (UE) (NATO, 2017; UE, 2013; UE, 2017a), o Conceito Estratégico da Defesa Nacional (CEDN) estabelece, como elemento essencial da estratégia nacional, o estatuto de Portugal como coprodutor de segurança internacional, sublinhando neste particular, o papel das FFAA, mas também de outros setores do Estado, relevando a necessidade de definir uma estratégia integrada, civil e militar, para fazer face às ameaças e riscos (NATO, 2017; UE, 2013; UE, 2017a). Salienta ainda, o potencial disruptivo de ataques efetuados no e através do ciberespaço, perpetrados por Estados, terroristas, criminalidade organizada e indivíduos isolados, podendo afetar infraestruturas críticas, bem como o normal funcionamento da economia e sociedade (Governo, 2013a).

No respeito por estas resoluções, e no que às FFAA diz respeito, edificou-se em 2014 a Capacidade de Ciberdefesa com a criação do CCD na dependência da Direção de Comunicações e Sistemas de Informação (DIRCSI) do EMGFA, através do Decreto-Lei n.º

[2] Ataque à rede distribuição de energia da Ucrânia (2016); Campanha de *ramsonware* -Wannacry - 2017 - afetou milhões de utilizadores e organizações no mundo e que também teve impacto em Portugal.

184/2014. Esta estrutura do EMGFA vem desempenhando um papel importantíssimo na modernização das infraestruturas existentes, com vista a dotar o CCD e os Ramos das FFAA, através dos seus núcleos *Computer Incident Response Capability* (CIRC), das condições necessárias para a condução das operações identificadas na Orientação Politica para a Ciberdefesa (OPC) (Governo, 2013b), na execução das medidas tipificadas na ENSC, e na Diretiva Estratégica do EMGFA 2018-2021 (DEEMGFA), onde é estabelecido o objetivo estratégico de "DINAMIZAR a edificação da capacidade de Ciberdefesa nacional" (EMGFA, 2018, p. 17).

A Ciberdefesa está assim na primeira linha das opções estratégicas ao nível do Governo (Governo, 2019) e das FFAA, contudo, não se observam mudanças efetivas no comportamento da Instituição Militar, quer nas ações que efetuam sobre os seus Sistemas de Informação e Tecnologias de Informação e Comunicações (SITIC), quer na forma é pensada a evolução organizacional da FA, seja ela no campo doutrinário, operacional, logístico ou de gestão de pessoal.

O fator humano é o elo mais fraco numa cadeia complexa, constituída por equipamentos, aplicações e procedimentos de operação e manutenção (FA, 2011). Em concordância, a FA identifica na sua Política de Ciberdefesa, a formação e treino, assim como a prevenção, como pilares e garante da inclusão na organização do conhecimento sobre a Ciberdefesa, introduzindo a consciência sobre esta realidade e o cuidado que ela merece e promovendo, simultaneamente, a tão desejada "cultura de segurança" (FA, 2011).

Apesar do esforço do EMGFA em promover ações de formação e treino nos Ramos, quer através de exercícios nacionais e internacionais no âmbito da Ciberdefesa[3], quer em formações especializadas para os elementos constituintes dos CIRC, parece não existir capacidade militar (DOTMLPFI[4]) para massificar esse treino dentro da Instituição Militar e em particular na FA. Concomitantemente, não existem definidas métricas que permitam avaliar o conhecimento, perceção e consciencialização dos militares e civis da FA sobre a Ciberdefesa, tal como também não está claro o impacto que um determinado nível de *Awareness* possa ter no cumprimento dos desígnios políticos e estratégicos da Nação e na contribuição para a sua segurança e defesa.

[3] Participação anual em exercícios de âmbito NATO como o *CWIX*, *CyberCoalition* e *LockedShields* e de âmbito nacional como o CiberPerseu e o CiberDex.
[4] *Doutrine, Organization, Training, Leadership, Material, Personnel, Facilities and Interoperability*

2.1.1. *Awareness*

O conceito de *Awareness* é o aspeto central nesta investigação, traduzindo-se na perceção e consciência individual e organizacional sobre o papel das ações desenvolvidas sobre os SITIC, as ameaças e as vulnerabilidades para a organização e para as pessoas, assim como um conhecimento atual das medidas de segurança e prevenção a adotar por forma a minimizar o risco (Nunes, 2018). É a medição do seu nível que possibilitará analisar as condicionantes que impactam no desenvolvimento da Ciberdefesa e da exploração do ciberespaço pela Instituição que, unificadas, têm a definição abaixo concetualizada.

2.1.2. Capacidade Ciberdefesa

A capacidade Ciberdefesa baseia-se na articulação harmoniosa de um conjunto de elementos que se complementam e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade (Governo, 2013c). na Figura 1 é possível verificar como a capacidade de Ciberdefesa está dependente destas interações.

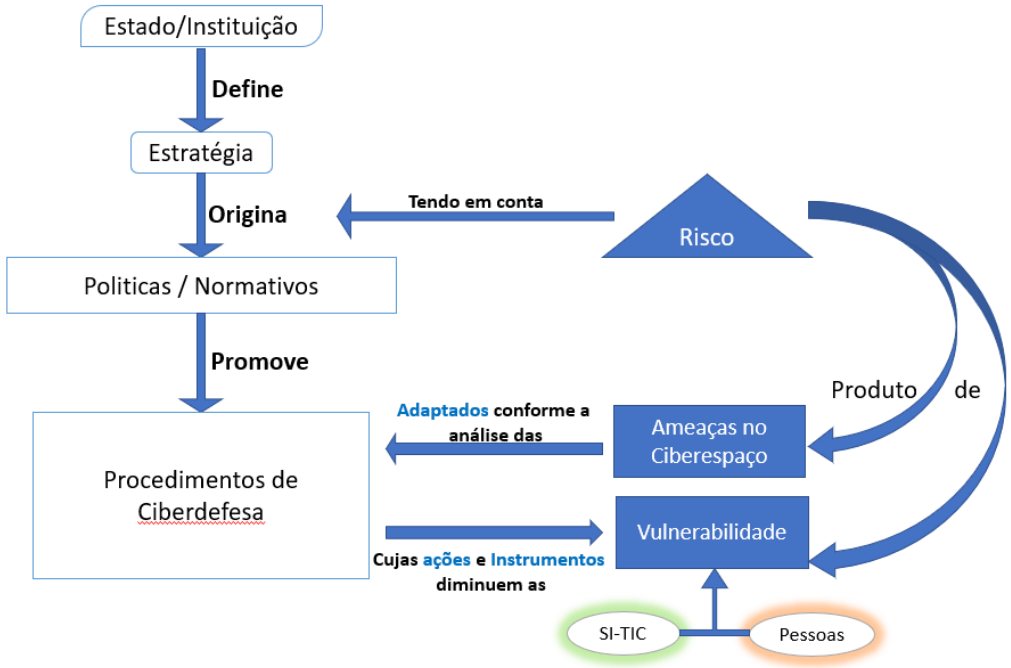

Figura 1 – Capacidade de Ciberdefesa

Neste contexto, o Governo e as estruturas militares entenderam seguir a metodologia para a definição de capacidade militar identificada pelo Departamento de Defesa (DoD) dos Estados Unidos da América (EUA) e potenciada pela NATO com o acrónimo DOTMLPFI

(Hoeserlande, s.d) que se refere a Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade. De acordo com a versão mais recente do memorando dos trabalhos desenvolvidos pelo Grupo de Trabalho para o Desenvolvimento da Capacidade de Ciberdefesa das Forças Armadas (GT-CCFA), foi identificado o seguinte estado da Ciberdefesa nas FFAA (FA, 2018):

– Doutrina: ausência de uma Doutrina Estratégica, Operacional e Tática de Ciberdefesa, onde apenas se consubstanciam algumas táticas, técnicas e procedimentos (TTP) relativas a resposta a incidentes de segurança da informação e responsabilidades afetas a cada uma das entidades envolvidas;

– Organização: necessidade de edificação de um Comando para a Ciberdefesa das Forças Armadas (CCDFA) com capacidade de funcionamento H24/7 otimizando a estrutura base de Ciberdefesa dos Ramos e dos Núcleos CIRC com vista a potenciar a cooperação multilateral com outras entidades e estados;

– Treino: dinamizar a educação e formação em Ciberdefesa com planos de formação técnica específicos para militares do CCDFA e Núcleos CIRC dos Ramos, ao mesmo tempo que se inclui ensino na vertente de Ciberdefesa nos estabelecimentos de Ensino Militares com vista a incrementar a sensibilização e cultura de segurança nas FFAA;

– Material: modernizar e sustentar os parques informáticos centralizando processos aquisitivos e criando planos de sustentação das infraestruturas;

– Liderança: preocupação na gestão da mudança e na convergência de esforços de todas as entidades de topo envolvidas, em especial na garantia de fontes de financiamento adequadas;

– Pessoal: adequar a realidade dos recursos humanos afetos à Ciberdefesa, aos desafios que se colocam, garantindo a sua gestão de carreira e manutenção dos efetivos;

– Infraestruturas: identificar novas infraestruturas para acomodar o CCDFA com as capacidades requeridas. Os CIRC dos Ramos já possuem infraestruturas adequadas, tendo sido coadjuvados pelo EMGFA na sua edificação;

– Interoperabilidade: implementação de plataforma única de partilha de informação ao nível da Defesa Nacional e celebração de protocolos com vista à dinamização do intercâmbio de informação, capacidades e recursos humanos com atores externos.

2.1.3. Ciberespaço

Sendo o meio sobre o qual se desenvolve esta investigação, o ciberespaço define-se como um ambiente complexo, de valores e interesses materializando uma área de

responsabilidade coletiva, que resulta da interação entre pessoas, informação, sistemas de informação, equipamentos tecnológicos e redes digitais, incluindo a Internet (Associação para a Promoção e Desenvolvimento da Sociedade de Informação [APDSI], 2016). Desafiador da soberania dos Estados e da aplicabilidade das leis, este meio é cada vez mais influenciador das decisões políticas ao mesmo tempo que a sua velocidade de evolução e multiplicidade de funções dificulta a governação de quem dele faz uso (Militão, 2014).

2.1.4. Ciberdefesa e Cibersegurança

Nesta investigação, conforme sugere a Figura 2, seguiu-se uma abordagem de separação dos conceitos Ciberdefesa e Cibersegurança. Ainda que próximos, o primeiro decorre exclusivamente da ação das FFAA na aplicação das medidas de segurança (podendo utilizar também a dimensão ofensiva ou de exploração) para proteger os componentes da infraestrutura SITIC contra ciberataques, sendo estes assumidos como uma forma de guerra cibernética, que pode ocorrer em combinação com um ataque físico ou não, destinando-se a perturbar os sistemas de informação de um adversário (Governo, 2013b), enquanto a Cibersegurança reveste-se das precauções e ações que podem ser utilizadas para proteger o ciberespaço contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas, procurando manter a integridade, disponibilidade e a confidencialidade das informações nelas contidas (UE, 2013).

Em suma, paralelamente ao que acontece nos outros três domínios da guerra, a Ciberdefesa preocupa-se com "o conflito entre Estados dentro e através do ciberespaço e todas as consequências que daí advêm" (Klimburg, 2012, cit. por Santos, 2015, p. 9) e é exercida exclusivamente pelas FFAA, enquanto a Cibersegurança tem como área de ação o cibercrime e o *hacktivismo*[5] que estão associados às forças de segurança e a entidades civis como o Centro Nacional de Cibersegurança (CNCS) (Nunes, 2018).

[5] conceito amplo que alia o ativismo ao uso de métodos de *hacking* normalmente declarados como ilegais.

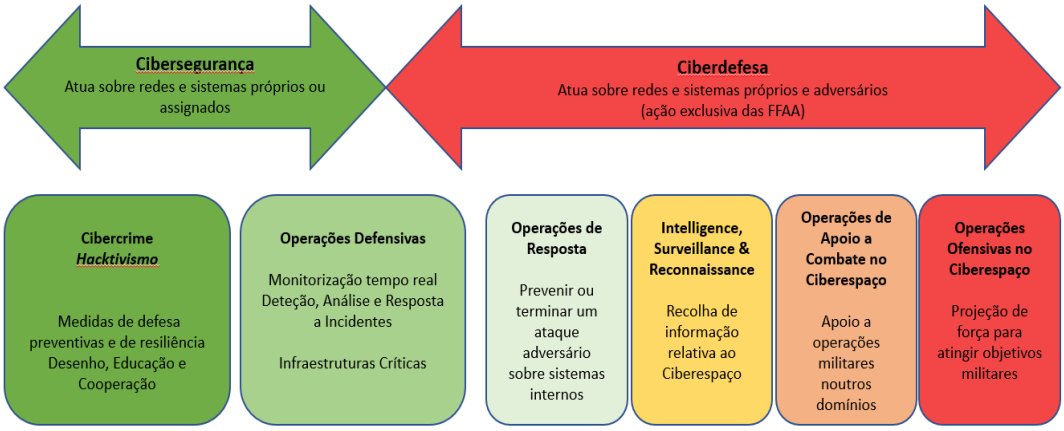

Figura 2 – Cibersegurança e Ciberdefesa

Fonte: adaptado a partir de Rodolfo (2017)

Contudo, decorrente das características especificas do ambiente e de algumas infraestruturas e setores da Nação de responsabilidade partilhada, existirá sempre uma interdependência entre estes dois conceitos e obrigatoriamente relações próximas entre os atores que os utilizam, sendo uma das fortes razões para a necessidade do estabelecimento de uma governação sólida que, em cenário de crise, coordene as atividades, mantendo a clara distinção de competências existentes no campo convencional aplicada ao ciberespaço (Nunes, 2018).

2.1.5. Risco, ameaças e vulnerabilidades

A segurança dos ativos de uma Instituição, interligada ao ciberespaço (ainda que não ligada à Internet), é uma das prioridades do mundo atual por consequência do crescente aumento de atores que vislumbram neste meio uma oportunidade de proveito, independentemente da motivação (e.g. religiosa, económica, política) que rege esse desiderato (Nunes, 2018). Sendo o risco, o produto da presença da ameaça com a exploração da vulnerabilidade, levando a um determinado impacto no funcionamento de um sistema, organização ou Estado e perda de confidencialidade, integridade e disponibilidade da informação manipulada (*European Union Agency for Network and Information Security* [ENISA], 2016; IDN, 2013; Nunes, 2018), fica patente que a forma mais eficaz de reduzir o risco passa pelo combate às vulnerabilidades.

O combate a estas vulnerabilidade deverá passar pela aplicação de diferentes linhas de ação (Nunes, 2018):

– identificar recursos críticos nacionais com maior grau de ameaça;

– conhecer vulnerabilidades dos recursos identificados, sendo que nem todas se situam no plano tecnológico;

– edificar estruturas de proteção e defesa;
– formar e educar as organizações para a presença e reconhecimento das ameaças.

2.2. Modelo de Maturidade de *Awareness* em Ciberdefesa

Por ausência de métricas ou modelo definido identificável, quer na literatura consultada, quer no resultado das entrevistas aos especialistas em Ciberdefesa (Apêndice D), determinou-se um Modelo de Maturidade de *Awareness* em Ciberdefesa (MMAC) (Apêndice B) com parâmetros que por um lado permitem definir o Nível atual de *Awareness* da Instituição e por outro contribuem para a identificação de mecanismos e instrumentos que promovam o seu incremento.

Figura 3 – Modelo de Maturidade de *Awareness* em Ciberdefesa (resumo)

Fonte: Adaptado a partir de Blum (2015) e Spitzner (2016)

A Figura 3 resume o MMAC usado para a definição do Nível de *Awareness* praticado pela Instituição, onde figuram os aspetos fundamentais na avaliação que será feita dos resultados obtidos por intermédio dos diferentes instrumentos de medida utilizados, que neste TII foram a análise documental, as entrevistas a especialistas na área de Ciberdefesa e o questionário aos Militares e Civis da FA.

O detalhe de cada um dos cinco níveis está disponível no Apêndice B.

2.3. Modelo de análise

A presente investigação tem por base o modelo conceptual disponível no Apêndice A.

Para se alcançar uma medição criteriosa, para cada um dos cinco níveis identificados do MMAC constituíram-se três vetores (Pessoas, Processos e Tecnologia) que contribuem

decisivamente para o processo de transformação organizacional (Ramakrishman & Testani, 2011) que se pretende avaliar.

É sobre cada um dos parâmetros (PESS_1; PESS_2; PROC_1;…;TECN_2) associados a estes vetores que se vão analisar os resultados obtidos através dos instrumentos de medida, podendo cada parâmetro ser medido através de um ou mais instrumentos.

Considera-se um determinado Nível de *Awareness* atingido quando todos os parâmetros de cada um dos vetores desse Nível, e dos anteriores, se verifica, podendo ser admissível que, e.g., um ou mais parâmetros se encontrem no Nível 4 mas que o Nível de *Awareness* da Instituição não ultrapasse o Nível 2.

Após conhecido o nível de *Awareness*, serão analisadas as vulnerabilidades e ameaças associadas aos parâmetros, tendo em conta o nível de cada um e, por fim, serão propostos instrumentos que incrementem o nível nesses mesmos parâmetros.

3. Metodologia e método

Apresenta-se, neste capítulo, a metodologia e o método que orientam esta investigação.

3.1. Metodologia

Conforme Instituto Universitário Militar (IUM) (2018a), a metodologia da presente investigação segue um percurso constituído por três fases:

- Exploratória, com recurso a análise documental, entrevistas exploratórias, enquadramento conceptual, formulação do problema, objetivos e perguntas, conforme mapa conceptual do modelo de análise disponível no Apêndice A.
- Analítica, por intermédio da recolha, apresentação e análise dos dados do questionário e das entrevistas semiestruturadas realizadas.
- Conclusiva, orientada para a avaliação e discussão dos resultados, apresentação das conclusões, contributos para o conhecimento, limitações, sugestões para estudos futuros e recomendações.

No que respeita ao tipo de raciocínio, o presente estudo de caso é indutivo, ao partir da observação de factos particulares para, através da sua associação, estabelecer generalizações (Santos & Lima, 2016, p. 20), fundamentada numa estratégia de investigação mista (qualitativa com reforço quantitativo) com o intuito de, por um lado, obter convergência e robustez dos resultados – triangulação e reforço – e por outro lado validar, com dados, os resultados da avaliação qualitativa efetuada (Bryman, 2012, p. 632, cit. por Santos & Lima, 2016, p. 127).

3.2. Método

De seguida são apresentados os procedimentos efetuados com especial enfoque nos instrumentos de recolha e nas técnicas de tratamento de dados utilizadas.

3.2.1. Participantes e procedimento

Após enquadradas as competências e atividades das entidades que contribuem, dentro da FA, para as operações no ciberespaço e por análise da documentação e legislação nacional existente, foram identificados como entidades-chave neste estudo: o Diretor de Informação da FA; a Divisão de Comunicações e Sistemas de Informação (DIVCSI); o Diretor da Direção de Comunicações e Sistemas de Informação (dDCSI) e o Chefe da Secção de Ciberdefesa da Repartição de Tecnologias de Informação (RTI-SCD); a Direção de Instrução (DINST) e o Departamento Jurídico da FA (DJFA), a quem foram propostas entrevistas semiestruturadas. O CCD, apesar de ser uma estrutura fora da FA, foi também considerado

como entidade-chave nesta investigação por ser o elo de ligação à restante estrutura Nacional de Cibersegurança e principal produtor de doutrina e formação na área, ao nível das FFAA. Foi solicitada disponibilidade para contributos durante a fase exploratória e para integrar a investigação, tendo havido recetividade e consentimento de todos.

Derivado do peso que a componente humana tem nesta área, tornava-se obrigatório trazer para a investigação os militares e civis da FA e a sua avaliação do *Awareness* individual realizado por intermédio de um Questionário submetido para aprovação a Sua Ex. o Chefe de Estado-Maior da Força Aérea.

3.2.2. Instrumentos de recolha de dados

Decorrente do indicado acima, foram construídos sete guiões de entrevista semiestruturada (Apêndice C), adaptados a cada uma das entidades entrevistadas onde, em especial na entrevista ao Chefe da Secção de Ciberdefesa da FA, foram pedidos dados numéricos concretos de alguns indicadores. As entrevistas foram recolhidas por *email* com pedido expresso de utilização e citação neste trabalho. Por impossibilidade de agenda, não foi possível contar com os contributos do Diretor da Informação da FA e da DINST.

Adicionalmente, foi elaborado um questionário e submetido para resposta a todos os militares e civis da FA (Apêndice E).

3.2.3. Técnica de tratamento de dados

Para avaliação do Nível de *Awareness* em Ciberdefesa da FA, tendo em conta o MMAC identificado, no espaço qualitativo, recorreu-se à interpretação da informação recolhida, das entrevistas semiestruturadas e da literatura existente, enquanto no espaço quantitativo, efetuou-se uma "(…) recolha de dados observáveis e quantificáveis, baseados na observação de factos, acontecimentos e fenómenos objetivos (…)" (Santos & Lima, 2016, p. 27), por via da realização de um questionário a todos os militares e civis da FA sobre a temática e tendo também em conta dados e indicadores recolhidos das entrevistas semiestruturadas.

Decorrente dessa avaliação, utilizando a metodologia DOTMLPFI, propôs-se um conjunto de instrumentos associados aos diversos parâmetros com vista ao incremento do Nível de *Awareness* e, consequentemente, à minimização do risco afeto à presença das vulnerabilidades na Capacidade de Ciberdefesa.

A amostra recolhida pelo Questionário, representativa do universo FA, corresponde a 614 respostas completas do Questionário, com um grau de confiança de 95% e uma margem de erro de 10%. O Questionário encontrava-se dividido em cinco partes que correspondem à: caracterização pessoal; perceção organizacional da Ciberdefesa na FA; perceção sobre as

políticas, normas e procedimentos existentes; utilização da tecnologia; e, por fim, à perceção das necessidades de treino e formação.

Os dados foram recolhidos e tratados, inicialmente online, no *GoogleForms*, e, posteriormente, analisados através de uma aplicação informática designada de *IBM® SPSS® Statistics* seguindo técnicas de estatística descritiva.

4. Apresentação dos dados e discussão dos resultados

Neste capítulo serão analisados e discutidos os resultados dando resposta às Perguntas Derivadas (PD) e à Pergunta de Partida (PP).

4.1. Nível de *Awareness* em Ciberdefesa da FA

O modelo de análise utilizado para medição e identificação do Nível de Maturidade e resposta à PD1 está detalhado no Apêndice B.

De acordo com o Chefe do CCD, H. Jesus (entrevista por *email*, 18 de junho de 2019), o "fator humano é o elo mais fraco nas organizações" no que diz respeito à ciberhigiene[6] e, como tal, interessa identificar a perceção e consciência que os militares e civis da FA têm da capacidade institucional instalada nesta área assim como da sua responsabilidade individual na manutenção de um nível de segurança adequado nos seus SITIC, contribuindo de uma forma direta para a dimensão defensiva da Ciberdefesa.

Apesar da opinião generalizada por parte dos entrevistados sobre a transversalidade desta matéria, identificaram-se um conjunto de questões de caracterização pessoal no sentido de descrever a segregação do conhecimento em Ciberdefesa por via do grau de habilitações literárias, idade ou funções desempenhadas na Instituição, podendo os resultados obtidos ser consultados no Apêndice F.

Dos inquiridos que dizem ter um nível Elevado/Muito Elevado de *Awareness* em Ciberdefesa (25% do total do universo), verifica-se que 28% destes (7% do total do universo) desconhecem as estruturas de Ciberdefesa das FFAA o que, associado aos dados recolhidos sobre a forma como os militares e civis adquiriram esse nível de *Awareness* em Ciberdefesa (Gráfico 2), se pode interpretar numa aparente confusão de conceitos com as atividades de Cibersegurança, como consubstancia o Gráfico 1.

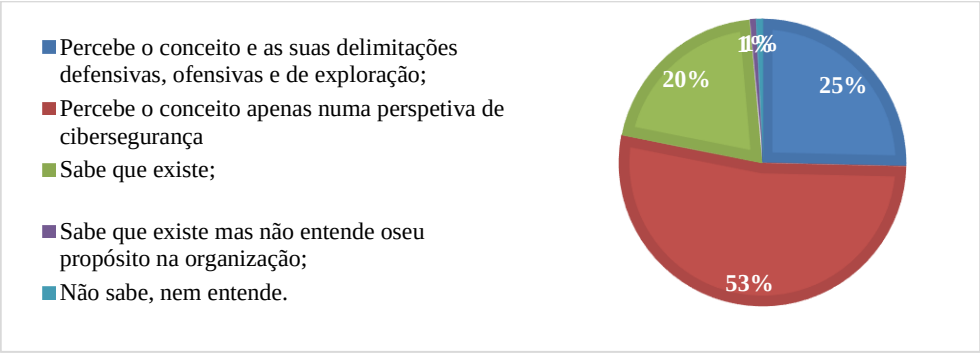

Gráfico 1 – Entendimento sobre conceito de Ciberdefesa

[6] Aplicação de boas práticas do mundo digital

Na questão de múltipla resposta que originou o Gráfico 2, identifica-se uma aquisição maioritária de conhecimento em Ciberdefesa proveniente de fontes civis, no entanto destaca-se o elevado número de inquiridos que obteve essa perceção com recurso às divulgações internas da FA. Este indicador, associado ao facto de mais 76% dos inquiridos conhecerem a estrutura de Ciberdefesa da FA (independentemente da capacidade de identificar os seus quantitativos humanos/tecnológicos ou ações desenvolvidas), é revelador da crescente veiculação da informação, podendo o parâmetro PESS_3 do MMAC, associado ao vetor Pessoas, ser enquadrado no Nível 3, havendo ainda assim possibilidade de melhoria na transmissão de informação e cultura em Ciberdefesa dentro da Instituição (Blum, 2015).

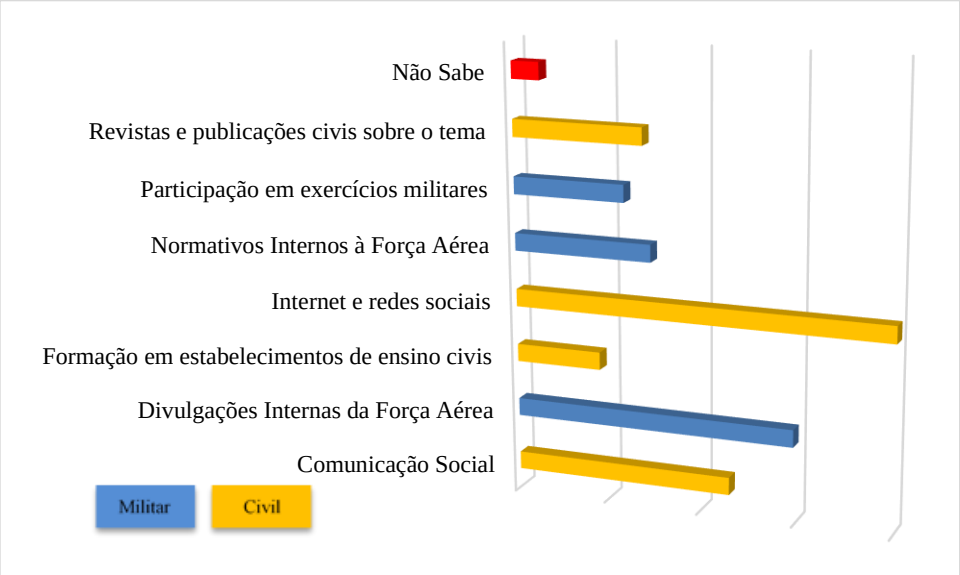

Gráfico 2 – Forma de aquisição de *Awareness* em Ciberdefesa

No que concerne à perceção do vetor Tecnologia, associado à Ciberdefesa na FA, por parte dos militares e civis da FA é notório o *Awareness* existente para a presença das capacidades definidas de auditoria e resposta a incidentes (Gráfico 3), para a qual muito contribuiu a constituição do CIRC, conforme advogado pelo dDCSI, Sr. BGen José Morgado (entrevista por *email*, 24 de abril de 2019), reforçado com os resultados da resposta à questão sobre a existência de mecanismos de análise e registo de ações e atividades efetuadas no posto de trabalho, email e acesso à internet, e à pergunta respeitante ao conhecimento sobre a implementação de mecanismos de segurança e proteção ao nível dos SITIC, ambos com resultados superiores a 80% (82% e 86,5% respetivamente). Em termos de incidentes com necessidade de resposta humana, registaram-se aproximadamente 45 casos, assinalando-se ainda milhares de situações de tentativa de intrusão e outros eventos

internos (e.g. vírus e ficheiros maliciosos) que foram barradas pelos equipamentos de segurança geridos pela Ciberdefesa da FA (A. Castro, *op. cit.*). O conjunto destes dois indicadores colocam os parâmetros PROC_3 e TECN_2 no Nível 3 do MMAC.

A obsolescência dos SITIC é uma realidade na FA (A. Castro, *op. cit.*) que nos últimos anos se tem combatido com o reforço de verbas e imposição de ações minimizadoras de risco, em especial no que diz respeito à erradicação ao sistema operativo Microsoft WindowsXP do posto de trabalho (J. Morgado, *op. cit.*). Contudo não está presente um plano que faça face a todos os elementos do catálogo SITIC por atualizar, considerando-se assim o parâmetro TECN_1 no Nível 3 do MMAC.

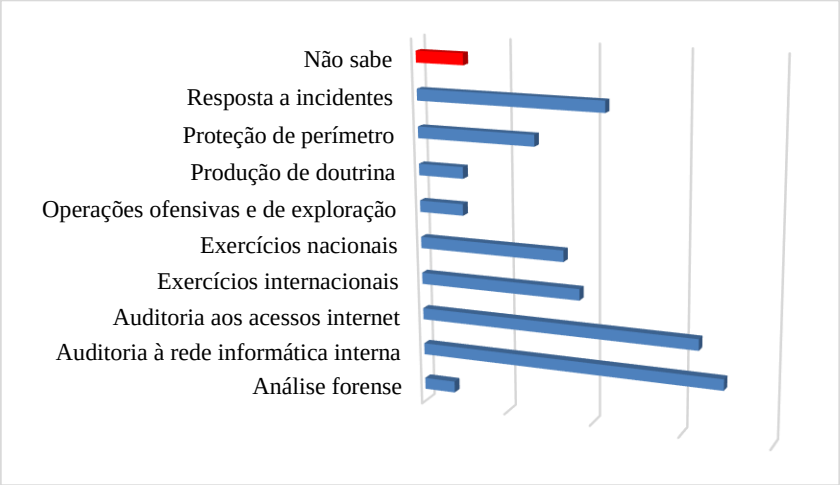

Gráfico 3 – Atividades desenvolvidas pela Ciberdefesa

Registe-se ainda o reconhecimento da existência de organização e treino pela participação em exercícios nacionais e internacionais (J. Morgado, *op.-cit.*). Durante o ano de 2018, a FA participou em mais de dez exercícios com presença de equipas dedicadas à Ciberdefesa, onde se destacam os exercícios nacionais CiberPerseu e Lusitano e os internacionais LockedShields e CyberCoalition, contribuído de forma significativa para a formação da comunidade técnica – parâmetro PESS_2 no Nível 2.

No que diz respeito à identificação da missão da Ciberdefesa na FA e razões para lhe ser conferida prioridade no investimento, os militares e civis da FA souberam identificar corretamente, conforme Gráfico 4, as áreas prioritárias explanadas na ENSC, sendo revelador do conhecimento das diretivas superiores que têm sido emitidas neste domínio (H. Jesus, *op. cit.*). Existe, todavia, um aspeto ao qual os militares e civis da FA atribuem pouca relevância: cumprimento da Lei. Segundo a Diretora do DJFA, Sra. TCor. C. Santos (entrevista por email, 20 de maio 2019), existe "uma certa displicência das pessoas dado que

associam o ciberespaço a um espaço de impunidade, talvez relacionada com a falta de aplicação dos mecanismos legais coercivos que já se encontram previstos na Lei do CiberCrime".

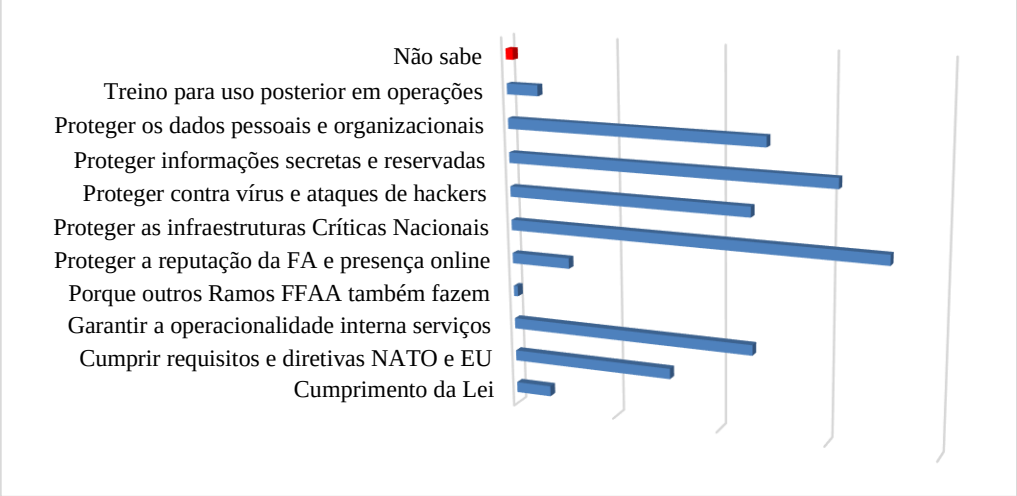

Gráfico 4 – Razões para o Investimento em Ciberdefesa

Abordando o vetor Pessoas do MMAC, verifica-se que militares e civis da FA, conforme defendido por A. Telha (entrevista por *email*, 9 de junho de 2019) "estão minimamente cientes das suas responsabilidades" e têm "uma ideia geral dos comportamentos a adotar" (A. Castro, entrevista por *email*, 3 de junho de 2019) comprovado pelo seguinte gráfico.

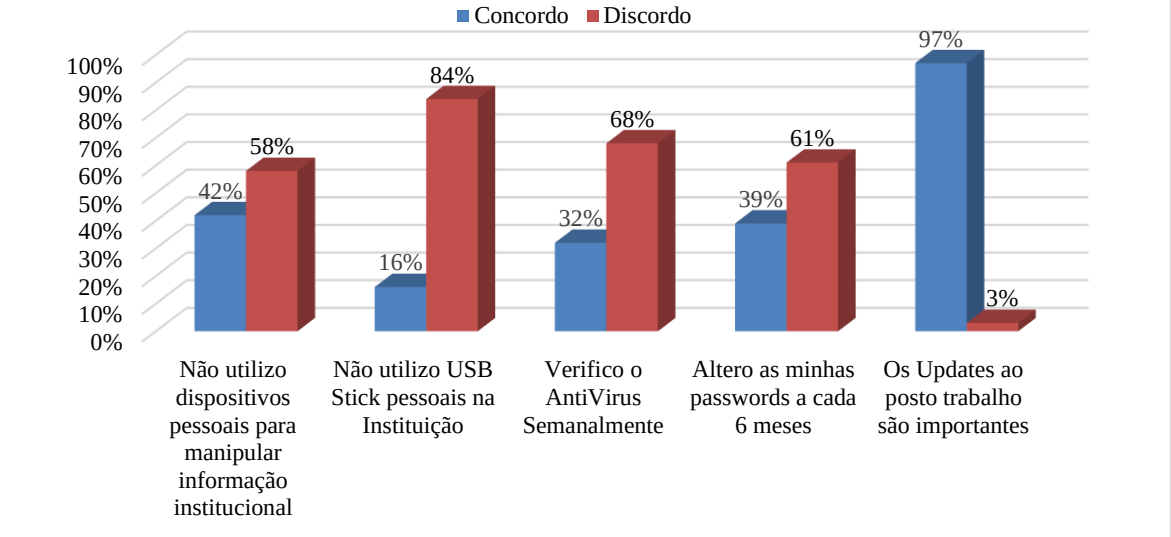

Gráfico 5 – Respostas a questões de comportamento individual em SITIC

No que concerne ao conhecimento dos normativos e regras em vigor na área de SITIC e Ciberdefesa, verifica-se que a grande maioria dos inquiridos sabe da sua existência, mas não conhece o seu conteúdo (Gráfico 6), numa percentagem que, somada aos que não sabem da sua existência, ultrapassa os 60% do universo.

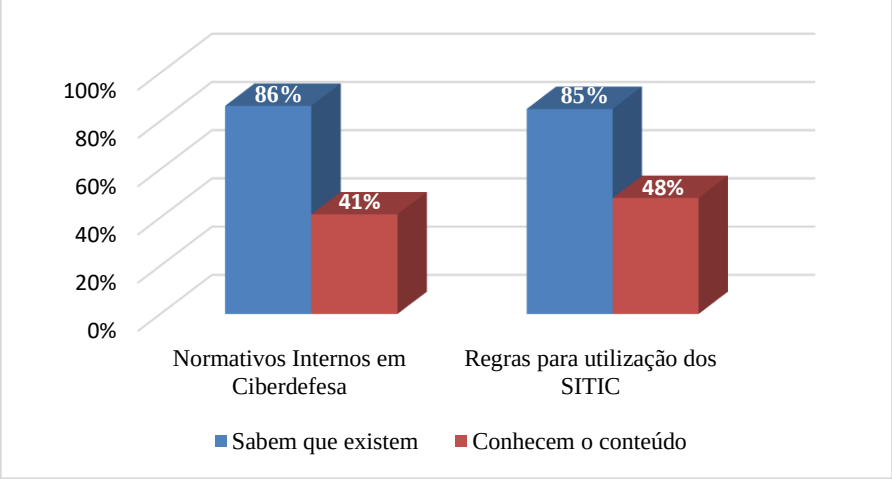

Gráfico 6 – Conhecimento das normas e regras em Ciberdefesa e SITIC

Tendo em conta os resultados identificados, fica patente a ausência de reforço por parte da Instituição na garantia do cabal conhecimento dos assuntos constantes das políticas, normas e regras existentes que regulam as atividades no ciberespaço, com impacto direto naquilo que são os comportamentos e perceção dos seus membros sobre os impactos das suas ações (Gráfico 7), contribuindo para a apreciação do parâmetro PROC_1 no Nível 3.

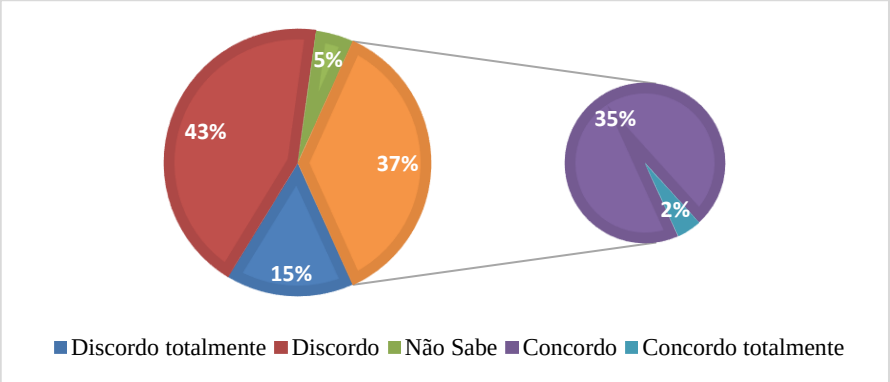

Gráfico 7 – Os Militares e Civis da FA estão informados sobre as consequências das suas ações sobre os SITIC

Interligando a análise já enquadrada pelo Gráfico 5, avalia-se o parâmetro PESS_1 do MMAC no Nível 2 pelas noções mínimas de Cibersegurança assumidas pelos militares e

civis da FA na utilização dos SITIC, apesar da disponibilização de normas e diretivas dentro da Instituição (A. Telha, *op. cit.*; J. Morgado, *op. cit.)*

Embora existam esforços no sentido de promover a obtenção de conhecimento em Ciberdefesa com palestras nas unidades de ensino, acompanhamento das auditorias nas unidades e outras ações não planeadas, fica patente através do Gráfico 8, que os militares e civis da FA entendem que a Instituição não tem contribuído de forma decisiva para a melhoria do seu *Awareness* em Ciberdefesa, colocando o parâmetro PROC_2 no Nível 2 do MMAC.

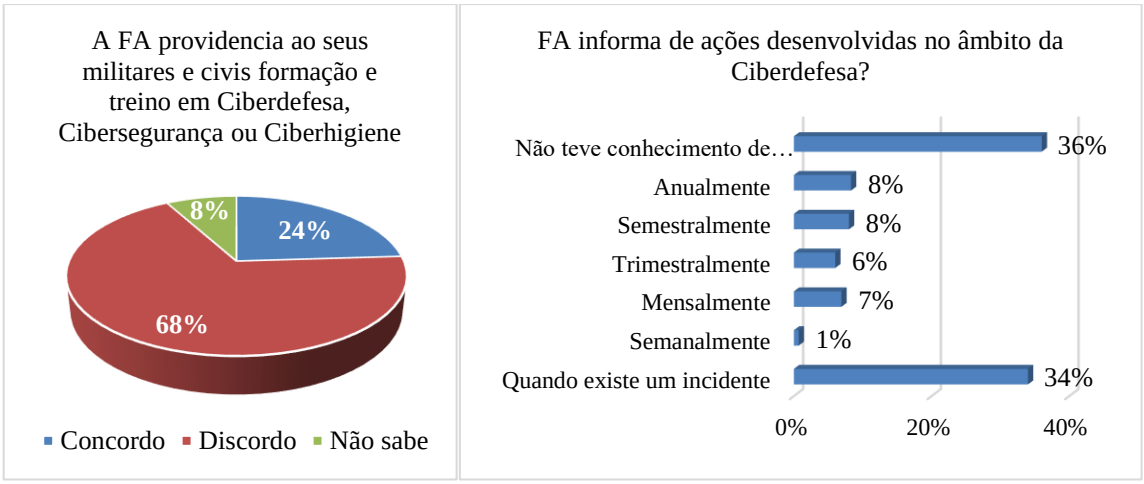

Gráfico 8 – Perceção sobre existência de formação, treino e divulgação de ações desenvolvidas no âmbito da Ciberdefesa

Ainda que esta carência de formação e divulgação resulte num posicionamento mais baixo na escala de maturidade (parâmetro PESS_2 no Nível 2), denota-se uma consciencialização e preocupação dos militares e civis da FA pela necessidade de implementação de planos e medidas formativas que, segundo as respostas ao questionário efetuado (Gráfico 9), deverão desenvolver-se maioritariamente com a Integração nos programas de instrução de Base do Militar (estabelecimentos de ensino) e ações de divulgação, colóquios ou seminários, incidindo os últimos, prioritariamente, sobre membros da Instituição cujas atribuições incluam aspetos relacionados com segurança da informação. Sendo efetuada, colocaria o parâmetro PESS_2 no Nível 4 do MMAC.

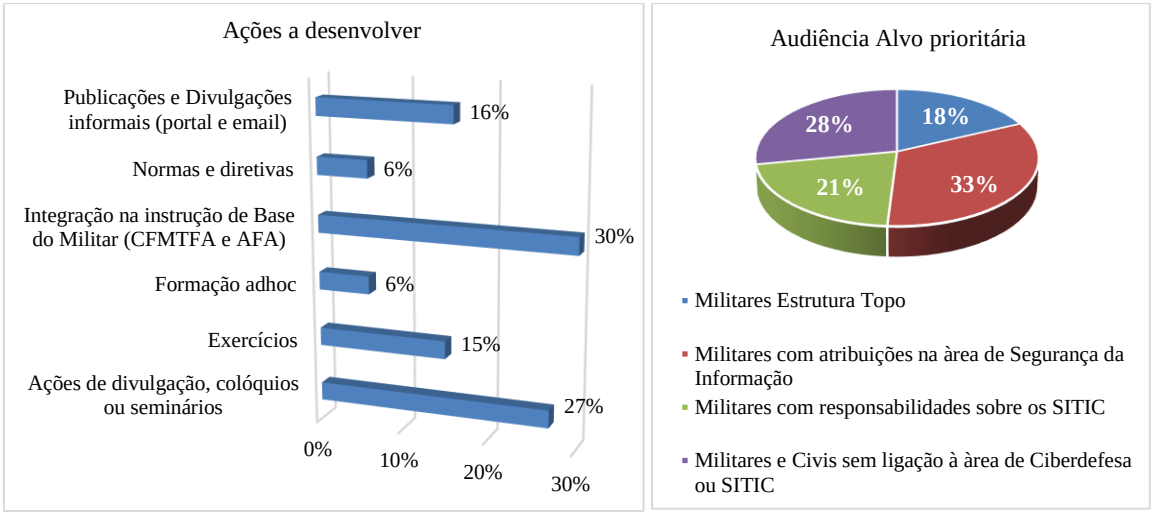

Gráfico 9 – Como melhorar conhecimentos em Ciberdefesa e audiência alvo prioritária

Ressalve-se que, as diferenças de percentagem entre as audiências alvo prioritárias identificadas pelos inquiridos são mínimas, em concordância com as convicções dos especialistas entrevistados que entendem que todos os membros da FA devem ser alvo das medidas de aumento de *Awareness* e, preferencialmente, logo no momento da sua entrada na Instituição. Esta consciência individual da necessidade de geração de *Awareness* é um fator positivo a ter em conta na avaliação.

4.1.1. Síntese conclusiva e resposta à PD1

Em suma, analisando cada um dos vetores e seus parâmetros, tendo por base os instrumentos de medida identificados, chegamos às seguintes conclusões:

– No vetor Pessoas, a FA enquadra-se no nível 2 do MMAC uma vez que, apesar de existir um conhecimento dos procedimentos e estruturas de Ciberdefesa da FA por via de alguma divulgação interna (PESS_3-Nível_3), o respeito pelas regras e normativos instituídos não constitui o quotidiano das ações dos militares e civis da FA (PESS_1-Nível_2). Existe noção da necessidade de incremento de formação e divulgação nesta área, mas a Instituição não está ainda capaz de integrar ativamente esse treino e difusão nas capacidades e missão de todos os seus membros (PESS_2-Nível_2), conforme fica patente na ausência de orçamento dedicado diretamente a programas de *Awareness* em Ciberdefesa na FA (A. Telha, *op. cit.*; J. Morgado, *op. cit.*).

– No vetor Processos, o *Awareness* em Ciberdefesa na FA encontra-se também no Nível 2 de maturidade apesar de já ter alcançado importantes parâmetros do nível superior. A estrutura organizacional está definida nas suas relações com o conjunto das FFAA e existe uma definição dos papeis e responsabilidades associados à capacidade (PROC_1-Nível_3).

No entanto, observa-se que o fluxo de informação dentro da FA não está formalmente definido (ao contrário da relação com o CCD que está estabelecida no PEMGFA CSI/301) e que a revisão dos normativos enquadradores não acompanha a evolução da capacidade de Ciberdefesa e a sua necessidade crescente de um processo específico para a tomada de decisão dado o impacto e transversalidade das suas ações. Estão identificadas algumas atividades de consciencialização em Ciberdefesa, normalmente resultantes de incidentes ou enquadrados pelas atividades ou exercícios sob responsabilidade do EMGFA, mas não existe qualquer projeto de geração de *Awareness* nem tão pouco está identificada a audiência alvo (PROC_2-Nível_2). O CIRC está constituído e definido nas suas ações (PROC_3-Nível_3), mas não tem processos formais de ativação, resposta e comunicação implementados (A. Castro, *op. cit.*).

– Tecnologicamente, o nível de *Awareness* em Ciberdefesa na FA considera-se Definido – Nível 3 – uma vez que a Instituição tem implementados controlos e ferramentas que possibilitam ter uma perceção das vulnerabilidades e ameaças que constituem o risco para a Instituição (TECN_2-Nível_3). Em adição, a FA tem participado com a sua tecnologia e os seus homens em diferentes exercícios nacionais e internacionais o que, para além dos ganhos de conhecimento técnico e processual para os participantes, é gerador de *Awareness* pelo impacto positivo que produz na estrutura decisora superior. Apesar de ainda se lidar com equipamentos obsoletos, existe um processo de mitigação e renovação tecnológica identificado e em curso cuja conclusão, não afeta a ponderação (TECN_1-Nível_3) dada neste vetor Tecnológico.

Pela análise efetuada, e em resposta à PD1, *Qual é o Nível de Awareness em Ciberdefesa na FA?*, conclui-se que a Instituição, de acordo com o MMAC proposto e a análise feita sobre os três vetores do processo de transformação organizacional, está no Nível 2 – Em Desenvolvimento – de *Awareness* em Ciberdefesa apesar de, em especial no vetor Tecnologia se ter alcançado o Nível 3 em todos os parâmetros avaliados.

4.2. Ameaças e Vulnerabilidades resultantes do Nível de *Awareness*

Conforme mapa conceptual do modelo de análise (Apêndice A), foram identificados um conjunto de dimensões e indicadores que concorrem para a resposta à PD2 e que serão analisados de seguida, em consonância com o nível de *Awareness* identificado no ponto anterior para cada parâmetro de cada vetor.

De acordo com Garcia (2002, cit. por Coimbra, 2018, p. 6), "(…) as ameaças à segurança vêm principalmente do exterior (…)" contudo, "(…) os maiores perigos e os que

provocam danos superiores aos sistemas são aqueles que surgem no interior da organização, por pessoas internas, por causa da má formação ou mesmo por descuido ou desconhecimento". Este autor defende uma realidade validada pelos vários especialistas entrevistados e suportada pelo Gráfico 10 referente à comparação dos eventos bloqueados com origem externa e interna, afigurando-se assim como a maior ameaça decorrente do nível de *Awareness* identificado.

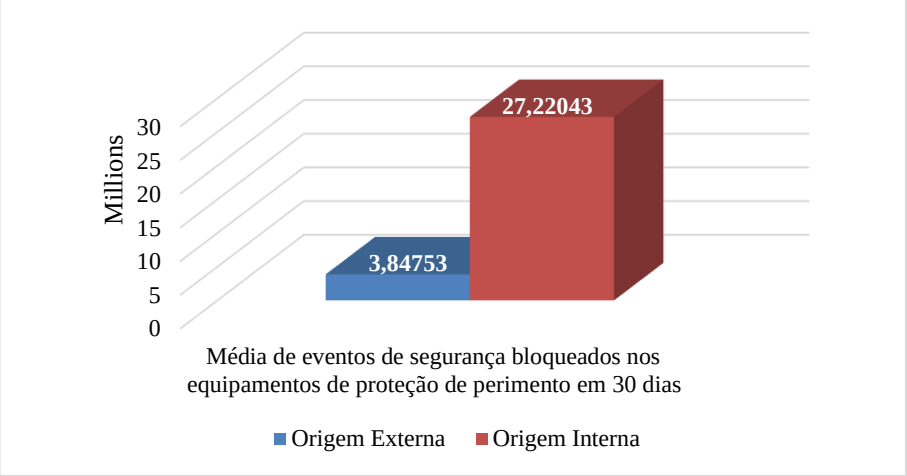

Gráfico 10 – Eventos bloqueados em *firewall* por localização

Relacionando com a posição da Instituição no Nível 2 do MMAC, infere-se que a insuficiente cultura de ciberhigiene, em especial na inobservância das normas e regras de utilização dos SITIC (PESS_1), a inexistência de programas de *Awareness* (PROC_2) e a ausência de uma entidade que governe todo o espetro de atividades neste âmbito (PROC_1), são vulnerabilidades que constituem um risco para a capacidade de Ciberdefesa da FA.

As limitações humanas e materiais para alocar à missão são também uma ameaça à geração de *Awareness* (A. Telha, *op. cit.*). No vetor Pessoas existe dificuldade em manter recursos humanos qualificados e que acompanhem a evolução tecnológica das ameaças e dos próprios SITIC (J. Morgado, *op. cit.*) (PESS_2). No vetor Tecnologia, os equipamentos obsoletos, bem como o software fora de suporte do fabricante, cuja substituição tarda a ser efetuada (TECN_1), representam riscos altíssimos por permitirem, com pouco esforço por parte de um atacante, a exploração de vulnerabilidades técnicas existentes podendo causar impactos substanciais para a Instituição (A. Castro, *op. cit.*). O *Wannacry* foi um exemplo claro de uma exploração deste tipo.

No vetor Tecnologia, assiste-se ainda à necessidade crescente de mobilidade por parte dos militares e civis da FA (TECN_1), sendo um dos fatores que mais complexidade acarreta

para a manutenção de uma atividade Institucional em segurança. As ameaças neste domínio são muitas e variadas e as vulnerabilidades são exponenciadas com a utilização BYOD e COPE[7] cada vez mais frequente na instituição, seja pela obsolescência dos equipamentos já referida anteriormente ou pelo comodismo de unificar a vida pessoal e institucional num único equipamento (conforme identificado através do Gráfico 5). A ausência de regras e normas especificas para estas situações e a incapacidade de monitorizar as suas ações, em especial no que concerne às integrações entre redes privadas e a internet, constituem vulnerabilidades que só poderão ser mitigadas com a edificação de doutrina e processos rigorosos (PROC_1) que regulem a sua utilização (A. Castro, *op. cit.*) e que ainda não foram atingidos no atual nível do MMAC.

Na interligação dos vetores Tecnologia e Processos, identifica-se como ameaça a inexistência de um catálogo de riscos, ameaças, vulnerabilidades e possíveis efeitos associado às infraestruturas e ativos críticos da FA (PROC_3). De acordo com o H. Jesus (*op. cit.*), a "mitigação das eventuais vulnerabilidades detetadas (…) e a análise de risco sobre os seus ativos" é responsabilidade dos Ramos, tendo sido para isso criados e dinamizados os CIRCs respetivos no sentido de terem ferramentas que permitam essas ações. De fato, tem-se assistido a uma evolução do inventário das vulnerabilidades existentes nos SITIC FA, contribuindo para tal as dez auditorias realizadas em 2018 (A. Castro, *op. cit.*), mas derivado mais uma vez da falta de recursos humanos e do tempo necessário à criação de produtos concretos, torna-se difícil passar à estrutura superior o conhecimento do potencial impacto de um ataque cibernético à Instituição, conduzindo inevitavelmente a um distanciamento estratégico e operacional desta problemática, reduzindo-a a uma posição estritamente tecnológico-tática (A. Castro, *op. cit.*) e diminuindo assim o grau de compromisso e patrocínio (PROC_2) que é fundamental para a melhoria continua da capacidade.

Para além do que já foi abordado nos parágrafos anteriores, o nível identificado de *Awareness* constitui uma ameaça em especial pela ausência de uma entidade agregadora e responsável pela totalidade do dispositivo de Ciberdefesa na FA (PROC_1) com capacidade de promover a necessidade de *Awareness* junto da estrutura superior da Instituição e de desenvolver as métricas (TECN_2) entendidas como importantes para o acompanhamento

[7] *BYOD* e *COPE*: acrónimos que identificam a forma de utilização dos dispositivos eletrónicos ao serviço de uma determinada Instituição/Organização: *BYOD – Bring Your Own Device* – corresponde à utilização de um dispositivo pessoal para uso na Organização; *COPE - Corporate Owned, Personally Enabled* – corresponde à utilização de um dispositivo da Organização também para fins pessoais (UE, 2017b).

da evolução da perceção e consciencialização organizacional em Ciberdefesa na FA. Essa inexistência, associada à falta de processos formais definidos de comunicação interna de eventos/incidentes e correção/mitigação/inibição de serviços com possível impacto operacional (PESS_3;PROC_2), representam vulnerabilidades que se consubstanciam na possível inoperância da estrutura de Ciberdefesa por pressão da necessidade de operação, conforme é exemplo a permanência em funcionamento na FA, há mais de cinco anos, de um quarto de postos de trabalho com um Sistema Operativo sem suporte do fabricante e com falhas de segurança conhecidas e impossíveis de corrigir (A. Castro, *op. cit.*).

4.2.1. Síntese conclusiva e resposta à PD2

De forma sucinta, e em resposta à PD2: *Quais são as ameaças e vulnerabilidades potenciadas pelo Nível atual de Awareness da FA?,* conclui-se que o Nível 2 de *Awareness* em Ciberdefesa acarreta ameaças e vulnerabilidades graves quer à geração e incremento do próprio *Awareness* organizacional, quer à capacidade total de Ciberdefesa da FA.

A aposta nas pessoas parece ser a forma mais acertada de diminuir a ameaça, seguida da implementação de doutrina e processos acompanhados de patrocínio da estrutura superior da FA e, por último do reforço da capacidade tecnológica com o foco na diminuição das vulnerabilidades passiveis de explorar pelas ameaças.

4.3. Instrumentos de incremento de *Awareness*

Com vista ao incremento de *Awareness* em Ciberdefesa na FA devem ser tomadas medidas que possibilitem a melhoria de todos os parâmetros constituintes do MMAC conduzindo objetivamente a uma diminuição das vulnerabilidades identificadas anteriormente, potenciando a capacidade associada às ações no ciberespaço.

Conforme identificado no ponto 2.1.2 desta investigação, a geração de capacidade militar implica uma avaliação seguindo os diferentes elementos da metodologia DOTMLPFI. Assim, tendo por base a análise efetuada e o estado de arte apresentado pelo GT-CCFA, propõem-se de seguida os instrumentos que, sendo aplicados, permitem aumentar o nível de *Awareness* em Ciberdefesa associando-os ao elemento gerador de capacidade militar.

4.3.1. Liderança

Ponto fulcral em qualquer transformação organizacional, está diretamente ligado com o vetor Pessoas e Processos. Qualquer projeto que envolva a totalidade da FA e que pretenda modificar comportamentos (PESS_1), tem necessariamente que possuir, além do aval e

envolvimento superior, o suporte financeiro, logístico e de recursos humanos (J. Morgado, *op. cit.*).

Deve-se identificar patrocinadores na estrutura superior da Instituição (promovendo-o com recurso a inquéritos, relatórios de atividades e demonstrações de exemplos noutras Organizações) (PROC_2). Torna-se fundamental a identificação de um *Chief Information Security Officer* (CISO) que governe todas as atividades relacionadas com a Ciberdefesa, conforme identificado nas boas práticas existentes (ENISA, 2017; Tchipako, 2017) evitando a difusão existente entre os papeis do Diretor de Informação, da DIVCSI e da DCSI em relação a este domínio específico (PROC_1) e podendo, entre outras atribuições, ser o responsável por desenhar e fazer aprovar um Programa de geração de *Awareness* (PROC_2) com metas, custos e identificação de objetivos estratégicos, contribuído deste modo para o incremento do nível nos parâmetros indicados.

4.3.2. Doutrina e Organização

Neste campo, ficaram claras as vulnerabilidades da FA no que respeita à produção de doutrina (PROC_1), à definição de métricas (TECN_2), ao estabelecimento de planos de comunicação/divulgação (PESS_3) e à formalização das relações entre as equipas técnicas e a tomada de decisão (A. Castro, *op. cit.*) (PROC_3). É fundamental a redefinição das políticas e normativos internos neste domínio, em especial a adequação do RFA390-6 à realidade atual do dispositivo (A. Telha, *op. cit.*).

Assim, associado a estes dois elementos, entende-se como instrumentos de aumento de *Awareness* e potenciador dos parâmetros vulneráveis:

(a) Em resposta a PROC_3, a criação de uma escala de ameaça no ciberespaço com impacto nas políticas de utilização e disponibilidade de serviços. Planos de contingência e mobilidade são muitos deles anteriores à existência do domínio ciberespaço (J. Morgado, *op.-cit.*) e, ainda que não seja consensual entre os especialistas entrevistados, é uma matéria a considerar e já em análise pelo CCD tendo em conta as ferramentas que podem auxiliar nessa definição (H. Jesus, *op. cit.*).

(b) Para aumento do TECN_2, a criação de métricas de *Awareness* e manutenção do seu histórico como forma de percecionar o estado real da Ciberdefesa na FA ao invés das atuais perceções resultantes da amostragem retirada dos exercícios ou auditorias (A. Telha, *op. cit.*). Alguns dos parâmetros a incluir:

- # pessoas vítimas de *Phishing*
- # de sistemas infetados
- # de incidentes reportados

- # de equipamentos *standalone*
- # de pessoas que completaram o programa de treino em Ciberdefesa

As métricas, tal como todas as atividades neste domínio, devem estar alinhadas com a missão e harmonizadas com os restantes Ramos das FFAA e outras áreas da FA, em especial a jurídica, cujo enquadramento é fundamental para melhor assessorar o decisor (C. Santos, *op. cit.*)

(c) Em relação a PROC_1, redefinição da posição da Ciberdefesa na estrutura orgânica da FA, mantendo a componente técnica do CIRC junto da DCSI mas aumentando a sua preponderância dentro da Instituição como forma de potenciar o seu acesso a financiamento (A. Castro, *op. cit.*) e a interação com a componente operacional e comando e controlo (A. Telha, *op. cit.*) cujas atividades se mantêm praticamente segregadas, com claro prejuízo da segurança dos meios e pessoas, em especial nos destacamentos no estrangeiro.

(d) Para incremento do PESS_3, a criação de um plano de comunicação que promova e incentive os membros da FA a adotar comportamentos que contribuam para o reforço da dimensão defensiva da Ciberdefesa, libertando a componente técnica para evoluir nas restantes dimensões, em apoio direto às operações (Spitzner, 2016).

4.3.3. Treino e Pessoal

O vetor Pessoas é o maior beneficiado do incremento destes dois elementos da capacidade militar. O treino e formação dos membros da Instituição é um aspeto fundamental em todas as atividades dentro da FA e a capacidade de operar em segurança os SITIC, pela sua transversalidade, deve ser assumida como uma necessidade básica para todos os membros da FA.

Assim, identificam-se como instrumentos:

(a) Novos Programas de Instrução (PDINST) para inclusão *ab initio* de conteúdos relacionados com Ciberdefesa, potenciando PESS_1 e PESS_2, seja na vertente prática de Cibersegurança, seja na vertente legal e organizacional da capacidade na FA e suas interações com as restantes estruturas da Defesa, garantindo revisões bienais por forma a incorporar novos assuntos relevantes e remover ou atualizar conceitos ultrapassados;

(b) Programa de formação On-line, à semelhança do desenvolvido recentemente pelo CNCS, que permita de uma forma interativa, simples e regular, manter atualizados os conhecimentos dos membros da Instituição neste domínio (A. Telha, *op. cit.*);

(c) *Briefings* à estrutura superior com a comunicação de resultados do programa de formação, dos exercícios, dos incidentes e das auditorias efetuadas contribuindo para incremento do parâmetro PROC_2;

(d) Como medida para aumento do nível no PESS_3 e TECN_2, relatórios públicos sobre resultados de exercícios, panorama da formação, evolução do nível de *Awareness* e necessidades reciclagem periódica.

Em relação ao vetor Pessoal, fica patente de todas as entrevistas efetuadas, a necessidade urgente de aumento de quantitativos para este domínio, devendo ser garantida a sua qualificação e atualização permanente (J. Morgado, *op. cit.*). Assumindo a dificuldade no recrutamento nesta área, surge como medida desejável, a reativação do quadro ENGINF com *baseline* comum em SITIC e especialização posterior no domínio ciberespaço (A. Castro, *op. cit.*).

4.3.4. Material, Infraestruturas e Interoperabilidade

Associado à valorização do vetor Tecnologia, com impacto direto nos seus dois parâmetros, entendem-se como instrumentos geradores de *Awareness:*

(a) Implementação de uma *framework* que regule todo o processo de governação da infraestrutura tecnológica e das suas relações com o objetivo e missão da FA;

(b) Catálogo de hardware e software de todos os ativos críticos da organização, suas vulnerabilidades e períodos de manutenção programada;

(c) Diretiva e plano anual de maturação tecnológica com revisão de requisitos de Ciberdefesa em linha com evolução dos *standards* internacionais;

(d) Implementação de um laboratório e um simulador de incidentes informáticos com capacidade para realizar ações sobre audiências alvo definidas por forma a dotar as equipas técnicas e os restantes membros da FA da perceção sobre as consequências dos incidentes reais;

(e) Realização de exercícios semestrais nas Unidades da FA, interligando todas as áreas de atividade, promovendo a posterior divulgação de resultados como forma de promover a participação.

4.3.5. Síntese conclusiva e resposta à PD3

Pelo exposto, em resposta à PD3: *Que instrumentos podem ser utilizados para aumentar o Nível de Awareness em Ciberdefesa na FA?,* verifica-se que estão disponíveis diversos instrumentos que, sendo adotados, contribuem decisivamente para a evolução positiva dos vetores de transformação organizacional que, segundo o MMAC, regulam o nível de *Awareness* em Ciberdefesa da FA.

Entre novos produtos tecnológicos e mudanças de impacto organizacional, fica à vista a obrigatoriedade de contar com um forte suporte da estrutura decisora da FA que, atendendo às pressões nacionais (Governo, 2019) e internacionais (UE, 2017a), parece estar recetiva ao investimento financeiro e humano neste domínio (A. Telha, *op. cit.*; H. Jesus, *op. cit.*).

4.4. O Nível de *Awareness* em Ciberdefesa na FA e a resposta à PP.

Em resposta à PP: *Será que o Nível de Awareness na FA em Ciberdefesa compromete a Capacidade Ciberdefesa da FA?*, conclui-se que sim, uma vez que analisandos os elementos influenciadores da capacidade (DOTMLPFI), verifica-se que são na sua maioria diretamente afetados pela presença de um Nível mais baixo de *Awareness* em cada um dos parâmetros estudados.

Se não forem diligenciadas ações no sentido de promover o seu incremento, como são exemplo os instrumentos apresentados no ponto 4.3 desta investigação, a FA estará mais exposta ao risco no ciberespaço e não será capaz de prestar apoio à componente aérea em todas as dimensões associadas à Capacidade de Ciberdefesa, conforme Figura 2, esgotando as suas atividades no acompanhamento dado às operações de proteção e mitigação das vulnerabilidades existentes e na edificação de doutrina e processos basilares para a sua correta aplicação.

A análise efetuada ao Nível de *Awareness* em Ciberdefesa da FA, tendo em conta o MMAC, revelou vincadas fragilidades nos vetores Pessoas e Processos, que possuem necessidades prementes de desenvolvimento dos elementos Doutrina, Organização e Treino associados à capacidade de Ciberdefesa, por forma a diminuir o risco de exposição às ameaças que são, nesta fase, principalmente resultado de deficientes comportamentos internos provocados pela inobservância dos normativos, desconhecimento das consequências das ações e falta de conhecimentos técnicos adequados na operação de SITIC.

O conjunto destes fatores, em associação com um vetor Tecnologia dependente de grande investimento financeiro, compromete a Capacidade de Ciberdefesa pela impossibilidade de dotar os membros da Instituição, estejam eles ou não ligados à componente técnica dos SITIC, das condições para desenvolver as suas competências em ações de ciberhigiene, Cibersegurança ou Ciberdefesa, aumentando assim o risco organizacional e limitando a atuação da FA não só no domínio ciberespaço, mas em todo o seu espetro operacional.

Apesar do emprego das dimensões ofensiva e de exploração serem, à semelhança do domínio aéreo, uma exclusividade do EMGFA (A. Castro, *op. cit.*), a FA necessita ter a

capacidade treinada e disponível para ser empregue quando acionada para um teatro conjunto e/ou combinado (J. Morgado, *op. cit.*). Atendendo às condicionantes anteriormente apresentadas, a incapacidade de se libertar das atividades relacionadas com a má exploração interna dos SITIC, impede a comunidade técnica de potenciar as outras dimensões, resultado na efetiva perda de capacidade em Ciberdefesa.

5. Conclusões

As novas tecnologias fazem parte do quotidiano de qualquer pessoa, assim como do funcionamento de qualquer organização, sendo impossível ficar à parte da permanente evolução associada. No ciberespaço, assiste-se ao desenvolvimento diário de novas estratégias em resposta à necessidade de controlar a anarquia que se foi instalando com a multiplicidade de efeitos indesejados, resultantes de atividades políticas, sociais e económicas e que condicionam a exploração do domínio.

Ao nível militar, as Nações e as Organizações têm seguido a tendência e edificaram uma capacidade de Ciberdefesa que permita proteger os seus ativos críticos e manter um dos pilares do estado salvaguardado de interferência cibernética externa.

Contudo, as ameaças têm evoluído a uma velocidade idêntica à da própria exploração do domínio ciberespaço e algumas entidades têm sentido dificuldades em acompanhar esta pressão, incapazes de internamente corrigir as vulnerabilidades existentes ou de promover a importância da necessidade ao escalão de decisão.

Uma forma de ilustrar a dimensão e a importância desta temática, reside na apresentação de casos concretos, como é exemplo a recente intervenção pública do Prof. José Tribolet (2019) onde afirmou que a "fragilidade dos nossos sistemas vitais, os sistemas críticos que fazem a sociedade funcionar, é assustadora". No mesmo fórum, Sua Ex. o Almirante Silva Ribeiro, Chefe de EMGFA (2019) afirmou ter existido "um incidente informático grave e direcionado dentro do EMGFA". Ambas as intervenções colocam a nu a ameaça existente no ciberespaço e, em conjunto com as métricas apresentadas neste trabalho contribuem para a identificação da necessidade premente de combater as vulnerabilidades existentes e o reforço do *Awareness* da Instituição neste domínio.

A metodologia seguida neste estudo carateriza-se por um raciocínio indutivo, assente numa estratégia de investigação mista (qualitativa com reforço quantitativo) e no estudo de caso como desenho de pesquisa. Materializa-se, ao nível da recolha de dados, na análise documental e na análise ao conteúdo de entrevistas semiestruturadas a entidades-chave com responsabilidades na Capacidade de Ciberdefesa na FA, e dos resultados do questionário aos militares e civis da FA.

A fim de estudar o OG, e a correspondente PP que conduziu esta investigação, foram elencados três OE, operacionalizados em três PD.

Assim, para responder à PD1 e, consequentemente, ao OE1: *Avaliar o Nível de Awareness em Ciberdefesa na FA*, observou-se a literatura existente e as respostas às entrevistas realizadas a entidades-chave neste domínio e, por ausência de um MMAC ou

qualquer outro tipo de métricas disponíveis, foi necessário proceder à sua criação, definição e parametrização como forma de garantir um Nível coerente na avaliação a desenvolver. Com recurso aos cinco níveis do MMAC e assente no modelo de análise baseado nos vetores: Pessoas, Processos e Tecnologia, foram avaliados os diferentes dados retirados dos instrumentos de medida e verificou-se que:

I. No vetor Pessoas, tendo em conta a análise aos parâmetros abaixo indicados, a FA encontra-se no Nível 2 de Maturidade.

– PESS_1-Nível_2: Os membros da instituição têm apenas conhecimentos mínimos em Cibersegurança, não dominando cabalmente o conceito de Ciberdefesa nem os normativos que lhe estão adstritos;

– PESS_2-Nível_2: As ações de formação nesta área, mesmo as exclusivas da comunidade técnica, não são prioritárias no espaço organizacional e ainda estão longe de se poderem desenvolver ao abrigo de planos de formação definidos;

– PESS_3-Nível_3: As divulgações são parcas, limitando-se a boletins informativos e a ações *ad hoc* realizadas após a condução de auditorias ou exercícios na dependência do EMGFA.

II. No vetor Processos analisando os respetivos parâmetros, enquadramos a FA no Nível 2 de Maturidade:

– PROC_1-Nível_3: Existem processos e políticas formalmente identificados, mas para além dos papeis difusos dentro da organização, assiste-se à dificuldade em acompanhar a atualização da capacidade;

– PROC_2-Nível_2: Estão em desenvolvimento programas e atividades de *Awareness*, mas sem identificação de audiências alvo ou fitas de tempo;

– PROC_3-Nível_3: O CIRC está constituído e definido faltando a criação de doutrina adicional que regule a sua ativação e defina estados de operação.

III. No vetor Tecnologia a FA está posicionada no Nível 3 de Maturidade.

– TECN_1-Nível_3: Existe aplicação de controlos sobre os equipamentos *legacy*;

– TECN_2-Nível_3: Estão definidas estruturas de resposta a incidentes.

Decorrente da avaliação feita, conclui-se que o Nível de *Awareness* em Ciberdefesa na FA está enquadrado no Nível 2 – Em Desenvolvimento –, ainda que possua parâmetros correspondentes ao Nível Definido.

A fim de responder à PD2, e cumprir o OE2: *Analisar as vulnerabilidades e ameaças da FA de acordo com o Nível de Awareness em Ciberdefesa*, analisou-se cada um dos

parâmetros associados ao MMAC e detalharam-se as possíveis vulnerabilidades e ameaças para a FA tendo em conta o seu posicionamento no Nível de *Awareness*.

Ficou patente a importância dos parâmetros relacionados com o vetor Pessoas uma vez que foram reconhecidos por todos os especialistas entrevistados e na análise documental como o elo mais fraco dentro do domínio ciberespaço. Foram identificadas como vulnerabilidades neste vetor:

- inobservância da Lei, normas e regras de utilização SITIC;
- dificuldade em manter recursos humanos qualificados;
- ausência de formação e comunicação interna.

Ao nível do vetor Processos as ameaças e vulnerabilidades encontradas fora as seguintes:

- inexistência de programas de *Awareness;*
- ausência de uma entidade que governe todo o espetro de atividades em Ciberdefesa com capacidade para gerar patrocínios da estrutura decisora;
- edificação de doutrina atualizada e processos rigorosos;
- ausência de catálogo de riscos, ameaças e vulnerabilidades.

Ao nível tecnológico, as vulnerabilidades são mais visíveis (uma vez que são o meio mais exposto à ameaça) mas não implica que seja o ponto decisivo para a diminuição do risco:

- inexistência de métricas consistentes de *Awareness* e de incidentes no ciberespaço;
- incapacidade de acompanhar as evoluções tecnológicas, em especial na mobilidade, de uma forma assumida como segura;
- Muitos SITIC obsoletos, embora com planos identificados para a sua atualização.

A resposta à PD3, e subsequentemente ao OE3: *Propor os instrumentos cuja utilização poderá elevar o Nível de Awareness em Ciberdefesa na FA.*, baseou-se em análise documental e de conteúdo das entrevistas às entidades-chave em Ciberdefesa. Em concreto, e considerando que se trata de um cenário de elevada complexidade operacional, tecnológica e financeira, concluiu-se que, no sentido de conseguir incrementar o nível de *Awareness* da Instituição, é necessário a adoção de vários instrumentos aplicáveis aos diferentes vetores analisados, que diminuam o risco e aumentem a capacidade efetiva de Ciberdefesa, dos quais se destacam:

- identificação de um CISO e de *framework* que regule o processo de governação das SITIC e da Ciberdefesa;

– estabelecimento de um plano de implementação para um programa de *Awareness* onde deve constar formação interna on-line;

– criação de métricas de *Awareness*;

– edificação de doutrina atualizada e processos mais rigorosos;

– plano de renovação tecnológica financiado.

Face ao exposto, em resposta à PP, e ao correspondente OG: *Avaliar o impacto que o Nível de Awareness em Ciberdefesa na FA tem na Capacidade de Ciberdefesa da FA*, verificou-se que o Nível de *Awareness* afeta pontos fulcrais na capacidade de Ciberdefesa como a Organização, Treino, Pessoal e Infraestruturas e demonstrou-se que um nível baixo de *Awareness*, ainda para mais numa FA muito tecnológica e dependente dos SITIC, produz um impacto que não só compromete a capacidade de Ciberdefesa, como pode colocar em risco toda a missão da FA.

Decorrentes da presente investigação, e como principais **contributos para o conhecimento**, a FA está agora na posse dos seguintes dados:

– O *Awareness* em Ciberdefesa na FA está enquadrado no Nível 2;

– Existe uma preponderância bastante vincada do Nível de *Awareness* na FA sobre geração de Capacidade de Ciberdefesa pela Instituição e na forma como esta pode executar as suas ações no ciberespaço e em todo o espetro de operações;

– É necessária a constituição de Instrumentos que possibilitem o aumento dos conhecimentos, perceção e consciência dos assuntos ligados à Ciberdefesa por forma permitir à FA atingir níveis mais elevados de *Awareness* neste domínio das operações, mitigando o maior número de vulnerabilidades possível, diminuindo consequentemente a exposição ao risco.

Este TII, decorrente do processo de avaliação das capacidades, identifica **duas limitações** que importam considerar: estado do recrutamento e retenção de mão-de-obra qualificada neste domínio tecnológico; constrangimentos financeiros que revestem a área das SITIC há vários anos.

Se na primeira limitação, é reconhecida transversalidade na Instituição, com dificuldades claras por parte da FA no recrutamento e retenção de militares com competências, perdendo-os para o mercado de trabalho civil que, neste momento, possui condições bastante mais atrativas em especial do ponto de vista financeiro, já no caso da segunda limitação existe alguma secundarização da renovação tecnológica dos SITIC, assim

como da renovação da capacidade técnica dos militares que os administram, dentro daquilo que são as prioridades da Instituição.

Ainda que a análise destas limitações, e suas consequências, estejam fora do âmbito da investigação, revestem-se de alguma importância pelo impacto que têm na geração de capacidades na Instituição. Contudo, os resultados aqui apresentados são alheios às consequências dessas limitações e espelham aquilo que os instrumentos de medida identificam como o caminho a seguir para melhorar o *Awareness* em Ciberdefesa da FA.

No que respeita a **estudos futuros**, parece pertinente investigar a implementação de uma *framework* para a governação e suporte à decisão com implementação de controlos baseados em *standards* conhecidos. Parece também pertinente, dentro deste domínio, o estudo sobre a adoção de um simulador de incidentes no ciberespaço para treino e prevenção dos militares e civis da FA, em especial a comunidade técnica. Por último, estudar a viabilidade da implementação de um mecanismo de avaliação de proficiência em SITIC, à semelhança do que acontece com a avaliação da proficiência no domínio de línguas estrangeiras.

Em consequência desta investigação, **recomenda-se** à DIVCSI a revisão do RFA390-6 para atualização das estruturas existentes na Ciberdefesa das FFAA e alguns conceitos emergentes. Recomenda-se ainda à DIVCSI a elaboração de um estudo de Estado-Maior com vista à identificação de uma *framework* associada à governação dos SITIC na FA. Recomenda-se à DCSI, a elaboração de um catálogo atualizado de ativos com necessidades especiais de segurança, sua localização e medidas de mitigação de risco disponíveis. Recomenda-se, finalmente, à DINST a às Comissões Técnicas Especializadas a revisão dos PDINST por forma a incluir um módulo na área da Ciberdefesa que potencie, desde a entrada na Instituição, o conhecimento e *Awareness* em Ciberdefesa.

Referências Bibliográficas

Blum, D. (2015, 10 de agosto). Security Architects Partners – How to Assess Security Maturity and Make Improvements. [Publicação em blogue]. Retirado de https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/

Carmo, H., & Ferreira, M. M. (2008). *Metodologia da Investigação Guia para Auto-Aprendizage* (2.ª edição ed.). Lisboa: Universidade Aberta.

Coimbra, S. (2018). *Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da força aérea. Política de segurança e prevenção* (Trabalho de Investigação Individual do Curso de Promoção a Oficial Superior). Instituto Universitário Militar [IUM], Lisboa.

Decreto-Lei n.º 69/2014, de 9 de maio (2014). Aprovação da *orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança*. Diário da República, 1.ª Série, 2712-2719. Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei n.º 184/2014, de 29 de dezembro (2014). Aprovação da *Lei Orgânica do Estado-Maior General das Forças Armadas*. Diário da República, 1.ª Série, 6382-6397. Lisboa: Ministério da Defesa Nacional.

Estado-Maior-General das Forças Armadas. (2008). *PEMGFA/CSI/301 - Organização e normas para resposta a incidentes de segurança informática nas comunicações e sistemas de informação das FFAA*. Lisboa: Divisão de Comunicações e Sistemas de informação.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva Estratégica do EMGFA 2018-2021*. Retirado de 2019, de https://www.emgfa.pt/documents/435jnqg1vmd7.pdf

European Union Agency for Network and Information Security. (2016). *Good Practice Guide on Vulnerability Disclosure* [versão PDF]. doi:10.2824/610384.

European Union Agency for Network and Information Security. (2017). Cyber Security Culture in organisations [versão PDF]. Doi:10.2824/10543

Força Aérea Portuguesa. (2011). *RFA 390-6 Política de Ciberdefesa da Força Aérea.* Alfragide: Estado-Maior.

Força Aérea Portuguesa. (2018). Memorando do Grupo de Trabalho para o Desenvolvimento da Capacidade de Ciberdefesa das Forças Armadas (GT-CCFA). Alfragide: Divisão de Comunicações e Sistemas de Informação.

Governo de Portugal. (2013a). *Conceito Estratégico de Defesa Nacional*. Resolução de Conselho de Ministros n.º 19/2013 de 21 de março. Lisboa.

Governo de Portugal. (2013b). *Orientação Política para a Ciberdefesa*. Ministério da Defesa Nacional. Despacho n.º 13691/2013. Lisboa.

Governo de Portugal. (2013c). *Reforma «Defesa 2020»*. Resolução de Conselho de Ministros n.º 26/2013 de 19 de abril. Lisboa.

Governo de Portugal. (2015). *Estratégia Nacional para a Segurança do Ciberespaço.* Resolução de Conselho de Ministros n.º 36/2015 de 21 de março. Lisboa.

Governo de Portugal. (2018). *Diretiva Ministerial de Orientação Política para o Investimento na Defesa.* Despacho n.º 4103/2018 de 23 de abril. Lisboa.

Governo de Portugal. (2019). *Intervenção do Ministro da Defesa Nacional, João Gomes Cravinho, no âmbito do VI Seminário SIRP "Ciberdemocracia e cibersegurança"*. Retirado de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=aaedc281-b06d-44e6-8fca-78741253abb4

Hoeserlande, P. (s.d.). Blogue Webdiver – Thinkbox – What about DOTMLPFI? [Publicação em blogue]. Retirado de https://www.webdiver.be/Non_diving/Docs/Article-03-What-about-DOTMLPFI.pdf.

Instituto da Defesa Nacional. (2013). *IDN Cadernos n.º 12: Estratégia da Informação e Segurança no Ciberespaço*. Calçada das Necessidades: EUROPRESS

North Atlantic Treaty Organization. (2016, 8 de julho). *Cyber Defense Pledge – NATO SUMMIT 2016, Warsaw*. [Página *Online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_133177.htm

North Atlantic Treaty Organization. (2017). *Allied joint Publication* (AJP) – *Allied Joint Doctrine for Communication and Information Systems: AJP-6 (A). Brussels: NATO Standardization Office*

Nunes, P. V. (Coord.) (2018). *IDN Cadernos n.º 28: Contributos para uma Estratégia Nacional de Ciberdefesa*. Calçada das Necessidades: EUROPRESS

Militão, O. (2014). *Guerra da Informação: a cibersegurança, a Ciberdefesa e os novos desafios colocados ao sistema internacional* (Tese de Dissertação de Mestrado em Ciência Política e Relações Internacionais na Área de Especialização em Relações Internacionais). Universidade Nova de Lisboa – Faculdade de Ciências Sociais e Humanas, Lisboa.

Ramakrishman, S. & Testani, M. (2011, março). *People, Process, Technology – The Three Elements for a Successful Organizational Transformation*. Em: Institute of Industrial

& Systems engineers, *Path forward to business transformation*. Conferência organizada pela IBM - Center for Learning and Development.

Rodolfo, C. (2017, março). *A AFCEA e a sua ação nas áreas da Segurança e Defesa*. Conferencia Internacional sobre Cibersegurança. Instituto Politécnico da Guarda – Escola Superior de Tecnologia e Gestão, Guarda.

Santos, L. A. B., & Lima, J. M. M. V. (Coord.) (2016). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação.* Cadernos do IESM, 8. Lisboa: Instituto de Estudos Superiores Militares. Retirado de https://cidium.ium.pt/docs/publicacoes/CADERNO_8.pdf.

Santos, S. I. (2015). *A Ação do estado em Matéria de Cibersegurança* (Trabalho de Seminário de Investigação em Administração Pública). Universidade de Lisboa – Instituto Superior de Ciências Sociais e Políticas [ISCSP], Lisboa.

Spitzner, L. (2016, 6 de março). *SANS – Defining the Security Awareness Maturity Model.* [Página *Online*]. Retirado de https://www.sans.org/security-*Awareness*-training/blog/defining-security-*Awareness*-maturity-model

Tchipako, E. (2017). *CISO nas Organizações: Análise do impacto do enquadramento organizacional do CISO na Maturidade da Segurança de Informação* (Tese de Dissertação para obtenção do Grau de Mestre em Engenharia Informática e de Computadores). Instituto Superior Técnico, Lisboa.

União Europeia. (2013). *Cybersecurity Strategy of the European Union.* Brussels: High Representative of the European union for Foreign Affairs and Security Policy.

União Europeia. (2017a). *Cybersecurity in the EU - Common Security and Defence Policy* [versão PDF]. Brussels: *Scientific Foresight Unit of European Parliament*. doi:10.2861/853031.

União Europeia. (2017b). *Bring your own device: a major security concern*. Retirado de https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_BYOD%20-%20a%20major%20security%20concern%20v1.pdf

Apêndice A — Mapa conceptual do modelo de análise

Objetivo Geral:	Avaliar o impacto que o Nível de *Awareness* em Ciberdefesa na FA tem na capacidade de Ciberdefesa da FA				
Pergunta de Partida	Será que o Nível de *Awareness* na FA em Ciberdefesa compromete a Capacidade de Ciberdefesa da FA?				
Objetivos Específicos	**Pergunta Derivada**	**Conceito**	**Dimensão**	**Indicadores**	**Técnicas de recolha de dados**
OE1 – Avaliar o Nível de *Awareness* em Ciberdefesa na FA.	**PD1** – Qual é o Nível de *Awareness* em Ciberdefesa na FA?	*Awareness*	Individual	Ações de Proteção Identidade	Análise documental Entrevistas semiestruturadas Questionário
				Conhecimentos em SITIC	
			Organizacional	Conhecimento e relação com a estrutura de Ciberdefesa na FA	
				Avaliação da atuação e qualidade da Ciberdefesa na FA	
			Técnico	Participação em exercícios com Capacidade Ciberdefesa	
				Nível de conhecimento dos procedimentos na FA	
		Ciberespaço	Risco	Número de Incidentes de Segurança registados	
				Relação da FA e das FFAA com os *Media*, Sociedade e Nações	
		Cibersegurança	Políticas, Diretivas e Normas	Número de Bloqueios a Sites Não-Autorizados	
				Nível de conhecimento das normas na FA associadas aos SITIC	
				Registo de Software Instalado Não-Autorizado	
OE2 – Analisar as vulnerabilidades e ameaças da FA de acordo com o Nível de *Awareness* em Ciberdefesa.	**PD2** – Quais são as ameaças e vulnerabilidades potenciadas pelo Nível atual de *Awareness* da FA?	Ciberdefesa	Defensiva	Número de eventos de Segurança registados	Análise documental
				Número de Auditorias de Segurança aos SITIC	
				Número de exercícios realizados	
			Informações (*Intelligence*)	Número de Operações de recolha de informação	
			Ofensiva	Número de exercícios realizados	

				Número de Operações Ofensivas	Entrevistas semiestruturadas
		Ameaça	Externa	Número de eventos de intrusão/maliciosos detetados	Questionário
			Interna	Boas práticas na utilização dos SITIC FA	
		Vulnerabilidades	SITIC	Versões de *Hardware* e *Software* desatualizadas	
				BYOD e *COPE*	
			Humanas	Número de militares com funções dedicadas à Ciberdefesa	
				Nível de formação dos recursos humanos	
OE3 – Propor instrumentos cuja utilização poderá elevar o Nível de *Awareness* em Ciberdefesa na FA.	**PD3** – Que instrumentos podem ser utilizados para aumentar o Nível de *Awareness* em Ciberdefesa na FA?	Capacidade Ciberdefesa	DOTMLPFI	Doutrina existe e está disponível	Análise documental
				Processos e mecanismos de fluxo célere da informação entre atores	
				Nível de formação dos recursos humanos	
				Número de recursos humanos	
				Número de exercícios Nacionais e Internacionais	Entrevistas semiestruturadas
				Plano de comunicação	
				Vanguarda dos equipamentos e infraestruturas e disponíveis na Ciberdefesa	
				Processos de mitigação de eventos de segurança informática são conhecidos e treinados	

Apêndice B — Modelo de Maturidade de *Awareness* em Ciberdefesa

Para medir o Nível de *Awareness* em Ciberdefesa na FA foi necessário identificar um Modelo de Maturidade de *Awareness* em Ciberdefesa (MMAC) a partir do qual se pudessem analisar os resultados obtidos por intermédio dos diferentes instrumentos de medida utilizados, que neste trabalho de investigação foram a análise documental, as entrevistas a especialistas na área de Ciberdefesa e o questionário aos Militares e Civis da FA.

	Nível 1	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**
Vetor	**Inicial**	**Em Desenvolvimento**	**Definido**	**Governado**	**Otimizado**
PESSOAS (PESS_1)	Os membros da instituição sem *Awareness*	Os membros da Instituição têm conhecimentos mínimos em cibersegurança	Os membros da Instituição têm conhecimentos e aplicam procedimentos básicos de cibersegurança	Os membros da instituição possuem *Awareness* em Ciberdefesa respeitando os normativos definidos	Os membros da instituição contribuem para a Ciberdefesa da Instituição
PESSOAS (PESS_2)	Ações de formação inexistentes	Ações de formação exclusivas para comunidade técnica	Ações de formação em estabelecimentos de ensino	Formação inicial de base para todos os membros da Instituição e ações de refrescamento definidas e medidas.	Os membros da instituição estão validados no seu domínio de conhecimentos em Ciberdefesa.
PESSOAS (PESS_3)	Divulgações inexistentes	Divulgações de origem e tipologia técnica	Divulgações internas *ad hoc*	Divulgações internas com periodicidade definida.	Integração das divulgações nos *Briefings* das Unidades e Comandos
PROCESSOS (PROC_1)	Processos reativos e não coordenados	Existe uma Estrutura Organizacional identificada	Existem Papeis, Políticas e Processos formalmente identificados, mas difusos	Existe Governação sobre o dispositivo de Ciberdefesa e clara definição de Papeis e Responsabilidades	Existe ação e consciencialização geral em Ciberdefesa com delimitação e interação de Responsabilidades internas e externas
PROCESSOS (PROC_2)	Iniciativas isoladas da comunidade técnica sem programa de *Awareness*	Inventário Básico de processos e programa de *Awareness* em desenvolvimento para fins de auditoria	Está identificado um plano de atividades de *Awareness*, mas execução é limitada	Os líderes da Instituição promovem o planeamento e execução de atividades tendo em vista a promoção do *Awareness*	Existe suporte total dos decisores e as atividades de Ciberdefesa estão alinhadas com o estado das operações em curso
PROCESSOS (PROC_3)	Segurança dos SITIC sob responsabilidade dos elementos que efetuam a administração dos SITIC	Existem equipas especificas constituídas no âmbito da segurança dos SITIC	CIRC definido e constituído	Existe um processo formal para ativação dos CIRC em resposta a incidentes no ciberespaço	Existe uma escala de ameaça definida para o ciberespaço e consequentes mudanças de estado de alerta

TECNOLOGIA (TECN_1)	Hardware e Software obsoleto e sem possibilidade de *update* em operação	Construção de Catálogo de Hardware e Software obsoleto e desenvolvimentos de ações de mitigação	Imposição de ações de renovação tecnológica com aplicação de controlos e eventuais medidas de exceção para equipamentos legacy	Plano de maturação tecnológica continua está presente e é patrocinado	Acompanhamento da evolução tecnológica em conjunto com laboratórios de I&D
TECNOLOGIA (TECN_2)	Presença de riscos e ameaças mas não existem controlos	Controlos tecnológicos em desenvolvimento, mas não documentados	Estão definidas estruturas de resposta a incidentes no ciberespaço e controlos documentados	Existem métricas definidas de *Awareness*, controlos de segurança automáticos e membros da instituição são monitorizados	As métricas e controlos fazem parte de um plano de melhoria continua da capacidade Ciberdefesa
Estado Desejado					Integração continua da Ciberdefesa na Capacidade militar com retorno de investimento

Fonte: Adaptado a partir de Blum (2015) e Spitzner (2016)

Os cinco Níveis de *Awareness* são detalhados da seguinte forma:

– **Nível 1 – Inicial:**

Ausência de programas de *Awareness* definidos assim como de processos organizados, confinados a pequenas ações de Cibersegurança não estruturadas, sem métricas e sem regulação. Os membros da Instituição não estão cientes dos riscos dos seus comportamentos nem das ameaças.

Atualmente, este Nível é inaceitável nas organizações que utilizem o ciberespaço para desenvolver as suas atividades (Blum, 2015).

– **Nível 2 – Em desenvolvimento:**

Mantem-se a inexistência de um programa de *Awareness* definido. Assiste-se à criação de uma orgânica especifica para a componente de Ciberdefesa e início da identificação dos processos associados á geração de *Awareness* e capacidade. Os membros da Instituição possuem noções mínimas de Cibersegurança associados à sua atividade nos SITIC da Instituição, mas sem perceção dos efeitos associados às suas ações e do papel que desempenham na prevenção, identificação e reporte dos incidentes.

Tipicamente, as organizações neste nível possuem apenas pequenas estruturas técnicas de proteção de perímetro e a capacidade de resposta a incidentes e reposição de dados são muito embrionárias. Nesta fase é privilegiada a edificação de capacidades de registo de incidentes e ativos que possam contribuir para a definição de processos (Blum, 2015).

– **Nível 3 – Definido:**

São definidas e divulgadas formalmente políticas, processos e estruturas afetas à Ciberdefesa dentro da Instituição, assim como edificadas estruturas técnicas de resposta a incidentes e ameaças no ciberespaço. São identificados programas com vista ao incremento do nível de *Awareness* em Ciberdefesa dos membros da Instituição e respetiva

mudança nos seus comportamentos no ciberespaço, no entanto, a sua execução limitada e irregular, assim como a inexistência de métricas, impede o desenvolvimento cabal da capacidade de Ciberdefesa organizacional. Os membros da Instituição, por força das políticas e normativos veiculados estão mais habilitados a operar no ciberespaço, seja dentro da Instituição, em casa ou em missão, possuindo noções básicas de Cibersegurança e reconhecendo as ameaças mais comuns. Corresponde à fase inicial de mudança de comportamentos e investimento organizacional (Spitzner, 2016).

Este incremento de conhecimentos dos membros da Instituição, permite à comunidade técnica focar-se na melhoria das condições de recolha, análise e registo de eventos e gestão de configurações, assim como a participação em exercícios e formações de âmbito conjunto e combinado que promovem a sofisticação dos mecanismos de Cibersegurança e Ciberdefesa e, como resultado, a geração de novos conteúdos com vista à divulgação e consequente *Awareness* (Blum, 2015).

– **Nível 4 – Governado:**

O dispositivo de Ciberdefesa está totalmente definido e integrado com os processos, políticas e leis da instituição, sendo patrocinado pela estrutura de topo que assume o ciberespaço como importante ativo para a valorização da instituição. São promovidas atividades e ações promotoras da consciencialização em Ciberdefesa refletindo-se no domínio e correta aplicação de boas práticas de Cibersegurança. Existem métricas e mecanismos de monitorização das capacidades dentro da Instituição e ainda promoção de interoperabilidade com outras Organizações, com foco no treino dos processos de resposta e mitigação de incidentes e ameaças (Spitzner, 2016).

O foco, controlo e manutenção das capacidades humanas, processuais e tecnológicas são um fator chave para alcançar este nível. A liderança da Instituição deve manter o patrocínio das atividades geradoras de *Awareness* e a implementação, tão automática quanto possível, de mecanismos que lidem com a continua alteração das ameaças, leis, tecnologias e relações estabelecidas entre os diferentes atores no ciberespaço (Blum, 2015).

– **Nível 5 – Otimizado:**

Neste Nível todos os processos estão automatizados, documentados e integrados num processo de melhoria continua que é otimizado de acordo com as métricas registadas e alteração das condições da ameaça no ciberespaço. Existe uma consciencialização geral em Ciberdefesa dentro da Instituição e um suporte total da estrutura decisora para o alinhamento das atividades deste domínio com as restantes operações e capacidades militares. Os membros da Instituição contribuem para a geração da capacidade de Ciberdefesa e as ameaças, tipificadas de acordo com uma escala, regulam mudanças e adaptação de comportamentos, que são medidos no seu progresso e no impacto resultante das ações do programa de *Awareness* desenvolvido (Spitzner, 2016).

Atingir o nível cinco não significa atingir o ponto máximo da capacidade uma vez que este modelo pressupõe uma continua monitorização, adaptação e evolução do processo de geração de *Awareness,* até pela também constante modificação da ameaça. A instituição deve estar preparada para o contínuo investimento na geração de *Awareness* e na criação de condições humanas e tecnológicas adequadas para revisão dos processos e adaptação à atualidade (Blum, 2015).

Devem ainda ser respeitados os requisitos para passagem entre Nível de Maturidade, presentes na Quadro 1, em linha com os Parâmetros identificados no modelo.

Quadro 1 - Requisitos para a passagem entre Níveis de Maturidade:

N1 para N2	N2 para N3	N3 para N4	N4 para N5
• Identificadas as necessidades e standards que a FA deverá cumprir (como Ramo das FFAA e membro da NATO e UE) • Identificada uma estrutura organizacional • Desenvolvido ou adquirido treino específico	• Identificados patrocinadores na estrutura superior da Instituição • Desenhado e aprovado um Projeto de geração de *Awareness* com metas, custos e identificação de objetivos.	• Plano de geração de *Awareness* enquadrado nas atividades e missão. • Introduzida a comunicação de resultados de programas nos briefings mensais à estrutura superior	• Identificadas métricas chave de Ciberdefesa relacionadas com os objetivos e missão da Instituição • Execução e análise constante de medições das métricas • Acompanhamento da evolução tecnológica e os requisitos de Ciberdefesa de uma forma anual
Entregáveis	Entregáveis	Entregáveis	Entregáveis
✓ Relatórios de necessidades ✓ Doutrina Inicial de Geração de Capacidade	✓ Análise de risco das diversas audiências alvo ✓ Projeto de implementação do programa ✓ Documentação dos tópicos de aprendizagem ✓ Plano de execução	✓ Controlo das modificações e atualizações de objetivos, necessidades financeiras e estado dos recursos humanos e tecnologia	✓ Métricas em Ciberdefesa ✓ Avaliação da evolução das audiências alvo

Fonte: Adaptado a partir de Blum (2015) e Spitzner (2016)

Apêndice C — Guião das entrevistas semiestruturadas

As questões de seguida elencadas fizeram parte de cada um dos guiões enviados às entidades entrevistadas. Houve necessidade, em alguns casos, de efetuar adaptações ou retirada de perguntas por forma a ir ao encontro das características, funções e área de conhecimentos do entrevistado. Por limites de espaço neste TII não é possível colocar os guiões de uma forma individualizada.

1- Os avanços das TIC introduzem novos fatores competitivos bem como vários riscos. Em resposta a essas evoluções tecnológicas, as organizações parecem mudar o modo como conduzem suas atividades, verificando-se uma dependência crescente na disponibilidade, confiabilidade e integridade dos seus dados. Qual é o impacto do rápido avanço tecnológico (dispositivos móveis, *Cloud*, etc.) e da crescente necessidade de "*work anywhere*" na segurança das organizações e da sua informação? Como se deve lidar com isso?

2- A organização tem conhecimento dos seus ativos/infraestruturas mais importantes e das suas vulnerabilidades?

3- Existem procedimentos de auditoria de segurança? Como são feitas? Há recurso a entidades externas?

4- Existem métricas sobre os níveis de conhecimento ou perceção em Ciberdefesa ou Cibersegurança na FA?

5- Existem, são conhecidos e/ou avaliados relatórios de ameaças neste domínio? Como flui a informação da FA para outros ramos das FFAA? E em sentido contrário? Em que estrutura está delegada a resposta?

6- Existem procedimentos definidos de mitigação ou resposta contra incidentes dentro deste domino, em especial no que diz respeito à informação às estruturas superiores da FA?

7- O que é que foi feito, se é que existiu, após o incidente mais disruptivo (ou potencialmente mais disruptivo) identificado pela FA nesta área? (formação do pessoal; aquisição de mais equipamentos; mudança de políticas ou procedimentos)

8- Sendo um ator com responsabilidades na componente de Ciberdefesa, entende que os militares e civis da FA estão cientes das suas responsabilidades individuais na manutenção de um nível de segurança adequado dos nossos SITIC?

9- Qual é que entende ser o nível de comprometimento do escalão superior da FA em relação à Ciberdefesa?

10- Existem declarações do EMGFA-CCD onde se aponta um objetivo de possuir capacidades Ofensivas no âmbito da Ciberdefesa a curto prazo. Posto isto, qual é o seu entendimento no nível e participação da componente de Ciberdefesa em missões de carater operacional?

11- Que tipo de iniciativas existem ou estão previstas ocorrer na FA nesta área da Ciberdefesa, quer no campo das ações de divulgação quer no campo do treino dos militares das equipas com responsabilidade nessa área? E em relação aos restantes militares e civis?

12- Acha necessário desenvolver um plano/estratégia de comunicação dentro da FA para aumentar o *Awareness*?
a. Identificar o publico alvo? Necessidades diferentes para grupos/áreas diferentes (Ops, finance, logistics)?
b. Como identificar os resultados dessas campanhas? Métricas?
c. Os resultados/relatórios dos exercícios efetuados são uma boa avaliação do estado do *Awareness*?

13- Entende que ainda há falta de habilitações, formação ou conhecimento adequado neste domínio tendo em conta os possíveis impactos nas infraestruturas da FA? Qual deverá ser o posicionamento da FA na resposta à problemática de falta de quadros técnicos especializados neste domínio? Entende a contratação civil ou outsourcing como uma possibilidade?

14- Quais são para si os principais inibidores que impedem a Instituição de implementar eficazmente medidas no âmbito de Ciberdefesa?

15- Tem ideia do valor gasto em 2018 com os militares e civis da FA em campanhas de *Awareness* ou formação neste campo? As verbas foram em exclusivo para pessoal ligado às equipas de Ciberdefesa?

Perguntas enquadradas na metodologia DOTMLPFI (Capacidade Militar)
Doutrina

16- Como é que o desenvolvimento de doutrina ao nível do EMGFA e NATO influenciará a condução das operações de Ciberdefesa na FA?

17- Quais são os impactos das leis nacionais e internacionais na condução de operações no ciberespaço?

18- As TTPs (técnicas, táticas e procedimentos) estão ajustadas à doutrina existente? Os militares e civis da FA têm conhecimento dessas TTPs?

19- Em atividades no ciberespaço, a doutrina existente auxilia os operadores e o comando nas suas ações?

20- Existem linhas de orientação estratégicas especificas dentro da FA para a Ciberdefesa ou é seguida a doutrina EMGFA e NATO?

Organização

21- A Ciberdefesa na FA está corretamente posicionada em termos de estrutura orgânica? Entende que deve ser reequacionada a sua posição na estrutura da organização?

22- Quais são as principais limitações existentes na FA em termos organizativos? (dificuldades orgânicas)

Treino

23- Existem programas com vista à orientação e preparação das chefias e dos Estados-Maiores para o domínio operacional do ciberespaço?

24- Existe uma integração de formação em Ciberdefesa nas atuais ações ou planos de formação em exploração na FA, em especial pela entidade responsável na FA pela formação (DINST)?

25- Como se pode adaptar a FA, no sentido de integrar uma capacidade de treino disponibilizado/ministrado pelo EMGFA e outras estruturas nacionais e internacionais (exercícios, formações)?

26- Em que medida as contínuas alterações tecnológicas e de doutrina impactam no modelo de formação desenvolvido na FA?

27- Que tipo de técnicas (formação, exercícios, conferencias) mais se adequam para melhorar o treino em Ciberdefesa na FA?

28- Entende que as técnicas de treino podem e devem ser aplicadas a todos os militares e civis da mesma forma, ou deverá haver segmentação?

29- Entende que a formação nesta área da Ciberdefesa pode ser conduzida por entidades civis ou deve ser exclusiva de estruturas militares? Em que áreas deverá ser exclusiva?

30- A consciencialização, por intermédio do treino, deverá ser conduzida de forma individual ou coletiva?

31- Existe algum método de avaliação das competências em Ciberdefesa ou em utilização de SI-TIC disponível na FA, à semelhança do que acontece, por exemplo, como a avaliação em língua inglesa (SLP)?

Material

32- De que modo os atuais SI-TIC impactam, ou não, na capacidade de Ciberdefesa da FA?

33- Que tecnologias entende como críticas e de carácter obrigatório no investimento em material?

34- A FA tem as condições necessárias para efetuar todo o espetro de operações no Ciberespaço? Pretende ter?

35- Existe um orçamento específico dedicado a este domínio?

Liderança

36- Que tipo de suporte pode dar a estrutura decisora da FA na disponibilização de condições para formação e treino dos militares e civis da Instituição por forma a aumentar os níveis de *Awareness* em Ciberdefesa?

37- Qual a posição da estrutura decisora da FA em relação à capacidade de Ciberdefesa na FA?

38- A FA possui uma entidade que é líder e responsável pela estratégia em Ciberdefesa e sua delimitação?

39- Como avalia a existência de necessidade de implementação de um processo de tomada de decisão específico para a aplicação, ou não, de ações no ciberespaço? Ou seja, em caso de necessidade de atuação defensiva ou ofensiva estão estabelecidos procedimentos? Existem planos de mobilidade ou modificação de "estados de segurança" tendo em conta as ameaças?

Pessoal

40- Como é que são recrutados e retidos os militares que trabalham nesta área de Ciberdefesa?

41- Que tipo de competências devem estar afetos aos elementos que trabalham em Ciberdefesa. Apenas Técnicas ou existe uma forte preponderância na componente e conhecimentos do foro Operacional?

42- Que conhecimentos devem ter os elementos que serão responsáveis pela formação e treino?

43- As novas gerações estão especialmente *aware* para o ciberespaço. No entanto, não se perceciona que essa habilidade tenha impacto direto na forma como utilizam o ciberespaço na FA, potenciando por vezes as vulnerabilidades da Instituição com comportamentos considerados, no mínimo, negligentes. Que respostas podem ser dadas a este problema?

44- Tem-se assistido a uma diminuição dos recursos humanos com capacidade e formação especifica para operar no ciberespaço. Em adição, o recrutamento não tem sido eficaz para este tipo de recursos. Entende que recorrer a civis, sejam enquadrados no quadro da função publica, seja em contratação por outsourcing será uma saída para a dificuldade de manter esta capacidade técnica especifica?

45- A unificação das equipas dos Ramos das FFAA numa única estrutura conjunta poderá ser uma hipótese para diminuir as necessidades de pessoal?

Infraestruturas

46- As infraestruturas (físicas e lógicas) disponíveis na FA são adequadas para o desenvolvimento, testes e treino de operações no ciberespaço? E em destacamentos ou redes de missão?

47- Entende que deveriam ser agregadas todas as infraestruturas disponíveis de Ciberdefesa das FFAA num local conjunto?

Interoperabilidade

48- A FA participa em operações, exercícios ou ações de formação em parceria com outros Ramos das FFAA e com outras Instituições?

49- Que tipo de tecnologias permitem a interoperabilidade da FA neste domínio?

Apêndice D — Análise das entrevistas

Nº Questão	Resumo/Tema da questão feita à entidade	CCD	DivCSI	dDCSI	Chefe-SCD	DJFA
8	**Utilizadores e as suas ações como contributo para Ciberdefesa**	- O fator humano é o elo mais fraco. - Os militares estão cientes das suas responsabilidades	- Os militares e civis estão minimamente cientes das suas responsabilidades - Sinais que indicam necessidade de melhoria da perceção da ameaça	- Penso que não. - Os militares e civis têm consciência do impacto das suas ações/omissões, mas não é materializada no conhecimento específico das suas responsabilidades.	- Os militares e civis têm uma ideia geral dos comportamentos a adotar. - A realidade mostra que a aplicação do conhecimento está longe do ideal	- Cada vez mais os comandantes, diretores ou chefes das U/E/O da FA estão cientes das suas responsabilidades nesta matéria.
44 **47**	**Especialistas em Ciberdefesa:** **Como lidar com necessidades formação e pessoal?**	- está previsto o recrutamento de civis para o IOC 2021 (mobilidade interna e Ad-Hoc de especialistas	- Dificuldades humanas e materiais para alocar à missão	- Existe dificuldade em manter qualificações dos quadros atendendo à evolução da tecnologia e das ameaças.	- reativação do quadro ENGINF com baseline comum em SITIC e especialização posterior acessória no domínio do ciberespaço. - ações de reciclagem periódica na formação	- tem havido um esforço para dotar os juristas da FA da formação adequada neste domínio que, para além de escassa, é muitas vezes lateral às questões jurídicas de fundo.
38	**Suporte estrutura superior para condições formação e treino**	N/A	- sim, mas pode criar mais condições	- qualquer projeto que envolva a totalidade da FA obriga a aval superior e apoio e suporte (financeiro, logístico, etc.) da estrutura de topo	- Encontra-se em fase de planeamento a inclusão de um módulo/disciplina de segurança informática nos centros de formação da FA.	- formação neste domínio não é de todo suficiente.
				- As verbas autorizadas em sede de PCN e PCME têm sido perto de 0, o que aliado a uma diversificação constante dos vetores de ataque e adaptabilidade da parte atacante conduzem a perdas de efetividade no combate às ameaças/eventos de segurança informática.		
29	**Formação e Treino**	N/A	- existem palestras (AFA, Centro Estudos, Centros de formação) - deve ser promovido um programa de *Awareness* on-line - refrescamento de 2 anos	- deve ser estudado o assunto para que se identifiquem as técnicas mais adequadas	- já existem atividades letivas no CFMTFA neste domínio - Ações de *Awareness* em palestras, simpósios ou conferencias nas unidades. - periodicidade ainda por definir. - ferramentas de treino online	- tem havido um esforço para dotar os juristas da FA da formação adequada neste domínio que, para além de escassa, é muitas vezes lateral às questões jurídicas de fundo.
32	**Divulgação e Formação e treino:** **- publico alvo**	- todos e qualquer cidadão que possa contribuir para a segurança do ciberespaço nacional	- todos os militares e civis da FA - em caso de destacamentos, formação especifica adequada às ameaças dessa zona externa.	- Todos os militares e civis da FA têm de ter um padrão mínimo de conhecimentos. - Pessoas e comunidades de interesse especificas devem ter uma formação mais direcionada e adequada à sua maior exposição ao risco	- Todos os militares e civis da FA	- comunidade jurista e consequente geração de *Awareness* no meio
33	**Método de avaliação de competências em SITIC e Ciberdefesa**	N/A	- Não existe. - Não se identificam vantagens claras para a existência dessa competência. (exceto para validar se os programas de formação estão ou não a dar resultado)	- Não existe. - necessária a existência de um modelo de maturidade que permita aferir o desenvolvimento das competências. - a existência de um modelo permite a criação de métodos de avaliação individual	- não existe	N/A
13	**Plano de comunicação para aumento de *Awareness***	- Em desenvolvimento um projeto para melhorar o *Awareness* nos 3 ramos - Existem: Palestras FNDs; Cursos IUM e IDN;	- É necessário desenvolver o plano	- é essencial desenvolver o plano - é necessário estabelecer uma estratégia e um plano com objetivos estabelecidos e metas a alcançar	- algumas palestras às Unidades/Órgãos - no entanto, uma formação ab-initio geraria mais *Awareness* pelo alcance em número de envolvidos	- estratégia de comunicação nesta área, deve abranger os 3 Ramos das FFAA, também no sentido de harmonizar as ações e os procedimentos
13	**Planos de comunicação:** **- Como identificar resultados e métricas?**	- medidos pela diminuição de incidentes detetados. - tem sido observada uma postura mais cuidadosa (diminuição de comportamentos de risco)	- não existem. Têm de ser encontradas métricas para permitir aos decisores avaliar a eficácia das campanhas.	- não existe um modelo de maturidade - não existem métricas com níveis definidos. - importante saber os estados de desenvolvimento que devem ser atingidos e como aferir esse desenvolvimento	N/A	N/A

13	**Planos de comunicação: - os relatórios de exercícios são uma boa avaliação?**	- sim. Contribuem cabalmente para o aumento do *Awareness*.	- são um bom ponto de partida - a avaliação por amostragem pode não refletir o universo.	- nomeadamente do CiberPerseu, permitem retirar indicadores relevantes, mas não dão uma panorâmica global do *Awareness*	- Não existem *Lessons Lerned* nos exercícios conjuntos o que dificulta a melhoria contínua	N/A
16	**Valor gasto com *Awareness* em Ciberdefesa na FA**	N/A	- Não foi gasto qualquer valor de forma direta	- Não foi gasto qualquer valor de forma direta em campanhas de *Awareness* ou formação na área	- a formação a pessoal técnico foi assegurada pelo EMGFA	N/A
22	**Posicionamento da Ciberdefesa na estrutura orgânica FA**	N/A	- O CIRC está corretamente posicionado junto à capacidade técnica da DCSI. - falta interação com a componente operacional e C2	- correto: parte técnica na DCSI, parte estratégica na DivCSI. - deve ser criada uma repartição de Ciberdefesa dentro da DCSI com respetivo aumento de pessoal qualificado	- tendo uma vertente transversal, deveria ter um papel mais preponderante ao nível orgânico. Facilitaria a tomada de decisão, as ações no terreno, o estabelecimento/cumprimento de diretivas e o acesso a financiamento.	inserção do jurista numa equipa multidisciplinar com maior contacto com a parte técnica
15 35	**Principais dificuldades na implementação eficaz de medidas na Ciberdefesa?**	N/A	- Deve existir uma abordagem "security By Design" que envolve todos os que se relacionam com Informação e a tratam. E essa abordagem não se resume ao CIRC.	- falta de conhecimento na área Ciber (o que é; o que faz; quais os perigos/impactos) - Falta de pessoal especializado - Falta de tempo para implementação de novos processos	- Custos financeiros da manutenção de proficiência neste domínio parecem conduzir a um distanciamento por parte da estrutura superior da FA, considerando estas problemáticas sob uma visão estritamente tecnológica, quando a mesma merece uma abordagem estratégica	- Falta de pessoal especializado e nos quadros permanente de juristas com vista a: acompanhamento das atividades e exercícios conjuntos; estudo e desenvolvimento de doutrina jurídica no domínio da Ciberdefesa
4	**Existência de métricas nas FFAA**	- As métricas são responsabilidades dos Ramos - Em desenvolvimento uma harmonização entre CCD e ramos	- Existem métricas por amostragem retiradas dos exercícios conduzidos na Instituição	- Não existem métricas definidas. - Apenas alguns feedbacks dos resultados exercícios e da observação in loco dessas atividades	- Não existem métricas "formais". - Existe uma perceção do estado baseada nos resultados de eventos (reais ou exercícios)	N/A
5	**Ativos vs ameaças**	- a análise do risco é responsabilidade dos Ramos.	N/A	- Ameaças reconhecidas a partir dos relatórios gerados pelas ferramentas de auditoria	- equipamentos móveis são um desafio complexo e constante. - falta de "know how" técnico para lidar com as ameaças e mitigar/corrigir as vulnerabilidades nos SITIC.	N/A
5	**Relatórios de ameaças**	- existem relatórios partilhados pela comunidade Ciberdefesa - existem informações recolhidas pelos serviços de informações do estado	N/A	- Natureza conjunta do Ciberdefesa promove contatos diretos entre FA e CCD para troca de informação relativa a ameaças e ataques	- relatórios de exercícios - relatórios de ferramentas real-time - relatórios partilhados pela e com a comunidade	N/A
39	**Estados de alerta**	- existe um estado de alerta específico para a Ciberdefesa, retirado a partir do SIEM	- considera-se que os planos de mobilização e estados de alerta existentes são genéricos o suficiente para se poderem aplicar a Ciberdefesa	- Especificamente para a Ciberdefesa, não existem! Os planos de contingência e mobilidade devem ser revistos tendo em conta a realidade cibernética	- papel de definição de estados e ações deve ser assumido pelo EMGFA-CCD	- perceção errónea sobre o facto das consequências das ações no mundo virtual não produzirem efeitos físicos
6	**Procedimentos mitigação e resposta a incidentes e Fluxo de Informação**	- existem TTPs conforme documento PEMGFA CSI/301 - comunicação com os Ramos bidirecional com recurso a email, portais e plataformas de registo de incidentes	- Existem processos e normativos, mas estão desatualizados face à atualidade das capacidades (PEMGFA CSI/301) - existe informalmente uma boa iteração entre CCD e CIRC dos Ramos - capacidades de monitorização podem ser melhoradas	- DCSI tem processos internos estabelecidos. - não existem processos formais de passagem de info à estrutura superior da FA, exceto os normais canais hierárquicos quando a incidente o justifica. - Na comunicação com o CCD existem processos estabelecidos (PEMGFA CSI/301). - necessária a criação de um processo específico de tomada de decisão, em especial para aplicação da capacidade ofensiva.	- Existem TTPs dependentes do nível e tipologia de ataques e adequada tecnologia conjunta (reporting para o CCD). - natureza conjunta do Ciberdefesa promove contatos diretos entre FA e CCD para troca de informação relativa a ameaças e ataques	N/A

9 **17** **21** **39**	**Doutrina NATO e UE e ausência de doutrina Nacional. Que visão tem a Estrutura de topo das FFAA e o Estado?**	- Existe orientação política (OPC 2013) - MDN dá prioridade (2019), traduzida na LPM - ENSC 2019 permitirá a criação de Doutrina - Chefias Militares pretendem dinamização da Ciberdefesa com IOC em 2021	- Estrutura Superior da FA está ciente da importância da Ciberdefesa - Dificuldades humanas e materiais para alocar à missão - Existe uma política de Ciberdefesa na FA (RFA 390-6 de FEV11) com princípios chave. - Não existe ciclo de revisão estipulado.	- Estrutura Superior da FA está perfeitamente alinhada e em acordo com a prioridade dada à Ciberdefesa. - Falta de recursos humanos qualificados - Cabe à DivCSI a elaboração da estratégia (RFA 390-6) - São tidas em conta os normativos EMGFA e de outras instituições nacionais (CNCS) e internacionais (NATO e UE).	- documentação e doutrina existente é reduzida - Dificuldades humanas e materiais para alocar à missão - é fulcral existir doutrina rigorosa para utilização e exploração dos SITIC na FA	- Perante casos reais de ataque às estruturas de defesa, a falta de harmonização de doutrina, instrumentos de regulação e até mesmo procedimentos entre os vários Ramos das FFAA pode incorrer no risco de respostas e ações diferentes e dificuldades legais.
10	**Capacidade Ofensiva e emprego em missões operacionais reais**	- A NATO conta com o contributo dos países aliados para a capacidade ofensiva - CCD e Ramos têm desenvolvido a capacidade de forma conjunta - Aplicação da capacidade no exercício Lusitano, FND e FRI em apoio direto aos outros domínios.	- A FA apoiará o EMGFA-CCD através do seu CIRC, mas entende que as ações de Exploração e Ofensivas devem ser exclusivas do EMGFA	- modelo híbrido e colaborativo entre Ramos e EMGFA-CCD - capacidade Exploração e Ofensiva exclusivas do CCD. - Os militares FA devem ter a formação nessas dimensões para poderem potenciar o CCD quando chamados (augmentees)	- A FA não dispõe de capacidade total de atuação no ciberespaço - A FA deve manter uma capacidade mínima de atuar sobre os seus sistemas específicos, suportando-se do CCD quando necessário.	- Caso venha a adotar, não poderá ser esquecida qualquer norma de direito interno ou internacional. - o Direito, independentemente da forma de que decorrem, constitui um pilar essencial na condução das operações.
41	**Utilização da dimensão defensiva como potenciador da capacidade total de Ciberdefesa**	- Cimeira de Varsóvia e Cyber Defense Pledge compromete as Nações a respeitar um mínimo comum de capacidade defensiva. - O CCD considera relevante o desenvolvimento das 3 dimensões	- A inclusão da componente defensiva na missão primária da Organização é incontornável. - Deve ser reavaliada a forma como está a ser aplicada, por forma a melhorar a sua eficácia.	- Só usada na proteção de SITIC Destacados. - Não existem planos internos de aplicação da capacidade Ciberdefesa em apoio direto à utilização de meios aéreos, em operação. - Cabe ao EMGFA identificar o emprego dos meios, quer aéreo, quer cibernético.	N/A	- displicência por se associar o ciberespaço a um espaço de impunidade, em especial por não serem dadas a conhecer a aplicação dos mecanismos legais coercivos que se encontram previstos na Lei do Cibercrime
27	**Exercícios e Operações:** **- Potenciadores de capacidade**	- pilar do desenvolvimento da capacidade: partilha de conhecimentos e TTPs. - Equipas de Geometria Variável	- os exercícios potenciam a capacidade - lições aprendidas	- permitem criar rotinas, partilhas conhecimentos e boas práticas	- CiberPerseu muito voltado para os utilizadores, potencia a compreensão e perceção da Ciberdefesa - Para a comunidade técnica, potenciam a troca de conhecimentos, experiências e incremento da interoperabilidade	- capacidade LEGAD é fundamental para enquadrar as situações juridicamente, e aconselhar da melhor forma o decisor.
25	**Exercícios e Operações:** **- Impacto no Meio Militar e *Awareness***	- Treino global aumentando a consciencialização e o nível de defesa coletiva	- importante impacto na instituição. - aumento capacidade de reação na FA	- participação em exercícios e sua publicidade constitui em si mesmo um instrumento de aumento de *Awareness* em Ciberdefesa dos restantes militares e civis da FA.	– um ambiente de treino/exercício como o Opeval ou Taceval será um ambiente adequado para promover o *Awareness*.	- ferramenta essencial para posteriormente enquadrar juridicamente as situações reais.
3	**Procedimentos para auditoria e** **Analise resultados?**	N/A	- são um bom ponto de partida para avaliar o *Awareness*.	- permitem retirar alguns indicadores interessantes, no entanto não dão uma panorâmica global do *Awareness* em Ciberdefesa	- Fora do enquadramento IGFA - falta de doutrina e capacitação institucional - recurso exclusivo a militares - reporte dos resultados técnicos via cadeia hierárquica.	- Existe um relacionamento da FA com as autoridades judiciárias sempre que esteja em causa a prática de um crime, sendo aplicável a legislação nacional em vigor, se necessário.
2	**Conhecimento dos ativos, sistemas críticos e suas vulnerabilidades**	- os Ramos devem ter um cadastro dos seus ativos, infraestruturas e sistemas críticos	N/A	- Existe um catálogo de hardware e software importantes para a organização	- A aposta das organizações na mobilidade; - maior integração entre redes privadas e a internet	N/A
2 **34**	**Impacto do estado dos SITIC FA na capacidade de Ciberdefesa**	N/A	N/A	- muito material obsoleto (computadores, ativos de rede, sistemas legados, etc) - Hardware que não permite as últimas versões de *firmware* que corrigem vulnerabilidades críticas. - software fora de suporte pelo fabricante, permite que com muito pouco esforço por parte de um atacante, este procure uma vulnerabilidade que se encontra bem documentada online, e que num equipamento ou SO a explore causando impactos substanciais.		N/A

Nota: Para facilitar a análise, resumiram-se neste quadro as respostas constantes das entrevistas às entidades-chave, sendo representativas de transcrições com pequenos ajustes para facilitar a disposição. Os espaços em branco correspondem a perguntas que não foram colocadas à entidade.

Apêndice E — Questionário aos Militares e Civis da FA

Questões de caracterização pessoal

1- Indique a sua faixa etária
a. Entre 17 e 25 anos
b. Entre 26 a 35 anos
c. Entre 36 e 45 anos
d. Mais de 45 anos

2- Indique as suas habilitações literárias
a. Ensino Básico ou Inferior
b. Ensino secundário
c. Bacharelato/Licenciatura
d. Mestrado
e. Doutoramento ou superior

3- Indique a sua categoria dentro da FA
a. Oficiais
b. Sargentos
c. Praças
d. Civis

4- Indique a área primordial de conhecimentos exercida no desempenho das suas funções
a. Comando
b. Apoio à decisão
c. Operações
d. Logística e Manutenção
e. Recursos humanos
f. Tecnologias da Informação e Comunicações

Organização

5- Como classifica o seu Nível de *Awareness* em Ciberdefesa?
a. Muito elevado
b. Elevado
c. Razoável
d. Baixo
e. Muito baixo

6- Independentemente da perceção que tem sobre o seu Nível de *Awareness* em Ciberdefesa, indique de que forma(s) adquiriu esse nível.
(poderá selecionar mais do que uma opção)
a. Formação em estabelecimentos de ensino civis
b. Revistas e publicações civis sobre o tema
c. Internet e redes sociais
d. Divulgações Internas da Força Aérea
e. Participação em exercícios militares
f. Normativos Internos à Força Aérea
g. Comunicação Social

7- Como classifica o seu entendimento sobre o conceito de Ciberdefesa?
a. Percebe o conceito e as suas delimitações defensivas, ofensivas e de exploração;
b. Percebe o conceito apenas numa perspetiva de cibersegurança;
c. Sabe que existe;
d. Sabe que existe mas não entende o seu propósito na organização;
e. Não sabe, nem entende.

8- Como avalia o seu conhecimento sobre a existência ou não de estruturas militares que se ocupam diariamente da Ciberdefesa nas FFAA?
a. Conheço as estruturas existentes nas FFAA
b. Conheço apenas a estrutura da FA
c. Não tenho presente a existência ou não de estruturas fora da FA
d. Desconheço a existência de tais estruturas

9- Indique o número de pessoas que, na sua perceção, trabalham especificamente em Ciberdefesa na Força Aérea
a. Entre 1 e 3
b. Entre 4 e 6
c. Entre 7 e 10
d. Mais de 10
e. Não sabe

10- Indique as áreas em que, na sua perceção, existe atualmente atuação efetiva por parte da estrutura de Ciberdefesa na Força Aérea
(escolha as três (3) áreas que considera mais pertinentes e frequentes)
a. Análise forense
b. Auditoria à rede informática interna
c. Auditoria aos acessos internet
d. Exercícios internacionais
e. Exercícios nacionais
f. Operações ofensivas e de exploração
g. Produção de doutrina
h. Proteção de perímetro
i. Resposta a incidentes
j. Não sabe

11- Como avalia a prioridade dada pela estrutura de topo da FA em relação à Ciberdefesa?
a. Muita alta
b. Alta
c. Em linha com outras áreas
d. Baixa
e. Não sabe

12- Em que medida concorda com a seguinte afirmação: "A FA em todas as suas áreas de atuação, dá bastante importância à incorporação de medidas relacionadas com Ciberdefesa"
a. Concordo em absoluto
b. Concordo
c. Discordo
d. Discordo em absoluto
e. Não sabe

13- Em que medida concorda com a seguinte afirmação: "A aplicação de medidas de Ciberdefesa tendem a obstruir a missão atribuída à FA"
a. Concordo em absoluto
b. Concordo
c. Discordo
d. Discordo em absoluto
e. Não sabe

14- Qual entende ser a principal razão pela qual se deve investir na Ciberdefesa?
(escolha as três (3) razões que na sua opinião têm carácter prioritário)
a. Cumprimento da lei
b. Cumprir com requisitos e diretivas NATO e EU
c. Garantir a operacionalidade interna dos serviços
d. Porque os outros Ramos das FFAA também o fazem
e. Proteger a reputação da FA e a sua presença online
f. Proteger as infraestruturas Críticas Nacionais
g. Proteger contra vírus e ataques de hackers
h. Proteger informações secretas e reservadas
i. Proteger os dados pessoais e organizacionais
j. Treino para uso posterior da capacidade em teatro de operações

Normas e Procedimentos

15- Como avalia o seu conhecimento sobre a existência de normativos internos em Ciberdefesa na FA?
a. Conheço perfeitamente
b. Conheço
c. Sei que existem, mas não conheço
d. Desconheço a sua existência

16- Como avalia a seguinte afirmação: "A FA possui regras especificas para a utilização do email, internet e posto de trabalho."
a. Sim. Já as li.
b. Sim, mas não tive oportunidade de as ler
c. Não existem.
d. Não sabe

Ferramentas e atividades Cibersegurança

17- Qual a perceção que tem sobre o estado atual dos equipamentos e infraestrutura SI-TIC na FA?
a. Muito adequada
b. Adequada
c. Razoável
d. Desadequada
e. Obsoleta

18- Com que frequência utiliza o seu dispositivo pessoal (PC, Tablet ou Telemóvel) para aceder e/ou manipular informação de serviço (e-mail, documentos, aplicações)?
a. Com muita frequência
b. Frequentemente
c. Raramente
d. Nunca

19- Em que medida concorda com a seguinte afirmação: "A FA possui mecanismos de analise e registo de ações e atividades efetuadas ao nível do posto de trabalho, email e do acesso à internet."
a. Concordo em absoluto
b. Concordo
c. Discordo
d. Discordo em absoluto
e. Não sabe

20- Qual ou quais dos seguintes tipos de ações ou controlos entende que são atualmente usados na FA ao nível dos SI-TIC?
(Escolha, até um máximo de cinco (5), aqueles que considera mais pertinentes e frequentes)

a. Aplicação automática de updates de software
b. Auditorias a equipamentos
c. Proteção antivírus, antimalware e antispam
d. Backup aos dados da organização
e. Controlo de acessos aos servidores e serviços
f. Políticas de Passwords fortes
g. Políticas de bloqueio de acessos em caso de incidente
h. Controlos específicos para equipamentos moveis
i. Encriptação de dados
j. Acesso exclusivo à organização por intermédio de equipamentos da organização
k. Monitorização do acesso à internet
l. Redes segregadas (operacionais, administrativas e wireless)

21- Como entende os eventos de *update* de *software* e Sistema Operativo que ocorrem frequentemente no seu posto de trabalho da Instituição?
a. Muito importantes
b. Importantes
c. Pouco importantes
d. Pouco importantes e com impacto no trabalho diário
e. Desnecessários

22- Com que regularidade verifica o estado do antivírus nos seus dispositivos (computador, smartphone, tablet, etc.) pessoais?
a. Todas as semanas
b. 1 vez por mês
c. Quando instala uma nova versão
d. Nunca
e. Não possuo antivírus no computador pessoal

23- Utiliza dispositivos amovíveis (ex: USB Stick) pessoais simultaneamente para fins particulares e em computadores da Instituição?
a. Sempre
b. Frequentemente
c. Apenas quando não existe outra opção
d. Nunca

24- Quando instala aplicações no seu dispositivo móvel, tem atenção à informação sobre as necessidades de permissões a outras aplicações ou funcionalidades do telemóvel.
a. Sim, mas instalo sempre
b. Sim, e procuro alternativas que evitem acessos desnecessários
c. Não.
d. Não sabe /não possui telemóvel com capacidade para aplicações

25- Com que frequência altera as suas passwords pessoais?
a. > 2 anos
b. Entre 1 e 2 anos
c. Entre 6meses e 1ano
d. Entre 3 e 6 meses
e. Quando é obrigado

26- Entende que adota comportamentos que protejam a sua identidade digital no local de trabalho? Assinale as ações que correspondem ao seu comportamento habitual.
a. Nunca partilhei a minha password de utilizador com um camarada
b. Bloqueio o meu computador quando me ausento da secretária
c. Acedo com frequência ao email pessoal e a outros sítios de internet com introdução de credenciais
d. Utilizo o email da organização para assuntos pessoais como banco, subscrições de publicações ou compras online
e. Quando recebo emails fraudulentos ou com conteúdo malicioso, reporto
f. Uso uma password complexa com pelo menos 8 caracteres de diferentes tipologias
g. Tenho a(s) minha(s) password(s) escrita(s) num papel na secretária ou gaveta

27- Em caso de ser confrontado com aquilo que aparenta ser um problema de segurança informática no seu Posto de Trabalho na FA, que ações tomaria?
a. Identificava o erro, comunicava imediatamente o incidente e desligava o computador da rede;

b. Identificava o erro, comunicava o incidente, mas mantinha-me a trabalhar;
c. Comunicava o incidente, guardava os documentos necessários para um dispositivo USB e iria trabalhar para outro computador;
d. No final do dia comunicava o erro;

28- Em caso de ser confrontado com aquilo que aparenta ser um problema de segurança informática, na FA, a quem comunicaria formalmente o incidente?
a. Chefe Hierárquico
b. Centro de Informática Local ou *Servicedesk*
c. Estrutura de Ciberdefesa da FA
d. Gabinete Nacional de Segurança
e. Oficial de Segurança da Unidade
f. Polícia Judiciária
g. Não sabe

29- Quais das seguintes ameaças abaixo identificadas considera mais críticas e impactantes para a Instituição?
– (escolha as três (3) ameaças que considera mais críticas)

a. *Spam* e *Phishing*
b. Vírus e outros tipos de *software* maliciosos
c. Acesso ilegítimo externo a sistema
d. Violação direitos de autor
e. Modificação de dados
f. Engenharia social (Redes Sociais)
g. Redes de Missão estrangeiras
h. Curiosidade interna

Formação e Treino

30- Em que medida concorda com a afirmação: "A FA providencia formação e treino aos seus militares e civis por forma a estes melhorarem o seu nível de conhecimentos em cibersegurança e na forma como utilizar os recursos de rede disponíveis".
a. Concordo totalmente
b. Concordo
c. Discordo
d. Discordo totalmente
e. Não Sabe

31- Em que medida concorda com a afirmação: "A FA informa os seus militares e civis sobre regras de conduta e responsabilidades na utilização dos SI-TIC da Instituição".
a. Concordo totalmente
b. Concordo
c. Discordo
d. Discordo totalmente
e. Não Sabe

32- Em que medida concorda com a afirmação: "Os militares e civis da FA estão informados sobre as consequências de acessos indevidos a sistemas de informação e às alterações de software não autorizadas nos postos de trabalho"
a. Concordo totalmente
b. Concordo
c. Discordo
d. Discordo totalmente
e. Não Sabe

33- Com que frequência, se é que acontece, a FA informa de ações desenvolvidas no âmbito da Ciberdefesa?
a. Quando existe um incidente
b. Semanalmente
c. Mensalmente
d. Trimestralmente
e. Semestralmente
f. Anualmente
g. Não teve conhecimento de nenhum

34- Qual considera ser a melhor forma de melhorar os conhecimentos em Ciberdefesa na Força Aérea?
a. Integração nos programas de instrução de Base do Militar (DINST)
b. Formação *adhoc*
c. Ações de divulgação, colóquios ou seminários
d. Exercícios
e. Publicações e Divulgações informais (portal e email)
f. Normas e diretivas

35- Quem, na sua opinião, deveria prioritariamente assistir a formações, seminários ou conferencias com vista a melhorar a sua perceção e conhecimentos em Ciberdefesa?
a. Militares da estrutura de topo da organização
b. Militares cujas atribuições incluam aspetos relacionados com segurança da informação
c. Militares com responsabilidade nos SI-TIC
d. Militares e civis sem ligação a área de Ciberdefesa ou aos SITIC

…

Apêndice F — Auto-perceção[8] sobre *Awareness* em Ciberdefesa dos Militares e Civis da FA

Nível de *Awareness*	Faixa Etária: Entre 17 e 25 anos	Entre 26 a 35 anos	Entre 36 e 45 anos	Mais de 45 anos	% População
Baixo/Muito baixo	15% / 1%	22,5% / 7%	25% / 10%	25% / 5%	
Razoável	58% / 4%	51% / 15%	50% / 19%	53% / 14%	
Elevado/Muito Elevado	27% / 2%	26% / 8%	25% / 9%	22% / 6%	
	7%	30%	38%	25%	

% Totais do Nível de *Awareness* percecionado	
Baixo/Muito baixo	23%
Razoável	52%
Elevado/Muito Elevado	25%

Nível de *Awareness*	Habilitações Literárias: Ensino Básico ou Inferior	Ensino secundário	Bacharelato/ Licenciatura	Mestrado	Doutoramento ou superior	% População
Baixo/Muito baixo	100% / 1%	22% / 8%	24% / 10%	26% / 4%	0% / 0%	
Razoável	0% / 0%	50% / 19%	23% / 24%	47% / 8%	100% / 1%	
Elevado/Muito Elevado	0% / 0%	28% / 9%	53% / 11%	27% / 5%	0% / 0%	
	1%	36%	45%	17%	1%	

Nível de *Awareness*	Área de Desempenho Funções: Apoio à decisão	Comando	Logística, Financeira ou Manutenção	Operações	Recursos humanos	Tecnologias da Informação e Comunicações	% População
Baixo/Muito baixo	14% / 2%	17% / 1%	29% / 9%	27% / 7%	35% / 3%	5% / 1%	
Razoável	59% / 6%	64% / 6%	54% / 18%	44% / 10%	47% / 4%	49% / 8%	
Elevado/Muito Elevado	27% / 3%	19% / 1%	17% / 6%	29% / 6%	18% / 2%	46% / 7%	
	11%	8%	33%	23%	9%	16%	

[8] Verifica-se que a percentagem de indivíduos que entendem ter um Nível de *Awareness* em Ciberdefesa Baixo/Muito Baixo (23% do total do universo) é, na generalidade, idêntico em todos os graus de habilitações, idade ou funções desempenhadas, exceção feita no caso dos militares com funções na área SITIC que se revelam mais confiantes nas suas perceções.